SPECTRALLY EFFICIENT ANTI-JAMMING SYSTEM DESIGN IN WIRELESS NETWORKS

by

Lei Zhang

A DISSERTATION

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

DOCTOR OF PHILOSOPHY

Electrical Engineering

2011

ABSTRACT

SPECTRALLY EFFICIENT ANTI-JAMMING SYSTEM DESIGN IN WIRELESS NETWORKS

by

Lei Zhang

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 legitimate user's signal is deliberately interfered by the adversary. Along with the wide spread of various wireless devices, especially with the advent of user reconfigurable intelligent devices, jamming attack is no longer limited to military applications, but has become an urgent and serious threat to civilian communications as well. Motivated by this observation, in this dissertation, we consider hostile jamming modeling, classification, and spectrally efficient anti-jamming system design and analysis.

First, we investigate the cognitive jamming modeling and classification in wireless communications. Instead of using existing jamming models that assume the jamming remains invariant during the signal transmission period, we focus on time-varying jamming and its classification based on time-frequency analysis and the relative correlation between the signal and the jamming interference: (i) We introduce the general concepts of time-varying jamming coherence time and time-frequency jamming coherence bandwidth, and propose a new jamming classification scheme based on these parameters; (ii) We introduce the concept of disguised jamming, where the jamming is highly correlated with the signal, and has a power level close or equal to the signal power; (iii) Based on time-frequency analysis and approximation theory, we propose algorithms to estimate the time-varying coherence time and the time-frequency coherence bandwidth for both stationary and locally stationary jamming.

Next, we break new ground on anti-jamming system design in wireless networks based on message-driven frequency hopping (MDFH). MDFH is a highly efficient spread spectrum

technique that is particularly robust under strong jamming. However, it experiences considerable performance losses under disguised jamming. To overcome this drawback, we propose an anti-jamming MDFH (AJ-MDFH) system. The main idea is to transmit a secure ID sequence along with the information stream. The ID sequence is generated through a cryptographic algorithm using the shared secret between the transmitter and receiver, it is then exploited by the receiver for signal extraction. It is shown that AJ-MDFH can effectively reduce the performance degradation caused by disguised jamming while remains robust under strong jamming. We investigate ID constellation design and its impact on the performance of AJ-MDFH under both noise jamming and disguised jamming. In addition, we extend AJ-MDFH to a multi-carrier scheme, which can increase the system efficiency and jamming resistance significantly through jamming randomization and frequency diversity, and can readily be used as a collision-free multiple access system. Our analysis indicates that: while AJ-MDFH has strong anti-jamming property, its spectral efficiency is very close to that of MDFH, which is several times higher than that of the conventional FH.

Finally, we analyze the capacity of MDFH and AJ-MDFH under disguised jamming using the arbitrarily varying channel (AVC) model. We show that under the worst case disguised jamming, as long as the secure ID sequence is unavailable to jammer (which is ensured by AES), the AVC corresponding to AJ-MDFH is nonsymmetrizable. This implies that the deterministic code capacity of AJ-MDFH with respect to the average probability of error is positive. On the other hand, due to lack of shared randomness, the AVC corresponding to MDFH is symmetric, resulting in zero deterministic code capacity. We further calculate the capacity of AJ-MDFH and show that it converges as the ID constellation size goes to infinity, which echoes with convergence result for the probability of error of AJ-MDFH. We also extend the capacity analysis to multiuser AJ-MDFH system (MC-AJ-MDFH) and show that it outperforms the multiple access scheme for conventional FH (FHMA).

Future research will be conducted on adaptive transceiver design under cognitive jamming scenario.

Dedicated to my family and friends

ACKNOWLEDGMENTS

I would like to take this opportunity to express my deep appreciation to my advisor, Dr. Tongtong Li, for her constant support, guidance and encouragement throughout my Ph.D. years. She makes great effort to help me through many difficulties in academic research and personal development and growth. She herself sets a great example on these areas for me.

I want to thank Dr. Jonathan Hall from Department of Mathematics, Dr. Subir Biswas and Dr. Selin Aviyente 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. Jian Ren from Department of Electrical and Computer Engineering, who introduces me to the area of network security and provides many insights on the security related issues in my research.

I am deeply indebted to my labmates including Dr. Huahui Wang, Dr. Qi Ling, Dr. Weiguo Liang, Dr. Leonard Lightfoot, Ms. Abdelhakim Mai and Mr. Xiaochen Tang, for their valuable discussions on the research issues, as well as their helpful advices on the daily life on and off the campus. I am also 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 Yun Li, Di Tang, Leron Lightfoot, Wenbo Qiao, Jian Li, Jiankun Liu, Mingwu Gao, Guanqun Zhang, Ming Gu, Wei Wang, Ya Mo and Dave Conger for being my great friends and for all the fun we have together.

I would like to thank my parents for their unyielding love and continuous support through all the ups and downs, without which nothing could ever be possible. A special thanks goes to my roommate, Mr. Hao Wen, for providing valuable suggestions and encouragement during last two years of my Ph.D. program.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

Chapter 1

INTRODUCTION

In the past few decades, wireless communication has fundamentally changed people's way of lives. Accelerated by the breakthroughs in wireless technologies such as OFDM and MIMO, wireless communication nowadays is able to provide high speed connections for broadband multimedia applications including Video on Demand (VoD) and videoconferencing [1, 2, 3]. Comparing with its wireline counterpart, wireless communication does not only provide comparable data rate but also possesses other attractive features such as ubiquitous network coverage and mobility support. Due to these notable features, wireless communication sees an explosive growth in the recent years [4].

As more and more critical information is transmitted wirelessly for applications such as e-commerce and e-banking services, the security issues in wireless communication pose serious challenges for the development of next generation wireless networks, and wireless communication security becomes an active research field [5, 6, 7]. Although most of the higher layer security threats against wireline network can also be applied to wireless network, the latter suffers from additional vulnerabilities. Due to lack of the protective physical boundary, wireless communication systems are susceptible to PHY layer vulnerabilities such as unauthorized detection, interception and jamming interference [8, 9]. Jamming interference can introduce several forms of distortion to the transmitted signal and disrupt the legal user's communication. Therefore, it becomes a major challenge for secure and reliable PHY layer design in wireless networks. Motivated by this challenge, in this dissertation, we mainly focus on the jamming issue in the wireless networks.

1.1 Jamming Interference in Wireless Communications

Depending on the sources of the interference, the jamming can be classified into two categories with distinctive characteristics: when the interference is introduced by the sources within the wireless system, it is called system inherent jamming; when the interference is introduced by a malicious jammer, it is called hostile jamming.

1.1.0.1 System Inherent Jamming

In the single user environment, the wireless system includes the transmitter, the receiver and the wireless channel as the transmission medium. To maximize the usage of precious spectrum resource, wireless systems usually employ multiple access techniques to support multiple users transmitting simultaneously within the same frequency range. In the multiuser environment, these active transmitting users are also part of the wireless system. Both wireless channels and multiuser environment impose fundamental limitations on the performance of wireless systems [10, 11, 12]. (i) Due to the physical factors such as multipath propagation, wireless channel introduces inter-symbol interference (ISI) where the delayed replicas of previous symbols interfere with the current transmitted symbol. (ii) When orthogonality among different users are broken either by wireless channel or by transmitter and/or receiver, the multiuser interference (MUI) will be introduced by the signals from other active transmitting users.

Since the sources of system inherent jamming are located within the system, their characteristics can be either known to or controlled by the system. Therefore, the system inherent jamming can be effectively mitigated by system design techniques and system management protocols.

- The wireless channel can be well characterized by some physical parameters such as coherence time and coherence bandwidth, which can be obtained from appropriate channel models [13, 14]. With the knowledge of these channel characteristics, ISI can

be suppressed using appropriate design techniques. For example, in frequency selective fading channels, the ISI of PAM signals can be suppressed by adding a channel equalizer at the receiver [15, 16, 17]; for OFDM signals, ISI can be eliminated by inserting guard intervals between adjacent symbols [18, 19].

- Since signal characteristics of the users can be controlled by the system, MUI can be canceled by employing system management protocols. For example, in OFDMA systems, the MUI can be eliminated by scheduling the users to transmit on non-overlapping orthogonal subcarriers [20]; in multiuser MIMO systems, MUI can be mitigated by precoding techniques such that the signal transmits only towards the direction of the intended user without causing interference to users at other directions [21, 22].

Many of these techniques and protocols have been incorporated to the system design for 3G/4G wireless networks [23, 24].

1.1.0.2 Hostile Jamming

The malicious jammer with appropriate transmitter can intentionally interrupt the legitimate user's communication by saturating its receiver with noise or false information through deliberate radiation of radio signals [25, 26]. The jammer differs from active users in two ways: (i) The jamming can vary arbitrarily and is unpredictable. Its characteristics are difficult to obtain and are often not available to the system. (ii) The malicious jammer does not obey the system management protocols, thus the conventional MUI mitigation techniques no longer work under hostile jamming.

Due to these harmful characteristics, hostile jamming becomes an effective way to carry out denial-of-service (DoS) attack and is often used in military fields. However, with the advent of reconfigurable cognitive radios widely available, hostile jamming attack is much

easier to be launched and has become an urgent and serious threat to civilian communications as well.

1.2 Problem Descriptions

In this dissertation, we focus on hostile jamming modeling, classification and spectrally efficient anti-jamming system design and analysis.

1.2.1 Limitations of Existing Models

Traditionally, hostile jamming has been characterized in either frequency domain or time domain:

- Tone-jamming [27], where the jamming power is concentrated around carrier frequencies.

- Band-jamming [28, 29, 30, 31, 32], 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 [28, 29], partial-band [30, 31, 32]. 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.

- Partial-time jamming [33, 34, 35], 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.

In reality, a smart jammer can be used for more effective jamming attacks. The smart jammer is often equipped with receiver that captures the transmitted signal of the legitimate user. With sufficient intelligence, the smart jammer can determine the transmission scheme used by the legitimate user and adjust the jamming strategy accordingly to maximize the adverse effect. The jamming generated by the smart jammer is called cognitive jamming, also known as adaptive jamming or time-varying jamming. Apparently, cognitive jamming cannot be accurately characterized by existing jamming models, and cognitive jamming modeling and classification technique needs to be developed.

1.2.2 Limitations of Existing Jamming Resistant Systems

In general, wireless communication systems do not possess jamming resistant features except the spread spectrum systems. Spread spectrum techniques have been considered for secure communication since mid 1950 [36, 28, 29, 25, 37]. In this section, we provide a brief overview of existing spread spectrum systems and their characteristics [28, 25, 38].

By definition, spread spectrum systems occupy a larger bandwidth than the minimum necessary to transmit the information. In other words, the bandwidth of spread spectrum signal W is much greater than the bit rate of information messages R, and the expansion factor $G_p = \frac{W}{R}$ is usually referred to as the processing gain. The spreading is accomplished using a code which is independent of the data. The receiver is synchronized with the transmitter and uses the identical code for despreading and subsequent data recovery. To prevent interception or jamming by malicious user, the code should be shared only between the corresponding transmitter and receiver of legitimate user and kept secret from other undesirable users.

1.2.2.1 Existing Spread Spectrum Systems

Two techniques are often employed for spread spectrum systems: Direct-Sequence Spread Spectrum (DSSS) and Frequency Hopping Spread Spectrum (FHSS). The DSSS systems have

been extensively studied in the literature [39, 40, 41, 42, 43] and successfully incorporated into the 3G wireless communication standards. On the other hand, FHSS systems have been widely adopted in military communication systems. Other spread spectrum systems based on the hybrids of these two spreading techniques have also been proposed, but their performances do not significantly differ from those of these two basic ones.

Direct Sequence Spread Spectrum System Direct sequence spread spectrum is a technology that is more suitable for integration with bandwidth-efficient linear modulation such as QAM or PSK. In DSSS, the key operation of spectrum spreading is achieved by a PN sequence, also known as PN code ore PN chip. The PN sequence is usually binary, consisting of 0's and 1's, which are polar signaling of $+1$ and -1. To minimize interference and to facilitate chip synchronization, the PN sequence has certain desirable autocorrelation and cross-correlation properties. By spreading the overall signal energy over a broader bandwidth, DSSS systems provide nice security features against potential hostile jamming and interception:

- It is difficult for the unauthorized receiver to recover the information signal without the knowledge of PN code used at the transmitter.
- By applying sufficient processing gain, the power spectrum of the DSSS signal distributes over a broad bandwidth, resulting in a low flat power spectral density which has the similar characteristic as that of noise. It is then difficult for malicious user to separate spread spectrum signal from background noise. In this way, the spread spectrum signal can "hide" within the noise floor and prevent itself from being detected by malicious user.
- DSSS is especially robust under narrowband jamming by reducing the jamming power through the despreading process. Since the narrowband jamming interfere with only a small portion of signal energy and does not block out the entire signal spectrum, narrowband jamming is not effective against DSSS signals.

Frequency Hopping Spread Spectrum System In Frequency Hopping Spread Spectrum (FHSS) system, each user can vary its carrier frequency according to the predetermined, pseudorandom pattern, thereby effectively occupies a broader spectrum. By using PN sequence to control the frequency synthesizer, the transmitted signal hops to a new carrier frequency at the beginning of each hopping period. At the receiver, the received signal is shifted back to original signal band by using the identical PN sequence. Based on the duration of the hopping period, FHSS 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. There are several unique features of FHSS system:

- Since FHSS can produce signals of much wider bandwidth compared to DSSS, it can achieve much higher processing gain.
- As the carrier hops randomly over a wide range of frequencies, it is hard for the adversary to track or jam the active transmission without knowledge of the its hopping pattern.
- FHSS system is more robust to wideband jamming, since the signal power can be concentrated on a narrower frequency band during each hopping period. The receiver can filter out the jamming locates outside the current signal transmission band.

1.2.2.2 Limitations of Existing Spread Spectrum Systems

There are two major drawbacks in existing spread spectrum systems:

Inadequate Security In spread spectrum system, the PN sequence should only be shared between the transmitter and receiver of the legitimate user and kept secret from the malicious user. In practice, the PN sequence is usually generated by linear feedback shift register (LFSR) and can be uniquely determined by the initial state of LFSR (i.e., seed). Therefore,

it is more convenient for legitimate user to share the seed instead of sharing the PN sequence directly. Again, the seed should be kept secret from the malicious user. The inherent security of spread spectrum systems is based on the assumption that the malicious user without the knowledge of the seed is unable to predict the PN sequence. However, the seed can be consistently estimated based on the noisy observations of the generated PN sequence, which can be easily extracted from received spread spectrum signal [44, 45]. To overcome this drawback, a secure PN sequence generation algorithm needs to be designed.

Low Spectral Efficiency In multiuser environment, due to the system limitations, MUI can become a severe problem for spread spectrum systems:

- In conventional DSSS system, the channel multipath and asynchronous transmission activity can introduce nonzero cross-correlation among the users' signals. This leads to self-jamming to the DSSS system. Although some MUI suppression techniques such as multiuser detection algorithms have been proposed to tackle this problem [46, 47], their complexity may be too high to be affordable in many applications.

- In conventional FHSS system, each user hops independently based on its own PN sequence. A collision occurs whenever there are more than one users transmitting over the same frequency band. When there is a collision, it is reasonable to assume that the probability of error is 0.5. Therefore, the overall information bit rate of spread spectrum can be significantly limited, resulting in low spectral efficiency.

Existing spread spectrum systems work reasonably well for voice centric communications which only requires relatively narrow bandwidth. However, their low spectral efficiency provides insufficient information capacity for today's high speed multimedia wireless services. This turns out to be the most significant obstacle in developing anti-jamming features for high speed wireless wireless communication systems, for which spectrum is one of the most

precious resources. In this dissertation, we will develop spectrally efficient anti-jamming systems as a potential solution to this problem.

1.3 Proposed Research Directions

This dissertation focuses on the study of hostile jamming modeling, classification, and spectrally efficient anti-jamming wireless network design by integrating advanced signal processing techniques and cryptographic techniques into the PHY layer transceiver structure. More specifically, the proposed research directions are briefly summarized in the following subsections.

1.3.1 Cognitive Jamming Modeling and Classification

In literature, jamming signals are generally categorized into band jamming, tone jamming and partial-time jamming. Existing work on jamming detection and jamming prevention was 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. In practice, however, the jammer may very likely switch frequently from one pattern to another, with each jamming pattern only lasting a very short period of time. In other words, the jammer may launch smart, cognitive jamming, also known as adaptive jamming or time-varying jamming. Note that no particular anti-jamming system is effective under all jamming attacks, for optimum jamming mitigation, the transmitter has to be cognitive as well. Effective cognitive anti-jamming system design depends on successful jamming detection, modeling and classification.

In this part of dissertation, we focus on cognitive jamming modeling and classification based on time-frequency analysis and the relative correlation between the signal and the jamming interference: (i) We introduce the general concepts of time-varying jamming coherence time and time-frequency jamming coherence bandwidth, and propose a new jamming

classification scheme based on these parameters; (ii) We introduce the concept of disguised jamming, where the jamming is highly correlated with the signal, and has a power level close or equal to the signal power. It is complementary to the traditional strong jamming; (iii) Based on time-frequency analysis and approximation theory, we develop algorithms to estimate the time-varying jamming coherence time and the time-frequency jamming coherence bandwidth for both stationary and locally stationary jamming.

1.3.2 Anti-jamming System Design Based on Message-Driven Frequency Hopping

Mainly limited by multiple access interference, the spectral efficiency of existing jamming resistant systems are very low due to inefficient use of the large bandwidth. Recently, a *three-dimensional* modulation scheme, known as message-driven frequency hopping (MDFH) was proposed in [48, 49]. The most significant property of MDFH is that: by embedding a large portion of information into the hopping frequency selection process, additional information transmission is achieved with no extra cost on either bandwidth or power [50]. In fact, transmission through hopping frequency control essentially adds another dimension to the signal space, thus increases the system spectral efficiency by multiple times. MDFH is particularly robust under strong jamming. However, it experiences considerable performance losses under disguised jamming from sources that mimic the true signal.

To improve the performance of MDFH under disguised jamming, in this part of dissertation, we propose an anti-jamming MDFH (AJ-MDFH) scheme. The main idea is to insert some signal identification (ID) information during the transmission process. This ID information is generated through a cryptographic algorithm using the shared secret between the transmitter and the receiver. Therefore, it can be used by the receiver to locate the true carrier frequency or the desired channel. At the same time, it is computationally infeasible to be recovered by malicious users. Comparing with MDFH, AJ-MDFH can effectively reduce the performance degradation caused by disguised jamming. At the same time, it is robust

under strong jamming just as MDFH. The spectral efficiency of AJ-MDFH is very close to that of MDFH, which is several times higher than conventional FH. We investigate the ID constellation design and its impact on the performance of AJ-MDFH under both noise jamming and disguised jamming. It is shown that when noise is present, the detection error probability of AJ-MDFH under the worst case disguised jamming converges as the size of the constellation increases. This result justifies the use of practical finite size constellations in AJ-MDFH. It is observed that multi-carrier AJ-MDFH (MC-AJ-MDFH) can increase the system efficiency and jamming resistance significantly through jamming randomization and enriched frequency diversity.

1.3.3 Capacity Analysis of MDFH Based Systems under Disguised Jamming

In this part of dissertation, we analyze the capacity of MDFH and AJ-MDFH under disguised jamming. Both MDFH and AJ-MDFH can be modeled as arbitrarily varying channels, which is characterized as $W : \mathcal{X} \times \mathcal{J} \to \mathcal{S}$, where $\mathcal{X}$ is the transmitted signal space, $\mathcal{J}$ is the jamming space and $\mathcal{S}$ is the estimated information space. For any $\mathbf{x} \in \mathcal{X}$, $\mathbf{J} \in \mathcal{J}$ and $\mathbf{s} \in \mathcal{S}$, $W(\mathbf{s}|\mathbf{x}, \mathbf{J})$ denotes the conditional probability that $\mathbf{s}$ is detected at the receiver, given that $\mathbf{x}$ is the transmitted signal and $\mathbf{J}$ is the jamming. If $\mathcal{J} = \mathcal{X}$ and $W(\mathbf{s}|\mathbf{x}, \mathbf{J}) = W(\mathbf{s}|\mathbf{J}, \mathbf{x})$ for any $\mathbf{x}, \mathbf{J} \in \mathcal{X}, \mathbf{s} \in \mathcal{S}$, the AVC is said to have a *symmetric kernel* [51]. More generally, if the jammer can choose a stochastic method to generate $\mathbf{J}$, such that W becomes symmetric, then the AVC is said to be symmetrizable. The deterministic code capacity of the AVC for the average probability of error is positive iff the AVC is nonsymmetrizable. [52, 53]

Based on the results in AVC capacity analysis, we show that under the worst case disguised jamming, the AVC corresponding to MDFH has symmetric kernel, resulting in zero deterministic code capacity. On the other hand, under the worst case disguised jamming - ID jamming, as long as the ID sequence is unavailable to the jammer, the AVC corresponding to AJ-MDFH is *nonsymmetrizable*, resulting in positive deterministic code capacity. Note that the secure ID in AJ-MDFH is generated using AES, to symmetrize AJ-MDFH is equivalent

to break AES, which is computationally infeasible in practical systems. We derive the capacity of AJ-MDFH under ID jamming, for which the mutual information is maximized for all possible input probability distributions and minimized for all possible jamming distributions. We show that the capacity converges as the constellation size M goes to infinity and extend the capacity analysis to multiuser AJ-MDFH system (MC-AJ-MDFH). It is observed that: under reasonable SNR levels ($\geq$ 10dB), the capacity of AJ-MDFH under ID jamming is close to the jamming-free case, and it outperforms the conventional FH systems by big margins. These results confirm the superior performance of the AJ-MDFH under disguised jamming.

1.4 Overview of the Dissertation

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

- How to model the cognitive jamming phenomenons and classify jamming patterns effectively?
- How to improve the anti-jamming feature of MDFH, while maintaining its high spectral efficiency?
- How do the MDFH and AJ-MDFH perform under various jamming scenarios?

The dissertation is structured as follows.

Chapter 2 explores the cognitive jamming modeling and classification in wireless communications. First, we introduce the time-varying autocorrelation function and time-varying power spectral density to characterize time-varying jamming phenomenons and to include all the existing jamming models as special cases. Second, we introduce the concepts of time-varying jamming coherence time and time-frequency jamming coherence bandwidth based on the characteristics of these parameters. We also introduce two types of jamming classification criterions: (i) Based on time-frequency analysis of jamming statistics, we can classify

the jamming into fast jamming versus slow jamming and flat jamming versus frequency selective jamming; (ii) Based on relative power and correlation between signal and jamming, we can classify the jamming into strong jamming and disguised jamming. Finally, we develop algorithms based on time-frequency analysis and approximation theory to estimate the coherence time and coherence bandwidth for stationary jamming and locally stationary jamming.

Chapter 3 presents spectrally efficient anti-jamming system design based on message-driven frequency hopping (MDFH). First, we provide a brief review of MDFH, which improves spectral efficiency considerably by embedding part of information into the process of hopping frequency selection. Despite being robust under strong jamming, MDFH experiences considerable performance losses under disguised jamming from sources that mimic the true signal. Anti-jamming MDFH is developed to mitigate this security vulnerability by inserting a secure ID sequence in the transmission process. Second, we investigate ID constellation design and its impact on the performance of AJ-MDFH under both noise jamming and disguised jamming. Third, we extend the single carrier AJ-MDFH to multi-carrier AJ-MDFH (MC-AJ-MDFH), which can increase the system efficiency and jamming resistance significantly through jamming randomization and enriched frequency diversity. Finally, we analyze the performance of the proposed system.

Chapter 4 analyzes the capacity of MDFH and AJ-MDFH under disguised jamming using the AVC model. First, we show that under the worst case disguised jamming, the AVC kernel corresponding to MDFH is symmetric. That is, the deterministic code capacity of MDFH under worst case disguised jamming is zero. Second, we prove that under the worst case disguised jamming - ID jamming, as long as the ID sequence is unavailable to the jammer, the AVC corresponding to AJ-MDFH is nonsymmetrizable. Note that the secure ID in AJ-MDFH is generated using AES, to symmetrize AJ-MDFH is equivalent to break AES, which is computationally infeasible in practical systems. This result implies that AJ-MDFH has

positive capacity under ID jamming. Third, we derive the deterministic capacity of AJ-MDFH under ID jamming. We show that the capacity converges as the constellation size M goes to infinity. Finally, we extend the capacity analysis to the multiuser AJ-MDFH system (MC-AJ-MDFH) and show that it outperforms the multiple access scheme for conventional FH (FHMA).

Chapter 5 summarizes the contributions and conclusions of the dissertation. An outline of future work is also provided.

Chapter 2

COGNITIVE JAMMING MODELING AND CLASSIFICATION

In this chapter, we consider cognitive jamming modeling and classification based on time-frequency analysis and the relative correlation between the signal and the jamming interference. We introduce the general concepts of time-varying jamming coherence time and time-frequency jamming coherence bandwidth, and propose a new jamming classification scheme based on these parameters. We also introduce the concept of disguised jamming, for which the jamming is highly correlated with the signal, and has a power level close or equal to the signal power. We point out that very often, disguised jamming can be much more harmful than the traditional strong jamming. Algorithms based on time-frequency analysis and approximation theory are developed to estimate the time-varying jamming coherence time and the time-frequency jamming coherence bandwidth for both stationary and locally stationary jamming. Simulation examples are provided to demonstrate the proposed approaches.

2.1 Introduction

One of the most commonly used techniques for limiting the effectiveness of an opponent's communications is referred to as *jamming*. 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). In literature, jamming signals are generally categorized into three classes: (i) *Band jamming*, generally modeled as a zero-mean wide sense stationary Gaussian random process with a flat power spectral density (PSD) over the bandwidth of interest. Band jamming is further classified into *full-band jamming* [28] and *partial-band jamming* [31]; (ii) *Tone jamming*, typically a sinusoid waveform whose power

is concentrated on the carrier frequency. Tone jamming includes single-tone jamming and multi-tone jamming [27]. (iii) *Partial-time jamming*, modeled as a two-state Markov process, for which the jammer is on in state 1, and is off in state 0. State 1 occurs with probability of ρ, and state 0 occurs with probability $(1-\rho)$ [33].

Existing work on jamming detection and jamming prevention was 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 [54, 55, 56], for example. In practice, however, the jammer may very likely switch frequently from one pattern to another, with each jamming pattern only lasting a very short period of time. In other words, the jammer may launch smart, cognitive jamming, also known as adaptive jamming or time-varying jamming. Note that no particular anti-jamming system is effective under all jamming attacks. For optimum jamming mitigation, the transmitter has to be cognitive as well. Cognitive jamming modeling and classification are critical for dynamic anti-jamming system design.

This chapter focuses on cognitive jamming modeling and classification based on time-frequency analysis. We introduce the concepts of time-varying jamming coherence time and time-frequency jamming coherence bandwidth. By comparing the time-varying jamming coherence time with the signal symbol period, we classify the jamming into fast jamming and slow jamming; By comparing the time-frequency jamming coherence bandwidth with the signal bandwidth, we classify the jamming into flat jamming and frequency selective jamming. Note that at one time instant, the jamming coherence bandwidth may vary from one frequency to another. Therefore, a multi-band signal may experience flat jamming and frequency selective jamming simultaneously at different frequency bands. We also introduce the concept of disguised jamming, where the jamming is highly correlated with the signal, and has a power level close or equal to the signal power. It is complementary to the traditional strong jamming. Algorithms based on time-frequency analysis and approximation theory are provided to estimate the time-varying coherence time and time-frequency coherence

bandwidth for stationary jamming and locally stationary jamming. Simulation results are provided to demonstrate the proposed approaches.

2.2 Cognitive Jamming Modeling and Classification

Jamming interference can be divided into two classes: system inherent jamming and hostile jamming. The system inherent jamming, such as the intersymbol interference caused by multipath propagation, or multiuser interference due to simultaneous multiple access to the same frequency bands, can generally be reduced or minimized using various interference cancelation methods. In this section, we will focus on the characterization of random hostile jamming through two perspectives: (i) The time-frequency analysis of the jamming statistics; (ii) The correlation between the jamming and the signal.

2.2.1 Jamming Modeling using Time-Varying Power Spectral Density

We start 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 hostile jamming signal. $J(t)$ can either be stationary or nonstationary. Let $R_J(t,\tau) = E\{J(t+\tau)J(t)\}$ be the autocorrelation function of $J(t)$. The time-varying PSD is defined as

$$S_J(t,f) = \mathcal{F}\{R_J(t,\tau)\} = \int_{-\infty}^{\infty} R_J(t,\tau)e^{-j2\pi f\tau}d\tau. \tag{2.2}$$

The time-varying jamming power is given by $P_J(t) = \int_{-\infty}^{\infty} S_J(t,f)df$. We assume that $P_J(t)$ is finite and $P_J(t) \leq P_{J,max}$, where $P_{J,max}$ is the maximum jamming power. The reason that we allow the jamming power to be time-varying, rather than always using the total available jamming power, is because that strong jamming that uses the whole jamming power may

not always be the worst jamming [57]. If $J(t)$ is wide-sense stationary, then $R_J(t,\tau), S_J(t,f)$ and $P_J(t)$ all become time-invariant.

It turns out that *all the existing jamming models can be characterized using the time-varying power spectral density, $S_J(t,f)$.* In fact, let f_0 and f_1 be the start and ending frequency of the available frequency band, respectively; $[t_0,t_1]$ the time duration period of the message signal, and P_J the constant jamming power.

- If $S_J(t,f) = \dfrac{P_J}{f_1-f_0} \triangleq N_J, \forall f \in [f_0,f_1], \forall t \in [t_0,t_1]$, then $J(t)$ with PSD $S_J(t,f)$ is reduced to the traditional full-band jamming. Partial-band jamming can be defined in a similar manner.

- If $S_J(t,f) = P_J\delta(f-f_k), \forall t \in [t_0,t_1]$, where $f_k \in [f_0,f_1]$ and δ is the Dirac delta function, then we obtain the single-tone jamming. For multi-tone jamming,
$$S_J(t,f) = \sum_{k=1}^{K} P_J(t,k)\delta(f-f_k), \ s.t. \sum_{k=1}^{K} P_J(t,k) = P_J, \tag{2.3}$$
where K is the number of jamming tones, and $P_J(t,k)$ stands for the jamming power allocated for the kth tone f_k.

- If $\forall f \in [f_0,f_1]$,
$$S_J(t,f) = \begin{cases} 0, & \text{if } t \in [t_0,t_m) \text{ or } t \in (t_n,t_1], \\ \dfrac{P_J}{f_1-f_0}, & \text{if } t \in [t_m,t_n], \end{cases} \tag{2.4}$$
where t_m and t_n $(t_m \le t_n)$ are certain intermediate time instants within $[t_0,t_1]$, then we obtain the partial-time jamming.

Motivated by the observations above, we propose to model $J(t)$ through 2D analysis of $R_J(t,\tau)$ and its Fourier transform $S_J(t,f)$.

2.2.2 Jamming Classification Based on Time-frequency Analysis

In this section, we introduce the concepts of *time-varying jamming coherence time* and *time-frequency jamming coherence bandwidth* for $J(t)$.

- *Time-varying jamming coherence time:* For a given time instant t, let $[0, T_c(t)]$ be the period over which $R_J(t, \tau)$ is essentially non-zero and flat. This implies that $J(t+\tau)$ and $J(t)$ are highly correlated when $\tau \leq T_c(t)$. We define $T_c(t)$ as the *time-varying jamming coherence time* of $J(t)$. $T_c(t)$ is used to characterize the time-varying nature of $J(t)$ in the time domain. In other words, $T_c(t)$ is a statistical measure of the time duration over which $J(t)$ is essentially invariant.

- *Time-frequency jamming coherence bandwidth:* For a given time instant t and frequency υ, let $[\upsilon - \frac{B_c(t,\upsilon)}{2}, \upsilon + \frac{B_c(t,\upsilon)}{2}]$ be the frequency range over which the magnitude of the time-varying jamming PSD, $|S_J(t, f)|$, is essentially nonzero and can be considered to be flat. That is, at time instant t, two frequency components around υ with separation greater than $B_c(t, \upsilon)$ are affected differently by the jamming. We define $B_c(t, \upsilon)$ as the *time-frequency jamming coherence bandwidth at time t and frequency υ.*

Let T_s and B_s be the symbol period and bandwidth of the information signal, respectively, where T_s and B_s can be time-varying as well, such as in adaptive transmitters. We further introduce the following jamming classification criterions:

- For any given time instant t, if $T_s > T_c(t)$, then it means that the jamming changes rapidly within the symbol duration of the signal, we say that the signal is experiencing *fast jamming at time t*. Otherwise, we say that the signal is experiencing *slow jamming*.

- For any given time instant t, let $f_c(t)$ be the center frequency of the signal. If $B_c(t, f_c(t)) > B_s$, that is, the jamming coherence bandwidth at $\upsilon = f_c(t)$ is larger than the signal bandwidth, we say that the signal is experiencing *flat jamming at time t*. Otherwise, we say that the signal is experiencing *frequency selective jamming*. For multi-carrier signals, $B_c(t, \upsilon)$ needs to be evaluated at each carrier frequency. Therefore, a multi-band signal may experience flat jamming and frequency selective jamming simultaneously at different frequency bands.

Remark 1 *Comparing with the traditional time-varying channel modeling, it should be pointed out that our jamming model is based on the time-frequency statistics of $J(t)$, while the channel model is based on the statistics of the time-varying channel impulse response $h(t,\tau)$, which is the system response at t to an impulse applied at $t-\tau$.*

2.2.3 Strong Jamming and Disguised Jamming

Let $P_s(t)$ and $P_J(t)$ denote the time-varying signal power and jamming power, respectively. If $P_J(t) >> P_s(t)$, we say that the signal is experiencing strong jamming. Most communication systems become paralyzed under strong jamming attacks. However, with recent advances in anti-jamming system design [57], we can see that strong jamming may not be the worst jamming. On the other hand, *disguised jamming*, where the jamming is highly correlated with the signal and has a power level close or equal to the signal power, can be more harmful.

Consider the cross-correlation of the signal $s(t)$ and jamming interference $J(t)$ defined as $R_{s,J}(t_1,t_2) = E\{s(t_1)J(t_2)\}$. For band jamming or tone jamming, we are more interested in the case $t_1 = t_2 = t$. During the $(k+1)$th symbol interval $[kT_s,(k+1)T_s]$, we can approximate the cross-correlation between $s(t)$ and $J(t)$ with the time average

$$\rho_k = \frac{1}{T_s\sqrt{P_{s,k}P_{J,k}}}\int_{kT_s}^{(k+1)T_s} s(t)J(t)dt, \tag{2.5}$$

where $P_{s,k} = \frac{1}{T_s}\int_{kT_s}^{(k+1)T_s} s^2(t)dt$ and $P_{J,k} = \frac{1}{T_s}\int_{kT_s}^{(k+1)T_s} J^2(t)dt$.

Note that $0 \le |\rho_k| \le 1$. We say that $J(t)$ is a disguised jamming over $[kT_s,(k+1)T_s]$ if

1. $s(t)$ and $J(t)$ are highly correlated. More specifically, $|\rho_k| > \rho_0$, where ρ_0 is an application-oriented, predefined threshold.

2. The jamming-to-signal ratio (JSR) is close to 0dB. More specifically, $|\frac{P_J}{P_s} - 1| < \epsilon_P$, where ϵ_P is an application-oriented, predefined jamming-to-signal ratio threshold.

Disguised partial-time jamming is generally targeted at partial-time transmissions, for which the signal is transmitted on certain time slots within a frame. To locate disguised jamming in this scenario, (2.5) should be extended to the case $t_1 \neq t_2$.

Intuitively, disguised jamming makes it difficult for the receiver to identify the true signal from disguised interference. To combat with disguised jamming, the transmitter and the receiver need to have some preshared secret information, which can be used as the secure ID for the true signal so that it can be effectively extracted [57]. On the other hand, study on disguised jamming can also be used in electronic interference of an opponent's communication.

2.3 Estimation of Time-Varying Jamming Coherence Time and Time-Frequency Jamming Coherence Bandwidth

For jamming classification, we consider two scenarios: (i) $J(t)$ is stationary; (ii) $J(t)$ is locally stationary [58, 59, 60], which means that for any t, there exists a time interval of size $l(t)$, $[t - \frac{l(t)}{2}, t + \frac{l(t)}{2}]$, such that $J(t)$ can be approximated by a stationary process within this interval. The size of the intervals, $l(t)$ may change with time t. This assumption is reasonable in the sense that a particular jamming pattern may last for a short time and then the jammer switches to another pattern.

2.3.1 Stationary Jamming

When $J(t)$ is stationary, the autocorrelation function $R_J(t,\tau) = E\{J(t+\tau)J(t)\}$ and its Fourier transform $S_J(t,f)$ are both independent of t. We have $R_J(\tau) = E\{J(t+\tau)J(t)\}$ and $S_J(f) = \mathcal{F}\{R_J(\tau)\} = \int_{-\infty}^{\infty} R_J(\tau)e^{-j2\pi f\tau}d\tau$. In this case, $T_c(t)$ and $B_c(t,\upsilon)$ become time-invariant, and are denoted as T_c and $B_c(\upsilon)$, respectively.

By definition, $[0, T_c]$ is the period over which $R_J(\tau)$ is flat and essentially nonzero. That is,

$$|R_J(\tau)| > \alpha_0 R_J(0), \tag{2.6}$$

where $\alpha_0 \in [0.5, 0.95]$ is a predefined constant for coherence time estimation.

For any given frequency υ, let $[\upsilon - \frac{B_c(\upsilon)}{2}, \upsilon + \frac{B_c(\upsilon)}{2}]$ be the frequency range over which $S_J(f)$ is essentially nonzero and can be considered to be flat. Consider the case that $S_J(f)$ has only one main lobe in the positive frequency range, centered at f_c. (i) When $f_c = 0$, $J(t)$ is a baseband stationary process. For $\upsilon = 0$, $B_c(0)$ can be estimated through

$$\int_{-\frac{B_c(0)}{2}}^{\frac{B_c(0)}{2}} |S_J(f)|^2 df \geq \alpha_1 \|S_J\|_2^2, \tag{2.7}$$

where $\alpha_1 \in [0.5, 0.95]$ is a predefined constant for coherence bandwidth estimation. For any $\upsilon \neq 0$, $B_c(\upsilon)$ can be estimated from $B_c(0)$ as: $B_c(\upsilon) = B_c(0) - 2|\upsilon|$, if $0 < |\upsilon| < \frac{B_c(0)}{2}$; $B_c(\upsilon) = 0$, if $|\upsilon| \geq \frac{B_c(0)}{2}$. (ii) When $f_c > 0$, $J(t)$ is a passband stationary process. For $|\upsilon| = f_c$, $B_c(\upsilon)$ can be estimated through

$$\int_{f_c-\frac{B_c(\upsilon)}{2}}^{f_c+\frac{B_c(\upsilon)}{2}} |S_J(f)|^2 df \geq \frac{\alpha_1}{2} \|S_J\|_2^2. \tag{2.8}$$

For $|\upsilon| \neq f_c$, $B_c(\upsilon)$ can be estimated from $B_c(f_c)$ as: $B_c(\upsilon) = B_c(f_c) - 2||\upsilon| - f_c|$, if $0 < ||\upsilon| - f_c| < \frac{B_c(f_c)}{2}$; $B_c(f) = 0$, if $||\upsilon| - f_c| \geq \frac{B_c(f_c)}{2}$.

2.3.2 Locally Stationary Jamming

2.3.2.1 Definition

First, partition the active time axis into intervals $[t_p, t_{p+1}]$ of size $l_p = t_{p+1} - t_p$, with $\lim_{p\to\infty} t_p = \infty$ and $\lim_{p\to-\infty} t_p = -\infty$. We cover each interval $[t_p, t_{p+1}]$ with a window function $g_p(t)$. We construct the window function $g_p(t)$ such that it satisfies the following conditions: (i) For $\forall p \in \mathbb{Z}$, the support of $g_p(t)$ only intersects with the support of $g_{p-1}(t)$ and $g_{p+1}(t)$. The supports of $g_p(t)$ and $g_{p-1}(t)$ intersects in $[t_p - \eta_p, t_p + \eta_p]$. (ii) $g_p(t)$ and $g_{p-1}(t)$ are symmetric with respect to t_p, i.e., $g_p(t) = g_{p-1}(2t_p - t)$ over $[t_p - \eta_p, t_p + \eta_p]$. (iii) For $\forall t \in \mathbb{R}$, $\sum_{p=-\infty}^{\infty} |g_p(t)|^2 = 1$. The window functions are illustrated in Figure 2.1. It can be

shown that under these three conditions, the local cosine family defined by

$$\left\{\phi_{p,k}(t) = g_p(t)\sqrt{\frac{2}{l_p}}\cos\left[\frac{\pi(k+1/2)}{l_p}(t-t_p)\right]\right\}_{k\in\mathbb{N},p\in\mathbb{Z}} \tag{2.9}$$

formulates an orthonormal basis of $L^2(\mathbb{R})$ [61]. From (2.9), we can see that the support of $\phi_{p,k}(t)$ is $[t_p - \eta_p, t_{p+1} + \eta_{p+1}]$, and its center frequency is $\xi_{p,k} = \dfrac{\pi(k+1/2)}{l_p}$.

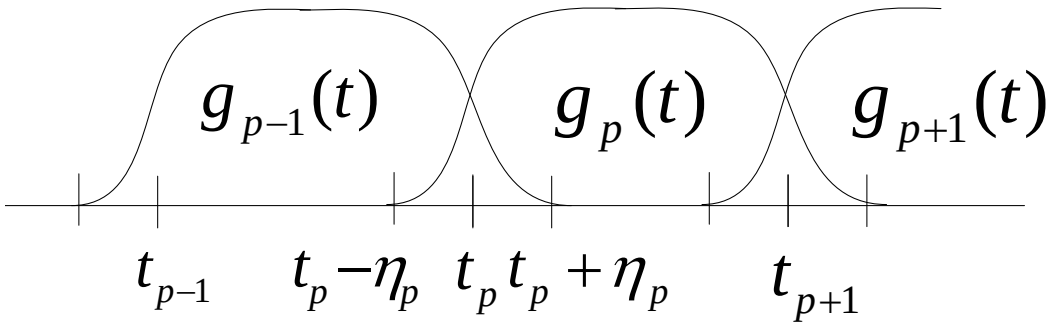


Figure 2.1: An example of window functions.

For $R_J(t,\tau) = E\{J(t+\tau)J(t)\}$, let $s = t+\tau$, then $R_J(t,\tau)$ can be rewritten as $R_J(t,s) = E\{J(t)J(s)\}$. For $\forall f \in L^2(\mathbb{R})$, define the covariance operator by

$$Tf(t) = \int_{-\infty}^{\infty} R_J(t,s)f(s)ds. \tag{2.10}$$

Following [61], locally stationary jamming processes can be defined as follows.

Definition 1 *A jamming $J(t)$ is said to be locally stationary if there exists a local cosine basis $\{\phi_{p,k}(t)\}_{k\in\mathbb{N},p\in\mathbb{Z}}$ such that for some constant $\mu < 1$ and $A > 0$, we have that for all $p \neq q$,*

$$\frac{\max(l_p, l_q)}{\min(l_p, l_q)} \leq A|p-q|^{\mu}, \tag{2.11}$$

and for all $n > 1$, we can find a constant Q_n such that for all $(p,q,j,k) \in \mathbb{Z}^2 \times \mathbb{N}^2$,

$$\left|\langle T\phi_{p,k}, \phi_{q,j}\rangle\right| \leq \frac{Q_n}{(1+|p-q|^n)(1+|\max(l_p,l_q)(\xi_{p,k}-\xi_{q,j})|^n)}. \tag{2.12}$$

Here $\{l_p\}$ specify the supports of $\{\phi_{p,k}(t)\}$ and indicate the intervals over which $J(t)$ is approximately stationary. Condition (2.12) implies that $|\langle T\phi_{p,k}, \phi_{q,j}\rangle|$ decays rapidly as we

increase $|p-q|$ and $|\xi_{p,k}-\xi_{q,j}|$. This means that the operator T is "almost" diagonalized by $\{\phi_{p,k}(t)\}$. In other words, each $\phi_{p,k}(t)$ is "almost" an eigenvector of T.

In fact, define $u = t + \tau/2$, then

$$\begin{aligned} R_J(t,\tau) &= E\{J(t+\tau)J(t)\} \\ &= E\{J(u+\frac{\tau}{2})J(u-\frac{\tau}{2})\} \triangleq C_J(u,\tau). \end{aligned} \tag{2.13}$$

Define $W_J(u,f) = \int_{-\infty}^{\infty} C_J(u,\tau)e^{-j2\pi f\tau}d\tau$. Note that for a locally stationary process, if $u \in [x - \frac{l(x)}{2}, x + \frac{l(x)}{2}]$, then

$$C_J(u,\tau) \approx 0, \text{ if } \tau > d(x), \tag{2.14}$$

where $d(x)$ is the so-called decorrelation length, and generally $d(x) < \frac{l(x)}{2}$. By definition, the time-varying jamming coherence time at $t = x$ should satisfy $T_c(x) \leq d(x)$. For any $\xi \in \mathbb{R}$ and $\forall (u,f) \in [x - \frac{l(x)}{2}, x + \frac{l(x)}{2}] \times [\frac{\xi}{2\pi} - \frac{1}{2d(x)}, \frac{\xi}{2\pi} + \frac{1}{2d(x)}]$, $W_J(u,f)$ can be approximated by $W_J(u,f) \approx W_J(x,\xi)$. Let $g_x(t)$ be a smooth window function with support $[x - \frac{l(x)}{2}, x + \frac{l(x)}{2}]$. The local cosine function corresponds to the time-frequency rectangle $[x-\frac{l(x)}{2}, x+\frac{l(x)}{2}]\times[\frac{\xi}{2\pi}-\frac{1}{2d(x)}, \frac{\xi}{2\pi}+\frac{1}{2d(x)}]$ can be represented as $\phi_{x,\xi}(t) = g_x(t)\cos(\xi t+\theta)$.[1] Following the argument in [61],

$$T\phi_{x,\xi}(t) \approx W_J(x,\xi)\phi_{x,\xi}(t). \tag{2.15}$$

That is, $\phi_{x,\xi}(t)$ is almost an eigenvector of T.

2.3.2.2 Best Basis Search and Spectrum Estimation

Let $\{\phi_n(t)\}_{n\in\mathbb{N}}$ be an orthonormal basis of $L^2(\mathbb{R})$, which implies that for any $f(t) \in L^2(\mathbb{R})$, $f(t)$ can be decomposed as $f(t) = \sum_{n\in\mathbb{N}} \langle f, \phi_n\rangle \phi_n(t)$. It follows that $Tf(t) = \sum_{n\in\mathbb{N}} \langle f, \phi_n\rangle T\phi_n(t)$.

[1] The local cosine function $\phi_{p,k}(t)$ defined in (2.9) can be represented as $\phi_{x_p,\xi_{p,k}}(t) = g_{x_p}(t)\cos(\xi_{p,k}t + \theta_{p,k})$ with $x_p = \frac{1}{2}(t_p + t_{p+1})$, $g_{x_p}(t) = \sqrt{\frac{2}{l_p}}g_p(t)$, $\xi_{p,k} = \frac{\pi(k+1/2)}{l_p}$ and $\theta_{p,k} = -\xi_{p,k}t_p$.

That is, the operator T is completely determined by $T\phi_n(t)$. For any $m \in \mathbb{N}$,

$$T\phi_m(t) = \sum_{n\in\mathbb{N}} \langle T\phi_m, \phi_n\rangle \phi_n(t). \tag{2.16}$$

Note that in practice, $Tf(t)$ can only be approximated by a finite sum. A natural question is: for a fixed number of items in the sum, which basis will result in the best approximation? Let $\mathcal{D} = \{\mathcal{B}^\gamma\}_{\gamma\in\Gamma}$ be a dictionary of orthonormal basis $\mathcal{B}^\gamma = \{\phi_n^\gamma\}_{n\in\mathbb{N}}$ of $L^2(\mathbb{R})$, indexed by $\gamma \in \Gamma$ where Γ denotes the collection of all the index sets in the dictionary. Define B_K^γ as

$$\langle B_K^\gamma \phi_m^\gamma, \phi_n^\gamma\rangle = \begin{cases} \langle T\phi_m^\gamma, \phi_n^\gamma\rangle, & \text{if } |n-m| \le K, \\ 0, & \text{Otherwise.} \end{cases} \tag{2.17}$$

For a fixed K, the best basis is the one which minimizes the norm $\|T - B_K^\gamma\|_s$, defined as

$$\|T - B_K^\gamma\|_s = \sup_{\|f\|_2=1} \|(T - B_K^\gamma)f\|_2. \tag{2.18}$$

Since local cosine functions are approximate eigenvectors of the corresponding covariance operator T, we search the best basis in a dictionary of local cosine bases, with $K = 0$ in (2.17) such that the operator T is diagonalized. Once the best basis $\{\phi_n^{\gamma 0}\}_{n=1}^N$ is selected, we have

$$\begin{aligned} R_J(t,s) &= E\{J(t)J(s)\} \\ &\approx E\left\{\sum_{m=1}^N \langle J, \phi_m^{\gamma 0}\rangle \phi_m^{\gamma 0}(t) \sum_{n=1}^N \langle J, \phi_n^{\gamma 0}\rangle \phi_n^{\gamma 0}(s)\right\} \\ &= \sum_{m=1}^N \sum_{n=1}^N E\left\{\langle J, \phi_m^{\gamma 0}\rangle \langle J, \phi_n^{\gamma 0}\rangle\right\} \phi_m^{\gamma 0}(t)\phi_n^{\gamma 0}(s), \end{aligned} \tag{2.19}$$

where $E\left\{\langle J, \phi_m^{\gamma 0}\rangle \langle J, \phi_n^{\gamma 0}\rangle\right\}$ can be rewritten as

$$\begin{aligned} E\left\{\langle J, \phi_m^{\gamma 0}\rangle \langle J, \phi_n^{\gamma 0}\rangle\right\} &= E\left\{\int_{-\infty}^{\infty} J(t)\phi_m^{\gamma 0}(t)dt \cdot \int_{-\infty}^{\infty} J(s)\phi_n^{\gamma 0}(s)ds\right\} \\ &= \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} E\{J(t)J(s)\}\phi_m^{\gamma 0}(t)\phi_n^{\gamma 0}(s)dtds \\ &= \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} R(t,s)\phi_n^{\gamma 0}(s)ds \cdot \phi_m^{\gamma 0}(t)dt \\ &= \langle T\phi_n^{\gamma 0}, \phi_m^{\gamma 0}\rangle. \end{aligned} \tag{2.20}$$

Following from (2.19) and (2.20), we have

$$R_J(t,s) = \sum_{m=1}^{N}\sum_{n=1}^{N}\langle T\phi_n^{\gamma 0}, \phi_m^{\gamma 0}\rangle \phi_m^{\gamma 0}(t)\phi_n^{\gamma 0}(s) \approx \sum_{n=1}^{N}\langle T\phi_n^{\gamma 0}, \phi_n^{\gamma 0}\rangle \phi_n^{\gamma 0}(t)\phi_n^{\gamma 0}(s). \tag{2.21}$$

Let $d_n = \langle T\phi_n^{\gamma 0}, \phi_n^{\gamma 0}\rangle = E\{\ |\langle J, \phi_n^{\gamma 0}\rangle|^2\}$, then the time-varying autocorrelation function can be estimated as

$$R_J(t,\tau) \approx \sum_{n=1}^{N} d_n \phi_n^{\gamma 0}(t)\phi_n^{\gamma 0}(t+\tau). \tag{2.22}$$

Let x_n and ξ_n denote the center time and the center frequency corresponding to $\phi_n^{\gamma 0}$, respectively. That is,

$$\phi_n^{\gamma 0}(t) = g_{x_n}(t)\cos(\xi_n t + \theta_n). \tag{2.23}$$

In the time domain, the smooth function $g_{x_n}(t)$ is approximately nonzero and flat over the time support $[x_n - \frac{l(x_n)}{2}, x_n + \frac{l(x_n)}{2}]$. Assuming $J(t)$ has a finite duration, and can be covered by P window functions $\{g_p(t)\}_{p=1}^{P}$ associated with the best basis functions $\{\phi_n^{\gamma 0}\}_{n=1}^{N}$. Let $\mathcal{N}_p$ denote the set of indexes for the best basis functions corresponding to $g_p(t)$. Then, $g_{x_n}(t) = \sqrt{\frac{2}{l_p}} g_p(t)$ for any $n \in \mathcal{N}_p$, and $\cup_{p=1}^{P}\mathcal{N}_p = \{1, \cdots, N\}$. We have

$$R_J(t,\tau) \approx \sum_{p=1}^{P} \frac{2}{l_p} g_p(t) g_p(t+\tau) \sum_{n\in\mathcal{N}_p} d_n \cos(\xi_n t + \theta_n)\cos(\xi_n t + \xi_n \tau + \theta_n). \tag{2.24}$$

For a given time $t \in (t_p, t_{p+1})$, $R_J(t,\tau)$ is mainly determined by $|\mathcal{N}_p|$ cosine terms in (2.24) corresponding to a set of basis functions $\{\phi_n^{\gamma 0}(t)\}_{n\in\mathcal{N}_p}$ (See Figure 2.1). Note that d_n can be estimated from Q realizations of $J(t)$ using the best basis as

$$\hat{d}_n = \frac{1}{Q}\sum_{q=1}^{Q} |\langle J^q, \phi_n^{\gamma 0}\rangle|^2. \tag{2.25}$$

Therefore, $R_J(t,\tau)$ can be estimated by replacing d_n with $\hat{d}_n$ in (2.24). For any t, $T_c(t)$ can then be estimated from $R_J(t,\tau)$ using the method described in (2.6). Note that at the border time instant $t = t_p$ $(p = 2, \cdots, P)$, $R_J(t_p,\tau)$ is determined by cosine terms associated with both $\mathcal{N}_{p-1}$ and $\mathcal{N}_p$. For conservative estimation, we have $T_c(t_p) \triangleq \min\{T_c(t_p - \tau_\epsilon), T_c(t_p + \tau_\epsilon)\}$ where τ_ϵ is a small time difference.

Following from (2.22), the time-varying PSD can be obtained as

$$S_J(t,f) \approx \sum_{n=1}^{N} d_n e^{j2\pi ft} \phi_n^{\gamma 0}(t) \Phi_n^{\gamma 0}(f), \tag{2.26}$$

where $\Phi_n^{\gamma 0}(f) = \int_{-\infty}^{\infty} \phi_n^{\gamma 0}(\tau) e^{-j2\pi f\tau} d\tau$. In the frequency domain, $G_{x_n}(f+\frac{\xi_n}{2\pi})$ and $G_{x_n}(f-\frac{\xi_n}{2\pi})$ are approximately nonzero and flat over the frequency ranges $[\frac{\xi_n}{2\pi} - \frac{1}{2l(x_n)}, \frac{\xi_n}{2\pi} + \frac{1}{2l(x_n)}]$ and $[-\frac{\xi_n}{2\pi} - \frac{1}{2l(x_n)}, -\frac{\xi_n}{2\pi} + \frac{1}{2l(x_n)}]$, respectively. Note that

$$\Phi_n^{\gamma 0}(f) = \frac{1}{2}\left[G_{x_n}(f - \frac{\xi_n}{2\pi}) e^{j\theta_n} + G_{x_n}(f + \frac{\xi_n}{2\pi}) e^{-j\theta_n} \right], \tag{2.27}$$

where $G_{x_n}(f) = \int_{-\infty}^{\infty} g_{x_n}(\tau) e^{-j2\pi f\tau} d\tau$. It then follows from (2.24) - (2.27) that

$$S_J(t,f) \approx \sum_{p=1}^{P} \frac{1}{l_p} g_p(t) e^{j2\pi ft} \sum_{n\in\mathcal{N}_p} d_n \cos(\xi_n t + \theta_n) \left[G_p(f - \frac{\xi_n}{2\pi}) e^{j\theta_n} + G_p(f + \frac{\xi_n}{2\pi}) e^{-j\theta_n} \right]. \tag{2.28}$$

For any $t \in (t_p, t_{p+1})$, $|S_J(t,f)|$ is also mainly determined by $|\mathcal{N}_p|$ terms in (2.28) corresponding to $\{\phi_n^{\gamma 0}(t)\}_{n\in\mathcal{N}_p}$. More specifically, over the two frequency range $[\frac{\xi_n}{2\pi} - \frac{1}{2l_p}, \frac{\xi_n}{2\pi} + \frac{1}{2l_p}]$ and $[-\frac{\xi_n}{2\pi} - \frac{1}{2l_p}, -\frac{\xi_n}{2\pi} + \frac{1}{2l_p}]$, $|S_J(t,f)|$ can be approximated by $|\frac{d_n}{l_p}\cos(\xi_n t + \theta_n)|$. Hence, $B_c(t,\upsilon)$ can be estimated from $|S_J(t,f)|$ using the method described in (2.7)-(2.8). Similarly, at each border time instant $t = t_p$, $B_c(t_p,\upsilon) \triangleq \min\{B_c(t_p - \tau_\epsilon, \upsilon), B_c(t_p + \tau_\epsilon, \upsilon)\}$.

2.3.3 Binary Tree Based Basis Search Algorithm

We now discuss a practical binary tree based algorithm for fast "best basis" search.

2.3.3.1 Dictionary Construction

To reduce the complexity of the best basis search, a dictionary with admissible binary tree structure is preferred [62, 63]. The admissible binary tree is defined by any binary tree whose nodes have either 0 or 2 branches. Each tree node corresponds to a time interval. Assume the

jamming $J(t)$ is observed over $0 \leq t \leq M$. The root of the tree corresponds to the whole time interval $[0, M]$. The left and right branch nodes correspond to the time interval $[0, M/2]$ and $[M/2, M]$, respectively. Each node is further split until the tree depth N_D is reached. The node (p, j) at depth j and position p corresponds to the time interval $[pM2^{-j}, (p+1)M2^{-j}]$. The window function $g_p^j(t)$ is used to cover the time interval corresponding to each node (p, j). Given a smooth function $\beta(t)$ which satisfies: $\beta(t) = 0$ if $t < -\eta$, $\beta(t) = 1$ if $t > \eta$, and $\beta^2(t) + \beta^2(-t) = 1$. The window function can be constructed as

$$g_p^j(t) = \begin{cases} \beta(t - pM2^{-j}), & \text{if } t < pM2^{-j} + \eta, \\ 1, & \text{if } pM2^{-j} + \eta \leq t \leq (p+1)M2^{-j} - \eta, \\ \beta((p+1)M2^{-j} - t), & \text{if } t > (p+1)M2^{-j} - \eta, \end{cases} \tag{2.29}$$

where $M2^{-j} \geq 2\eta$. A full admissible binary tree with depth $N_D = 2$ and corresponding window functions are illustrated in Figure 2.2.

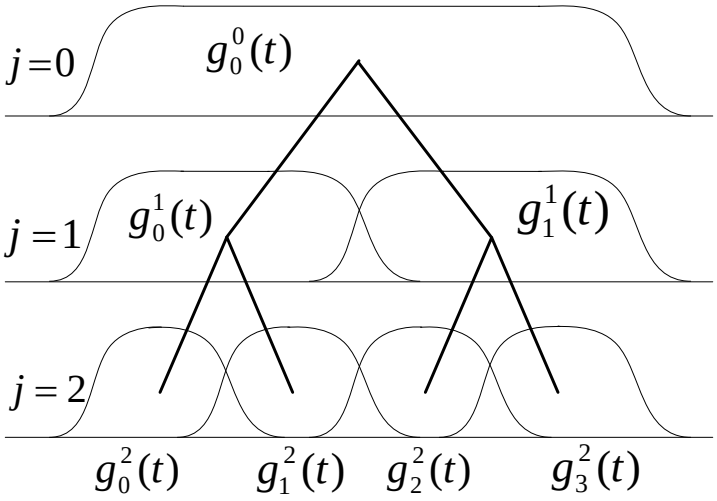


Figure 2.2: An example of full admissible binary tree with depth $N_D = 2$ and corresponding window functions.

Note that the window function $g_p^j(t)$ is associated with the local cosine family through

$$\left\{ \phi_{p,k}^j(t) = g_p^j(t) \sqrt{\frac{2}{M2^{-j}}} \cos\left[\pi \left(k + \frac{1}{2} \right) \frac{t - M2^{-j}p}{M2^{-j}} \right] \right\}_{0 \leq k < M2^{-j}}. \tag{2.30}$$

For leaf nodes from the admissible binary tree indexed by γ, i.e., $(p, j) \in \gamma$, the local cosine family $\mathcal{B}^\gamma = \{\phi_{p,k}^j(t)\}_{(p,j)\in\gamma, 0 \leq k < M2^{-j}}$ formulates an orthogonal basis [63]. The dictionary

$\mathcal{D} = \{\mathcal{B}^\gamma\}_{\gamma\in\Gamma}$ is constructed with all admissible binary trees of depth no more than N_D. Given an orthogonal basis $\mathcal{B}^\gamma$ and Q realizations of $J(t)$, following (2.25), the corresponding diagonal coefficients $d^j_{p,k} = \langle T\phi^j_{p,k}(t), \phi^j_{p,k}(t)\rangle = E\{\ |\langle J, \phi^j_{p,k}(t)\rangle|^2\}$ can be estimated as $\hat{d}^j_{p,k} = \frac{1}{Q}\sum_{q=1}^{Q} |\langle J^q, \phi^j_{p,k}\rangle|^2$.

2.3.3.2 Best Basis Search Using Dynamic Programming

Let $C(p,j) = \sum_{k=0}^{M2^{-j}-1} |\hat{d}^j_{p,k}|^2$. The Hilbert-Schmidt norm of the diagonal operator B_0^γ defined in (2.17) can be estimated as $\|B_0^\gamma\|_h^2 = \sum_{(j,p)\in\gamma} C(p,j)$. To obtain the best basis, we need to search in the dictionary for best basis that maximizes $\|B_0^\gamma\|_h^2$. Let $\mathcal{B}^p_j$ denote the set of basis functions $\{\phi^j_{p,k}(t)\}_{0\le k<M2^{-j}}$ and $\mathcal{O}^p_j$ the set of best basis functions associated with node (p,j). It can be shown that $\|B_0^\gamma\|_h^2$ is maximized if we construct the $\mathcal{O}^p_j$ using the following rule [63]:

$$\mathcal{O}^p_j = \begin{cases} \mathcal{O}^{2p}_{j+1} \cup \mathcal{O}^{2p+1}_{j+1}, & \text{if } C(p,j) < C(2p,j+1) + C(2p+1,j+1), \\ \mathcal{B}^p_j, & \text{otherwise.} \end{cases} \tag{2.31}$$

By making best basis selection at each node recursively using bottom-up progression, the overall best basis can be determined at the root node $\mathcal{B}^{\gamma 0} = \mathcal{O}^0_0$. The computational complexity of the best basis search is reduced to $O(M[\log_2 M]^2)$. The best basis search algorithm is summarized in Table 2.1.

2.4 Simulation Results

In this section, we illustrate the estimation of the time-varying jamming coherence time and the time-frequency jamming coherence bandwidth through simulation examples. $M = 4096$ samples are obtained from the random jamming process, which is assumed to be real-valued zero-mean Gaussian. The time duration of the jamming is normalized to 1, and the frequency

Table 2.1: The best basis search algorithm.

for $j = (J-1) : -1 : 0$ and $p = 0 : (2^j - 1)$ **do**
  Compute $C(p,j) = \sum_{k=0}^{M2^{-j}-1} |\hat{d}_{p,k}^j|^2$
  if $j == J-1$ **then**
    Mark node (p,j) as leaf
  else
    if $C(p,j) \geq C(2p, j+1) + C(2p+1, j+1)$ **then**
      Mark node (p,j) as leaf
    else
      Leave node (p,j) unmarked and $C(p,j) = C(2p, j+1) + C(2p+1, j+1)$
    end if
  end if
end for

is normalized by the sampling rate. The jamming-to-noise ratio (JNR) is defined as the ratio of the jamming power to the noise power.

Example 1: Stationary jamming The jamming here has coherence time $T_c = 7/4096$, and coherence bandwidth $B_c(0) = 0.1056$. The JNR is set to be 10dB. We use the Welch-Bartlett method [64] to estimate the jamming PSD $S_J(f)$, and choose $\alpha_0 = 0.5$, $\alpha_1 = 0.95$. The true and estimated $S_J(f)$ are illustrated in Figure 2.3. The estimated jamming coherence time and bandwidth are $\hat{T}_c = 6/4096$ and $\hat{B}_c(0) = 0.1060$, respectively. We can see that the estimation results are quite accurate.

Example 2: Locally stationary jamming In this example, the jamming consists of 3 stationary intervals with equal length. The JNRs in the three intervals are set to be $(10, 15, 15)$dB, and the normalized center frequencies of $S_J(t,f)$ in the three intervals are $(0, 0.15, 0.3)$, respectively. The estimated best basis consists of local cosine functions associated with 5 different window supports, corresponding to intervals $l_1 \sim l_5$. The true and estimated $R_J(t,\tau)$ and $|S_J(t,f)|$ are illustrated in Figure 2.4 - Figure 2.7, respectively. It can be observed that $|\hat{S}_J(t,f)|$ concentrates within the same time-frequency areas as $|S_J(t,f)|$.

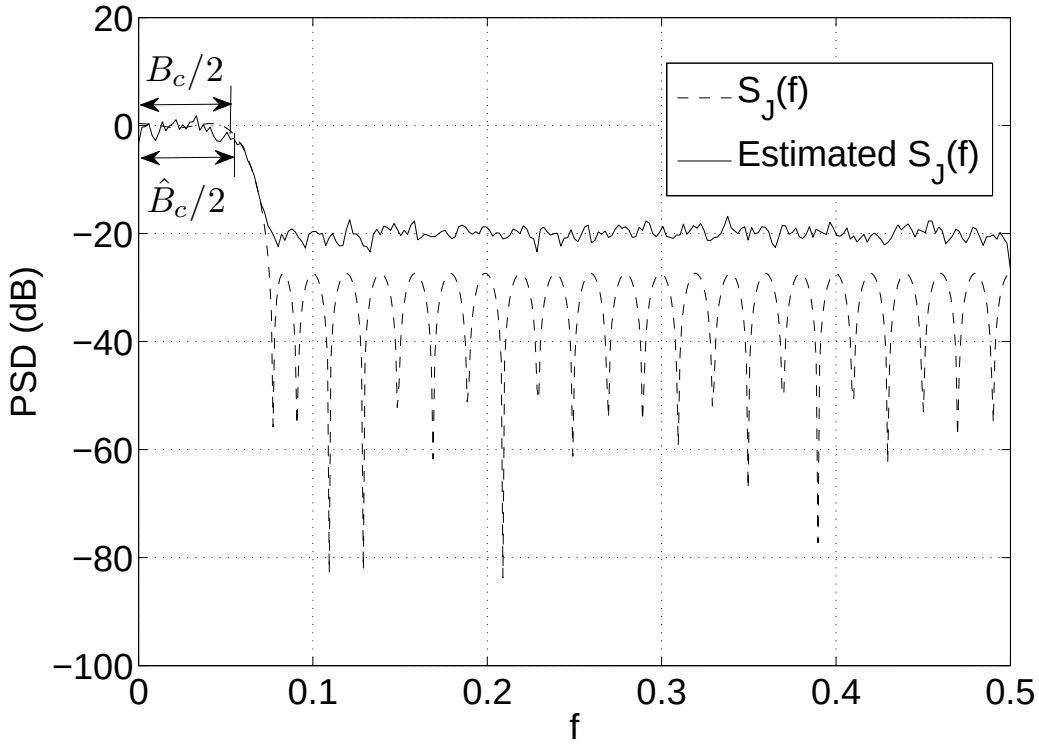


Figure 2.3: Example 1: The true and estimated jamming PSD $S_J(f)$.

For example, for $t = 0.4375$ and $\upsilon = 0.15$, $T_c(0.4375) = 2/4096$ and $B_c(0.4375, 0.15) = 0.0801$. With $\alpha_0 = 0.5$, $\alpha_1 = 0.7$, the estimated results are: $\hat{T}_c(0.4375) = 1/4096$ and $\hat{B}_c(0.4375, 0.15) = 0.0762$.

2.5 Summary

This chapter provides a 2D framework for cognitive jamming modeling and classification. For the first time in literature, all the existing jamming models are summarized and extended to the time-varying case under one general scheme. We further introduce the concepts of time-varying jamming coherence time and time-frequency jamming coherence bandwidth, and classify jamming as fast versus slow jamming, and flat versus frequency selective jamming. We also introduced the concept of disguised jamming, as it can be much more harmful than the traditional strong jamming. Time-frequency analysis and approximation theory

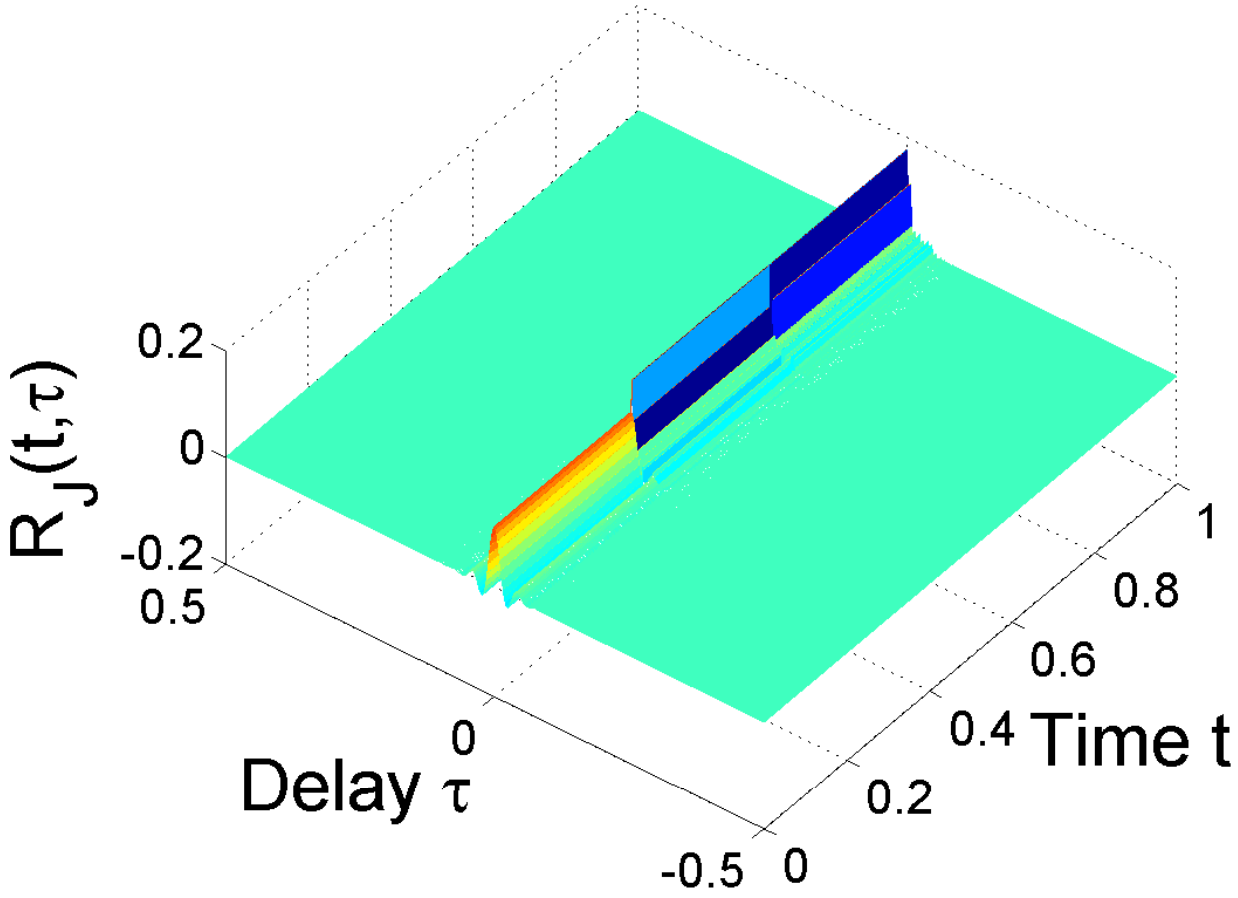


Figure 2.4: Example 2: The true jamming autocorrelation function $R_J(t, \tau)$. For interpretation of the references to color in this and all other figures, the reader is referred to the electronic version of this dissertation.

based algorithms are developed to estimate these statistics for both stationary and locally stationary jamming.

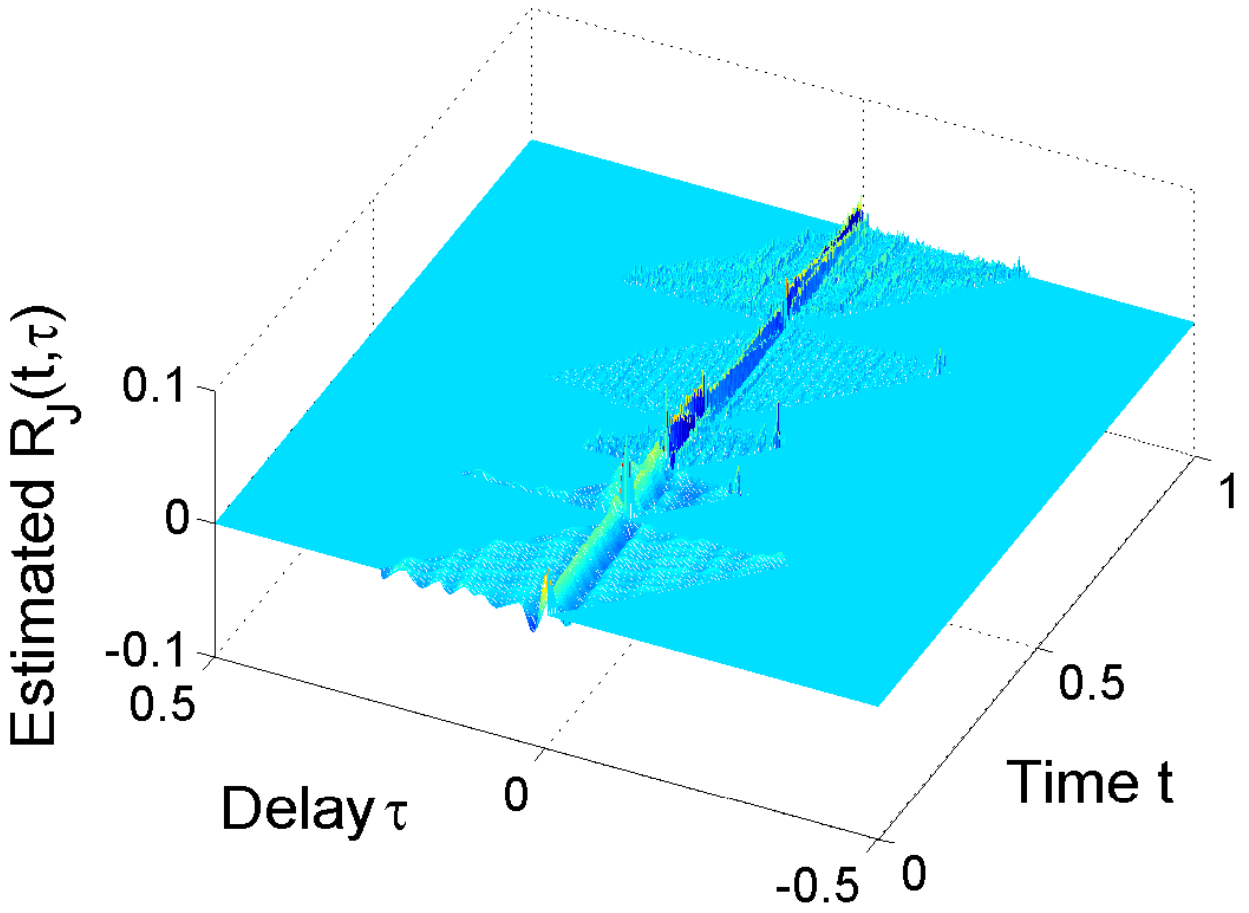


Figure 2.5: Example 2: The estimated $R_J(t, \tau)$ using time-frequency analysis.

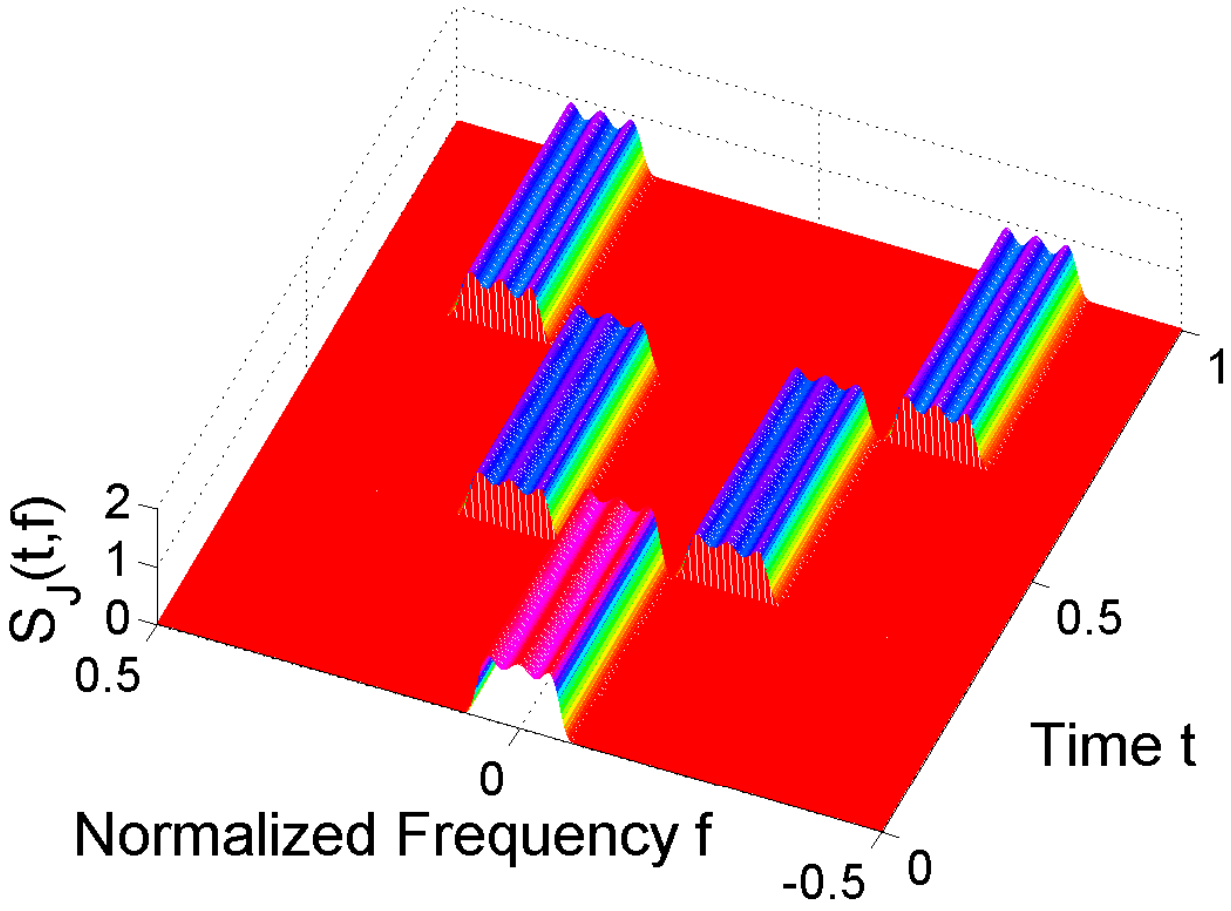


Figure 2.6: Example 2: The magnitude of the true time-varying jamming PSD $|S_J(t, f)|$.

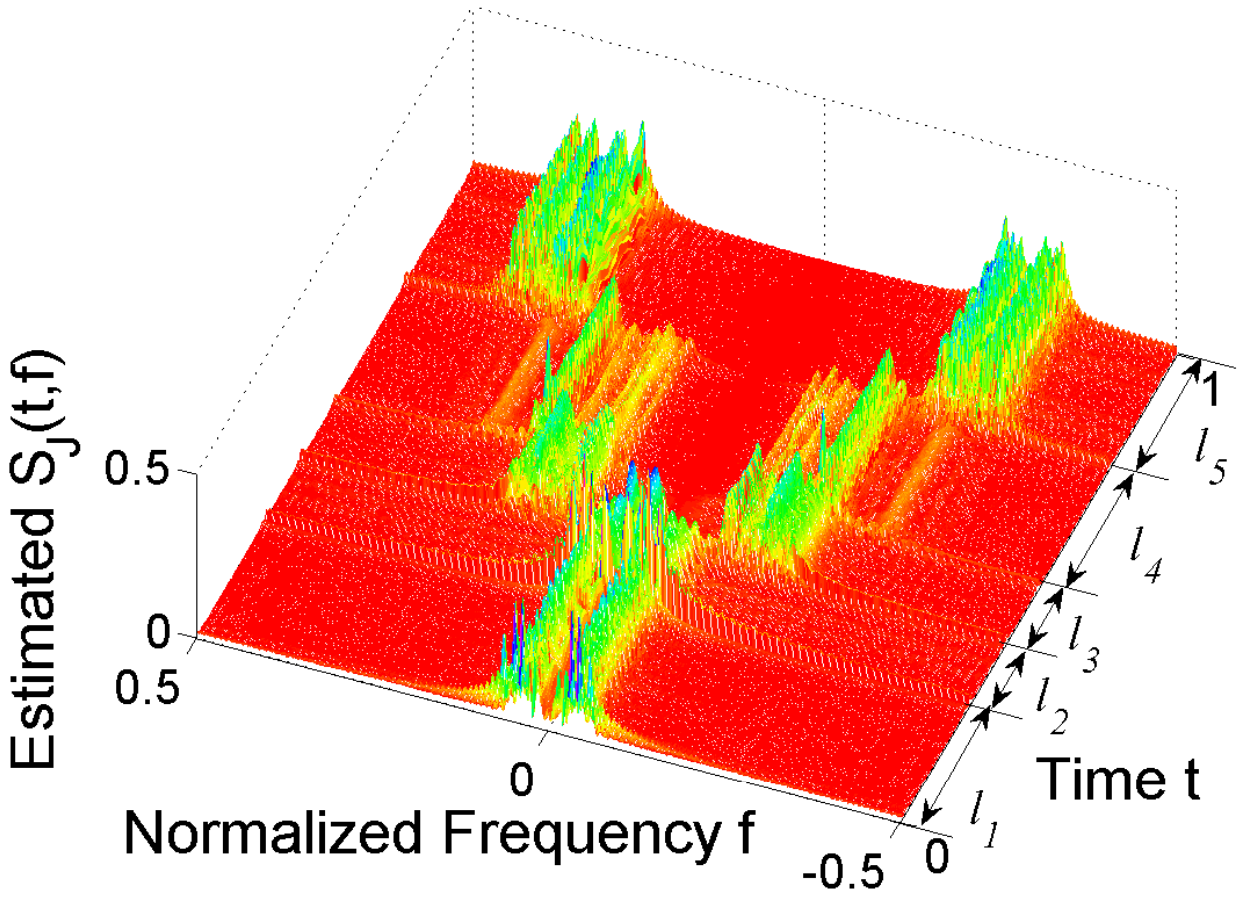


Figure 2.7: Example 2: The magnitude of the estimated $|S_J(t, f)|$ using time-frequency analysis.

Chapter 3

ANTI-JAMMING MESSAGE-DRIVEN FREQUENCY HOPPING SYSTEM DESIGN

In this chapter, we consider robust and spectrally efficient anti-jamming system design in wireless networks. We start with message-driven frequency hopping (MDFH), which is recently proposed as a highly efficient spread spectrum technique. It is observed that while MDFH is robust under strong jamming, it experiences considerable performance losses under disguised jamming from sources that mimic the true signal. To overcome this limitation, we propose an anti-jamming MDFH (AJ-MDFH) system. The main idea is to transmit a secure ID sequence along with the information stream. The ID sequence is generated through a cryptographic algorithm using the shared secret between the transmitter and the receiver, it is then exploited by the receiver for effective signal extraction. It is shown that AJ-MDFH can effectively reduce the performance degradation caused by disguised jamming, and is also robust under strong jamming. In addition, we extend AJ-MDFH to multi-carrier case, which can increase the system efficiency and jamming resistance significantly through jamming randomization and frequency diversity, and can readily be used as a collision-free multiple access system.

3.1 Introduction

As a widely used spread spectrum technique, frequency hopping (FH) was originally designed for secure communication under hostile environments [65, 66, 67, 68, 69]. In conventional FH, each user hops independently based on its own PN sequence, a collision occurs whenever there are two or more users transmitting over the same frequency band. Mainly limited by the collision effect, the spectral efficiency of conventional FH is very low [70, 50]. To improve the spectral efficiency, FH systems that exploit high-dimensional modulation scheme have

been studied in the literature [71, 72, 73, 74, 75]. However, the performance of these systems are still limited by the collision effect, also known as self-jamming.

Recently, a *three-dimensional* modulation scheme, known as message-driven frequency hopping (MDFH), was proposed in [49]. The basic idea of MDFH is that part of the message acts as the PN sequence for carrier frequency selection at the transmitter. More specifically, selection of carrier frequencies is directly controlled by the encrypted information stream rather than by a pre-selected pseudo-random sequence as in conventional FH. The most significant property of MDFH is that: by embedding a large portion of information into the hopping selection process, additional information transmission is achieved with no extra cost on either bandwidth or power. In fact, transmission through hopping frequency control adds another dimension to the signal space, and the resulted coding gain can increase the system spectral efficiency by multiple times [49].

In this chapter, we analyze the performance of MDFH under hostile jamming. It is observed that: MDFH is particularly powerful under *strong jamming* scenarios, and outperforms the conventional FH by big margins. The underlying argument is that: for MDFH, even if the signal is jammed, strong jamming can enhance the power of the jammed signal and hence increases the probability of correct detection. When the system experiences *disguised jamming*, that is, when the jamming is highly correlated with the signal, and has a power level close or equal to the signal power, it is then difficult for the MDFH receiver to distinguish jamming from the true signal, resulting in performance losses.

To improve the performance of MDFH under disguised jamming, in this chapter, first, we propose an anti-jamming MDFH (AJ-MDFH) scheme. The main idea is to insert some signal identification (ID) information during the transmission process. This secure ID information is generated through the Advanced Encryption Standard (AES) [76] using the shared secret between the transmitter and the receiver. The ID information can be exploited by the receiver to locate the true carrier frequency. Moreover, protected by advanced encryption techniques, it is computationally infeasible for malicious users to recover the ID sequence.

In other words, in AJ-MDFH, secure ID signals are introduced to distinguish the true information channel from the disguised channels invoked by jamming interference. Our analysis indicates that: comparing with MDFH, AJ-MDFH can effectively reduce the performance degradation caused by disguised jamming. At the same time, its spectral efficiency is very close to that of MDFH, which is several times higher than that of conventional FH.

Second, we investigate ID constellation design and its impact on the performance of AJ-MDFH under both noise jamming and disguised jamming. Noise jamming, where the jamming is modeled as Gaussian noise, has been widely adopted in literature [77, 78, 79]. But disguised jamming can be much more harmful for most communication systems. For AJ-MDFH, the worst case disguised jamming is ID jamming, for which the jammer tries to mimic the ID signal, and sends symbols from the same constellation as that of the ID signal. We show that under noise jamming, the detection error probability is mainly determined by the signal to jamming and noise ratio. In this case, for a given power constraint, constant modulus constellation delivers the best results in terms of detection error probability. Under ID jamming, the situation is more complex. In the ideal case when the system is noise-free, increasing the ID constellation size can increase the ID uncertainty, hence reduce the probability of error. In this case, the ideal constellation size is $M = \infty$. However, when noise is present, we prove that the detection error probability converges as M goes to infinity. In other words, there exists a threshold M_t, increasing the constellation size over M_t will result in little improvement in error probability. This result justifies the use of practical, finite size constellations in AJ-MDFH.

Finally, we extend the single carrier AJ-MDFH to multi-carrier AJ-MDFH (MC-AJ-MDFH). It is observed that by exploiting secure group generation mechanism, MC-AJ-MDFH can increase the system efficiency and jamming resistance significantly through *jamming randomization* and enriched frequency diversity. Moreover, by assigning different carrier groups to different users, MC-AJ-MDFH can also be used as a collision-free multiple access system. We analyze the proposed system through both theoretical derivation as well

as numerical results. Our analysis indicates that: while AJ-MDFH is much more robust than MDFH under various jamming attacks, its spectral efficiency is very close to that of MDFH, which is several times higher than that of conventional FH.

This chapter is organized as follows. In Section 3.2, the anti-jamming performance of MDFH is analyzed under both strong jamming and disguised jamming. In Section 3.3, the proposed AJ-MDFH scheme is introduced, together with the carrier detection metrics. ID constellation design is investigated in Section 3.4. The multi-carrier extension of AJ-MDFH is introduced in Section 3.5. Spectral efficiency is analyzed in Section 3.6. Simulation examples are provided in Section 3.7 and we conclude in Section 3.8.

3.2 A Brief Review of Message-Driven Frequency Hopping

In this section, we briefly review the message-driven frequency hopping (MDFH) system, and evaluate its performance under different jamming scenarios.

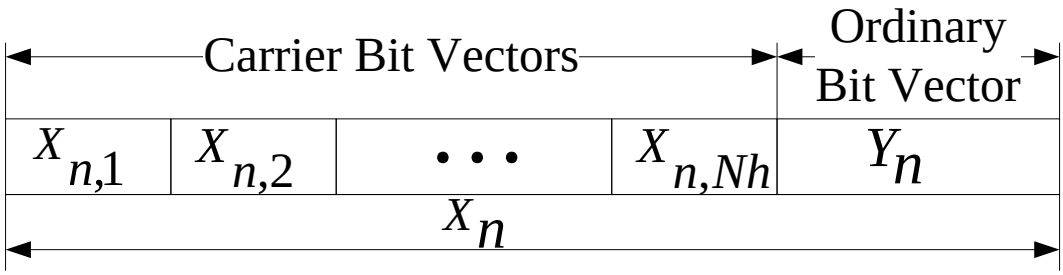
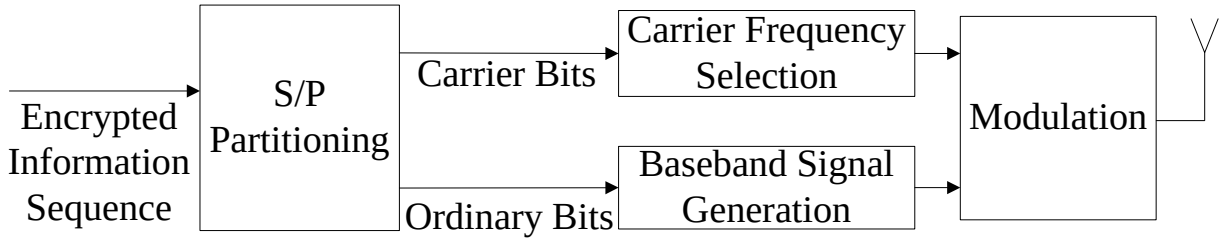


Figure 3.1: The nth block of the information.

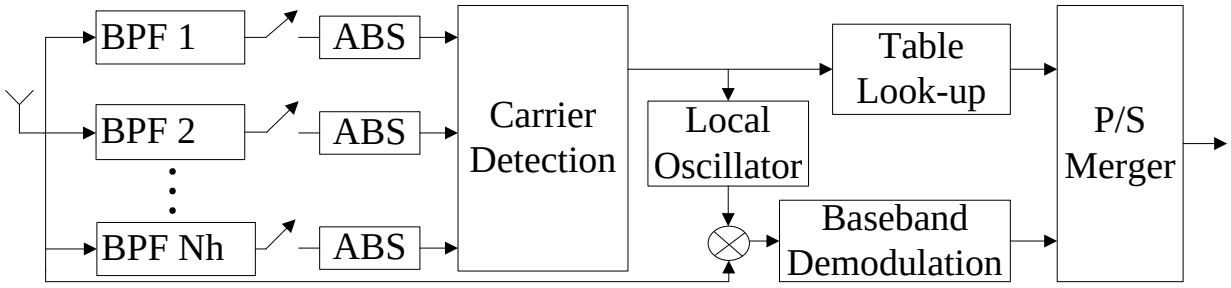
3.2.1 System Description

The basic idea of MDFH is that a major part of the information is transmitted through carrier frequency selection in the hopping process. In other words, the hopping pattern is determined by the encrypted message information itself.

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. The number of bits used to specify an individual channel



(a) Transmitter structure



(b) Receiver structure

Figure 3.2: Transmitter and receiver structure of MDFH, here ABS means taking the absolute value.

here is $B_c = \lfloor \log_2 N_c \rfloor$, where $\lfloor x \rfloor$ denotes the 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 total 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 channel. Without loss of generality, here we assume that $N_c = 2^{B_c}$.

Let Ω be the selected constellation that contains M symbols, 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 $N_h = \dfrac{T_s}{T_h}$. We assume that N_h is an integer larger than or equal to one.

The transmitter and the receiver structure of MDFH is shown in Figure 3.2. We start by dividing the *encrypted* information stream into blocks of length $L \triangleq N_h B_c + B_s$. Each block is parsed into $N_h B_c$ *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 channels successively. Denote the nth block by X_n, as

illustrated in Figure 3.1. Note that in MDFH, the whole block X_n is transmitted within one symbol period.

At the receiver, the transmitting frequency is captured using a filter bank as in the FSK receiver rather than using the frequency synthesizer. 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 (BPF), each centered at f_i ($i = 1, 2, \cdots, N_c$), is deployed at the receiver front end, followed by a demodulator equipped with matched filter and sampler. At each hopping period, the carrier frequency (hence the information embedded in frequency selection) can be blindly detected at each hop. The ordinary bits can then be extracted from the selected channels through the regular demodulation process.

In a jamming-free environment, carrier frequency detection can be performed by selecting the channel with maximum received power. However, when jamming is present, the Jamming detection algorithm can be incorporated at the receiver to improve the system performance. One way to do this is to use a threshold based detector as follows [80]:

1. Classify each channel according to the power detection threshold η. Let P_i denote the received signal power over the ith channel. If $P_i < \eta$, then there is only noise over channel i, we say that the channel is *inactive*; otherwise, if $P_i \geq \eta$, we say that the channel is *active*.

2. Let $\mathcal{I}_a = \{i | P_i > \eta, i = 1, 2, \cdots, N_c\}$ be the set of the index of all the active channels, then the estimated hopping frequency index, denoted by $\hat{k}$, is determined by

$$\hat{k} = \arg \min_{i \in \mathcal{I}_a} \{P_i\}. \tag{3.1}$$

   The carrier bits can be recovered based on $\hat{k}$; the ordinary bits are extracted following the regular demodulation process.

3.2.2 Performance of MDFH under Hostile Jamming

First, we introduce the concept of *disguised jamming*. *Disguised jamming* denotes the case where the jamming is highly correlated with the signal, and has a power level close or equal to the signal power. More specifically, let $s(t)$ and $J(t)$ be the user's signal and jamming interference, respectively. Define

$$\rho = \frac{1}{T_0\sqrt{P_s P_J}} \int_{t_1}^{t_2} s(t)J^*(t)dt \tag{3.2}$$

as the normalized cross-correlation coefficient of $s(t)$ and $J(t)$ over the time period $[t_1, t_2]$, where $T_0 = t_2 - t_1$,

$$P_s = \frac{1}{T_0} \int_{t_1}^{t_2} |s(t)|^2 dt$$

and

$$P_J = \frac{1}{T_0} \int_{t_1}^{t_2} |J(t)|^2 dt.$$

We say that $J(t)$ is a disguised jamming to signal $s(t)$ over $[t_1, t_2]$ if

1. $J(t)$ and $s(t)$ are highly correlated. More specifically, $|\rho| > \rho_0$, where ρ_0 is an application-oriented, predefined correlation threshold.

2. The jamming to signal ratio (JSR) is close to 0dB. More specifically, $|\frac{P_J}{P_s} - 1| < \epsilon_P$, where ϵ_P is an application-oriented, predefined jamming-signal ratio threshold.

In this dissertation, we consider disguised jamming over each hopping period, that is, $[t_1, t_2] = [mT_h, (m+1)T_h]$ for some integer m. In *the worst case*, the constellation Ω and the pulse shaping filter of the information signal are known to the jammer, the jammer can then disguise itself by transmitting symbols from Ω over a fake channel using the same power level. That is, $J(t) = e^{i\theta}s(t)$ for some phase θ.

We compare the performance of MDFH with that of conventional FH in AWGN channels, under both noise jamming and disguised jamming. The result (with no channel coding) is shown in Figure 3.3. The jamming-to-signal ratio is defined as $JSR = \frac{P_J}{P_s}$, where P_J and

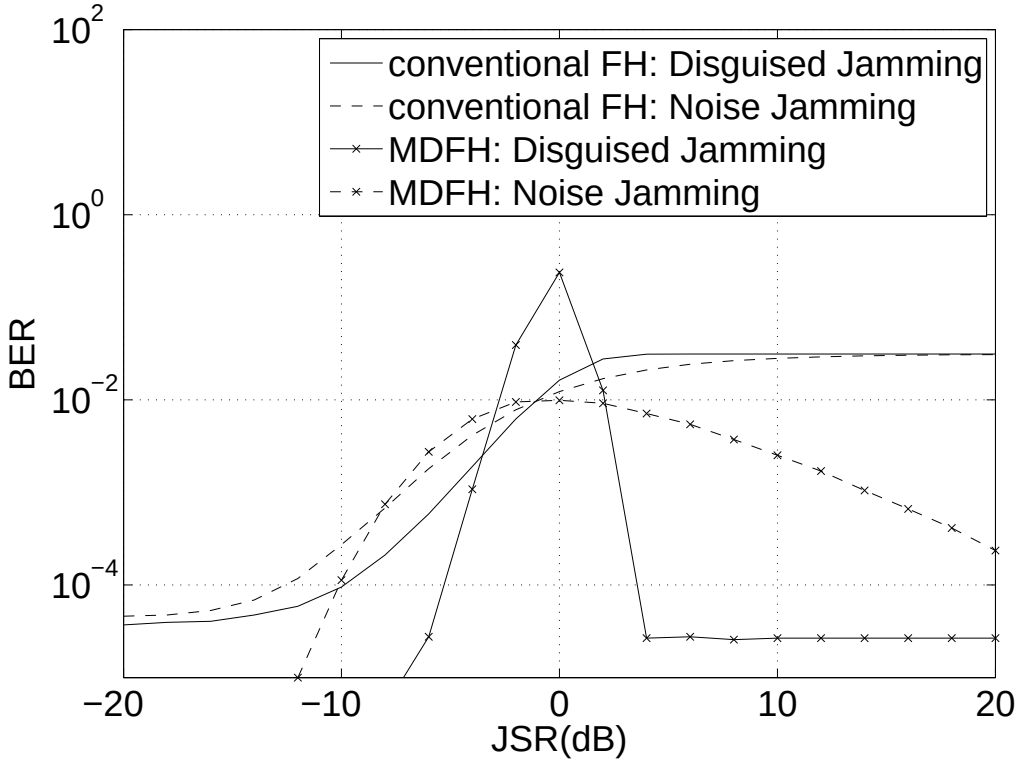


Figure 3.3: Performance comparison under single band jamming, $E_b/N_0 = 10$dB, $N_c = 64, N_h = 3$. MDFH uses QPSK modulation and conventional FH uses 4-FSK modulation. In this case, the spectral efficiency of MDFH is roughly 3.3 times that of conventional FH.

P_s denote the jamming power and signal power per hop, respectively. As can be seen, *MDFH delivers excellent performance under strong jamming (i.e., $JSR \gg 1$) scenarios*, and outperforms conventional FH by big margins. Note that in this case, the spectral efficiency of MDFH is 3.3 times that of conventional FH. The underlying argument is that: when the jamming power is much stronger than the signal power, jamming can be easily distinguished from the true signal when they are in different bands; even if jamming collides with the signal, the true carrier frequency can still be detected as jamming can even enhance the power of the jammed channel and hence increases the correct detection probability. For conventional FH, on the other hand, once the jamming power reaches a certain level, the system performance is mainly limited by the probability that the signal is jammed.

However, we also notice that under disguised jamming, the system experiences considerable performance losses, since it is difficult for the MDFH receiver to distinguish jamming from the true signal. The sensitivity of MDFH to disguised jamming is influenced by the SNR. To enhance the jamming resistance of MDFH under disguised jamming, we introduce the anti-jamming MDFH (AJ-MDFH) system.

3.3 Anti-jamming MDFH (AJ-MDFH) System

3.3.1 Transmitter Design

The main idea here is to insert some signal identification (ID) information during the transmission process. This secure ID information is generated through a cryptographic algorithm using the shared secret between the transmitter and the receiver, and can be used by the receiver to locate the true carrier frequency. Our design goal is to reinforce jamming resistance without sacrificing too much on spectral efficiency.

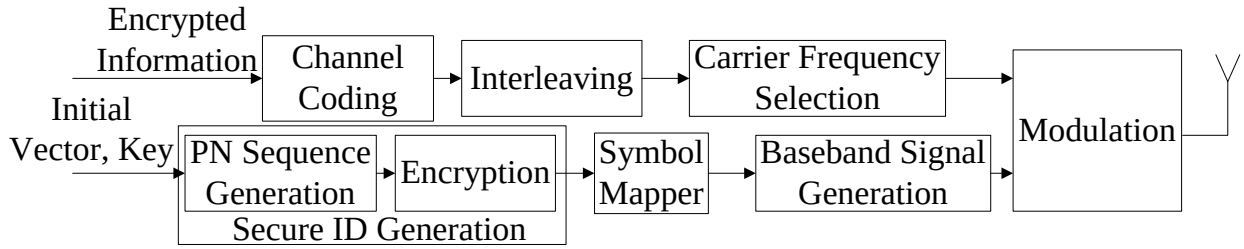


Figure 3.4: AJ-MDFH transmitter structure.

The transmitter structure of AJ-MDFH is illustrated in Figure 3.4. Each user is assigned a secure ID sequence. We propose to replace the ordinary bits in MDFH with the ID bits. In order to prevent impersonate attack, each user's ID sequence needs to be kept secret from the malicious jammer. The ID sequence can be generated using two steps as in [81]:

1. Generate a pseudo-random binary sequence using a 42-bit linear feedback shift register

(LFSR) specified by the characteristic polynomial

$$x^{42} + x^{35} + x^{33} + x^{31} + x^{27} + x^{26} + x^{25} + x^{22} + x^{21} + x^{19}$$
$$+x^{18} + x^{17} + x^{16} + x^{10} + x^{7} + x^{6} + x^{5} + x^{3} + x^{2} + x + 1.$$

2. Take the output of LFSR as the plaintext, group it into blocks of length K_L bits ($K_L = 128, 192$ or 256), and feed it into the Advanced Encryption Standard (AES) [76] encrypter of key size K_L. The AES output is then used as our ID sequence.

Recall that $B_c = \log_2 N_c$ and $B_s = \log_2 M$, where N_c is the number of channels, and M is the constellation size. We divide the source information into blocks of size B_c and divide the ID sequence into blocks of size B_s. Denote the nth source information block and ID bits block as X_n and Y_n, respectively. Let f_{X_n} be the carrier frequency corresponding to X_n and s_n the symbol corresponding to ID bit-vector Y_n. The transmitted signal can then be represented as

$$\begin{aligned} s(t) &= \sqrt{2} Re \left\{ \sum_{n=-\infty}^{\infty} s_n g(t - nT_h) e^{j2\pi f_{X_n} t} \right\} \\ &= \sqrt{2} Re \left\{ \sum_{n=-\infty}^{\infty} \sum_{i=1}^{N_c} \alpha_{i,n} s_n g(t - nT_h) e^{j2\pi f_i t} \right\}, \end{aligned} \tag{3.3}$$

where T_h is the duration of each hop, $g(t)$ is the pulse shaping filter,

$$\alpha_{i,n} = \begin{cases} 1 & \text{if } f_{X_n} = f_i, \\ 0 & \text{otherwise.} \end{cases}$$

3.3.2 Receiver Design

The receiver structure for AJ-MDFH is shown in Figure 3.5. The receiver regenerates the secure ID through the shared secret (including the initial vector, the LFSR information and the key). For each hop, the received signal is first fed into the bandpass filter bank. The output of the filter bank is first demodulated, and then used for carrier bits (i.e., the information bits) detection.

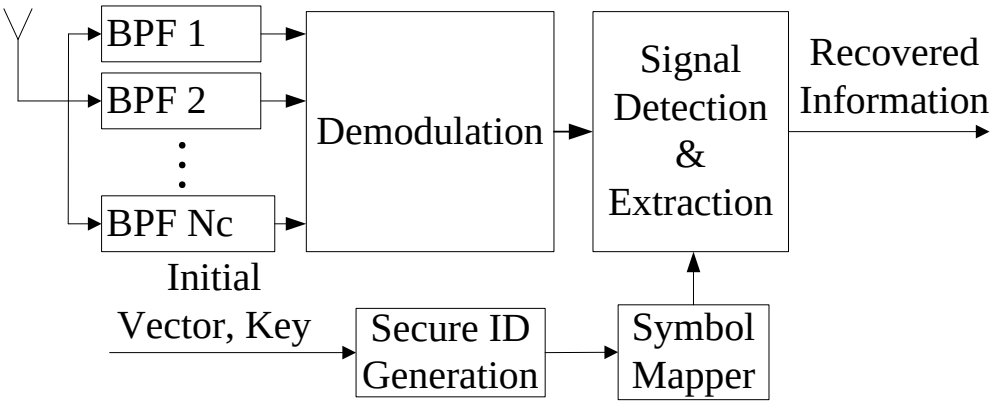


Figure 3.5: AJ-MDFH receiver structure.

3.3.2.1 Demodulation

Let $s(t)$, $J(t)$ and $n(t)$ denote the ID signal, the jamming interference and the noise, respectively. For AWGN channels, the received signal can be represented as

$$r(t) = s(t) + J(t) + n(t). \tag{3.4}$$

We assume that $s(t), J(t)$ and $n(t)$ are independent of each other.

For $i = 1, 2, \cdots, N_c$, the output of the ith ideal bandpass filter $\mathrm{f}_i(t)$ is $r_i(t) = \mathrm{f}_i(t) * r(t)$. For demodulation, $r_i(t)$ is first shifted back to the baseband, and then passed through a matched filter. At the nth hopping period, for $i = 1, \cdots, N_c$, the sampled matched filter output corresponds to channel i can be expressed as

$$r_{i,n} = \alpha_{i,n} s_n + \beta_{i,n} J_{i,n} + n_{i,n}, \tag{3.5}$$

where $s_n, J_{i,n}$ and $n_{i,n}$ correspond to the ID symbol, the jamming interference and the noise, respectively; $\alpha_{i,n}, \beta_{i,n} \in \{0, 1\}$ are binary indicators for the presence of ID signal and jamming, respectively. Note that the true information is carried in $\alpha_{i,n}$.

3.3.2.2 Signal Detection and Extraction

Signal detection and extraction is performed for each hopping period. *For notation simplicity, without loss of generality, we omit the subscript n in (3.5).* That is, for a particular

hopping period, (3.5) is reduced to:

$$r_i = \alpha_i s + \beta_i J_i + n_i, \quad \text{for } i = 1, \cdots, N_c. \tag{3.6}$$

Define $\mathbf{r} = (r_1, \ldots, r_{N_c})$, $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_{N_c})$, $\boldsymbol{\beta} = (\beta_1, \ldots, \beta_{N_c})$, $\mathbf{J} = (J_1, \ldots, J_{N_c})$ and $\mathbf{n} = (n_1, \ldots, n_{N_c})$, then (3.6) can be rewritten in vector form as:

$$\mathbf{r} = s\boldsymbol{\alpha} + \boldsymbol{\beta} \cdot \mathbf{J} + \mathbf{n}. \tag{3.7}$$

For single-carrier AJ-MDFH, at each hopping period, one and only one item in $\boldsymbol{\alpha}$ is nonzero. That is, there are N_c possible information vectors: $\boldsymbol{\alpha}_1 = (1, 0, \ldots, 0), \boldsymbol{\alpha}_2 = (0, 1, \ldots, 0), \cdots, \boldsymbol{\alpha}_{N_c} = (0, 0, \ldots, 1)$. If $\boldsymbol{\alpha}_k$ is selected, and the binary expression of k is $b_0 b_1 \cdots b_{B_c-1}$, with $B_c = \lfloor \log_2 N_c \rfloor$, then the estimated information sequence is $b_0 b_1 \cdots b_{B_c-1}$.

At each hopping period, the information symbol $\boldsymbol{\alpha}$, or equivalently, the hopping frequency index k, needs to be estimated based on the received signal and the ID information which is shared between the transmitter and the receiver. When the input information vectors are equiprobable, that is, $P(\boldsymbol{\alpha}_i) = \dfrac{1}{N_c}$ for $i = 1, 2, \ldots, N_c$, the MAP (maximum a posteriori probability) detector is reduced to the ML (maximum likelihood) detector. For the ML detector, the hopping frequency index $\hat{k}$ can be estimated as:

$$\hat{k} = \arg \max_{1 \le i \le N_c} Pr\{\mathbf{r} | \boldsymbol{\alpha}_i\}. \tag{3.8}$$

Recall that the information signal, the ID signal, the jamming interference and the noise are independent to each other. When $n_1, \ldots, n_{N_c}$, $J_1, \ldots, J_{N_c}$ are all statistically independent, $r_1, \ldots, r_{N_c}$ are also independent. In this case, the joint ML detector in (3.8) can be decomposed as:

$$\begin{aligned}
\hat{k} &= \arg \max_{1 \le i \le N_c} \prod_{j=1}^{N_c} Pr\{r_j | \boldsymbol{\alpha}_i\} \\
&= \arg \max_{1 \le i \le N_c} \prod_{j=1, j \ne i}^{N_c} Pr\{r_j | \alpha_j = 0\} \cdot Pr\{r_i | \alpha_i = 1\} \\
&= \arg \max_{1 \le i \le N_c} \prod_{j=1}^{N_c} Pr\{r_j | \alpha_j = 0\} \cdot \frac{Pr\{r_i | \alpha_i = 1\}}{Pr\{r_i | \alpha_i = 0\}}.
\end{aligned} \tag{3.9}$$

Since $\prod_{j=1}^{N_c} Pr\{r_j|\alpha_j = 0\}$ is independent of i, (3.9) can be further reduced to the likelihood ratio test

$$\hat{k} = \arg \max_{1 \le i \le N_c} \frac{Pr\{r_i|\alpha_i = 1\}}{Pr\{r_i|\alpha_i = 0\}}, \tag{3.10}$$

where $Pr\{r_i|\alpha_i = 1\} = \sum_{\beta_i} Pr\{r_i|\alpha_i = 1, \beta_i\}P(\beta_i)$ and $Pr\{r_i|\alpha_i = 0\} = \sum_{\beta_i} Pr\{r_i|\alpha_i = 0, \beta_i\}P(\beta_i)$, with $\beta_i \in \{0, 1\}$. In the ideal case when β_i is known for $i = 1, \cdots, N_c$, the ML detector above can be further simplified. If we assume that $n_1, \cdots, n_{N_c}$ are i.i.d. circularly symmetric Gaussian random variables of zero-mean and variance σ_n^2, and $J_1, \cdots, J_{N_c}$ are i.i.d. circularly symmetric Gaussian random variables of zero-mean and variance $\sigma_{J_i}^2$, then it follows from (3.6) and (3.10) that

$$\begin{aligned} \hat{k} &= \arg \max_{1 \le i \le N_c} \frac{\frac{1}{\pi\sigma_i^2} \exp\{-\frac{\|r_i - s\|^2}{\sigma_i^2}\}}{\frac{1}{\pi\sigma_i^2} \exp\{-\frac{\|r_i\|^2}{\sigma_i^2}\}} \\ &= \arg \max_{1 \le i \le N_c} \frac{\|r_i\|^2 - \|r_i - s\|^2}{\sigma_i^2}, \end{aligned} \tag{3.11}$$

where $\sigma_i^2 = \beta_i \sigma_{J_i}^2 + \sigma_n^2$.

Note that σ_i^2 is generally unknown. If we replace the overall interference power σ_i^2 with the instantaneous power of the received signal $\|r_i\|^2$, then it follows from (3.11) that:

$$\begin{aligned} \hat{k} &= \arg \max_{1 \le i \le N_c} \frac{\|r_i\|^2 - \|r_i - s\|^2}{\|r_i\|^2} \\ &= \arg \min_{1 \le i \le N_c} \frac{\|r_i - s\|^2}{\|r_i\|^2}. \end{aligned} \tag{3.12}$$

For more tractable theoretical analysis, we can replace $\|r_i\|^2$ with average signal power observed in channel i, $P_i = E\{\|r_i\|^2\}$. Define $Z_i \triangleq \frac{\|r_i - s\|}{\sqrt{P_i}}$, then we have

$$\hat{k} = \arg \min_{1 \le i \le N_c} Z_i. \tag{3.13}$$

3.4 ID Constellation Design and its Impact on System Performance

For AJ-MDFH, ID signals are introduced to distinguish the true information channel from disguised channels invoked by jamming interference. In this section, we investigate ID constellation design and its impact on the performance of AJ-MDFH under various jamming scenarios.

3.4.1 Design Criterion and Jamming Classification

The general design criterion of the ID constellation is *to minimize the probability of error under a given signal power*. Under this criterion, the following questions need to be answered: (1) How does the size of the constellation impact the system performance? (2) How does the type or shape of the constellation influence the detection error? Which type should we use for optimal performance? In this section, we will try to address these questions under different jamming scenarios.

In literature, jamming has generally been modeled as Gaussian noise [77, 78, 79], referred as *noise jamming*. Recall that disguised jamming denotes the jamming interference which has similar power and spectral characteristics as that of the true signal. For AJ-MDFH, when the ID constellation is known to, or can be guessed by the jammer, the jammer can then disguise itself by sending symbols taken from the same constellation over a different or fake channel. In this case, it could be difficult for the receiver to distinguish the true channel from the disguised channel, leading to high detection error probability. We refer to this kind of jamming as *ID jamming* or ID attack. That is, ID jamming is the worst case disguised jamming for AJ-MDFH.

3.4.2 Constellation Design under Noise Jamming

Without loss of generality, we consider the case where the ID symbol is transmitted through channel 1, i.e.,

$$\boldsymbol{\alpha} = (\alpha_1, \cdots, \alpha_{N_c}) = (1, 0, \cdots, 0). \tag{3.14}$$

Recall that for $i = 1, \cdots, N_c$, $r_i = \alpha_i s + \beta_i J_i + n_i$. Let $\tilde{n}_i = \beta_i J_i + n_i$, and denote its variance as $\sigma_i^2 = \beta_i \sigma_{J_i}^2 + \sigma_n^2$. σ_i^2 may vary from channel to channel. Following the definition in (3.13), we have $Z_1 = \dfrac{\|\tilde{n}_1\|}{\sqrt{\|s\|^2 + \sigma_1^2}}$, and $Z_i = \dfrac{\|\tilde{n}_i - s\|}{\sigma_i}$ for $2 \le i \le N_c$. It can be seen that Z_1 is a Rayleigh random variable with probability density function (PDF)

$$p_{Z_1}(z_1) = \frac{z_1}{\sigma^2} e^{-\frac{z_1^2}{2\sigma^2}}, \quad z_1 > 0, \tag{3.15}$$

where $\sigma^2 = \dfrac{\sigma_1^2}{2(\|s\|^2 + \sigma_1^2)}$. For $2 \le i \le N_c$, Z_i is a Rician random variable with PDF

$$p_{Z_i}(z_i) = \frac{z_i}{\sigma^2} e^{-\frac{z_i^2 + \nu^2}{2\sigma^2}} I_0\left(\frac{z_i \nu}{\sigma^2}\right), \quad z_i > 0, \tag{3.16}$$

where $\nu = \dfrac{\|s\|}{\sigma_i}$, $\sigma = \dfrac{1}{\sqrt{2}}$ and $I_0(x)$ is the modified Bessel function of the first kind with order zero.

According to (3.13), the carrier can be correctly detected if and only if $Z_1 < Z_i$ for all $2 \le i \le N_c$. Assuming that the symbols in constellation Ω are equally probable, then the carrier detection error probability is given by

$$\begin{aligned} P_e &= 1 - \sum_{s \in \Omega} Pr\{Z_1 < Z_2, \ldots, Z_1 < Z_{N_c} | s\} p_S(s) \\ &= 1 - \frac{1}{|\Omega|} \sum_{s \in \Omega} \int_0^\infty \prod_{i=2}^{N_c} Pr\{Z_i > z_1 | s, Z_1 = z_1\} p_{Z_1}(z_1) dz_1. \end{aligned}$$

Note that $Z_2, \cdots, Z_{N_c}$ are i.i.d. Rician random variables, then it follows from (3.15) and (3.16) that

$$P_e = 1 - \frac{1}{|\Omega|} \sum_{s \in \Omega} \int_0^\infty \prod_{i=2}^{N_c} Q_1\left(\frac{\sqrt{2}}{\sigma_i}\|s\|, \sqrt{2} z_1\right) \frac{2(\|s\|^2 + \sigma_1^2)}{\sigma_1^2} z_1 e^{-\frac{\|s\|^2 + \sigma_1^2}{\sigma_1^2} z_1^2} dz_1, \tag{3.17}$$

where Q_1 is the Marcum Q-function [82]. We have the following result:

Proposition 1 *Assuming the true channel index is k. Under noise jamming, an upper bound of the carrier detection error probability P_e can be obtained as:*

$$P_e^U = \frac{1}{|\Omega|}\sum_{s\in\Omega}\left[1-\left(1-\frac{\sigma_k^2}{\|s\|^2+2\sigma_k^2}e^{-\frac{\|s\|^2(\|s\|^2+\sigma_k^2)}{\sigma_m^2(\|s\|^2+2\sigma_k^2)}}\right)^{N_c-1}\right], \tag{3.18}$$

where $m = \arg\max\{\sigma_l^2\}$ for $1 \le l \le N_c, l \ne k$.

Proof: See Section 3.9.1. □

Assuming the true channel index is k, let $x = \dfrac{\|s\|^2}{\sigma_k^2}$ and $a(x) = 1-(1-\dfrac{1}{x+2}e^{-\zeta\frac{x^2+x}{x+2}})^{N_c-1}$. The upper bound of the detection error probability, P_e^U can be written as $P_e^U = a(x)$ with $\zeta = \sigma_k^2/\sigma_m^2$. Note that when $x \gg 1$, $a(x) \approx \dfrac{(N_c-1)}{x+2}e^{-\zeta\frac{x^2+x}{x+2}} \triangleq \tilde{a}(x)$. We now show that when $x \gg 1$, $\tilde{a}(x)$ is a convex function. The first and second derivative of $\tilde{a}(x)$ can be obtained as

$$\tilde{a}'(x) = -(N_c-1)\frac{\zeta x^2+(4\zeta+1)x+(2\zeta+2)}{(x+2)^3}e^{-\zeta\frac{x^2+x}{x+2}} \tag{3.19}$$

$$\begin{aligned}\tilde{a}''(x) &= (N_c-1)\frac{\zeta x^2+(4\zeta+2)x+(4-2\zeta)}{(x+2)^4}e^{-\zeta\frac{x^2+x}{x+2}} \\ &\quad +(N_c-1)\frac{\zeta(x^2+4x+2)[\zeta x^2+(4\zeta+1)x+(2\zeta+2)]}{(x+2)^5}e^{-\zeta\frac{x^2+x}{x+2}}\end{aligned} \tag{3.20}$$

Note that the second term of $\tilde{a}''(x)$ is always positive when $x > 0$. Note that the quadratic equation $\zeta x^2+(4\zeta+2)x+(4-2\zeta) = 0$ with discriminant $\Delta = 6\zeta^2+1 > 0$ has two distinct real roots. Let $x_0 = \sqrt{1/\zeta^2+6}-(1/\zeta+2)$ denote the larger real root. Define $c(y) \triangleq \sqrt{y^2+6}-(y+2)$ such that $x_0 = c(1/\zeta)$. Note that $c'(y) = \dfrac{y}{\sqrt{y^2+6}}-1 < 0$ and $c(0) = \sqrt{6}-2$. Since $1/\zeta > 0$, $x_0 = c(1/\zeta) < c(0)$. Hence for $x > \sqrt{6}-2 > x_0$, $\zeta x^2+(4\zeta+2)x+(4-2\zeta) > 0$ and $\tilde{a}''(x)$ is positive. Thus we proved that $\tilde{a}(x)$ is convex when $x > \sqrt{6}-2$.

By Jensen's inequality [83], we have

$$P_e^U \approx \frac{1}{|\Omega|}\sum_{s\in\Omega}\tilde{a}\left(\frac{\|s\|^2}{\sigma_k^2}\right) \geq \tilde{a}\left(\frac{1}{|\Omega|\sigma_k^2}\sum_{s\in\Omega}\|s\|^2\right) = \tilde{a}\left(\frac{P_s}{\sigma_k^2}\right). \tag{3.21}$$

The equality is achieved if and only if $\|s\|^2 = P_s$ for all $s \in \Omega$. This implies that: *under the condition that the signal to jamming and noise ratio over channel k satisfies* $\frac{\|s\|^2}{\sigma_k^2} \gg 1$, P_e^U *is approximately minimized when the constellation is constant modulus, that is,* $\|s\|^2 = P_s$ *for all* $s \in \Omega$.

An intuitive explanation for this result is that the signal power in constant modulus constellations is always equal to the maximal signal power available. Furthermore, it can be seen that P_e^U is independent of the constellation size $|\Omega|$, but is only a function of P_s/σ_k^2. Next, we will investigate how the constellation size affects the system performance under ID jamming.

3.4.3 Constellation Design under ID Jamming

Theorem 1 *For a given SNR and assuming PSK constellation is utilized, under ID jamming, the carrier detection error probability* P_e *is a function of constellation size* M *and*

$$\lim_{M\to\infty} P_e(M) = \bar{P}_e. \tag{3.22}$$

In other words, for any given $\epsilon > 0$, *there always exists an* M_t *such that for all* $M > M_t$, $|P_e(M) - \bar{P}_e| < \epsilon$.

The expression of $\bar{P}_e$ and the proof of the theorem can be found in Section 3.9.2. This theorem essentially says that: for a given SNR, due to the noise effect, increasing the constellation size over a threshold M_t will result in little improvement in detection error probability. *This result justifies the use of finite constellation in AJ-MDFH.*

3.5 Multi-carrier AJ-MDFH

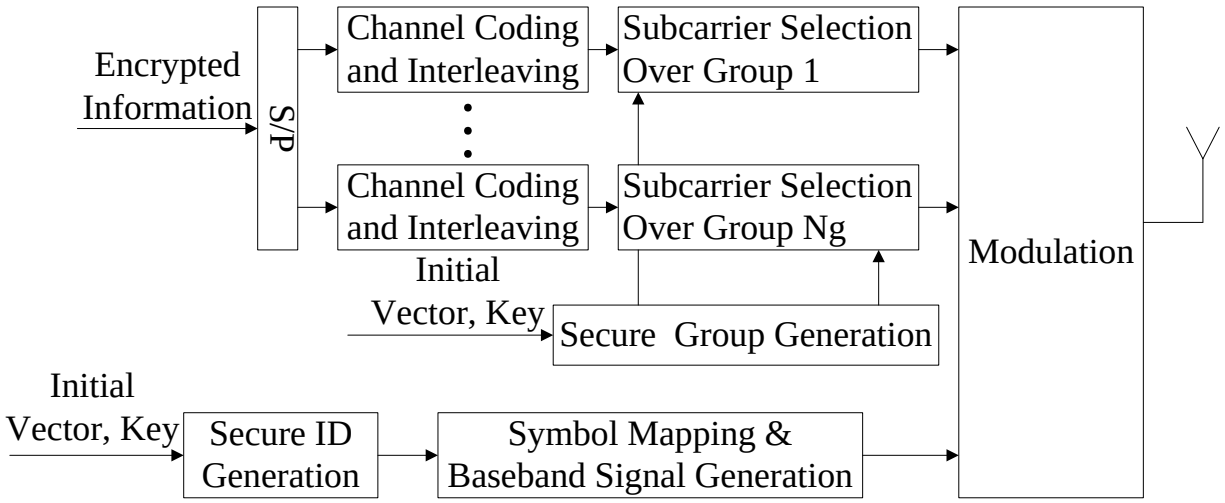
For more efficient spectrum usage and more robust jamming resistance, in this section, we extend the concept of MDFH to multi-carrier AJ-MDFH (MC-AJ-MDFH). The transmitter and the receiver structure of the MC-AJ-MDFH system are illustrated in Figure 3.6. The idea is to split all the N_c channels into N_g non-overlapping groups, and each subcarrier hops within the assigned group based on the AJ-MDFH scheme. To ensure hopping randomness of all the subcarriers, the groups need to be reorganized or regenerated securely after a pre-specified period, named group period. In the following, we will first describe the secure group generation algorithm, and then discuss the design of MC-AJ-MDFH with and without additional frequency diversity.

3.5.1 Secure Group Generation

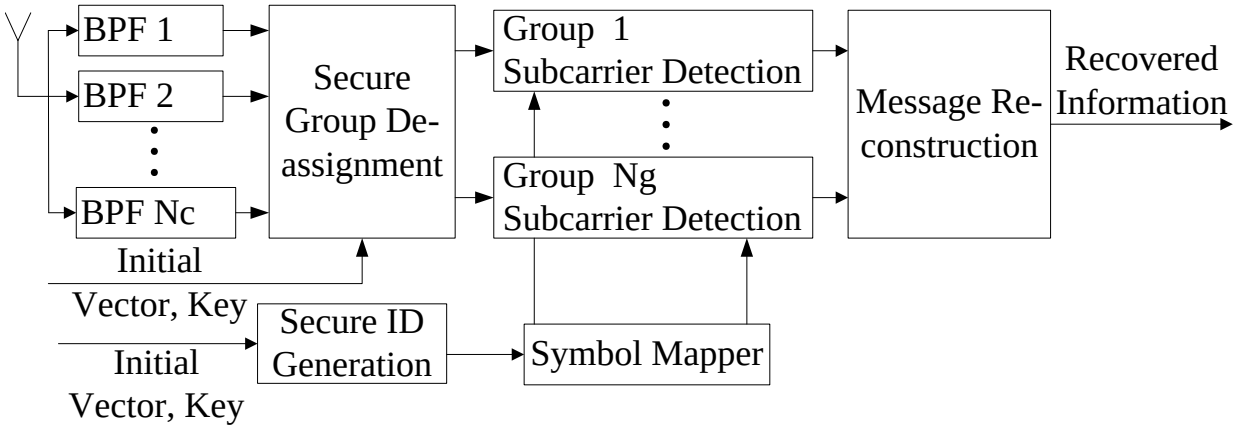
In this section, we propose a secure group generation algorithm to ensure that: (i) Each subcarrier hops over a new group of channels during each group period, so that it eventually hops over all the available channels in a pseudo-random manner; (ii) Only the legitimate receiver can recover the transmitted information correctly. Secure group generation is synchronized at the transmitter and the receiver. At the receiver, the received signal is fed to a bank of single-carrier AJ-MDFH receivers for signal extraction and recovery.

Recall that we assume there are a total of N_c available channels and there are N_g subcarriers in the system. For $l = 0, \cdots, N_g - 1$, the number of channels assigned to subcarrier i is denoted as N_g^i. As different subcarriers transmit over non-overlapping set of channels and we have $\sum_{i=0}^{N_g} N_g^i = N_c$.

For secure group generation, first, generate a pseudo-random binary sequence using a 32-bit linear feedback shift register (LFSR) as in Section 3.3, which is initialized by a secret sequence shared between the transmitter and the receiver. Encrypt the generated sequence into a ciphertext using the AES algorithm and a secure key. Pick an integer $L \in [\frac{N_c}{2}, N_c]$



(a) Transmitter structure



(b) Receiver structure

Figure 3.6: Transmitter and receiver structure of MC-AJ-MDFH.

and let $q = L \log_2 N_c = LB_c$. Take q bits from the ciphertext and put them as a q-bit vector $\mathbf{e} = [e_1, e_2, \cdots, e_q]$.

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

$$\mathbf{p_k} = [e_{(k-1)*B_c+1}, e_{(k-1)*B_c+2}, \cdots, e_{(k-1)*B_c+B_c}], \tag{3.23}$$

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

For $k = 1, 2, \cdots, L$, denote P_k as the decimal number corresponding to $\mathbf{p_k}$. And denote $P = [P_1, P_2, \cdots, P_L]$ as the permutation index vector. For $k = 0, 1, 2, \cdots, L$, denote $I_k =$

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

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

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

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

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

4. Vector F_L is used to assign the channels to N_g groups. We assign channels $\{f_{I_L(0)}, f_{I_L(1)}, \cdots, f_{I_L(N_g^0-1)}\}$ to the first group; Assign $\{f_{I_L(N_g^0)}, f_{I_L(N_g^0+1)}, \cdots, f_{I_L(N_g^0+N_g^1-1)}\}$ to the second group, and so on.

Because each frequency index appears in F_L once and only once, the proposed algorithm ensures that all the subcarriers are transmitting on non-overlapping sets of channels. In the following, we illustrate the secure group generation algorithm though a simple example.

Example: Assume the total number of available channels is $N_c = 8$, to be equally divided among $N_g = 2$ subcarriers; the permutation index vector $P = [4, 7, 4, 0]$, and the initial index vector $I_0 = [0, 1, 2, 3, 4, 5, 6, 7]$, as shown in Figure 3.7. Note that, the initial index vector I_0 can contain any random permutation of the sequence $\{0, 1, \cdots, N_c-1\}$, and $L \in [\frac{N_c}{2}, N_c]$. In this example, we choose $L = \frac{N_c}{2}$.

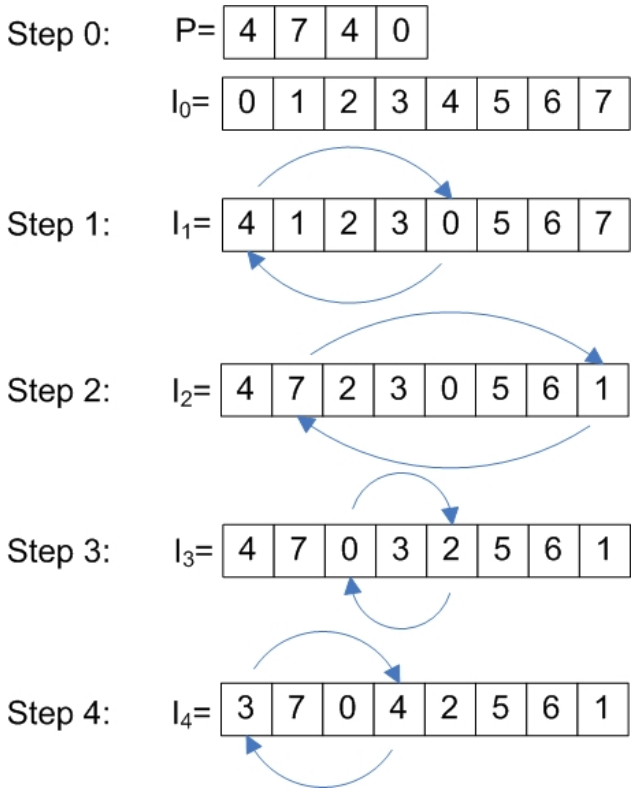


Figure 3.7: Example of the Secure Permutation Algorithm for $N_c = 8$ channels and $N_g = 2$ subcarriers.

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

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

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

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

3.5.2 Multi-Carrier AJ-MDFH without Diversity

In this case, each subcarrier transmits independent bit stream. The spectral efficiency of the AJ-MDFH system can be increased significantly. Let $B_c = \log_2 N_c$ and $B_g = \log_2 N_g$,

then the number of bits transmitted by the MC-AJ-MDFH within each hopping period is $B_{MC} = (B_c - B_g)N_g = (B_c - \log_2 N_g)N_g$. B_{MC} is maximized when $B_g = B_c - 1$ or $B_g = B_c - 2$, which results in $B_{MC} = 2^{B_c - 1}$. Note that the number of bits transmitted by the AJ-MDFH within each hopping period is B_c, it can be seen that $B_{MC} > B_c$ as long as $B_c > 2$. Take $N_c = 256$ for example, then the transmission efficiency of AJ-MDFH can be increased by $\frac{B_{MC}}{B_c} = \frac{2^{B_c - 1}}{B_c} = 16$ times.

We assume that jamming is random and equally distributed among all the groups. Then the overall carrier detection error probability P_e of MC-AJ-MDFH is equal to that corresponding to each subcarrier f_k for $k = 1, \cdots, N_g$. Let $P_{e,k}$ denote the carrier detection error probability corresponding to the kth subcarrier or the kth group, then we have $P_e = P_{e,k}$, and

$$\begin{aligned} P_{e,k} &= P_{0,k} \cdot P\{\text{incorrect carrier detection}|\text{signal not jammed}\} \\ &+ P_{1,k} \cdot P\{\text{incorrect carrier detection}|\text{signal jammed}\}, \end{aligned} \tag{3.24}$$

where $P_{0,k}, P_{1,k}$ denote the probability that the kth subcarrier is jamming-free or jammed, respectively.

3.5.3 Multi-carrier AJ-MDFH with Diversity

Under the multi-band jamming, diversity needs to be introduced to the AJ-MDFH system for robust jamming resistance especially. A natural solution to achieve frequency diversity is to transmit the same or correlated information through multiple subcarriers. The number of subcarriers needed to convey the same information differs in different jamming scenarios. Ideally, the number of correlated signal subcarriers should not be less than the number of jammed bands.

At the receiver, the received signals from different diversity branches are often combined for joint signal detection. To achieve better performance, appropriate diversity combination schemes need to be selected for different metrics used. In [84], the product combination

scheme was used for the square-law metrics. In [85, 86], the equal gain combination scheme was used for the normalized square-law metrics. If metric Z_i (see eq. (3.13)) is used for MC-AJ-MDFH, we propose to use the equal gain combination scheme, since Z_i can also be regarded as a normalized square-law metric.

Assume that the same information is transmitted through the hopping frequency index of N_d subcarriers over N_d groups $\{G_{n_1}, G_{n_2}, \ldots, G_{n_{N_d}}\}$ simultaneously, each group has the same number of channels, denoted as N_{gc}. Note that the secure group generation algorithm ensures that the channel index in each group is random and does not necessarily come in ascending or descending order. Let $Z_i^{n_l}$ denote the likelihood ratio of ith channel in group G_{n_l}, then the active hopping frequency index can be estimated as

$$\hat{k} = \arg \max_{1 \le i \le N_{gc}} \sum_{l=1}^{N_d} Z_i^{n_l}, \tag{3.25}$$

The diversity order N_d can be dynamic in different jamming scenarios to achieve tradeoff between performance and efficiency.

Overall, as demonstrated in Section 3.7, MC-AJ-MDFH can increase the system efficiency and jamming resistance significantly through jamming randomization and frequency diversity. Moreover, by assigning different carrier groups to different users, MC-AJ-MDFH can also be used as a collision-free multiple access system.

3.6 Spectral Efficiency Analysis

The spectral efficiency ν is defined as the ratio of the information bit rate R_b to the transmission bandwidth W_t, i.e., $\nu = \dfrac{R_b}{W_t}$. In this section, we will analyze and compare the spectral efficiency of the existing and proposed frequency hopping schemes, including conventional FH, MDFH and (MC-)AJ-MDFH.

We start with the *single-user case*. That is, no multiple access interference needs to be considered. Recall that T_s and T_h denotes the symbol period and the hopping duration, respectively; $N_h = T_s/T_h$ is the number of hops per symbol period. For fair comparison,

we assume that all systems have: (i) The same number of available channels N_c; (ii) The same hopping period T_h to ensure the hopping channels have the same bandwidth $W_c = 2/T_h$; (iii) The same frequency spacing Δf between two adjacent subcarriers, where $\Delta f \geq 1/T_h$ is chosen to avoid inter-carrier interference. Note that under these assumptions, all systems have the same total bandwidth $W_t = (N_c - 1)\Delta f + W_c$. For conventional FH using MFSK modulation, $\log_2 M$ bits are transmitted during each symbol period. The bit rate of conventional FH can be calculated as $R_b = \dfrac{\log_2 M}{T_s} = \dfrac{\log_2 M}{T_h N_h}$, and the corresponding spectral efficiency can be obtained as $\nu = \dfrac{R_b}{W_t} = \dfrac{\log_2 M}{T_h N_h W_t}$. The bit rate and spectral efficiency of other frequency hopping schemes can be obtained similarly. The results are listed in table 3.1. An illustration of the spectral efficiency comparison in the single-user case can be found in Section 3.7.

Table 3.1: The bit rate and spectral efficiency comparison in the single-user case

	conventional FH	MDFH	AJ-MDFH	MC-AJ-MDFH
R_b (b/s)	$\dfrac{\log_2 M}{T_h N_h}$	$\dfrac{N_h B_c + B_s}{N_h T_h}$	$\dfrac{B_c}{T_h}$	$\dfrac{(B_c - \log_2 N_g)N_g}{T_h}$
ν $(b/s/Hz)$	$\dfrac{\log_2 M}{T_h N_h W_t}$	$\dfrac{N_h B_c + B_s}{T_h N_h W_t}$	$\dfrac{B_c}{T_h W_t}$	$\dfrac{(B_c - \log_2 N_g)N_g}{T_h W_t}$

Next, we consider the more general *multiuser case*. The multiple access scheme for conventional FH, namely FHMA, was proposed in [66]. The multiple access extension of MDFH, denoted as E-MDFH, has been analyzed in [49]. Due to the variability in multiple access system design, a closed-form expression of the spectral efficiency is hard to obtain. Here we compare the total information bits allowed to be transmitted by each system under the same BER and bandwidth requirements, and illustrate the spectral efficiency comparison through the following example.

Let N_u denote the number of users and we choose the number of channels be $N_c = 64$ (i.e.,$B_c = 6$). For MC-AJ-MDFH, we choose $N_g = N_u = 4$; For E-MDFH, we choose 8-PSK to modulate $B_s = 3$ ordinary bits and $N_g = N_u = 4, N_h = 3$. For FHMA, we choose 64-FSK modulation, $N_h = 3$ and consider $N_u = 2, \cdots, 4$, respectively. The required BER is

10^{-4}. Figure 3.8 and Figure 3.9 depict the performance of these multiuser systems. From Figure 3.8, it can be seen that MC-AJ-MDFH and E-MDFH achieve the desired BER at $\frac{E_b}{N_0} \approx 6.5$dB and $\frac{E_b}{N_0} \approx 6.4$dB, respectively. From Firgure 3.9, it can be observed that: due to severe collision effect among different users, FHMA can only accommodate up to 2 users at $\frac{E_b}{N_0} \approx 6.5$dB for the desired BER. In this particular example, the spectral efficiency of both MC-AJ-MDFH and E-MDFH are approximately 4 times and 5 times that of FHMA.

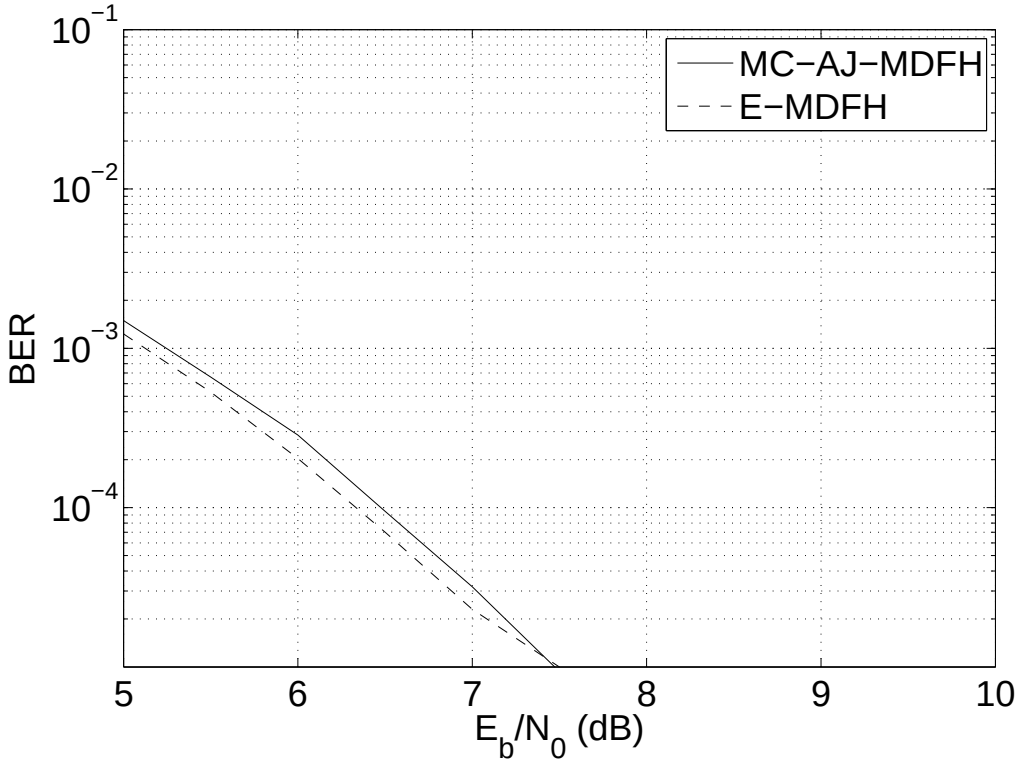


Figure 3.8: Performance of MC-AJ-MDFH and E-MDFH in multiuser case.

Based on our analysis above, as well as the performance analysis of AJ-MDFH under various jamming attacks in Section 3.7, it will be shown that: while AJ-MDFH is much more robust than MDFH under various jamming attacks, it can achieve a spectral efficiency that is very close to MDFH, which is several times higher than that of conventional FH. A comprehensive capacity analysis for MDFH and AJ-MDFH under disguised jamming is provided in Chapter 4.

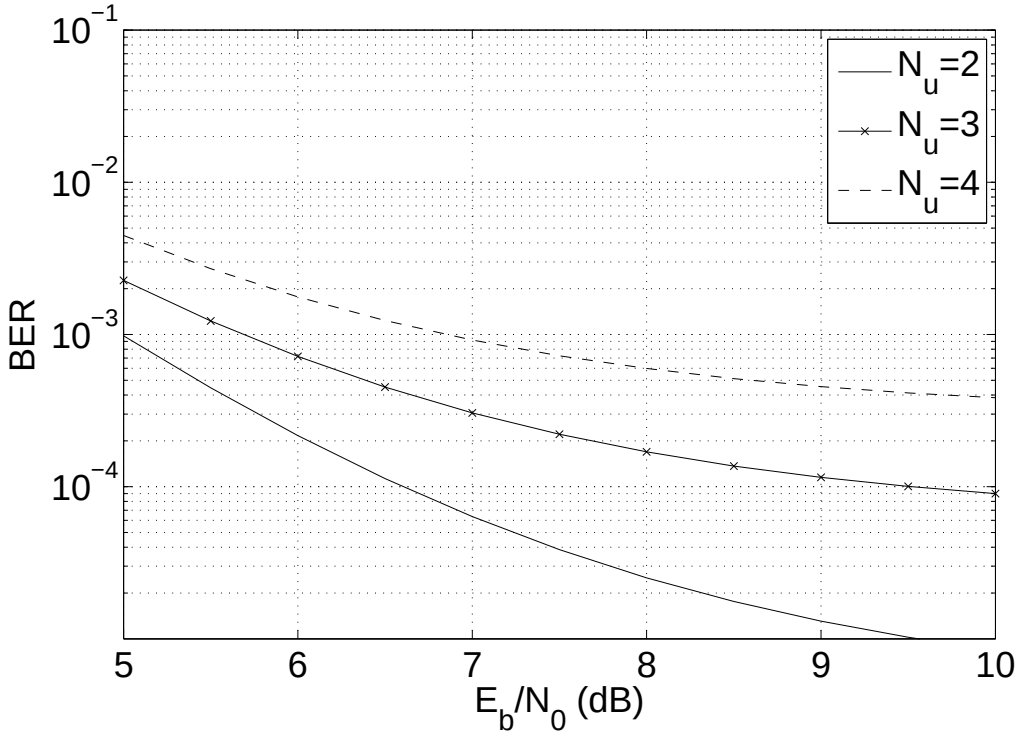


Figure 3.9: Performance of FHMA in multiuser case.

3.7 Simulation Results

In this section, simulation examples are provided to illustrate the performances of the proposed AJ-MDFH and MC-AJ-MDFH schemes under various jamming scenarios. For all the systems considered in the following examples, we assume the total number of available channels is $N_c = 64$, that is, $B_c = 6$.

Example 1: Impact of the ID constellation size In this example, we consider the impact of the ID constellation size on the BER performance of AJ-MDFH under single-band ID jamming. From Figure 3.10, it can be seen that in the ideal case where the system is noise free, the BER performance of AJ-MDFH improves continuously as the constellation size increases. However, when noise is present, the BER converges once the constellation size reaches a certain threshold M_t. For example, for $E_b/N_0 = 15$dB, we can choose $M_t = 36$. This example demonstrates the theoretical result in Theorem 1. In the following examples,

we choose $E_b/N_0 = 10$dB and use 32-PSK to modulate ID signal for AJ-MDFH and MC-AJ-MDFH.

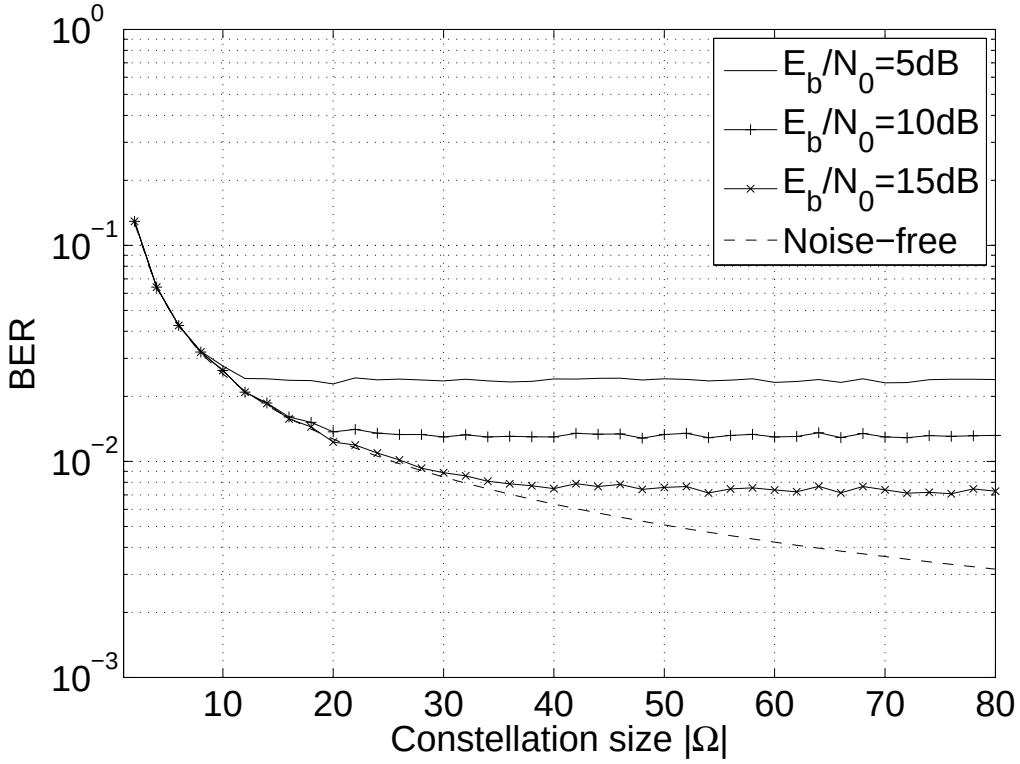


Figure 3.10: Example 1: The performance of AJ-MDFH with different constellation size, under single-band ID jamming.

Example 2: Performance comparison under single band jamming In this example, we consider both noise jamming and disguised jamming. SNR is taken as $E_b/N_0 = 10$dB and Jamming-to-Signal Ratio (JSR) is defined as the ratio of the jamming power to signal powers during one hop period. For conventional FH, 4-FSK modulation scheme is used and we assume that the adjacent frequency tones in 4-FSK correspond to the center frequencies of the adjacent MDFH channels. For MDFH, QPSK is used to modulate ordinary bits and the number of hops per symbol period is $N_h = 3$. From Figure 3.11, it can be observed that AJ-MDFH can effectively reduce the performance degradation caused by disguised jamming, while remaining robust under noise jamming. Note that JSR=0dB under disguised jamming corresponds to the ID jamming for AJ-MDFH. It can also be seen that the performance of

AJ-MDFH improves significantly when the jamming power differs from the signal power. This implies that uncertainty in the signal power is another dimension in combating ID jamming.

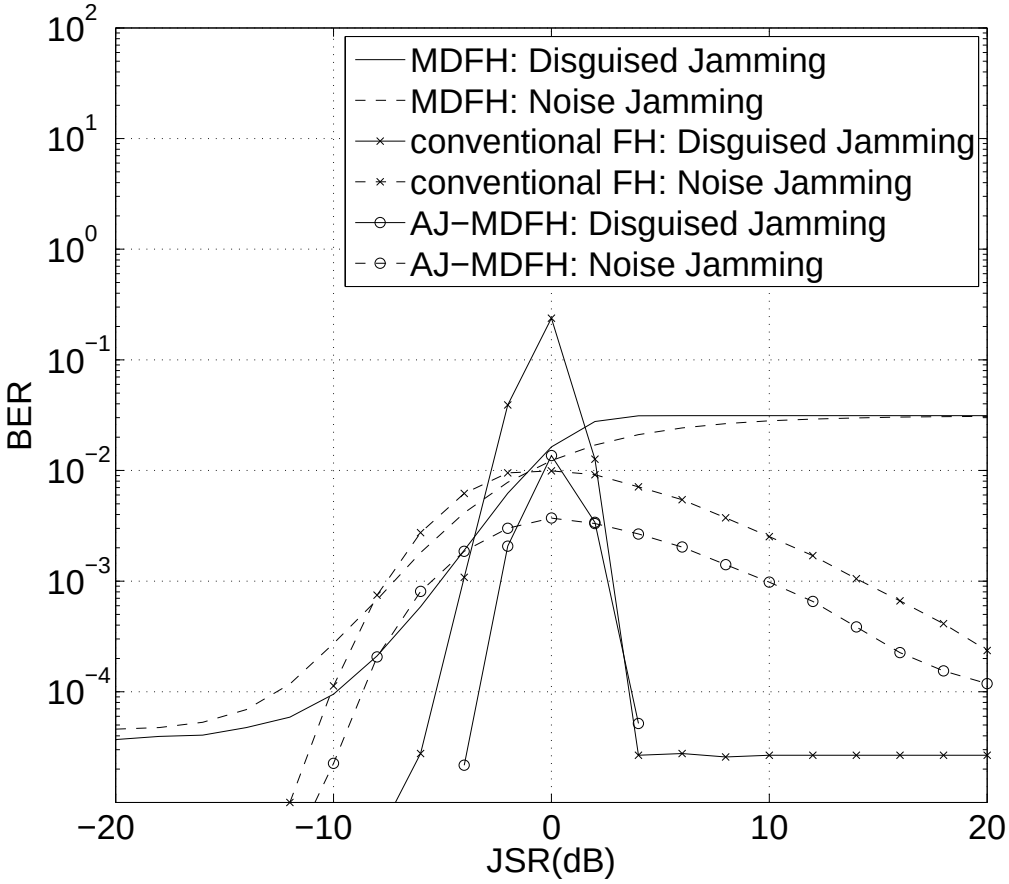


Figure 3.11: Example 2: Performance comparison under single band jamming.

Example 3: Performance comparison under multi-band disguised jamming In this example, $E_b/N_0 = 10$dB. For multi-band disguised jamming, the jammed bands are independently and randomly selected, and the jammer takes symbols randomly from the same constellation as the ID signal. For MC-AJ-MDFH without diversity, the channels are divided into 32 groups to maximize the spectral efficiency; for MC-AJ-MDFH with diversity, each symbol is transmitted simultaneously over 4 subcarriers to achieve frequency diversity. The equal gain combination scheme is adopted for the joint detection metric at the receiver.

From Figure 3.12, it can be seen that MC-AJ-MDFH delivers much better performance than AJ-MDFH under multi-band disguised jamming.

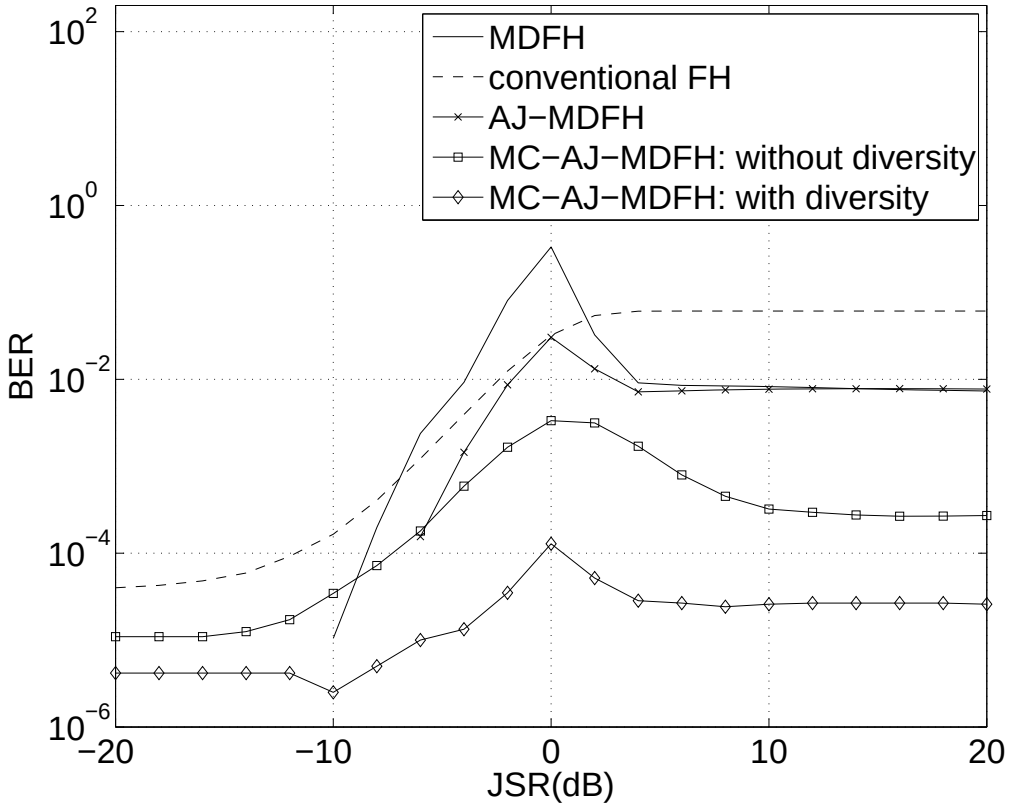


Figure 3.12: Example 3: Performance comparison under 2-band disguised jamming.

3.8 Summary

In this chapter, we proposed a highly efficient anti-jamming scheme, AJ-MDFH, based on the message-driven frequency hopping technique. It was shown that by inserting a secure ID sequence in transmission, AJ-MDFH can effectively reduce the performance degradation caused by disguised jamming, while being robust under strong jamming. The impact of ID constellation design on system performance was investigated under both noise jamming and ID jamming. It was proved that for a given power constraint, constant modulus constellation

delivers the best results under noise jamming in terms of detection error probability; While under ID jamming, when noise is present, the detection error probability converges as the constellation size goes to infinity. Moreover, AJ-MDFH can be extended to MC-AJ-MDFH by allowing simultaneous multi-carrier transmission. With jamming randomization and enriched frequency diversity, MC-AJ-MDFH can increase the system efficiency and jamming resistance significantly, and can readily be used as a collision-free multiple access scheme.

3.9 Proofs of Chapter 3

3.9.1 Proof of Proposition 1

It follows from (3.17) that

$$\begin{aligned} P_e &= 1 - \frac{1}{|\Omega|}\sum_{s\in\Omega}\int_0^\infty \prod_{l=2}^{N_c} Q_1\left(\frac{\sqrt{2}}{\sigma_l}\|s\|, \sqrt{2}z_1\right) p_{Z_1}(z_1)dz_1 \\ &\leq 1 - \frac{1}{|\Omega|}\sum_{s\in\Omega}\int_0^\infty Q_1^{N_c-1}\left(\frac{\sqrt{2}}{\sigma_m}\|s\|, \sqrt{2}z_1\right) p_{Z_1}(z_1)dz_1 \end{aligned} \tag{3.26}$$

where $m = \arg\max_{2\leq l\leq N_c}\{\sigma_l^2\}$. The inequality follows from the fact that for fixed $\|s\|$ and z_1, $Q_1\left(\frac{\sqrt{2}}{\sigma_l}\|s\|, \sqrt{2}z_1\right)$ is a monotonically decreasing function with respect to σ_l. The equality can be achieved when $\sigma_2 = \cdots = \sigma_{N_c}$.

Assume $N_c \geq 2$. For $N_c = 2$, it is easy to show that $P_e = P_e^U$ with $\sigma_m = \sigma_2$. Note that for fixed s and σ_m, $Q_1\left(\frac{\sqrt{2}}{\sigma_m}\|s\|, \sqrt{2}z_1\right) = Pr\{Z_m > z_1|s, z_1 = Z_1\}$ is a function of z_1. And for $N_c > 2$, $f(x) = x^{N_c-1}$ is convex when $x > 0$. By Jensen's inequality, we obtain

$$\begin{aligned} \int_0^\infty Q_1^{N_c-1}\left(\frac{\sqrt{2}}{\sigma_m}\|s\|, \sqrt{2}z_1\right) p_{Z_1}(z_1)dz_1 &\geq \left[\int_0^\infty Pr\{Z_m > z_1|s, Z_1 = z_1\}p_{Z_1}(z_1)dz_1\right]^{N_c-1} \\ &= \left[Pr\{Z_1 < Z_m|s\}\right]^{N_c-1}. \end{aligned} \tag{3.27}$$

According to [87], $Pr\{Z_1 < Z_m|s\}$ can be calculated as

$$Pr\{Z_1 < Z_m|s\} = 1 - \frac{\sigma_1^2}{\|s\|^2 + 2\sigma_1^2} e^{-\frac{\|s\|^2(\|s\|^2+\sigma_1^2)}{\sigma_m^2(\|s\|^2+2\sigma_1^2)}}. \tag{3.28}$$

Following (3.26)-(3.28),

$$P_e \leq \frac{1}{|\Omega|}\sum_{s\in\Omega}\left[1-\left(1-\frac{\sigma_1^2}{\|s\|^2+2\sigma_1^2}e^{-\frac{\|s\|^2(\|s\|^2+\sigma_1^2)}{\sigma_m^2(\|s\|^2+2\sigma_1^2)}}\right)^{N_c-1}\right] = P_e^U \quad \text{for} \quad N_c > 2. \quad (3.29)$$

Overall, $P_e \leq P_e^U$ for $N_c \geq 2$. □

3.9.2 Proof of Theorem 1

Note that the system is under ID attack. If the power of the M-ary PSK constellation is P_s, then the signal and jamming symbol can be written as $s = \sqrt{P_s}e^{j\frac{2\pi m_s}{M}}, J_j = \sqrt{P_s}e^{j\frac{2\pi m_J}{M}}$ respectively, where $M = |\Omega|$ and $0 \leq m_s, m_J \leq M-1$. Without loss of generality, we assume that: (i) Both the ID and jamming take the symbols in Ω with equal probability $1/M$; (ii) The signal is transmitted in channel 1 ($\alpha_1 = 1$) and channel j is jammed ($\beta_j = 1$). We consider the following two scenarios:

(i) When $j = 1$, jamming collides with the ID signal. In this case, $r_1 = s + J_1 + n_1$ and $r_l = n_l$ for $l = 2, \ldots, N_c$. We have $Z_1 = \frac{\|J_1 + n_1\|}{\sqrt{\|s+J_1\|^2+\sigma_n^2}}$ and $Z_l = \frac{\|n_l - s\|}{\sigma_n}$, where σ_n^2 is the noise variance. The detection error probability in this case can be calculated as

$$P_{e1} = 1 - \frac{1}{M^2}\sum_{s\in\Omega}\sum_{J_1\in\Omega}\int_0^\infty [Pr\{z_1 < Z_2|s, J_1, z_1\}]^{N_c-1} p_{Z_1}(z_1)dz_1. \quad (3.30)$$

Note that Z_1 is a Rician random variable with PDF $p_{Z_1}(z_1) = \frac{z_1}{\sigma^2}e^{-\frac{z_1^2+\nu^2}{2\sigma^2}} I_0\left(\frac{z_1\nu}{\sigma^2}\right)$, where $\nu = \frac{\sqrt{P_s}}{\sqrt{\|s+J_1\|^2+\sigma_n^2}}$, $\sigma^2 = \frac{\sigma_n^2}{2(\|s+J_1\|^2+\sigma_n^2)}$ and Z_l's are i.i.d. Rician random variables with $\nu = \frac{\sqrt{P_s}}{\sigma_n}$, $\sigma^2 = \frac{1}{2}$. Then (3.30) can be further written as

$$\begin{aligned} P_{e1} &= 1 - \frac{1}{|\Omega|^2}\sum_{s\in\Omega}\sum_{J_1\in\Omega}\int_0^\infty Q_1^{N_c-1}\left(\frac{\sqrt{2P_s}}{\sigma_n}, \sqrt{2}z_1\right) 2z_1\frac{\|s+J_1\|^2+\sigma_n^2}{\sigma_n^2} \\ &\quad \cdot e^{-\frac{(\|s+J_1\|^2+\sigma_n^2)z_1^2+P_s}{\sigma_n^2}} I_0\left(\frac{2z_1}{\sigma_n^2}\sqrt{P_s(\|s+J_1\|^2+\sigma_n^2)}\right) dz_1. \end{aligned} \quad (3.31)$$

For M-PSK constellation with power P_s, $\|s+J_1\|^2$ can be rewritten as

$$\begin{aligned}\|s+J_1\|^2 &= P_s\left\|\cos\frac{2\pi m_s}{M}+\cos\frac{2\pi m_J}{M}+j(\sin\frac{2\pi m_s}{M}+\sin\frac{2\pi m_J}{M})\right\|^2\\ &= 4P_s\left\|\cos\frac{\pi(m_s+m_J)}{M}\cos\frac{\pi(m_s-m_J)}{M}+j\sin\frac{\pi(m_s+m_J)}{M}\cos\frac{\pi(m_s-m_J)}{M}\right\|^2\\ &= 4P_s\cos^2\frac{\pi(m_s-m_J)}{M}\\ &= 2P_s\left[1+\cos\frac{2\pi(m_s-m_J)}{M}\right] \qquad (3.32)\end{aligned}$$

Define $\kappa \triangleq (m_s-m_J) \mod M$, which is uniformly distributed over $[0,M-1]$, then $\|s+J_1\|^2 = 2P_s(1+\cos\frac{2\pi\kappa}{M})$ and

$$\begin{aligned}P_{e1} &= 1-\frac{1}{M}\sum_{\kappa=0}^{M-1}\int_0^\infty Q_1^{N_c-1}\left(\frac{\sqrt{2P_s}}{\sigma_n},\sqrt{2}z_1\right)2z_1\left[\frac{2P_s}{\sigma_n^2}\left(1+\cos\frac{2\pi\kappa}{M}\right)+1\right]\\ &\quad\cdot e^{-\left[\frac{2P_s}{\sigma_n^2}\left(1+\cos\frac{2\pi\kappa}{M}\right)+1\right]z_1^2-\frac{P_s}{\sigma_n^2}}I_0\left(\frac{2z_1}{\sigma_n^2}\sqrt{2P_s^2\left(1+\cos\frac{2\pi\kappa}{M}\right)+P_s\sigma_n^2}\right)dz_1 \qquad (3.33)\end{aligned}$$

(ii) When $j=2,\ldots,N_c$, jamming does not collide with ID signal. In this case, $r_1=s+n_1$, $r_j=J_j+n_j$ and $r_l=n_l$. We have $Z_1=\frac{\|n_1\|}{\sqrt{P_s+\sigma_n^2}}$, $Z_j=\frac{\|J_j-s+n_j\|}{\sqrt{P_s+\sigma_n^2}}$ and $Z_l=\frac{\|n_l-s\|}{\sigma_n}$ for $l=2,\ldots,N_c, l\neq j$. The detection error probability in this case can be calculated as

$$P_{e2}=1-\frac{1}{|\Omega|^2}\sum_{s\in\Omega}\sum_{J_j\in\Omega}\int_0^\infty Pr\{Z_j>z_1|s,J_j,z_1\}[Pr\{Z_l>z_1|s,z_1\}]^{N_c-2}p_{Z_1}(z_1)dz_1. \qquad (3.34)$$

Note that Z_1 is a Rayleigh random variable with PDF $p_{Z_1}(z_1)=\frac{z_1}{\sigma^2}e^{-\frac{z_1^2}{2\sigma^2}}$, where $\sigma^2=\frac{\sigma_n^2}{2(P_s+\sigma_n^2)}$, Z_j is a Rician random variable with $\nu=\frac{\|J_j-s\|}{\sqrt{P_s+\sigma_n^2}}$, $\sigma^2=\frac{\sigma_n^2}{2(P_s+\sigma_n^2)}$ and Z_l's are i.i.d. Rician random variables with $\nu=\frac{\sqrt{P_s}}{\sigma_n}$, $\sigma^2=\frac{1}{2}$. Following similar derivation as

in (3.32), we have $\|J_j - s\|^2 = 2P_s(1-\cos\frac{2\pi\kappa}{M})$ and (3.34) can be further written as

$$\begin{aligned}
P_{e2} &= 1 - \frac{1}{|\Omega|^2}\sum_{s\in\Omega}\sum_{J_1\in\Omega}\int_0^\infty Q_1\left(\frac{\sqrt{2}}{\sigma_n}\|J_j - s\|, \frac{\sqrt{2(P_s+\sigma_n^2)}}{\sigma_n}z_1\right) \\
&\quad \cdot Q_1^{N_c-2}\left(\frac{\sqrt{2P_s}}{\sigma_n}, \sqrt{2}z_1\right)\frac{2(P_s+\sigma_n^2)}{\sigma_n^2}z_1 e^{-\frac{P_s+\sigma_n^2}{\sigma_n^2}z_1^2}dz_1 \\
&= 1 - \frac{1}{M}\sum_{\kappa=0}^{M-1}\int_0^\infty Q_1\left(\frac{2}{\sigma_n}\sqrt{P_s\left(1-\cos\frac{2\pi\kappa}{M}\right)}, \frac{1}{\sigma_n}\sqrt{2(P_s+\sigma_n^2)}z_1\right) \\
&\quad \cdot Q_1^{N_c-2}\left(\frac{\sqrt{2P_s}}{\sigma_n}, \sqrt{2}z_1\right)\frac{2(P_s+\sigma_n^2)}{\sigma_n^2}z_1 e^{-\frac{P_s+\sigma_n^2}{\sigma_n^2}z_1^2}dz_1. \qquad (3.35)
\end{aligned}$$

The overall detection error probability in noisy environment is given as

$$P_e = Pr\{j=1\}P_{e1} + Pr\{2\le j\le N_c\}P_{e2} = \frac{1}{N_c}P_{e1} + \frac{N_c-1}{N_c}P_{e2}. \qquad (3.36)$$

When $\frac{P_s}{\sigma_n^2}$ is fixed, it follows from (3.33) and (3.35) that P_e is a function of M given as

$$P_e = \frac{1}{M}\sum_{\kappa=0}^{M-1} b\left(\frac{2\pi\kappa}{M}\right), \qquad (3.37)$$

where

$$\begin{aligned}
b(x) &= 1 - \frac{1}{N_c}\int_0^\infty Q_1^{N_c-1}\left(\frac{\sqrt{2P_s}}{\sigma_n}, \sqrt{2}z_1\right)2z_1\left[\frac{2P_s}{\sigma_n^2}(1+\cos x)+1\right] \\
&\quad \cdot e^{-\left[\frac{2P_s}{\sigma_n^2}(1+\cos x)+1\right]z_1^2 - \frac{P_s}{\sigma_n^2}} I_0\left(\frac{2z_1}{\sigma_n^2}\sqrt{2P_s^2(1+\cos x)+P_s\sigma_n^2}\right)dz_1 \\
&\quad -\frac{N_c-1}{N_c}\int_0^\infty Q_1\left(\frac{2}{\sigma_n}\sqrt{P_s(1-\cos x)}, \frac{1}{\sigma_n}\sqrt{2(P_s+\sigma_n^2)}z_1\right) \\
&\quad \cdot Q_1^{N_c-2}\left(\frac{\sqrt{2P_s}}{\sigma_n}, \sqrt{2}z_1\right)\frac{2(P_s+\sigma_n^2)}{\sigma_n^2}z_1 e^{-\frac{P_s+\sigma_n^2}{\sigma_n^2}z_1^2}dz_1. \qquad (3.38)
\end{aligned}$$

As M approaches infinity, P_e converges. In fact, we have,

$$\begin{aligned}
\bar{P_e} &= \lim_{M\to\infty} P_e = \lim_{M\to\infty}\sum_{\kappa=0}^{M-1}\frac{b\left(\frac{2\pi\kappa}{M}\right)\cdot\frac{2\pi}{M}}{M\cdot\frac{2\pi}{M}} \\
&= \frac{1}{2\pi}\lim_{M\to\infty}\sum_{\kappa=0}^{M-1} b\left(\frac{2\pi\kappa}{M}\right)\cdot\frac{2\pi}{M} \\
&= \frac{1}{2\pi}\int_0^{2\pi} b(x)dx. \qquad (3.39)
\end{aligned}$$

Note that $b(x)$ is the detection error probability with $0 \leq b(x) \leq 1$. We have

$$0 \leq \bar{P_e} = \frac{1}{2\pi} \int_0^{2\pi} b(x)dx \leq 1. \tag{3.40}$$

That is: $\forall \epsilon > 0$, there always exists an integer M_t such that $\forall M > M_t$, $|P_e - \bar{P_e}| < \epsilon$. $\square$

Chapter 4

CAPACITY ANALYSIS OF MDFH BASED SYSTEMS UNDER DISGUISED JAMMING

In Chapter 3, we point out that under disguised jamming, where the jammer mimics the signal of the legal user, MDFH experiences considerable performance losses like other wireless systems. To overcome this, we propose an anti-jamming MDFH scheme, which enhances the jamming resistance of MDFH by enabling shared randomness between the transmitter and receiver using an AES generated ID sequence transmitted along the information stream. In this chapter, we analyze the capacity of MDFH and AJ-MDFH under disguised jamming. We show that under the worst case disguised jamming, as long as the secure ID sequence is unavailable to the jammer (which is ensured by AES), the AVC corresponding to AJ-MDFH is nonsymmetrizable. This implies that the deterministic capacity of AJ-MDFH with respect to the average probability of error is positive. On the other hand, due to lack of shared randomness, the AVC corresponding to MDFH is symmetric, resulting in zero deterministic capacity. We further calculate the capacity of AJ-MDFH under the worst case disguised jamming, and show that it converges as the ID constellation size goes to infinity.

4.1 Introduction

The basic idea of MDFH is that part of the information message acts as the PN sequence for carrier frequency selection at the transmitter. Transmission through hopping frequency control adds another dimension to the signal space, and the resulted coding gain can increase the system spectral efficiency significantly. In Chapter 3, we pointed out that MDFH is sensitive to disguised jamming, where the jammer mimics the signal of the legal user. Performance losses occur since it is difficult for the MDFH receiver to distinguish the disguised jamming from the signal. To overcome this limitation, we proposed the anti-jamming

MDFH (AJ-MDFH) scheme. The idea is to insert some secure signal identification (ID) information during the transmission process. The ID information can be regenerated at the receiver based on the pre-shared secret, and then be used for signal detection and extraction.

We further explored ID constellation design and its impact on the performance of AJ-MDFH. It was observed that constant modulus constellation would result in minimum probability of error under noise jamming, as the signal power is always equal to the maximal signal power available. Under the worst case disguised jamming, in which the jamming tries to mimic the ID symbols of the legal user (referred to as ID jamming [88]), we showed that under the ideal case when the system is noise-free, increasing the ID constellation size can increase the ID uncertainty, and hence reduce the probability of error. In this case, the ideal constellation size is $M = \infty$. However, when noise is present, we proved that the detection error probability under ID jamming converges as M goes to infinity. This result justifies the use of practical, finite size constellations in AJ-MDFH.

In this chapter, we analyze the capacity of MDFH and AJ-MDFH under disguised jamming. Both MDFH and AJ-MDFH are modeled as arbitrarily varying channels (AVCs) [89, 90, 91, 53, 92, 93], which is characterized as

$$W : \mathcal{X} \times \mathcal{J} \to \mathcal{S}, \tag{4.1}$$

where $\mathcal{X}$ is the transmitted signal space, $\mathcal{J}$ is the jamming space and $\mathcal{S}$ is the estimated information space. For any $\mathbf{x} \in \mathcal{X}$, $\mathbf{J} \in \mathcal{J}$ and $\mathbf{s} \in \mathcal{S}$, $W(\mathbf{s}|\mathbf{x}, \mathbf{J})$ denotes the conditional probability that $\mathbf{s}$ is detected at the receiver, given that $\mathbf{x}$ is the transmitted signal and $\mathbf{J}$ is the jamming. If $\mathcal{J} = \mathcal{X}$ and $W(\mathbf{s}|\mathbf{x}, \mathbf{J}) = W(\mathbf{s}|\mathbf{J}, \mathbf{x})$ for any $\mathbf{x}, \mathbf{J} \in \mathcal{X}, \mathbf{s} \in \mathcal{S}$, the AVC is said to have a *symmetric kernel* [51]. Define $\hat{W} : \mathcal{X} \times \mathcal{X} \to \mathcal{S}$ by

$$\hat{W}(\mathbf{s}|\mathbf{x}, \mathbf{J}) \triangleq \sum_{\mathbf{y} \in \mathcal{Y}} \pi(\mathbf{y}|\mathbf{J}) W(\mathbf{s}|\mathbf{x}, \mathbf{y}), \tag{4.2}$$

where $\pi : \mathcal{X} \to \mathcal{Y}$ is a probability matrix, and $\mathcal{Y} \subseteq \mathcal{J}$. If there exists a π such that

$$\hat{W}(\mathbf{s}|\mathbf{x}, \mathbf{J}) = \hat{W}(\mathbf{s}|\mathbf{J}, \mathbf{x}), \quad \forall \mathbf{x}, \mathbf{J} \in \mathcal{X}, \ \forall \mathbf{s} \in \mathcal{S}, \tag{4.3}$$

then W is said to be symmetrizable. The deterministic code[1] capacity of the AVC for the average probability of error is positive iff the AVC is nonsymmetrizable [52, 51, 53, 92].

The main contributions of this chapter can be summarized as follows:

- Under the worst case disguised jamming, the AVC corresponding to MDFH has symmetric kernel. That is, the deterministic code capacity of MDFH under the worst case disguised jamming is zero.

- For AJ-MDFH, under the worst case disguised jamming - ID jamming, we prove that: as long as the ID sequence is unavailable to the jammer, the AVC corresponding to AJ-MDFH is *nonsymmetrizable*. Note that the secure ID in AJ-MDFH is generated using AES [76, 94], to symmetrize AJ-MDFH is equivalent to break AES, which is computationally infeasible in practical systems. That is, the AVC corresponding to AJ-MDFH is computationally infeasible to be symmetrized. This result ensures that AJ-MDFH has positive capacity under ID jamming.

- We derive the capacity of AJ-MDFH under ID jamming, for which the mutual information is maximized for all possible input probability distributions and minimized for all possible jamming distributions. We show that the capacity converges as the constellation size M goes to infinity. It is observed that: (i) Under reasonable SNR levels ($\geq$ 10dB), the capacity of AJ-MDFH under ID jamming is close to the jamming-free case, and it outperforms the conventional FH system by big margins; (ii) For AJ-MDFH, since the information bits are transmitted through hopping frequency control, it is very robust to additive noise.

This chapter is organized as follows. A brief system description for MDFH and AJ-MDFH is provided in Section 4.2. The capacity of MDFH under disguised jamming is analyzed in Section 4.3. In Section 4.4, the capacity of AJ-MDFH is analyzed and derived

[1] A deterministic (n, k) code means that each k-bit data word is mapped to a unique n-bit codeword.

under ID jamming. In Section 4.5, we extend the capacity analysis to the multiuser AJ-MDFH system (MC-AJ-MDFH). The numerical examples are provided in Section 4.8 and we conclude in Section 4.9.

4.2 System Description

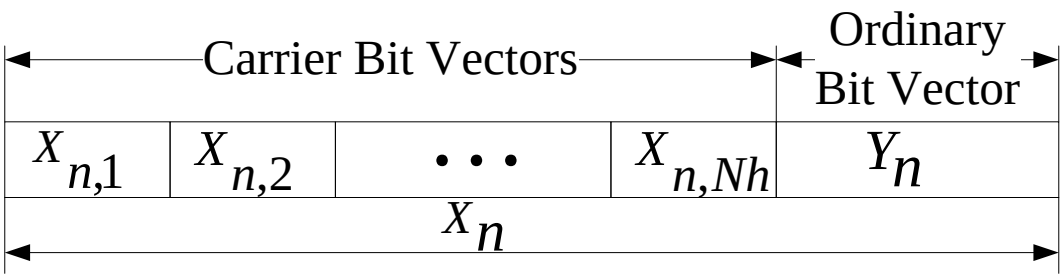
4.2.1 MDFH

The basic idea of MDFH is that part of the message acts as the PN sequence for carrier frequency selection at the transmitter. More specifically, selection of carrier frequencies is directly determined by the encrypted information stream rather than by a pre-selected pseudo-random sequence as in the conventional FH.

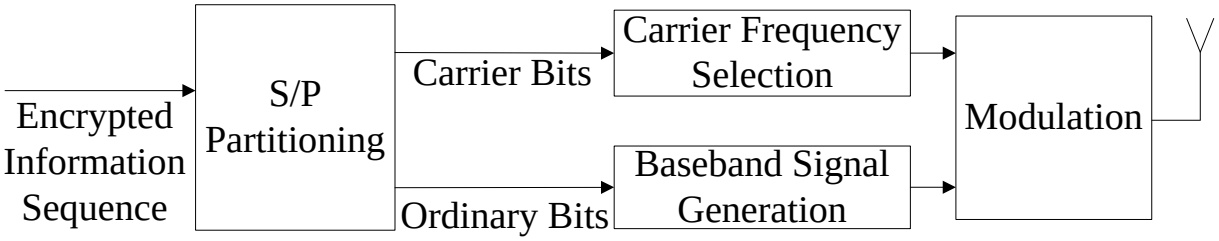
Let N_c be the total number of available channels, with $\{f_1, f_2, \cdots, f_{N_c}\}$ being the set of all available carrier frequencies. The number of bits required to specify an individual channel is $B_c = \lfloor \log_2 N_c \rfloor$, where $\lfloor x \rfloor$ denotes the largest integer less than or equal to x. Without loss of generality, we assume that $N_c = 2^{B_c}$. Let Ω be the selected constellation of size M, and denote $B_s = \log_2 M$ 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 $N_h = \dfrac{T_s}{T_h}$.

The transmitter structure of MDFH is shown in Figure4.1. The *encrypted* information stream is divided into blocks of length $L \triangleq N_h B_c + B_s$. Each block is parsed into $N_h B_c$ *carrier bits* and B_s *ordinary bits*. The carrier bits determine the hopping frequencies, and the ordinary bits are mapped to a symbol in Ω and transmitted through the channels identified by the carrier bits. The structure of the nth block, $X_n = [X_{n,1}, X_{n,2}, \cdots, X_{n,N_h}, Y_n]$, is shown in Figure 4.1a.

Let $f_{X_{n,l}}$ be the carrier frequency corresponding to $X_{n,l}$, $l \in \{1, \cdots, N_h\}$, s_n the symbol corresponding to ordinary bit vector Y_n, and $g(t)$ the pulse shaping filter. For the mth hopping period $[mT_h, (m+1)T_h]$ with $m = nN_h + l$, the transmitted signal can be represented



(a) Information block structure



(b) Transmitter

Figure 4.1: MDFH transmitter structure.

as

$$s(t) = \sqrt{2} Re \left\{ \sum_{i=1}^{N_c} \alpha_{i,m} s_n g(t - mT_h) e^{j2\pi f_i t} \right\}, \tag{4.4}$$

where $\alpha_{i,m} = 1$ if $f_{X_{n,l}} = f_i$, and $\alpha_{i,m} = 0$ otherwise.

Let $s(t)$, $J(t)$ and $n(t)$ denote the signal, the jamming interference and the noise, respectively. For AWGN channels, the received signal can be represented as

$$r(t) = s(t) + J(t) + n(t). \tag{4.5}$$

We assume that $s(t), J(t)$ and $n(t)$ are independent of each other. Feeding $r(t)$ into a bank of N_c bandpass filters, each centered at f_i $(i = 1, 2, \cdots, N_c)$, the output of the ith ideal bandpass filter $\mathrm{f}_i(t)$ is $r_i(t) = \mathrm{f}_i(t) * r(t)$. For demodulation, $r_i(t)$ is first shifted back to the baseband, and then passed through a matched filter. At the mth hopping period, for $i = 1, \cdots, N_c$, the sampled matched filter output corresponds to channel i can be expressed as

$$r_{i,m} = \alpha_{i,m} s_n + \beta_{i,m} J_{i,m} + n_{i,m}, \tag{4.6}$$

where $s_n, J_{i,m}$ and $n_{i,m}$ correspond to the signal symbol, the jamming interference and the noise, respectively; $\alpha_{i,m}, \beta_{i,m} \in \{0, 1\}$ are binary indicators for the presence of signal and jamming over channel i at the mth hopping period, respectively. Note that the user's information is carried in both $\alpha_{i,m}$ and s_n. For notation simplicity, without loss of generality, we omit the subscript m and n in (4.6). That is, for a particular hopping period, (4.6) is reduced to:

$$r_i = \alpha_i s + \beta_i J_i + n_i, \quad i = 1, \cdots, N_c. \tag{4.7}$$

The carrier bits and the ordinary bits can then be estimated from r_i [88].

4.2.2 AJ-MDFH

AJ-MDFH was proposed to improve the capacity of MDFH under disguised jamming by adding shared randomness between the transmitter and receiver. This is achieved by replacing the ordinary bits in MDFH with a secure identification (ID) information during the transmission process.

The system structure of AJ-MDFH is illustrated in Figure 4.2. Each user is assigned a secure ID sequence. For each hopping period, AJ-MDFH can also be characterized as

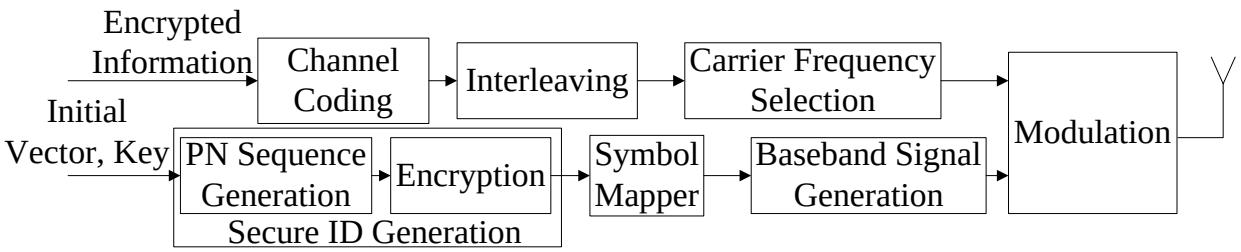
$$r_i = \alpha_i s + \beta_i J_i + n_i, \quad i = 1, \cdots, N_c, \tag{4.8}$$

except that s is now the ID symbol instead of the signal symbol. To prevent impersonate ID attack, the ID symbol is refreshed at each hopping period. For AJ-MDFH, the user's information is only carried in α_i. Recall that for AJ-MDFH, the ML receiver reduces to a normalized minimum distance receiver. Define $P_i = E\{\|r_i\|^2\}$, and

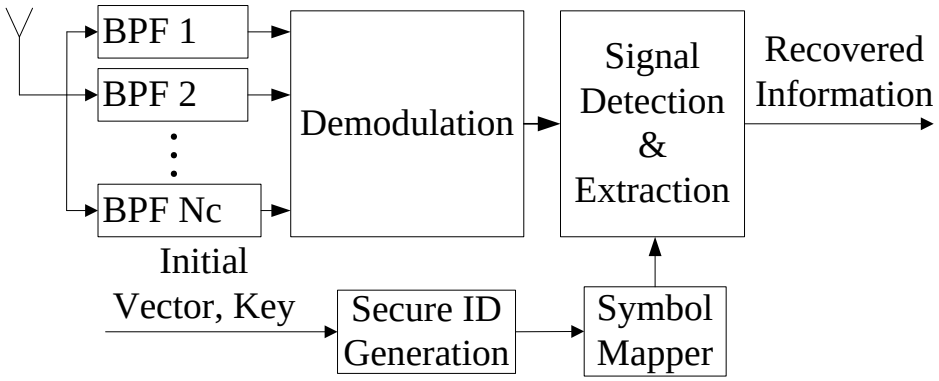
$$Z_i = \frac{\|r_i - s\|}{\sqrt{P_i}}. \tag{4.9}$$

Let $\mathcal{I}_c = \{1, \cdots, N_c\}$. Assuming $\alpha_i = \delta(k-i)$ for some $k \in \mathcal{I}_c$, at the receiver, k is estimated as

$$\hat{k} = \arg \min_{i \in \mathcal{I}_c} Z_i. \tag{4.10}$$



(a) Transmitter structure



(b) Receiver structure

Figure 4.2: Transmitter and receiver structure of AJ-MDFH.

For more efficient spectrum usage, the system can be extended to multi-carrier AJ-MDFH (MC-AJ-MDFH). The idea is to split all the N_c channels into N_g non-overlapping subgroups, and each carrier hops within the assigned subgroup based on the AJ-MDFH scheme [88].

4.3 Capacity of MDFH under Disguised Jamming

In this section, we will show that in MDFH, due to the fact that there is no shared secret between the transmitter and receiver, when the constellation Ω and the pulse shaping filter $g(t)$ are known to the jammer, the capacity of MDFH under worst case disguised jamming is actually zero.

Following (4.7), let $\mathbf{r} = (r_1, \ldots, r_{N_c})$, $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_{N_c})$, $\boldsymbol{\beta} = (\beta_1, \ldots, \beta_{N_c})$, $\mathbf{J}' = (J_1, \cdots, J_{N_c})$ and $\mathbf{n} = (n_1, \ldots, n_{N_c})$, the MDFH system under hostile jamming can be

modeled as:

$$\mathbf{r} = \boldsymbol{\alpha} s + \boldsymbol{\beta} \cdot \mathbf{J}' + \mathbf{n}. \tag{4.11}$$

Note that the information is contained in both $\boldsymbol{\alpha}$ and s. Define $\mathbf{x} = \boldsymbol{\alpha} s$, $\mathbf{J} = \boldsymbol{\beta} \cdot \mathbf{J}'$, then we have

$$\mathbf{r} = \mathbf{x} + \mathbf{J} + \mathbf{n}. \tag{4.12}$$

Let $\mathcal{A} = \{\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_{N_c}) | \alpha_i \text{ is 0 or 1, and } \sum_{i=1}^{N_c} \alpha_i = 1\}$. Define $\mathcal{X} = \{\boldsymbol{\alpha} s | \boldsymbol{\alpha} \in \mathcal{A}, s \in \Omega\}$ be the set of all possible information signal $\mathbf{x}$, and $\mathcal{J} = \{\mathbf{J} = (\beta_1 J_1, \cdots, \beta_{N_c} J_{N_c}) | J_i \in \Omega_J, \beta_i = 0, 1, i = 1, \cdots, N_c\}$ where Ω_J is the set of all possible jamming symbols. Let $\hat{\mathbf{x}}$ be the estimated version of $\mathbf{x}$ at the receiver, and $W_0(\hat{\mathbf{x}}|\mathbf{x}, \mathbf{J})$ the conditional probability that $\hat{\mathbf{x}}$ is estimated at the receiver given that the signal is $\mathbf{x}$, and the jamming is $\mathbf{J}$. The jammed MDFH system can be modeled as an arbitrarily varying channel (AVC) which is characterized by the probability matrix

$$W_0 : \mathcal{X} \times \mathcal{J} \to \mathcal{X}, \tag{4.13}$$

with

$$W_0(\hat{\mathbf{x}}|\mathbf{x}, \mathbf{J}) \geq 0, \qquad \hat{\mathbf{x}}, \mathbf{x} \in \mathcal{X}, \mathbf{J} \in \mathcal{J}, \tag{4.14}$$

$$\sum_{\hat{\mathbf{x}} \in \mathcal{X}} W_0(\hat{\mathbf{x}}|\mathbf{x}, \mathbf{J}) = 1, \quad \forall \mathbf{x} \in \mathcal{X}, \forall \mathbf{J} \in \mathcal{J}. \tag{4.15}$$

W_0 is called the kernel of the AVC.

Under the worst case single band disguised jamming,

$$\mathcal{J} = \{\boldsymbol{\beta} b | \boldsymbol{\beta} \in \mathcal{A}, b \in \Omega\} = \mathcal{X}. \tag{4.16}$$

That is, the jamming and the information signal are fully symmetric. Note that in MDFH, no shared randomness is exploited for signal detection at the receiver, the recovery of $\mathbf{x}$ is fully based on $\mathbf{r}$. Hence, we further have

$$W_0(\hat{\mathbf{x}}|\mathbf{x}, \mathbf{J}) = W_0(\hat{\mathbf{x}}|\mathbf{J}, \mathbf{x}). \tag{4.17}$$

This implies that the kernel of the AVC corresponding to MDFH, W_0, is symmetric.

In [92], it has been proved that the deterministic capacity (i.e., the largest rate achieved with deterministic codes) of an AVC with symmetric kernel is zero. Therefore, we have the result below.

Proposition 2 *The deterministic capacity of MDFH under the worst case single band disguised jamming is zero.*

4.4 Capacity of AJ-MDFH under Disguised Jamming

In this section, first, we will show that due to the shared randomness introduced by the secure ID sequence, the resulted kernel of the AVC corresponding to AJ-MDFH is nonsymmetrizable even under the worst case disguised jamming - ID jamming. We will further calculate the capacity of AJ-MDFH under ID jamming.

4.4.1 AVC Symmetricity Analysis

Recall that for AJ-MDFH,

$$\mathbf{r} = \boldsymbol{\alpha} s + \mathbf{J} + \mathbf{n}. \tag{4.18}$$

Under the worse case single band disguised jamming, $\mathbf{J} \in \mathcal{X}$, and can be represented as $\mathbf{J} = \boldsymbol{\beta} b$ for some $\boldsymbol{\beta} \in \mathcal{A}$ and $b \in \Omega$. Note that the information is only transmitted through $\boldsymbol{\alpha}$, the AVC corresponding to AJ-MDFH can be characterized using the probability matrix

$$W : \mathcal{X} \times \mathcal{X} \to \mathcal{A}, \tag{4.19}$$

with

$$\begin{aligned} W(\hat{\boldsymbol{\alpha}}|\mathbf{x}, \mathbf{J}) \geq 0, \qquad & \mathbf{x} = \boldsymbol{\alpha} s \in \mathcal{X}, \mathbf{J} = \boldsymbol{\beta} b \in \mathcal{X}, \hat{\boldsymbol{\alpha}}, \boldsymbol{\alpha}, \boldsymbol{\beta} \in \mathcal{A}, \\ \sum_{\hat{\boldsymbol{\alpha}} \in \mathcal{A}} W(\hat{\boldsymbol{\alpha}}|\mathbf{x}, \mathbf{J}) = 1, \quad & \forall\ (\mathbf{x}, \mathbf{J}) \in \mathcal{X}^2. \end{aligned} \tag{4.20}$$

Here $\hat{\boldsymbol{\alpha}}$ is the estimated version of α. In this section, we will first prove that: *under reasonable SNR levels, the kernel W defined in (4.19)-(4.20) is nonsymmetric.* Then prove a stronger result: *W is actually nonsymmetrizable.*

Recall that W is symmetric if and only if

$$W(\hat{\boldsymbol{\alpha}}|\mathbf{x},\mathbf{J}) = W(\hat{\boldsymbol{\alpha}}|\mathbf{J},\mathbf{x}),\ \forall \mathbf{x},\mathbf{J} \in \mathcal{X},\ \forall \hat{\boldsymbol{\alpha}} \in \mathcal{A}. \tag{4.21}$$

To prove that W is nonsymmetric, we need to show that there always exist some $\mathbf{x},\mathbf{J}$ and $\hat{\boldsymbol{\alpha}}$, such that the equality above does not hold. Following the discussion on ID constellation design in Chapter 3, we assume that Ω is a PSK constellation with power P_s, and define a mapping $v : \mathcal{I}_c \to \mathcal{A}$ as

$$v(k) = \boldsymbol{\alpha} \text{ if } \alpha_i = \delta(k-i), \forall i \in \mathcal{I}_c. \tag{4.22}$$

Lemma 1 *Suppose X, Y are independent continuous random variables. If $Z_1, \cdots, Z_N$ are i.i.d. continuous random variables, which are also independent of X, Y, then*

$$Pr\{X < Y \text{ and } X < Z_i, \forall 1 \le i \le N\} \ge Pr\{X < Y\} - NPr\{X \ge Z_{i_0}\}, \tag{4.23}$$

for any fixed $1 \le i_0 \le N$.

Proof: Let $\mathcal{A} = \{X < Y\}$ and $\mathcal{B} = \{X < Z_i, \forall 1 \le i \le N\} = \bigcap_{1 \le i \le N} \{X < Z_i\}$. The corresponding complement, $\bar{\mathcal{B}}$, can be written as

$$\bar{\mathcal{B}} = \bigcup_{1 \le i \le N} \{X \ge Z_i\}. \tag{4.24}$$

Note that $Pr\{\mathcal{A}\} = Pr\{\mathcal{A} \bigcap \mathcal{B}\} + Pr\{\mathcal{A} \bigcap \bar{\mathcal{B}}\}$,

$$\begin{aligned} Pr\{X < Y \text{ and } X < Z_i, \forall 1 \le i \le N\} &= Pr\{\mathcal{A} \bigcap \mathcal{B}\} \\ &= Pr\{\mathcal{A}\} - Pr\{\mathcal{A} \bigcap \bar{\mathcal{B}}\} \\ &\ge Pr\{\mathcal{A}\} - Pr\{\bar{\mathcal{B}}\} \\ &\ge Pr\{\mathcal{A}\} - \sum_{i=1}^{N} Pr\{X \ge Z_i\} \\ &= Pr\{X < Y\} - NPr\{X \ge Z_{i_0}\}, \end{aligned} \tag{4.25}$$

for any fixed $1 \leq i_0 \leq N$. $\square$

Proposition 3 *Assuming Ω is a PSK constellation with power P_s. Let $\mathbf{x} = \boldsymbol{\alpha}s$, $\mathbf{J} = \boldsymbol{\beta}b$, where $\boldsymbol{\alpha}, \boldsymbol{\beta} \in \mathcal{A}$, $\boldsymbol{\alpha} \neq \boldsymbol{\beta}$, and $s, b \in \Omega$, then*

$$W(\boldsymbol{\alpha}|\mathbf{x}, \mathbf{J}) \geq 1 - \frac{1}{2} e^{-\frac{\|b-s\|^2}{2\sigma_n^2}} - \epsilon, \tag{4.26}$$

where $\epsilon = \dfrac{N_c - 2}{\gamma + 2} \exp\{-\dfrac{\gamma(\gamma+1)}{\gamma+2}\}$ with $\gamma = \dfrac{P_s}{\sigma_n^2}$ denoting the SNR.

Proof: Let $\boldsymbol{\alpha} = v(k)$ and $\boldsymbol{\beta} = v(j)$. When $\boldsymbol{\beta} \neq \boldsymbol{\alpha}$, we have $j \neq k$ and

$$\begin{aligned} W(\boldsymbol{\alpha}|\mathbf{x}, \mathbf{J}) &= W(\boldsymbol{\alpha}|\boldsymbol{\alpha}s, \boldsymbol{\beta}b) \\ &= Pr\{Z_k < Z_j \text{ and } Z_k < Z_i, \forall i \in \mathcal{I}_c, i \neq j, k|\mathbf{x}, \mathbf{J}\}. \end{aligned} \tag{4.27}$$

It then follows from Lemma 1 that

$$W(\boldsymbol{\alpha}|\mathbf{x}, \mathbf{J}) \geq Pr\{Z_k < Z_j|\mathbf{x}, \mathbf{J}\} - (N_c - 2) Pr\{Z_k \geq Z_{i_0}|\mathbf{x}, \mathbf{J}\}, \tag{4.28}$$

for any fixed $i_0 \in \mathcal{I}_c, i_0 \neq k, j$. For any $i \in \mathcal{I}_c$, it follows from (4.8) and (4.9) that signal r_i and the corresponding metric Z_i can be written as

$$r_i = \begin{cases} s + n_k, & i = k, \\ b + n_j, & i = j, \\ n_i, & i \neq j, k, \end{cases} \qquad Z_i = \begin{cases} \dfrac{\|n_k\|}{\sqrt{P_s + \sigma_n^2}}, & i = k, \\ \dfrac{\|b - s + n_j\|}{\sqrt{P_s + \sigma_n^2}}, & i = j, \\ \dfrac{\|n_i - s\|}{\sigma_n}, & i \neq j, k. \end{cases} \tag{4.29}$$

Then, $Pr\{Z_k < Z_j|\mathbf{x}, \mathbf{J}\} = Pr\{\|n_k\| < \|b - s + n_j\||\mathbf{x}, \mathbf{J}\}$. For any $s, b \in \Omega$, both n_k and $b - s + n_j$ are circularly symmetric complex Gaussian random variables with $n_k \sim \mathcal{CN}(0, \sigma_n^2)$ and $b - s + n_j \sim \mathcal{CN}(b - s, \sigma_n^2)$. Then $Pr\{Z_k < Z_j|\mathbf{x}, \mathbf{J}\}$ can be calculated as [87, page 49]

$$Pr\{Z_k < Z_j|\mathbf{x}, \mathbf{J}\} = 1 - \frac{1}{2} e^{-\frac{\|b-s\|^2}{2\sigma_n^2}}. \tag{4.30}$$

Similarly, for any fixed $i_0 \in \mathcal{I}_c, i_0 \neq k, j$, we have $\dfrac{n_k}{\sqrt{P_s + \sigma_n^2}} \sim \mathcal{CN}(0, \dfrac{\sigma_n^2}{P_s + \sigma_n^2})$, $\dfrac{n_{i_0} - s}{\sigma_n} \sim \mathcal{CN}(-\dfrac{s}{\sigma_n}, 1)$ and

$$Pr\{Z_k \geq Z_{i_0}|\mathbf{x}, \mathbf{J}\} = Pr\{\frac{\|n_k\|}{\sqrt{P_s + \sigma_n^2}} \geq \frac{\|n_{i_0} - s\|}{\sigma_n}\} = \frac{1}{\gamma + 2} e^{-\frac{\gamma(\gamma+1)}{\gamma+2}}, \tag{4.31}$$

where $\gamma = \dfrac{P_s}{\sigma_n^2}$. It then follows from (4.28) that

$$W(\boldsymbol{\alpha}|\mathbf{x},\mathbf{J}) \geq 1 - \frac{1}{2}e^{-\frac{\|b-s\|^2}{2\sigma_n^2}} - \epsilon. \ \square \tag{4.32}$$

Note that ϵ is determined by the SNR γ as well as the number of channels N_c. When $SNR \geq 10$dB and $N_c = 512$, for example, $\epsilon \leq 0.004$.

Theorem 2 *Assuming Ω is a PSK constellation with power P_s. Let $\mathbf{x} = \boldsymbol{\alpha}s$, $\mathbf{J} = \boldsymbol{\beta}b$, where $\boldsymbol{\alpha}, \boldsymbol{\beta} \in \mathcal{A}$, $\boldsymbol{\alpha} \neq \boldsymbol{\beta}$, and $s, b \in \Omega$, $s \neq b$. Let $\gamma = \dfrac{P_s}{\sigma_n^2}$ and $\epsilon = \dfrac{N_c - 2}{\gamma + 2}\exp\{-\dfrac{\gamma(\gamma+1)}{\gamma+2}\}$, then*

$$W(\boldsymbol{\alpha}|\mathbf{x},\mathbf{J}) - W(\boldsymbol{\alpha}|\mathbf{J},\mathbf{x}) \geq 1 - e^{-\frac{\|b-s\|^2}{2\sigma_n^2}} - 2\epsilon. \tag{4.33}$$

Proof: Following Proposition 3, we have

$$W(\boldsymbol{\beta}|\mathbf{J},\mathbf{x}) \geq 1 - \frac{1}{2}e^{-\frac{\|b-s\|^2}{2\sigma_n^2}} - \epsilon. \tag{4.34}$$

An upper bound for $W(\boldsymbol{\alpha}|\mathbf{J},\mathbf{x})$ can be derived as

$$\begin{aligned} W(\boldsymbol{\alpha}|\mathbf{J},\mathbf{x}) &= 1 - W(\boldsymbol{\beta}|\mathbf{J},\mathbf{x}) - \sum_{\hat{\alpha}\neq\alpha,\beta} W(\hat{\boldsymbol{\alpha}}|\mathbf{J},\mathbf{x}) \\ &\leq 1 - W(\boldsymbol{\beta}|\mathbf{J},\mathbf{x}) \\ &\leq \frac{1}{2}e^{-\frac{\|b-s\|^2}{2\sigma_n^2}} + \epsilon. \end{aligned} \tag{4.35}$$

It then follows form (4.26) and (4.35) that

$$W(\boldsymbol{\alpha}|\mathbf{x},\mathbf{J}) - W(\boldsymbol{\alpha}|\mathbf{J},\mathbf{x}) \geq 1 - e^{-\frac{\|b-s\|^2}{2\sigma_n^2}} - 2\epsilon. \ \square \tag{4.36}$$

Proposition 4 *Assuming Ω is a PSK constellation with power P_s. Let $\mathbf{x} = \boldsymbol{\alpha}s$, $\mathbf{J} = \boldsymbol{\beta}b$, where $\boldsymbol{\alpha}, \boldsymbol{\beta} \in \mathcal{A}$, $\boldsymbol{\alpha} \neq \boldsymbol{\beta}$, and $s, b \in \Omega$, $s \neq b$, then*

$$W(\boldsymbol{\alpha}|\mathbf{x},\mathbf{J}) > W(\boldsymbol{\alpha}|\mathbf{J},\mathbf{x}), \tag{4.37}$$

whenever $\dfrac{\|b-s\|^2}{\sigma_n^2} > 2\ln\dfrac{1}{1-2\epsilon}$.

This result follows directly from Theorem 2. It implies that as long as s and b are "distinguishable" under the additive noise, the channel symmetricity between the jammer and the legal user is broken, and this increases the probability of correct decision.

Define $\hat{W} : \mathcal{X} \times \mathcal{X} \to \mathcal{A}$ by

$$\hat{W}(\hat{\boldsymbol{\alpha}}|\mathbf{x}, \mathbf{J}) \triangleq \sum_{\mathbf{y} \in \mathcal{Y}} \pi(\mathbf{y}|\mathbf{J}) W(\hat{\boldsymbol{\alpha}}|\mathbf{x}, \mathbf{y}), \tag{4.38}$$

where $\pi : \mathcal{X} \to \mathcal{Y}$ is a probability matrix, and $\mathcal{Y} \subseteq \mathcal{X}$. If there exists a π such that

$$\hat{W}(\hat{\boldsymbol{\alpha}}|\mathbf{x}, \mathbf{J}) = \hat{W}(\hat{\boldsymbol{\alpha}}|\mathbf{J}, \mathbf{x}), \quad \forall \mathbf{x}, \mathbf{J} \in \mathcal{X}, \ \forall \hat{\boldsymbol{\alpha}} \in \mathcal{A}, \tag{4.39}$$

then W is said to be symmetrizable. Next, we will show that under ID jamming, as long as the ID sequence is unavailable to the jammer, the AVC corresponding to AJ-MDFH is not only nonsymmetric, but also *nonsymmetrizable*.

Theorem 3 *Assuming Ω is a M-PSK constellation with power P_s. Let $\gamma = \frac{P_s}{\sigma_n^2}$, $\epsilon = \frac{N_c - 2}{\gamma + 2} \exp\{-\frac{\gamma(\gamma+1)}{\gamma+2}\}$ and $d_{\min} = \min_{s_1, s_2 \in \Omega, s_1 \neq s_2} \|s_1 - s_2\|$. Let $f(x) = \frac{1}{x+2} \exp\{-\frac{x(x+1)}{x+2}\}$. For $N_c > 2$ and $M > 2$, under the condition[2] that*

$$\gamma > f^{-1}(\frac{1}{2N_c}) \quad \textit{and} \quad \frac{d_{\min}^2}{\sigma_n^2} > \max(\frac{2\sqrt{\ln N_c}}{\sqrt{2}\gamma - \sqrt{\ln N_c}}, 2 \ln \frac{1}{1 - 2\epsilon}) \tag{4.40}$$

*the kernel W for the AVC corresponding to AJ-MDFH is **nonsymmetrizable**.*

We are going to show that for any probability matrix π, there exist some $\hat{\boldsymbol{\alpha}}_0 \in \mathcal{A}$, and $\mathbf{x}_0, \mathbf{J}_0 \in \mathcal{X}$, such that

$$\hat{W}(\hat{\boldsymbol{\alpha}}_0|\mathbf{x}_0, \mathbf{J}_0) \neq \hat{W}(\hat{\boldsymbol{\alpha}}_0|\mathbf{J}_0, \mathbf{x}_0). \tag{4.41}$$

To prove this result, we need the following two Lemmas:

Lemma 2 *For any given $\pi : \mathcal{X} \to \mathcal{X}$, there exists a pair $\mathbf{x}_0 = \boldsymbol{\alpha} s$ and $\mathbf{J}_0 = \boldsymbol{\beta} b$, $\boldsymbol{\alpha}, \boldsymbol{\beta} \in \mathcal{A}$, $s, b \in \Omega$, such that $\boldsymbol{\beta} \neq \boldsymbol{\alpha}, b \neq s$ and $\pi(-\mathbf{x}_0|\mathbf{J}_0) + \pi(\boldsymbol{\beta} s|\mathbf{J}_0) < 1$.*

[2]When M is fixed, the two conditions in (4.40) can be reduced to one condition on SNR. As an example, for $M = 32$ and $N_c = 64$, the kernel W is nonsymmetrizable when $\gamma > 8.3$dB.

Proof: Suppose for all $\mathbf{x} = \tilde{\boldsymbol{\alpha}}\tilde{s}$ and $\mathbf{J} = \tilde{\boldsymbol{\beta}}\tilde{b}$ with $\tilde{\boldsymbol{\beta}} \neq \tilde{\boldsymbol{\alpha}}, \tilde{b} \neq \tilde{s}$, the equality $\pi(-\mathbf{x}|\mathbf{J}) + \pi(\tilde{\boldsymbol{\beta}}\tilde{s}|\mathbf{J}) = 1$ holds. For $N_c > 2$ and $M > 2$, consider $\mathbf{x}_0 = \boldsymbol{\alpha}s$, $\mathbf{J}_0 = \boldsymbol{\beta}b$ with $\boldsymbol{\beta} \neq \boldsymbol{\alpha}, b \neq s$ and any $\mathbf{x}_1 = \boldsymbol{\lambda}c$, $\boldsymbol{\lambda} \in \mathcal{A}$, $c \in \Omega$ with $\boldsymbol{\lambda} \neq \boldsymbol{\alpha}, \boldsymbol{\beta}$ and $c \neq b, s$. On one hand, $\pi(-\mathbf{x}_0|\mathbf{J}_0) + \pi(\boldsymbol{\beta}s|\mathbf{J}_0) = 1$, which implies that $\mathbf{J}_0$ can only be mapped to $-\mathbf{x}_0$ and $\boldsymbol{\beta}s$. On the other hand, we also have $\pi(-\mathbf{x}_1|\mathbf{J}_0) + \pi(\boldsymbol{\beta}c|\mathbf{J}_0) = 1$, which implies that $\mathbf{J}_0$ can only be mapped to $-\mathbf{x}_1$ and $\boldsymbol{\beta}c$. Since $-\mathbf{x}_1 \neq -\mathbf{x}_0$ and $\boldsymbol{\beta}c \neq \boldsymbol{\beta}s$, this is a contradiction. Hence, we can always find a pair $\mathbf{x}_0$ and $\mathbf{J}_0$ such that $\pi(-\mathbf{x}_0|\mathbf{J}_0) + \pi(\boldsymbol{\beta}s|\mathbf{J}_0) < 1$. □

Lemma 3 $\mathcal{X}$ can be partitioned into six subsets with respect to $\mathbf{x}_0$ as $\mathcal{X} = \cup_{i=1}^{6}\mathcal{X}_i$, where

$$\begin{aligned}\mathcal{X}_1 &\triangleq \{\boldsymbol{\alpha}(-s)\},\ \mathcal{X}_2 \triangleq \{\boldsymbol{\alpha}s_0|s_0 \in \Omega, s_0 \neq -s\},\ \mathcal{X}_3 \triangleq \{\boldsymbol{\beta}s\},\ \mathcal{X}_4 \triangleq \{\boldsymbol{\beta}s_0|s_0 \in \Omega, s_0 \neq s\}\\ \mathcal{X}_5 &\triangleq \{\boldsymbol{\alpha}_0 s|\boldsymbol{\alpha}_0 \neq \boldsymbol{\alpha}, \boldsymbol{\beta}\},\ \mathcal{X}_6 \triangleq \{\boldsymbol{\alpha}_0 s_0|\boldsymbol{\alpha}_0 \neq \boldsymbol{\alpha}, \boldsymbol{\beta}, s_0 \neq s\}. \end{aligned} \tag{4.42}$$

Under the condition that $\gamma > f^{-1}(\frac{1}{2N_c})$ and $\frac{d_{\min}^2}{\sigma_n^2} > \max(\frac{2\sqrt{\ln N_c}}{\sqrt{2}\gamma - \sqrt{\ln N_c}}, 2\ln\frac{1}{1-2\epsilon})$,

$$W(\boldsymbol{\alpha}|\mathbf{x}_0, \mathbf{y}) = W(\boldsymbol{\beta}|\mathbf{x}_0, \mathbf{y}), \quad \forall \mathbf{y} \in \mathcal{X}_i, i = 1, 3. \tag{4.43}$$

$$W(\boldsymbol{\alpha}|\mathbf{x}_0, \mathbf{y}) - W(\boldsymbol{\beta}|\mathbf{x}_0, \mathbf{y}) > 0, \quad \forall \mathbf{y} \in \mathcal{X}_i, i = 2, 4, 5, 6. \tag{4.44}$$

Proof: See Section 4.10.1. □

For any $\mathbf{x} \in \mathcal{X}, \mathbf{y} \in \mathcal{Y}$, we assume $0 \leq \pi(\mathbf{y}|\mathbf{x}) \leq 1$. Here the value 1 corresponds to the case that $\mathcal{Y}$ is a single item subset; the value 0 excludes certain points in $\mathcal{X}$, and results in the case that $\mathcal{Y}$ is a proper subset of $\mathcal{X}$. Without loss of generality, we can assume that $\mathcal{Y} = \mathcal{X}$ and prove that (4.39) is not true for any probability matrix $\pi : \mathcal{X} \to \mathcal{X}$.

Proof of Theorem 3: Following Lemma 2, we pick $\mathbf{x}_0$, $\mathbf{J}_0$ such that $\boldsymbol{\beta} \neq \boldsymbol{\alpha}, b \neq s$ and $\pi(-\mathbf{x}_0|\mathbf{J}_0) + \pi(\boldsymbol{\beta}s|\mathbf{J}_0) < 1$. We will prove that $\hat{W}(\boldsymbol{\alpha}|\mathbf{x}_0, \mathbf{J}_0) = \hat{W}(\boldsymbol{\alpha}|\mathbf{J}_0, \mathbf{x}_0)$ and $\hat{W}(\boldsymbol{\beta}|\mathbf{x}_0, \mathbf{J}_0) = \hat{W}(\boldsymbol{\beta}|\mathbf{J}_0, \mathbf{x}_0)$ cannot hold simultaneously, by showing that

$$\hat{W}(\boldsymbol{\alpha}|\mathbf{x}_0, \mathbf{J}_0) - \hat{W}(\boldsymbol{\beta}|\mathbf{x}_0, \mathbf{J}_0) > \hat{W}(\boldsymbol{\alpha}|\mathbf{J}_0, \mathbf{x}_0) - \hat{W}(\boldsymbol{\beta}|\mathbf{J}_0, \mathbf{x}_0). \tag{4.45}$$

By Lemma 3, $\mathcal{X} = \cup_{i=1}^{6}\mathcal{X}_i$. For any $\hat{\boldsymbol{\alpha}}_0 \in \mathcal{A}$, we have

$$\hat{W}(\hat{\boldsymbol{\alpha}}_0|\mathbf{x}_0, \mathbf{J}_0) = \sum_{i=1}^{6}\sum_{\mathbf{y}\in\mathcal{X}_i} \pi(\mathbf{y}|\mathbf{J}_0) W(\hat{\boldsymbol{\alpha}}_0|\mathbf{x}_0, \mathbf{y}). \tag{4.46}$$

It then follows from (4.43) - (4.44) that

$$\hat{W}(\boldsymbol{\alpha}|\mathbf{x}_0,\mathbf{J}_0)-\hat{W}(\boldsymbol{\beta}|\mathbf{x}_0,\mathbf{J}_0)=\sum_{\substack{i=2,\\ i\neq 3}}^{6}\sum_{\mathbf{y}\in\mathcal{X}_i}[W(\boldsymbol{\alpha}|\mathbf{x}_0,\mathbf{y})-W(\boldsymbol{\beta}|\mathbf{x}_0,\mathbf{y})]\pi(\mathbf{y}|\mathbf{J}_0)\geq 0, \quad (4.47)$$

with the equality holds if and only if $\sum_{\substack{i=2,\\ i\neq 3}}^{6}\sum_{\mathbf{y}\in\mathcal{X}_i}\pi(\mathbf{y}|\mathbf{J}_0)=0$, i.e., $\pi(-\mathbf{x}_0|\mathbf{J}_0)+\pi(\boldsymbol{\beta}s|\mathbf{J}_0)=1$. Recall that we pick $\mathbf{x}_0$, $\mathbf{J}_0$ such that $\boldsymbol{\beta}\neq\boldsymbol{\alpha}, b\neq s$ and $\pi(-\mathbf{x}_0|\mathbf{J}_0)+\pi(\boldsymbol{\beta}s|\mathbf{J}_0)<1$. Therefore,

$$\hat{W}(\boldsymbol{\alpha}|\mathbf{x}_0,\mathbf{J}_0)-\hat{W}(\boldsymbol{\beta}|\mathbf{x}_0,\mathbf{J}_0)>0. \quad (4.48)$$

Similarly, $\mathcal{X}$ can be partitioned into six subsets with respect to $\mathbf{J}_0=\boldsymbol{\beta}b$, defined as

$$\begin{aligned}\mathcal{J}_1 &\triangleq \{\boldsymbol{\beta}(-b)\},\ \mathcal{J}_2\triangleq\{\boldsymbol{\beta}b_0|b_0\in\Omega,b_0\neq -b\},\ \mathcal{J}_3\triangleq\{\boldsymbol{\alpha}b\},\ \mathcal{J}_4\triangleq\{\boldsymbol{\alpha}b_0|b_0\in\Omega,b_0\neq b\}\\ \mathcal{J}_5 &\triangleq \{\boldsymbol{\beta}_0 b|\boldsymbol{\beta}_0\neq\boldsymbol{\alpha},\boldsymbol{\beta}\},\ \mathcal{J}_6\triangleq\{\boldsymbol{\beta}_0 b_0|\boldsymbol{\beta}_0\neq\boldsymbol{\alpha},\boldsymbol{\beta},b_0\neq b\}, \quad (4.49)\end{aligned}$$

and

$$\hat{W}(\hat{\boldsymbol{\alpha}}_0|\mathbf{J}_0,\mathbf{x}_0)=\sum_{i=1}^{6}\sum_{\mathbf{y}\in\mathcal{J}_i}\pi(\mathbf{y}|\mathbf{x}_0)W(\hat{\boldsymbol{\alpha}}_0|\mathbf{J}_0,\mathbf{y}). \quad (4.50)$$

Then we have

$$\hat{W}(\boldsymbol{\alpha}|\mathbf{J}_0,\mathbf{x}_0)-\hat{W}(\boldsymbol{\beta}|\mathbf{J}_0,\mathbf{x}_0)=\sum_{\substack{i=2,\\ i\neq 3}}^{6}\sum_{\mathbf{y}\in\mathcal{J}_i}[W(\boldsymbol{\alpha}|\mathbf{J}_0,\mathbf{y})-W(\boldsymbol{\beta}|\mathbf{J}_0,\mathbf{y})]\pi(\mathbf{y}|\mathbf{x}_0). \quad (4.51)$$

Moreover, under the same condition as in previous case,

$$\hat{W}(\boldsymbol{\alpha}|\mathbf{J}_0,\mathbf{x}_0)-\hat{W}(\boldsymbol{\beta}|\mathbf{J}_0,\mathbf{x}_0)\leq 0. \quad (4.52)$$

From (4.48) and (4.52), we can see that (4.45) holds, which implies that $\hat{W}(\boldsymbol{\alpha}|\mathbf{x}_0,\mathbf{J}_0)=\hat{W}(\boldsymbol{\alpha}|\mathbf{J}_0,\mathbf{x}_0)$ and $\hat{W}(\boldsymbol{\beta}|\mathbf{x}_0,\mathbf{J}_0)=\hat{W}(\boldsymbol{\beta}|\mathbf{J}_0,\mathbf{x}_0)$ cannot hold simultaneously. □

Note that the secure ID in AJ-MDFH is generated using AES, to symmetrize AJ-MDFH is thus equivalent to break AES, which is computationally infeasible in practical systems. That is, the AVC corresponding to AJ-MDFH is computationally infeasible to be symmetrized. This result ensures that when the ID sequence is unknown to the jammer, the deterministic capacity of AJ-MDFH is positive, and equal to the random code capacity [51, 92].

4.4.2 Capacity Calculation

Note that in AJ-MDFH, the message information is only transmitted through the carrier bits. Consider $\mathbf{x} = \boldsymbol{\alpha} s$ where $s \in \Omega$ and $\boldsymbol{\alpha} = (\alpha_1, \cdots, \alpha_{N_c}) \in \mathcal{A}$. Let i_S and i_J be the signal channel index and jamming channel index, respectively, and $\hat{i}_S$ the detected signal channel index at the receiver. For capacity analysis, define

$$W_1(\hat{k}|k,j) \triangleq Pr\{\hat{i}_S = \hat{k}|i_S = k, i_J = j\}. \tag{4.53}$$

Let $\mathbf{x} = \boldsymbol{\alpha} s$, $\mathbf{J} = \boldsymbol{\beta} b$ with $\boldsymbol{\alpha} = v(k)$, $\boldsymbol{\beta} = v(j)$. Let $\hat{\boldsymbol{\alpha}} = v(\hat{k})$, and assuming s and b are uniformly distributed over Ω, then the relationship between W_1 and W can be characterized as

$$W_1(\hat{k}|k,j) = \frac{1}{|\Omega|^2} \sum_{s\in\Omega} \sum_{b\in\Omega} W(\hat{\boldsymbol{\alpha}}|\mathbf{x} = \boldsymbol{\alpha} s, \mathbf{J} = \boldsymbol{\beta} b). \tag{4.54}$$

The detailed representation of W_1 is provided in Section 4.10.2, where we prove that W_1 has the following properties:

(P1): $W_1(k|k,k)$ and $W_1(i|k,k)$ are fixed values for any $i, k \in \mathcal{I}_c, i \neq k$.

(P2): $W_1(k|k,j)$, $W_1(j|k,j)$ and $W_1(i|k,j)$ are fixed values for any $i, j, k \in \mathcal{I}_c, j \neq k, i \neq j, k$.

Denote the set of all probability distributions on $\mathcal{I}_c$ as $\mathcal{P}(\mathcal{I}_c)$. Let P and ζ denote the probability distribution associated with i_S and i_J, respectively. $P, \zeta \in \mathcal{P}(\mathcal{I}_c)$. Let W_ζ denote the averaged probability matrix for a given ζ

$$\begin{aligned} W_\zeta(\hat{k}|k) &= W_\zeta(\hat{i}_S = \hat{k}|i_S = k) \\ &= \sum_{j\in\mathcal{I}_c} W_1(\hat{k}|k,j)\zeta(i_J = j). \end{aligned} \tag{4.55}$$

Let $I(P, W_\zeta)$ denote the mutual information [92] between the input and the output for the AJ-MDFH channel, defined as

$$I(P, W_\zeta) \triangleq \sum_{\hat{k}\in\mathcal{I}_c} \sum_{k\in\mathcal{I}_c} P(i_S = k) W_\zeta(\hat{k}|k) \log \frac{W_\zeta(\hat{k}|k)}{(PW)_\zeta(\hat{k})}, \tag{4.56}$$

where $(PW)_\zeta(\hat{k}) = \sum_{k' \in \mathcal{I}_c} W_\zeta(\hat{k}|k')P(k')$. Following Theorem 3, the AVC corresponding to AJ-MDFH is nonsymmetrizable. Its channel capacity for the average error probability is positive and can be calculated as [52, 53]

$$C = \max_{P \in \mathcal{P}(\mathcal{I}_c)} \min_{\zeta \in \mathcal{P}(\mathcal{I}_c)} I(P, W_\zeta) = \min_{\zeta \in \mathcal{P}(\mathcal{I}_c)} \max_{P \in \mathcal{P}(\mathcal{I}_c)} I(P, W_\zeta). \tag{4.57}$$

It can be observed from (4.57) that the legal user tries to choose P to maximize the mutual information, while the jammer tries to minimize it by choosing an appropriate ζ [95, 96]. Let $(P, \zeta) \in \mathcal{P}(\mathcal{I}_c) \times \mathcal{P}(\mathcal{I}_c)$ be a pair of mixed strategy chosen by the user and the jammer. The capacity can be achieved when a pair of saddle point strategy (P^*, ζ^*) are chosen, which can be characterized by the following two inequalities for all $(P, \zeta) \in \mathcal{P}(\mathcal{I}_c) \times \mathcal{P}(\mathcal{I}_c)$ [97, 98]:

$$I(P, W_{\zeta^*}) \leq I(P^*, W_{\zeta^*}) \leq I(P^*, W_\zeta). \tag{4.58}$$

Following the same arguments in [99], we have the following Lemma:

Lemma 4 In an AJ-MDFH channel, the saddle point strategy pair can be reached when both P and ζ are uniform distributions over $\mathcal{I}_c$. That is,

$$P^*(k) = \begin{cases} \frac{1}{N_c}, & k \in \mathcal{I}_c, \\ 0, & \text{otherwise}, \end{cases} \qquad \zeta^*(j) = \begin{cases} \frac{1}{N_c}, & j \in \mathcal{I}_c, \\ 0, & \text{otherwise}. \end{cases} \tag{4.59}$$

Proof: We need to show that both inequalities in (4.58) are satisfied if (P^*, ζ^*) is given in (4.59). First, assuming $\zeta = \zeta^*$, it can be shown that W_{ζ^*} is a symmetric matrix given in (4.80). It is shown in [100] that $I(P, W_{\zeta^*})$ is maximized when $P = P^*$. Hence

$$I(P, W_{\zeta^*}) \leq I(P^*, W_{\zeta^*}). \tag{4.60}$$

Next, assuming $P = P^*$, we will show that $I(P^*, W_\zeta)$ is minimized when $\zeta = \zeta^*$. For notation simplicity, we will consider the case $N_c = 2$, as the proof can be extended to $N_c > 2$. For $N_c = 2$, $\mathcal{I}_c = \{1, 2\}$,

$$W_\zeta(\hat{k}|k) = \sum_{j \in \mathcal{I}_c} W_1(\hat{k}|k, j)\zeta(i_J = j), \forall \hat{k}, k \in \mathcal{I}_c. \tag{4.61}$$

Define

$$W_\zeta = \begin{pmatrix} W_\zeta(1|1) & W_\zeta(2|1) \\ W_\zeta(1|2) & W_\zeta(2|2) \end{pmatrix}. \tag{4.62}$$

For any $\zeta \in \mathcal{P}(\mathcal{I}_c)$, let $q_1 = \zeta(i_J = 1)$, $q_2 = \zeta(i_J = 2) = 1 - q_1$,

$$W_\zeta = \begin{pmatrix} W_1(1|1,1)q_1 + W_1(1|1,2)q_2 & W_1(2|1,1)q_1 + W_1(2|1,2)q_2 \\ W_1(1|2,1)q_1 + W_1(1|2,2)q_2 & W_1(2|2,1)q_1 + W_1(2|2,2)q_2 \end{pmatrix}. \tag{4.63}$$

Let $p_1 = W_1(1|1,1)$ and $p_2 = W_1(1|1,2)$. Note that $W_1(k|k,k)$ is a fixed value for any $k \in \mathcal{I}_c$ and $W_1(k|k,j)$ is also a fixed value for $j,k \in \mathcal{I}_c, j \neq k$. We have

$$\begin{aligned} W_1(2|2,2) &= W_1(1|1,1) = p_1, \\ W_1(2|2,1) &= W_1(1|1,2) = p_2, \end{aligned} \tag{4.64}$$

and

$$\begin{aligned} W_1(1|2,2) &= W_1(2|1,1) = 1 - p_1, \\ W_1(1|2,1) &= W_1(2|1,2) = 1 - p_2. \end{aligned} \tag{4.65}$$

It follows from (4.63)-(4.65) that

$$W_\zeta = \begin{pmatrix} p_1q_1 + p_2q_2 & (1-p_1)q_1 + (1-p_2)q_2 \\ (1-p_2)q_1 + (1-p_1)q_2 & p_2q_1 + p_1q_2 \end{pmatrix}. \tag{4.66}$$

Consider $\zeta' \in \mathcal{P}(\mathcal{I}_c)$ with $\zeta'(i_J = 1) = q_2 = 1 - q_1$ and $\zeta'(i_J = 2) = q_1$, the corresponding probability matrix

$$W_{\zeta'} = \begin{pmatrix} p_2q_1 + p_1q_2 & (1-p_2)q_1 + (1-p_1)q_2 \\ (1-p_1)q_1 + (1-p_2)q_2 & p_1q_1 + p_2q_2 \end{pmatrix}. \tag{4.67}$$

For the uniform distribution ζ^*, i.e., $\zeta^*(i_J = 1) = \zeta^*(i_J = 2) = \frac{1}{2}$,

$$W_{\zeta^*} = \begin{pmatrix} \frac{p_1+p_2}{2} & 1 - \frac{p_1+p_2}{2} \\ 1 - \frac{p_1+p_2}{2} & \frac{p_1+p_2}{2} \end{pmatrix}. \tag{4.68}$$

It can be observed that $W_{\zeta*}(\hat{k}|k) = \frac{1}{2}W_{\zeta}(\hat{k}|k) + \frac{1}{2}W_{\zeta'}(\hat{k}|k)$ for all $\hat{k}, k \in \mathcal{I}_c$. That is, $W_{\zeta*} = \frac{1}{2}W_{\zeta} + \frac{1}{2}W_{\zeta'}$. Since $I(P^*, W_{\zeta})$ is a convex function of $W_{\zeta}(\hat{k}|k)$ [100, Theorem 2.7.4], according to Jensen's inequality,

$$I(P^*, W_{\zeta*}) = I(P^*, \frac{1}{2}W_{\zeta} + \frac{1}{2}W_{\zeta'}) \leq \frac{1}{2}[I(P^*, W_{\zeta}) + I(P^*, W_{\zeta'})]. \tag{4.69}$$

Recall that

$$I(P, W_{\zeta}) \triangleq \sum_{\hat{k}\in\mathcal{I}_c}\sum_{k\in\mathcal{I}_c} P(i_S = k)W_{\zeta}(\hat{k}|k)\log\frac{W_{\zeta}(\hat{k}|k)}{(PW)_{\zeta}(\hat{k})}, \tag{4.70}$$

where $(PW)_{\zeta}(\hat{k}) = \sum_{k'\in\mathcal{I}_c} W_{\zeta}(\hat{k}|k')P(k')$. Note that

$$\begin{aligned} W_{\zeta}(1|1) &= W_{\zeta'}(2|2), \quad W_{\zeta}(1|2) = W_{\zeta'}(2|1) \\ W_{\zeta}(2|1) &= W_{\zeta'}(1|2), \quad W_{\zeta}(2|2) = W_{\zeta'}(1|1). \end{aligned} \tag{4.71}$$

When the input is equiprobable, i.e., $P^*(1) = P^*(2) = \frac{1}{2}$, it can be observed that

$$\begin{aligned} (PW)_{\zeta}(1) &= \frac{1}{2}(W_{\zeta}(1|1) + W_{\zeta}(1|2)) \\ &= \frac{1}{2}(W_{\zeta'}(2|2) + W_{\zeta'}(2|1)) = (PW)_{\zeta'}(2), \end{aligned} \tag{4.72}$$

and similarly $(PW)_{\zeta}(2) = (PW)_{\zeta'}(1)$. It then follows from (4.70) and (4.72) that

$$\begin{aligned} I(P^*, W_{\zeta}) &= \sum_{k'\in\mathcal{I}_c}\sum_{k\in\mathcal{I}_c}\frac{1}{2}W_{\zeta}(\hat{k}|k)\log\frac{W_{\zeta}(\hat{k}|k)}{(PW)_{\zeta}(\hat{k})} \\ &= \sum_{k'\in\mathcal{I}_c}\sum_{k\in\mathcal{I}_c}\frac{1}{2}W_{\zeta'}(\hat{k}|k)\log\frac{W_{\zeta'}(\hat{k}|k)}{(PW)_{\zeta'}(\hat{k})} \\ &= I(P^*, W_{\zeta'}). \end{aligned} \tag{4.73}$$

Then

$$I(P^*, W_{\zeta*}) \leq I(P^*, W_{\zeta}). \tag{4.74}$$

Combining (4.60) and (4.74), we proved that $I(P^*, W_{\zeta*})$ is a pair of saddle point strategy.

□

In AJ-MDFH, when the jammer chooses the strategy ζ^* as in (4.59), the averaged probability matrix can be calculated as

$$W_{\zeta^*}(\hat{k}|k) = \sum_{j=1}^{N_c} W_1(\hat{k}|k,j)\zeta^*(j). \tag{4.75}$$

(i) When $\hat{k} = k$, (4.75) can be expanded as

$$W_{\zeta^*}(\hat{k}|k) = W_1(k|k,k)\zeta^*(k) + \sum_{j\in\mathcal{I}_c, j\neq k} W_1(k|k,j)\zeta^*(j). \tag{4.76}$$

Following property **(P1)** and **(P2)** of W_1, we have

$$W_{\zeta^*}(\hat{k}|k) = \frac{1}{N_c}W_1(k_0|k_0,k_0) + \frac{N_c-1}{N_c}W_1(k_0|k_0,j_0), \tag{4.77}$$

for any fixed $j_0, k_0 \in \mathcal{I}_c, j_0 \neq k_0$.

(ii) When $\hat{k} \neq k$, (4.75) can be expanded as

$$W_{\zeta^*}(\hat{k}|k) = W_1(\hat{k}|k,k)\zeta^*(k) + W_1(\hat{k}|k,\hat{k})\zeta^*(\hat{k}) + \sum_{j\in\mathcal{I}_c, j\neq\hat{k},k} W_1(\hat{k}|k,j)\zeta^*(j). \tag{4.78}$$

Following property **(P1)** and **(P2)** of W_1, we have

$$W_{\zeta^*}(\hat{k}|k) = \frac{1}{N_c}W_1(\hat{k}_0|k_0,k_0) + \frac{1}{N_c}W_1(\hat{k}_0|k_0,\hat{k}_0) + \frac{N_c-2}{N_c}W_1(\hat{k}_0|k_0,j_0), \tag{4.79}$$

for any fixed $\hat{k}_0, k_0, j_0 \in \mathcal{I}_c, \hat{k}_0 \neq k_0, j_0 \neq \hat{k}_0, k_0$. Define $w_1 \triangleq W_{\zeta^*}(k|k)$ and $w_2 \triangleq W_{\zeta^*}(\hat{k}|k), \hat{k} \neq k$, then W_{ζ^*} can be obtained as

$$W_{\zeta^*} = \begin{pmatrix} W_{\zeta^*}(1|1) & W_{\zeta^*}(2|1) & \cdots & W_{\zeta^*}(N_c|1) \\ W_{\zeta^*}(1|2) & W_{\zeta^*}(2|2) & \cdots & W_{\zeta^*}(N_c|2) \\ \vdots & \vdots & \ddots & \vdots \\ W_{\zeta^*}(1|N_c) & W_{\zeta^*}(2|N_c) & \cdots & W_{\zeta^*}(N_c|N_c) \end{pmatrix} = \begin{pmatrix} w_1 & w_2 & \cdots & w_2 \\ w_2 & w_1 & \cdots & w_2 \\ \vdots & \vdots & \ddots & \vdots \\ w_2 & w_2 & \cdots & w_1 \end{pmatrix}_{N_c\times N_c}. \tag{4.80}$$

Due to the structure of the matrix W_{ζ^*}, it then follows that for any $\hat{k}, k' \in \mathcal{I}_c$, $\sum_{k'\in\mathcal{I}_c} W_{\zeta^*}(\hat{k}|k') = \sum_{\hat{k}\in\mathcal{I}_c} W_{\zeta^*}(\hat{k}|k') = 1$, and

$$(P^*W)_{\zeta^*}(\hat{k}) = \sum_{k'\in\mathcal{I}_c} W_{\zeta^*}(\hat{k}|k')P^*(k') = \frac{1}{N_c}. \tag{4.81}$$

It then follows from (4.56) and (4.57) that

$$\begin{aligned} C &= I(P^*, W_{\zeta^*}) \\ &= \sum_{\hat{k}\in\mathcal{I}_c}\sum_{k\in\mathcal{I}_c}\frac{1}{N_c}W_{\zeta^*}(\hat{k}|k)\log\frac{W_{\zeta^*}(\hat{k}|k)}{\frac{1}{N_c}} \\ &= \sum_{\hat{k}\in\mathcal{I}_c}\sum_{k\in\mathcal{I}_c}\frac{1}{N_c}W_{\zeta^*}(\hat{k}|k)\log N_c + \sum_{\hat{k}\in\mathcal{I}_c}\sum_{k\in\mathcal{I}_c}\frac{1}{N_c}W_{\zeta^*}(\hat{k}|k)\log W_{\zeta^*}(\hat{k}|k) \\ &= \log N_c + \sum_{\hat{k}=1}^{N_c} W_{\zeta^*}(\hat{k}|1)\log W_{\zeta^*}(\hat{k}|1) \\ &= \log N_c + w_1\log w_1 + (N_c-1)w_2\log w_2. \end{aligned} \tag{4.82}$$

Following the discussions above and similar argument as in the proof of Proposition 1 in Chapter 3, we have:

Theorem 4 *Assuming Ω is an M-PSK constellation with power P_s. Let $\gamma = \frac{P_s}{\sigma_n^2}$. The deterministic capacity of AJ-MDFH under ID jamming is a function of M, N_c and γ of the form $C = C(M, N_c, \gamma)$. As M approaches infinity, C converges to*

$$\bar{C} = \log N_c + \bar{w}_1\log\bar{w}_1 + (N_c-1)\bar{w}_2\log\bar{w}_2, \tag{4.83}$$

where $\bar{w}_1 = \lim_{M\to\infty} w_1$ and $\bar{w}_2 = \lim_{M\to\infty} w_2$.

Proof: It can be observed from Section 4.10.2 that when Ω is an M-PSK constellation with power P_s, for any $j, k, \hat{k} \in \mathcal{I}_c$, $W_1(\hat{k}|k, j)$ can be written as a function of the form

$$W_1(\hat{k}|k,j) = \frac{1}{M}\sum_{\kappa=0}^{M-1} f_{j,k,\hat{k}}(\frac{2\pi\kappa}{M}, N_c, \gamma). \tag{4.84}$$

It then follows from (4.76) that

$$w_1 = \frac{1}{M}\sum_{\kappa=0}^{M-1}\left[f_{w_1}(\frac{2\pi\kappa}{M}, N_c, \gamma)\right], \tag{4.85}$$

where

$$f_{w_1}(\frac{2\pi\kappa}{M}, N_c, \gamma) = \frac{1}{N_c}f_{k_0,k_0,k_0}(\frac{2\pi\kappa}{M}, N_c, \gamma) + \frac{N_c-1}{N_c}f_{j_0,k_0,k_0}(\frac{2\pi\kappa}{M}, N_c, \gamma), \tag{4.86}$$

for any fixed $j_0, k_0 \in \mathcal{I}_c, j_0 \neq k_0$. Similarly, from (4.78), we have

$$w_2 = \frac{1}{M} \sum_{\kappa=0}^{M-1} \left[f_{w_2}(\frac{2\pi\kappa}{M}, N_c, \gamma) \right], \tag{4.87}$$

where

$$\begin{aligned} f_{w_2}(\frac{2\pi\kappa}{M}, N_c, \gamma) &= \frac{1}{N_c} f_{k_0,k_0,\hat{k}_0}(\frac{2\pi\kappa}{M}, N_c, \gamma) + \frac{1}{N_c} f_{\hat{k}_0,k_0,\hat{k}_0}(\frac{2\pi\kappa}{M}, N_c, \gamma) \\ &+ \frac{N_c - 2}{N_c} f_{j_0,k_0,\hat{k}_0}(\frac{2\pi\kappa}{M}, N_c, \gamma), \end{aligned} \tag{4.88}$$

for any fixed $\hat{k}_0, k_0, j_0 \in \mathcal{I}_c, \hat{k}_0 \neq k_0, j_0 \neq \hat{k}_0, k_0$. Since both w_1 and w_2 are functions of M, N_c and γ, it then follows from (4.82) that the channel capacity C is a function of M, N_c and γ of the form $C = C(M, N_c, \gamma)$.

As M approaches infinity, w_1 converges to $\bar{w}_1$ as

$$\begin{aligned} \bar{w}_1 &= \lim_{M\to\infty} w_1 = \lim_{M\to\infty} \sum_{\kappa=0}^{M-1} \frac{f_{w_1}(\frac{2\pi\kappa}{M}, N_c, \gamma) \cdot \frac{2\pi}{M}}{M \cdot \frac{2\pi}{M}} \\ &= \frac{1}{2\pi} \lim_{M\to\infty} \sum_{\kappa=0}^{M-1} f_{w_1}(\frac{2\pi\kappa}{M}, N_c, \gamma) \cdot \frac{2\pi}{M} \\ &= \frac{1}{2\pi} \int_0^{2\pi} f_{w_1}(x, N_c, \gamma) dx. \end{aligned} \tag{4.89}$$

Similarly, we have

$$\bar{w}_2 = \lim_{M\to\infty} w_2 = \frac{1}{2\pi} \int_0^{2\pi} f_{w_2}(x, N_c, \gamma) dx. \tag{4.90}$$

Note that $w_1, w_2 \in (0, 1)$ and $x \log x$ is continuous within this range. As M approaches infinity, C converges to $\bar{C}$ as

$$\begin{aligned} \bar{C} = \lim_{M\to\infty} C &= \log N_c + \lim_{M\to\infty} w_1 \log w_1 + (N_c - 1) \lim_{M\to\infty} w_2 \log w_2 \\ &= \log N_c + \bar{w}_1 \log \bar{w}_1 + (N_c - 1)\bar{w}_2 \log \bar{w}_2. \ \square \end{aligned} \tag{4.91}$$

4.5 Capacity of Multiuser AJ-MDFH under Disguised Jamming

In this section, we will analyze the deterministic capacity of MC-AJ-MDFH system under the single band worst case disguised jamming - ID jamming.

Recall that in MC-AJ-MDFH, N_c channels are divided into N_g non-overlapping groups, and each subcarrier hops within the assigned group based on AJ-MDFH scheme. For each hopping period, let s_m and $\boldsymbol{\alpha}_m$ be the symbol and the indicator vector for mth subcarrier, respectively. Let $\mathbf{x}_m = \boldsymbol{\alpha}_m s_m$ denote the signal over mth subcarrier, and $\hat{\boldsymbol{\alpha}}_m$ the estimated version of $\boldsymbol{\alpha}_m$. Let $\mathcal{G}_m$ denote the indexes of the subcarrier group for mth subcarrier and $\bar{\mathcal{G}}_m = \mathcal{I}_c \backslash \mathcal{G}_m$ the complement of $\mathcal{G}_m$ in $\mathcal{I}_c$. The set of indicator vector used by mth subcarrier, denoted by $\mathcal{A}_m$, can be obtained by $\mathcal{A}_m = \{v(i) | \forall i \in \mathcal{G}_m\}$. Define $\mathcal{X}_m = \{\boldsymbol{\alpha}_m s_m | \boldsymbol{\alpha}_m \in \mathcal{A}_m, s_m \in \Omega\}$ be the set of all possible $\mathbf{x}_m$. Note that the ID jamming is denoted by $\mathbf{J} = \boldsymbol{\beta} b \in \mathcal{X}$. The AVC corresponding to the mth subcarrier can be characterized by the probability matrix

$$\tilde{W}_m : \mathcal{X}_m \times \mathcal{X} \to \mathcal{A}_m \tag{4.92}$$

with

$$\tilde{W}_m(\hat{\boldsymbol{\alpha}}_m | \mathbf{x}_m, \mathbf{J}) \geq 0, \sum_{\hat{\boldsymbol{\alpha}}_m \in \mathcal{A}_m} \tilde{W}_m(\hat{\boldsymbol{\alpha}}_m | \mathbf{x}_m, \mathbf{J}) = 1, \tag{4.93}$$

where $\mathbf{x}_m = \boldsymbol{\alpha}_m s_m \in \mathcal{X}_m, \mathbf{J} = \boldsymbol{\beta} b \in \mathcal{X}, \hat{\boldsymbol{\alpha}}_m, \boldsymbol{\alpha}_m \in \mathcal{A}_m, \boldsymbol{\beta} \in \mathcal{A}$.

Note that in MC-AJ-MDFH, both secure group information and ID sequence are protected by AES. Without the knowledge of the shared secret, the jammer is unable to determine the subcarrier group $\mathcal{G}_m$, which implies that $\mathcal{X}_m \neq \mathcal{X}$ thus kernel $\tilde{W}_m$ is nonsymmetric. Following the similar arguments as in Section 4.4, it can be further shown that kernel $\tilde{W}_m$ is also nonsymmetrizable and the AVC corresponding to mth subcarrier has positive capacity under ID jamming.

Let $i_{S,m}$ and $\hat{i}_{S,m}$ be the signal channel index and its estimated version at the receiver, respectively. Recall that i_J denote the jamming channel index. The probability matrix for carrier bits information of mth subcarrier can be defined as

$$W_{1,m}(\hat{k}_m | k_m, j) = Pr\{\hat{i}_{S,m} = \hat{k}_m | i_{S,m} = k_m, i_J = j\}. \tag{4.94}$$

Let $\boldsymbol{\alpha}_m = v(k_m), k_m \in \mathcal{G}_m, s_m \in \Omega$ and $\mathbf{J} = \boldsymbol{\beta} b$ with $\boldsymbol{\beta} = v(j), j \in \mathcal{I}_c$ and $b \in \Omega$. Assuming

s_m and b are uniformly distributed over Ω, $W_{1,m}$ can be obtained from $\tilde{W}_m$ by

$$W_{1,m}(\hat{k}_m|k_m,j) = \frac{1}{|\Omega|^2}\sum_{s_m\in\Omega}\sum_{b\in\Omega}\tilde{W}_m[v(\hat{k}_m)|v(k_m)s_m, v(j)b], \tag{4.95}$$

where $\tilde{W}_m[v(\hat{k}_m)|v(k_m)s_m, v(j)b]$ can be calculated as

$$\tilde{W}_m[v(\hat{k}_m)|v(k_m)s_m, v(j)b] = Pr\{Z_{\hat{k}_m} < Z_i, \forall i \in \mathcal{G}_m, i \neq \hat{k}_m|\mathbf{x}_m = \boldsymbol{\alpha}_m s_m, \mathbf{J} = \boldsymbol{\beta} b\}. \tag{4.96}$$

Assuming Ω is an M-PSK constellation with power P_s.

(i) When $j \in \mathcal{G}_m$, $W_{1,m}$ can be calculated following the similar derivations in Section 4.10.2, except that the detection is performed on subcarrier group $\mathcal{G}_m$ instead of on $\mathcal{I}_c$.

(ii) When $j \in \bar{\mathcal{G}}_m$, the group is jamming-free. Z_i can be obtained as

$$Z_i = \begin{cases} \dfrac{\|n_{k_m}\|}{\sqrt{P_s+\sigma_n^2}}, & i = k_m, \\ \dfrac{\|n_i - s_m\|}{\sigma_n}, & i \in \mathcal{G}_m, i \neq k_m. \end{cases} \tag{4.97}$$

Z_{k_m} is a a Rayleigh random variable with PDF $p_{Z_{k_m}}(z_{k_m}) = \frac{z_{k_m}}{\sigma^2}e^{-\frac{z_{k_m}^2}{2\sigma^2}}$, where $\sigma = \frac{\sigma_n}{\sqrt{2(P_s+\sigma_n^2)}}$. For any $s_m \in \Omega$, when $i \neq k_m$, Z_i's are i.i.d. Rician random variables with PDF $p_{Z_i}(z_i) = \frac{z_i}{\sigma^2}e^{-\frac{z_i^2+\nu^2}{2\sigma^2}} I_0\left(\frac{z_i\nu}{\sigma^2}\right)$, where $\nu = \sqrt{P_s}$ and $\sigma = \frac{1}{\sqrt{2}}$. It can be observed that the jamming does not affect the signal detection performance in this case. For any $\mathbf{x}_m = v(k_m)s_m, \mathbf{J} = v(j)b$ with $j \in \bar{\mathcal{G}}_m$, we have

$$\begin{aligned} W_{1,m} & (k_m|k_m,j) \\ = & \frac{1}{|\Omega|^2}\sum_{s_m\in\Omega}\sum_{b\in\Omega} Pr\{Z_{k_m} < Z_i, \forall i \in \mathcal{G}_m, i \neq k_m|\mathbf{x}_m, \mathbf{J}\} \\ = & \frac{1}{|\Omega|^2}\sum_{s_m\in\Omega}\sum_{b\in\Omega}\int_0^\infty \prod_{i\in\mathcal{G}_m, i\neq k_m} Pr\{Z_i > z_{k_m}|\mathbf{x}_m, \mathbf{J}, z_{k_m}\} p_{Z_{k_m}}(z_{k_m})dz_{k_m} \\ = & \int_0^\infty \left[Q_1\left(\frac{\sqrt{2P_s}}{\sigma_n}, \sqrt{2}z_{k_m}\right)\right]^{|\mathcal{G}_m|-1} \frac{2z_{k_m}(P_s+\sigma_n^2)}{\sigma_n^2} e^{-\frac{(P_s+\sigma_n^2)z_{k_m}^2}{\sigma_n^2}} dz_{k_m}, \end{aligned} \tag{4.98}$$

and for any $i, k_m \in \mathcal{G}_m, i \neq k_m$,

$$W_{1,m}(i|k_m, j) = \frac{1}{|\mathcal{G}_m| - 1}[1 - W_{1,m}(k_m|k_m, j)]. \tag{4.99}$$

Let $W_{\zeta,m}$ denote the averaged probability matrix of mth user under ID jamming with distribution ζ on $\mathcal{I}_c$ given as

$$W_{\zeta,m}(\hat{k}_m|k_m) = \sum_{j \in \mathcal{I}_c} W_{1,m}(\hat{k}_m|k_m, j)\zeta(i_J = j). \tag{4.100}$$

Due to the pseudorandom property of the secure group generation algorithm, i_J is uniformly distributed over N_c channels after the secure groups are recovered at the receiver, which is the same as the saddle point strategy given in (4.59). Following the similar derivations for AJ-MDFH in (4.75)-(4.78), we have the following results:

(i) When $\hat{k}_m = k_m \in \mathcal{G}_m$,

$$\begin{aligned} W_{\zeta^*,m}(\hat{k}_m|k_m) &= W_{1,m}(k_m|k_m, k_m)\zeta^*(k_m) + \sum_{j \in \mathcal{G}_m, j \neq k_m} W_{1,m}(k_m|k_m, j)\zeta^*(j) \\ &\quad + \sum_{j \in \bar{\mathcal{G}}_m} W_1(k_m|k_m, j)\zeta^*(j) \\ &= \frac{1}{N_c} W_{1,m}(k_{0,m}|k_{0,m}, k_{0,m}) + \frac{|\mathcal{G}_m| - 1}{N_c} W_{1,m}(k_{0,m}|k_{0,m}, j_0) \\ &\quad + \frac{N_c - |\mathcal{G}_m|}{N_c} W_{1,m}(k_{0,m}|k_{0,m}, u_{0,m}), \end{aligned}$$

for any fixed $j_0, k_{0,m} \in \mathcal{G}_m, j_0 \neq k_{0,m}$ and any fixed $u_{0,m} \in \bar{\mathcal{G}}_m$.

(ii) When $\hat{k}_m, k_m \in \mathcal{G}_m, \hat{k}_m \neq k_m$,

$$\begin{aligned} W_{\zeta^*,m}(\hat{k}_m|k_m) &= W_{1,m}(\hat{k}_m|k_m, k_m)\zeta^*(k_m) + W_{1,m}(\hat{k}_m|k_m, \hat{k}_m)\zeta^*(\hat{k}_m) \\ &\quad + \sum_{\substack{j \in \mathcal{G}_m \\ j \neq \hat{k}_m, k_m}} W_{1,m}(\hat{k}_m|k_m, j)\zeta^*(j) + \sum_{j \in \bar{\mathcal{G}}_m} W_{1,m}(k_m|k_m, j)\zeta^*(j) \\ &= \frac{1}{N_c} W_{1,m}(\hat{k}_{0,m}|k_{0,m}, k_{0,m}) + \frac{1}{N_c} W_{1,m}(\hat{k}_{0,m}|k_{0,m}, \hat{k}_{0,m}) \\ &\quad + \frac{|\mathcal{G}_m| - 2}{N_c} W_{1,m}(\hat{k}_{0,m}|k_{0,m}, j_0) + \frac{N_c - |\mathcal{G}_m|}{N_c} W_{1,m}(\hat{k}_{0,m}|k_{0,m}, u_{0,m}), \end{aligned}$$

for any fixed $\hat{k}_{0,m}, k_{0,m}, j_0 \in \mathcal{G}_m, \hat{k}_{0,m} \neq k_{0,m}, j_0 \neq \hat{k}_{0,m}, k_{0,m}$ and any fixed $u_{0,m} \in \bar{\mathcal{G}}_m$.

Define $w_{1,m} \triangleq W_{\zeta^*,m}(k_m|k_m)$ and $w_{2,m} \triangleq W_{\zeta^*,m}(\hat{k}_m|k_m), \hat{k}_m \neq k_m$. $W_{\zeta^*,m}$ can be written into a symmetric matrix of size $|\mathcal{G}_m| \times |\mathcal{G}_m|$ similar as in (4.80). The deterministic capacity for mth subcarrier group under ID jamming, C_m, can be obtained following (4.82) that

$$C_m = \log |\mathcal{G}_m| + w_{1,m} \log w_{1,m} + (|\mathcal{G}_m| - 1) w_{2,m} \log w_{2,m}, \tag{4.101}$$

which is achieved when $i_{S,m}$ is uniformly distributed over $\mathcal{G}_m$. Hence, the capacity of MC-AJ-MDFH can be obtained as

$$C_{MC} = \sum_{m=1}^{N_g} C_m. \tag{4.102}$$

4.6 Capacity of MDFH under Noise Jamming

Let $\mathbf{x} = \boldsymbol{\alpha} s \in \mathcal{X}$ and $\mathbf{J} \in \mathcal{J}$ denote the transmitted signal and the jamming, respectively, and $\hat{\mathbf{x}} = \hat{\boldsymbol{\alpha}} \hat{s} \in \mathcal{X}$ the estimated version of $\mathbf{x} = \boldsymbol{\alpha} s$ at the receiver. Let σ_J^2 denote the jamming power and $\mathcal{C}$ the set of all complex numbers. Under the single band noise jamming, we have $\mathbf{J} = \boldsymbol{\beta} b$ where $\boldsymbol{\beta} \in \mathcal{A}$ and $b \in \mathcal{C}$ is a circularly symmetric complex Gaussian random variable, i.e., $b \sim \mathcal{CN}(0, \sigma_J^2)$. The corresponding noise jamming space is

$$\mathcal{J} = \{\boldsymbol{\beta} b | \boldsymbol{\beta} \in \mathcal{A}, b \in \mathcal{C}\}. \tag{4.103}$$

Therefore, MDFH under noise jamming can be modeled as an AVC characterized by the probability matrix

$$W_0 : \mathcal{X} \times \mathcal{J} \to \mathcal{X}, \tag{4.104}$$

with

$$W_0(\hat{\mathbf{x}}|\mathbf{x}, \mathbf{J}) \geq 0, \qquad \hat{\mathbf{x}}, \mathbf{x} \in \mathcal{X}, \mathbf{J} \in \mathcal{J}, \tag{4.105}$$

$$\sum_{\hat{\mathbf{x}} \in \mathcal{X}} W_0(\hat{\mathbf{x}}|\mathbf{x}, \mathbf{J}) = 1, \quad \mathbf{x} \in \mathcal{X}, \mathbf{J} \in \mathcal{J}. \tag{4.106}$$

For the kernel to be symmetric, it is required that $\mathcal{J} = \mathcal{X}$. Since $\mathcal{J} \supset \mathcal{X}$ for noise jamming, the kernel corresponding to MDFH under noise jamming, W_0, is nonsymmetric.

Recall that to symmetrize W_0, we need to find a probability matrix $\pi(\mathbf{y}|\mathbf{J})$, where $\mathbf{J} \in \mathcal{X}$ and $\mathbf{y} \in \mathcal{Y}, \mathcal{Y} \subseteq \mathcal{J}$. This implies that to symmetrize $\mathcal{X}$ also requires $\mathbf{J} \in \mathcal{X}$. However, under the noise jamming, the jammer simply transmits random Gaussian noise and $\mathbf{J} \in \mathcal{J}$. This implies that the jammer has no intention to disguise itself as the true signal. Hence, the MDFH channel under noise jamming is nonsymmetrizable and has a positive capacity.

Recall that in MDFH, the information bits are divided into carrier bits and ordinary bits. At the receiver, the carrier bits are first detected by identifying the carrier channel, then the ordinary bits are extracted from the estimated carrier using conventional demodulation scheme. Following the MDFH receiver design, we have

$$W_0(\hat{\mathbf{x}} = \hat{\boldsymbol{\alpha}}\hat{s}|\mathbf{x}, \mathbf{J}) = W_{0,c}(\hat{\boldsymbol{\alpha}}|\mathbf{x}, \mathbf{J}) W_{0,o}(\hat{s}|\hat{\boldsymbol{\alpha}}, \mathbf{x}, \mathbf{J}). \tag{4.107}$$

Here, $W_{0,c} : \mathcal{X} \times \mathcal{J} \to \mathcal{A}$ is the AVC kernel corresponding to the carrier bits transmission channel, and $W_{0,o} : \mathcal{A} \times \mathcal{X} \times \mathcal{J} \to \Omega$ is the AVC kernel corresponding to the ordinary bits transmission channel. Note that $W_{0,o}$ depends on the output of $W_{0,c}$. We now derive the capacity of the carrier bits transmission channel and that of the ordinary bits transmission channel, respectively.

4.6.1 Capacity Derivation for Carrier Information Transmission Channel

Let i_S and i_J be the signal channel index and jamming channel index, respectively, and $\hat{i}_S$ the detected signal channel index at the receiver. For capacity analysis, define

$$W_{1,c}(\hat{k}|k, j) = Pr\{\hat{i}_S = \hat{k}|i_S = k, i_J = j\}. \tag{4.108}$$

Note that the signal symbol s is selected from Ω by the encrypted information, which is assumed to be random, and the jamming noise $b \sim \mathcal{CN}(0, \sigma_J^2)$ is independent of s. Let $\mathbf{x} = \boldsymbol{\alpha}s$, $\mathbf{J} = \boldsymbol{\beta}b$ with $\boldsymbol{\alpha} = v(k)$, $\boldsymbol{\beta} = v(j)$, and $\hat{\boldsymbol{\alpha}} = v(\hat{k})$. Then, the relationship between $W_{1,c}$ and $W_{0,c}$ can be characterized as

$$W_{1,c}(\hat{k}|k, j) = \frac{1}{|\Omega|} \sum_{s \in \Omega} \int_{\mathcal{C}} W_{0,c}[v(\hat{k})|v(k)s, v(j)b] p_B(b) db, \tag{4.109}$$

where $p_B(b) = \frac{1}{\pi\sigma_J^2}\exp\{-\frac{\|b\|^2}{\sigma_J^2}\}$ is the PDF for Gaussian noise b.

Assuming Ω is a PSK constellation with power P_s. Let $Y_i = \|r_i\|$ denote the square root of the received signal power in ith channel. When the threshold based (with threshold η) carrier detector is used, channel $\hat{k}$ is detected if $Y_{\hat{k}}$ is the smallest above the threshold η, and $W_{1,c}(\hat{k}|k,j)$ can be obtained as follows:

(i) When $j = k$, Y_i can be obtained as

$$Y_i = \begin{cases} \|s + b + n_k\|, & i = k, \\ \|n_i\|, & i \neq k, \end{cases} \tag{4.110}$$

Since $b \sim \mathcal{CN}(0, \sigma_J^2)$, we have $r_k \sim \mathcal{CN}(s, \sigma_J^2 + \sigma_n^2)$, $r_i \sim \mathcal{CN}(0, \sigma_n^2)$ and

$$\begin{aligned} W_{1,c} \quad & (k|k,k) \\ = \quad & \frac{1}{|\Omega|}\sum_{s\in\Omega}\int_{\mathcal{C}} Pr\{Y_k > \eta \text{ and } Y_i < \eta, \forall i \in \mathcal{I}_c, i \neq k|\mathbf{x}, \mathbf{J}\}p_B(b)db \\ = \quad & Q_1\left(\sqrt{\frac{2P_s}{\sigma_J^2 + \sigma_n^2}}, \sqrt{\frac{2}{\sigma_J^2 + \sigma_n^2}}\eta\right)(1 - e^{-\frac{\eta^2}{\sigma_n^2}})^{N_c - 1}. \end{aligned} \tag{4.111}$$

For $i \neq k$, $W_{1,c}(i|k,k)$ can be obtained following (4.165) in Section 4.10.2.

(ii) When $j \neq k$, Y_i can be calculated as

$$Y_i = \begin{cases} \|s + n_k\|, & i = k, \\ \|b + n_j\|, & i = j, \\ \|n_i\|, & i \neq j, k. \end{cases} \tag{4.112}$$

Note that $r_k \sim \mathcal{CN}(s, \sigma_n^2)$, $r_j \sim \mathcal{CN}(0, \sigma_J^2 + \sigma_n^2)$ and $r_i \sim \mathcal{CN}(0, \sigma_n^2)$. We then have

$$\begin{aligned} W_{1,c} \quad & (k|k,j) \\ = \quad & \frac{1}{|\Omega|} \sum_{s \in \Omega} \int_{\mathcal{C}} \big[Pr\{Y_k > \eta \text{ and } Y_j < \eta \text{ and } Y_i < \eta, \forall i \in \mathcal{I}_c, i \neq k | \mathbf{x}, \mathbf{J}\} \\ & + Pr\{Y_k > \eta \text{ and } Y_k < Y_j \text{ and } Y_i < \eta, \forall i \in \mathcal{I}_c, i \neq k | \mathbf{x}, \mathbf{J}\} \big] \, p_B(b) db \\ = \quad & \left[Q_1 \left(\frac{\sqrt{2P_s}}{\sigma_n}, \frac{\sqrt{2}}{\sigma_n} \eta \right) (1 - e^{-\frac{\eta^2}{\sigma_J^2 + \sigma_n^2}}) + \int_{\eta}^{\infty} e^{-\frac{y_k^2}{\sigma_J^2 + \sigma_n^2}} p_{Y_k}(y_k) dy_k \right] \\ & \cdot (1 - e^{-\frac{\eta^2}{\sigma_n^2}})^{N_c - 2}, \end{aligned} \tag{4.113}$$

where $p_{Y_k}(y_k) = \frac{y_k}{\sigma^2} e^{-\frac{y_k^2 + \nu^2}{2\sigma^2}} I_0 \left(\frac{y_k \nu}{\sigma^2} \right)$ with $\nu = \sqrt{P_s}$ and $\sigma = \frac{\sigma_n}{\sqrt{2}}$, and

$$\begin{aligned} W_{1,c} \quad & (j|k,j) \\ = \quad & \frac{1}{|\Omega|} \sum_{s \in \Omega} \int_{\mathcal{C}} \big[Pr\{Y_k < \eta \text{ and } Y_j > \eta \text{ and } Y_i < \eta, \forall i \in \mathcal{I}_c, i \neq k | \mathbf{x}, \mathbf{J}\} \\ & + Pr\{Y_j > \eta \text{ and } Y_j < Y_k \text{ and } Y_i < \eta, \forall i \in \mathcal{I}_c, i \neq k | \mathbf{x}, \mathbf{J}\} \big] \, p_B(b) db \\ = \quad & \left\{ \left[1 - Q_1 \left(\frac{\sqrt{2P_s}}{\sigma_n}, \frac{\sqrt{2}}{\sigma_n} \eta \right) \right] e^{-\frac{\eta^2}{\sigma_J^2 + \sigma_n^2}} + \int_{\eta}^{\infty} Q_1 \left(\frac{\sqrt{2P_s}}{\sigma_n}, \frac{\sqrt{2}}{\sigma_n} y_j \right) p_{Y_j}(y_j) dy_j \right\} \\ & \cdot (1 - e^{-\frac{\eta^2}{\sigma_n^2}})^{N_c - 2}, \end{aligned} \tag{4.114}$$

where $p_{Y_j}(y_j) = \frac{y_j}{\sigma^2} e^{-\frac{y_j^2}{2\sigma^2}}$ with $\sigma = \frac{\sigma_J}{\sqrt{2}}$. For $i \neq k, j$, $W_{1,c}(i|k,j)$ can be obtained following (4.169) in Section 4.10.2. The capacity of the carrier information transmission channel, denoted as C_c, can be obtained similarly following the capacity result in (4.82).

4.6.2 Capacity Derivation for Ordinary Information Transmission Channel

Let S be the signal symbol selected by the ordinary bits, B the Gaussian noise, and $\hat{S}$ the estimated version of S. For capacity analysis, define

$$W_{1,o}(\hat{s}|s,b) = Pr\{\hat{S} = \hat{s} | S = s, B = b\}. \tag{4.115}$$

Note that i_S is selected by the encrypted carrier bits information, which is assumed to be uniformly distributed over $\mathcal{I}_c$, and i_J is also assumed to be uniformly distributed over $\mathcal{I}_c$. Then, the relationship between $W_{1,o}$ and $W_{0,o}$ can be characterized as

$$W_{1,o}(\hat{s}|s,b) = \frac{1}{N_c^2} \sum_{\hat{k}\in\mathcal{I}_c} \sum_{k\in\mathcal{I}_c} \sum_{j\in\mathcal{I}_c} W_{0,o}[\hat{s}|v(\hat{k}), v(k)s, v(j)b] W_{1,c}(\hat{k}|k,j). \tag{4.116}$$

For noise jamming, $b \sim \mathcal{CN}(0,\sigma_J^2)$, and the averaged probability matrix for $W_{1,o}$ can be obtained as

$$\begin{aligned} W_{o,p_B}(\hat{s}|s) &= \int_{\mathcal{C}} W_{1,o}(\hat{s}|s,b) p_B(b) db \\ &= \frac{1}{N_c^2} \sum_{\hat{k}\in\mathcal{I}_c} \sum_{k\in\mathcal{I}_c} \sum_{j\in\mathcal{I}_c} \bar{W}_{0,o}[\hat{s}|v(\hat{k}), v(k)s, v(j)] W_{1,c}(\hat{k}|k,j), \end{aligned} \tag{4.117}$$

where

$$\bar{W}_{0,o}[\hat{s}|v(\hat{k}), v(k)s, v(j)] = \int_{\mathcal{C}} W_{0,o}[\hat{s}|v(\hat{k}), v(k)s, v(j)b] p_B(b) db. \tag{4.118}$$

When the minimum distance detector $\hat{s} = \arg\min_{\hat{s}\in\Omega} \|r_{\hat{k}} - \hat{s}\|$ is used for symbol s detection, $\bar{W}_{0,o}[\hat{s}|v(\hat{k}), v(k)s, v(j)]$ can be calculated as follows:

(i) When $\hat{k} = j = k$, $r_{\hat{k}} = r_k = s + b + n_k$. Let $D_{\hat{s}}$ denote the decision region for symbol $\hat{s}$. Since $b \sim \mathcal{CN}(0,\sigma_J^2)$ and $n_k \sim \mathcal{CN}(0,\sigma_n^2)$, we have $r_k \sim \mathcal{CN}(s, \sigma_J^2 + \sigma_n^2)$ and

$$\bar{W}_{0,o}[\hat{s}|v(k), v(k)s, v(k)] = \int_{D_{\hat{s}}} p_{r_k}(r_k) dr_k, \tag{4.119}$$

where $p_{r_k}(r_k) = \dfrac{1}{\pi(\sigma_J^2 + \sigma_n^2)} \exp\{-\dfrac{\|r_k - s\|^2}{\sigma_J^2 + \sigma_n^2}\}$ is the PDF of r_k.

(ii) When $j \neq k$ and $\hat{k} = k$, $r_{\hat{k}} = r_k = s + n_k$. We then have $r_k \sim \mathcal{CN}(s, \sigma_n^2)$ and

$$\bar{W}_{0,o}[\hat{s}|v(k), v(k)s, v(j)] = \int_{D_{\hat{s}}} p_{r_k}(r_k) dr_k, \tag{4.120}$$

where $p_{r_k}(r_k) = \dfrac{1}{\pi\sigma_n^2} \exp\{-\dfrac{\|r_k - s\|^2}{\sigma_n^2}\}$.

(iii) When $j \neq k$ and $\hat{k} = j$, $r_{\hat{k}} = r_j = b + n_k$. That is, the detected channel contains only noise. In this case, the detected symbol is randomly distributed over Ω

$$\bar{W}_{0,o}[\hat{s}|v(j), v(k)s, v(j)] = \frac{1}{|\Omega|}. \tag{4.121}$$

Similarly for $j = k, \hat{k} \neq k$ and $j \neq k, \hat{k} \neq j, k$, we have $r_{\hat{k}} = n_{\hat{k}}$ and

$$\bar{W}_{0,o}[\hat{s}|v(\hat{k}), v(k)s, v(k)] = \bar{W}_{0,o}[\hat{s}|v(\hat{k}), v(k)s, v(j)] = \frac{1}{|\Omega|}. \tag{4.122}$$

After obtaining $\bar{W}_{0,o}$ and $W_{1,c}$ from carrier information transmission channel, $W_{o,p_B}(\hat{s}|s)$ can be calculated as (4.117). Let Q denote the probability distribution associated with S. Then the capacity of the ordinary information transmission channel can be obtained as

$$C_o = \max_{Q} I(Q, W_{o,p_B}). \tag{4.123}$$

It can be shown that W_{o,p_B} is a symmetric matrix. Hence, the capacity is achieved when $Q = Q^*$ which is the uniform distribution over Ω. Overall, the channel capacity for MDFH under noise jamming can be calculated as

$$C_{MD} = C_c + C_o. \tag{4.124}$$

Note that $I(Q^*, W_{o,p_B})$ is a convex function of W_{o,p_B}, according to Jensen's inequality, the capacity can be upper bounded by

$$C_o = I(Q^*, W_{o,p_B}) \leq \frac{1}{N_c^2} \sum_{\hat{k} \in \mathcal{I}_c} \sum_{k \in \mathcal{I}_c} \sum_{j \in \mathcal{I}_c} W_{1,c}(\hat{k}|k, j) I(Q^*, \bar{W}_{0,o}[\hat{s}|v(\hat{k}), v(k)s, v(j)]), \tag{4.125}$$

where $I(Q^*, \bar{W}_{0,o}[\hat{s}|v(\hat{k}), v(k)s, v(j)])$ is the capacity of the detected carrier channel $\hat{k}$ when signal and jamming are in kth and jth channel respectively. The capacity of the ordinary information transmission channel is upper bounded by the averaged capacity over all carrier detection scenarios.

4.7 Capacity of AJ-MDFH under Noise Jamming

Under the worst case single band noise jamming, $\mathbf{J} = \boldsymbol{\beta} b$, $b \sim \mathcal{CN}(0, \sigma_J^2)$ where $\sigma_J^2 = P_s$, and

$$\mathcal{J} = \{\boldsymbol{\beta} b | \boldsymbol{\beta} \in \mathcal{A}, b \in \mathcal{C}\}, \tag{4.126}$$

where $\mathcal{C}$ denotes the set of all complex numbers. The AVC corresponding to the AJ-MDFH can be characterized by the probability matrix

$$W : \mathcal{X} \times \mathcal{J} \to \mathcal{A} \tag{4.127}$$

with

$$W(\hat{\boldsymbol{\alpha}}|\mathbf{x}, \mathbf{J}) \geq 0, \ \sum_{\hat{\boldsymbol{\alpha}} \in \mathcal{A}} W(\hat{\boldsymbol{\alpha}}|\mathbf{x}, \mathbf{J}) = 1, \tag{4.128}$$

where $\mathbf{x} = \boldsymbol{\alpha} s \in \mathcal{X}, \mathbf{J} = \boldsymbol{\beta} b \in \mathcal{J}, \hat{\boldsymbol{\alpha}}, \boldsymbol{\alpha}, \boldsymbol{\beta} \in \mathcal{A}$. Following the similar argument in Section 4.6, it can be seen that the AVC corresponding to AJ-MDFH under noise jamming is also nonsymmetrizable and has a positive capacity. Recall that for capacity derivation, we define the information transmission channel in AJ-MDFH as

$$W_1(\hat{k}|k, j) \triangleq Pr\{\hat{i}_S = \hat{k}|i_S = k, i_J = j\}, \tag{4.129}$$

which corresponds to the carrier information transmission channel in MDFH case. As the ID symbol s is randomly selected from Ω, the relationship between W_1 and W can be characterized as

$$W_1(\hat{k}|k, j) = \frac{1}{|\Omega|} \sum_{s \in \Omega} \int_{\mathcal{C}} W[v(\hat{k})|v(k)s, v(j)b] p_B(b) db. \tag{4.130}$$

Note that $b \sim \mathcal{CN}(0, P_s)$ in this case. Assuming Ω is the PSK constellation with power P_s. Following from similar calculation scheme of W_1 under disguised jamming in Section 4.10.2, we have

$$\begin{aligned} W_1 \quad & (k|k, k) \\ = \quad & \frac{1}{|\Omega|} \sum_{s \in \Omega} \int_{\mathcal{C}} Pr\{Z_k < Z_i, \forall i \in \mathcal{I}_c, i \neq k | \mathbf{x} = \boldsymbol{\alpha} s, \mathbf{J} = \boldsymbol{\beta} b\} p_B(b) db \\ = \quad & \frac{1}{|\Omega|} \sum_{s \in \Omega} \int_0^{\infty} \prod_{1 \leq i \leq N_c, i \neq k} Pr\{Z_i > z_k | \mathbf{x}, \mathbf{J}, z_k\} p_{Z_k}(z_k) dz_k. \end{aligned} \tag{4.131}$$

For any $s \in \Omega$, Z_k is a Rayleigh random variable with PDF $p_{Z_k}(z_k) = \frac{z_k}{\sigma^2} e^{-\frac{z_k^2}{2\sigma^2}}$ for $0 \leq z_k < \infty$, where $\sigma = \sqrt{\frac{P_s + \sigma_n^2}{2(2P_s + \sigma_n^2)}}$; for $i \neq k$, Z_i's are i.i.d. Rician random variables with

PDF $p_{Z_i}(z_i) = \frac{z_i}{\sigma^2} e^{-\frac{z_i^2+\nu^2}{2\sigma^2}} I_0\left(\frac{z_i\nu}{\sigma^2}\right)$ for $0 \le z_i < \infty$, where $\nu = \frac{\sqrt{P_s}}{\sigma_n}$ and $\sigma = \frac{1}{\sqrt{2}}$. Then (4.131) can be simplified as

$$W_1(k|k,k) = \int_0^\infty Q_1^{N_c-1}\left(\frac{\sqrt{2P_s}}{\sigma_n}, \sqrt{2}z_k\right) p_{Z_k}(z_k)dz_k. \tag{4.132}$$

For $i \neq k$, $W_1(i|k,k)$ can be obtained following (4.165) in Section 4.10.2.

When $j \neq k$, Z_k is Rayleigh distributed with PDF $p_{Z_k}(z_k) = \frac{z_k}{\sigma^2} e^{-\frac{z_k^2}{2\sigma^2}}$ where $\sigma = \frac{\sigma_n}{\sqrt{2(P_s+\sigma_n^2)}}$; Z_j is Rician distributed with PDF $p_{Z_j}(z_j) = \frac{z_j}{\sigma^2} e^{-\frac{z_j^2+\nu^2}{2\sigma^2}} I_0\left(\frac{z_j\nu}{\sigma^2}\right)$ where $\nu = \sqrt{\frac{P_s}{P_s+\sigma_n^2}}$ and $\sigma = \frac{1}{\sqrt{2}}$. Hence, we can obtain

$$\begin{aligned} W_1 \quad & (k|k,j) \\ = \quad & \frac{1}{|\Omega|}\sum_{s\in\Omega}\int_0^\infty \Pr\{Z_j > z_k|\mathbf{x},\mathbf{J},z_k\}\left[Pr\{Z_i > z_k|\mathbf{x},\mathbf{J},z_k\}\right]^{N_c-2} p(z_k)dz_k \\ = \quad & \int_0^\infty Q_1\left(\sqrt{\frac{2P_s}{P_s+\sigma_n^2}}, \sqrt{2}z_k\right) Q_1^{N_c-2}\left(\frac{\sqrt{2P_s}}{\sigma_n}, \sqrt{2}z_k\right) p_{Z_k}(z_k)dz_k, \end{aligned} \tag{4.133}$$

and

$$\begin{aligned} W_1 \quad & (j|k,j) \\ = \quad & \frac{1}{|\Omega|}\sum_{s\in\Omega}\int_0^\infty Pr\{Z_k > z_j|\mathbf{x},\mathbf{J},z_j\}\left[Pr\{Z_i > z_j|\mathbf{x},\mathbf{J},z_j\}\right]^{N_c-2} p_{Z_j}(z_j)dz_j \\ = \quad & \int_0^\infty e^{-\frac{(P_s+\sigma_n^2)z_j^2}{\sigma_n^2}} Q_1^{N_c-2}\left(\frac{\sqrt{2P_s}}{\sigma_n}, \sqrt{2}z_k\right) p_{Z_k}(z_j)dz_j. \end{aligned} \tag{4.134}$$

For $i \neq k, j$, $W_1(i|k,j)$ can be obtained following (4.169) in Section 4.10.2. The capacity of AJ-MDFH, denoted as C_{AJ},can be calculated following (4.82).

4.8 Numerical Results

In this section, simulation examples are provided to illustrate the capacity of the proposed AJ-MDFH and MC-AJ-MDFH schemes under the worst case disguised jamming. For all the

systems considered, we assume the total number of available channels is $N_c = 64$, that is, $B_c = 6$.

Example 1: Impact of the ID constellation size on capacity In this example, we consider the impact of the ID constellation size on the capacity of AJ-MDFH under the single band worst case disguised jamming (ID jamming). In Figure 4.3, it can be seen that the capacity under the ID jamming converges as the constellation size increases. Under reasonable SNR levels (for example, we require $\gamma > 8.3$dB when the constellation size $M = 32$ to ensure the AVC corresponding to AJ-MDFH is nonsymmetrizable), the capacity limit $\bar{C}$ is close to the corresponding jamming-free case indicated by the dashed line.

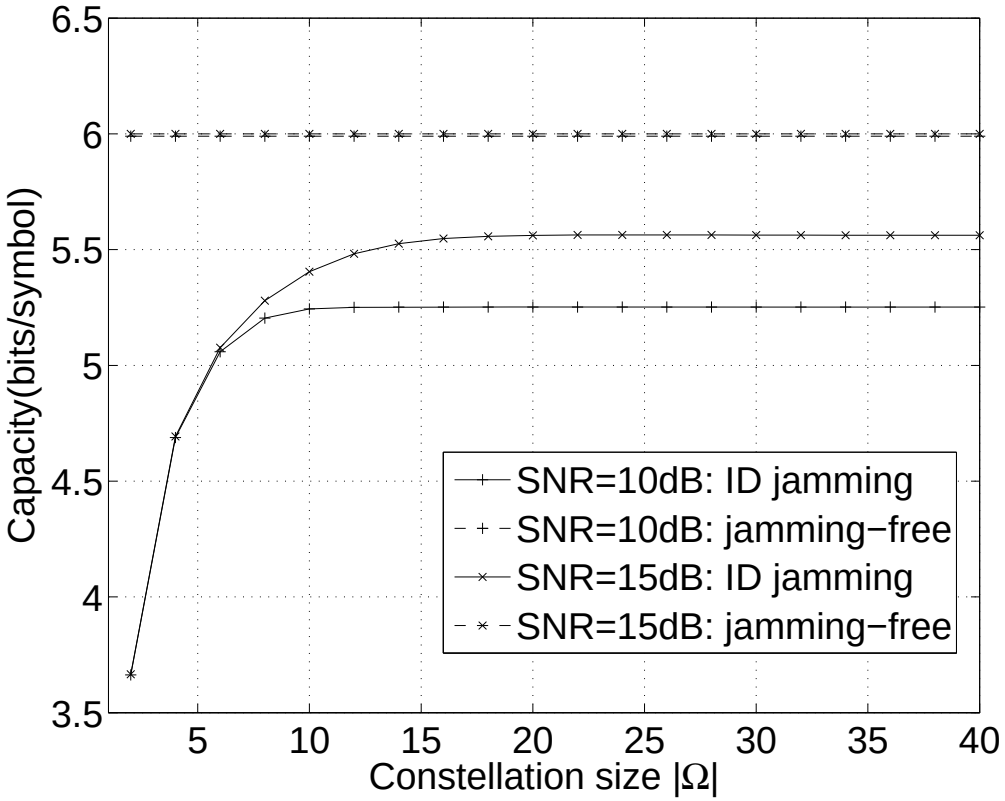


Figure 4.3: AJ-MDFH capacity with different PSK constellation size, under the worst case single band disguised jamming (ID jamming). $N_c = 64$.

Example 2: Capacity of the multiuser systems under ID jamming In this example, we choose MC-AJ-MDFH and FHMA as the multiuser systems for AJ-MDFH

and conventional FH, respectively, and consider the capacity of the two systems under the single band worst case disguised jamming [66, 101]. The SNR is taken as $E_b/N_0 = 10$dB and $T_h = 1$s. For FHMA, we choose $N_h = 3$; for MC-AJ-MDFH, we choose 32-PSK constellation. From Figure 3.10, it can be observed that due to the collision-free design and the use of ID sequence, under disguised jamming, MC-AJ-MDFH can effectively support much more users than FHMA, which is mainly limited by the collision effect among users.

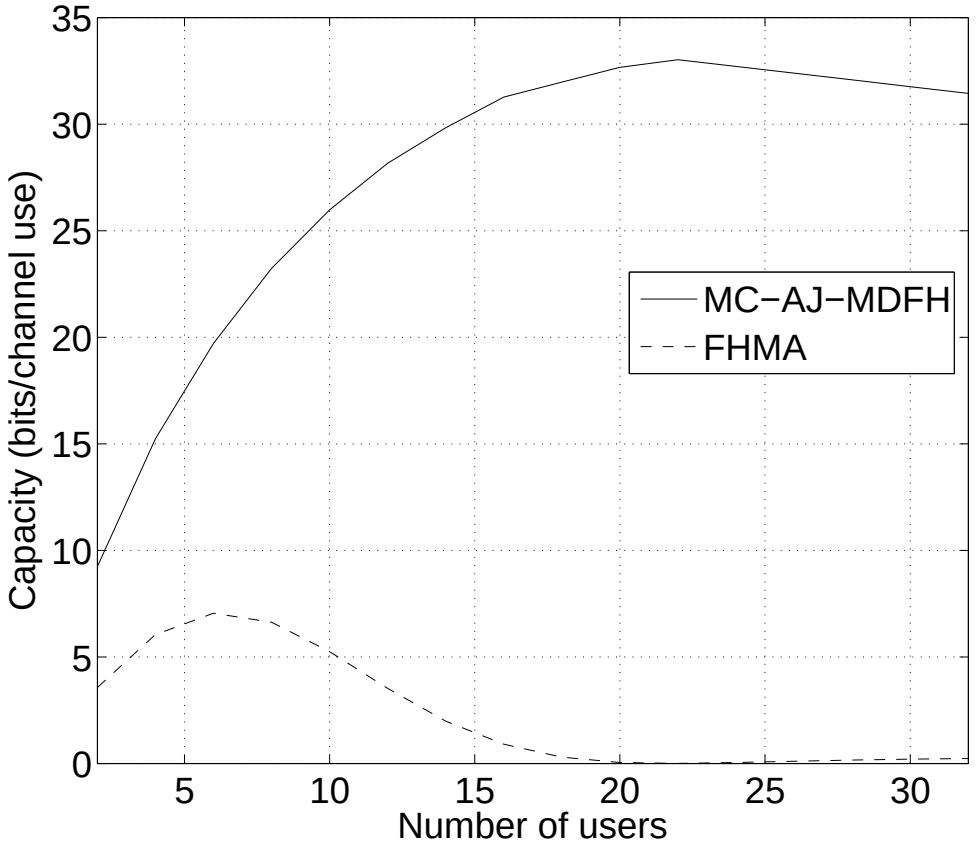


Figure 4.4: Capacity of MC-AJ-MDFH and FHMA under the worst case single band disguised jamming. $N_c = 64$, $SNR = 10$dB. Here, per channel use means the total bandwidth of all used channels over one hopping period.

Example 3: Capacity of AJ-MDFH and MDFH under worst case single band noise jamming Recall that in Section 3.2.2, it can be observed that the worst case noise jamming occurs when the noise and the signal has the same power, i.e., $\sigma_J^2 = P_s$. For

MDFH, we choose the uniform ring constellation (i.e., M-PSK when $M \to \infty$) [102]. for the upper bound analysis; for AJ-MDFH, we choose 32-PSK constellation for ID constellation. Figure 4.5 illustrates the capacity of AJ-MDFH and MDFH in this case. The capacity of AJ-MDFH under the worst case single band disguised jamming - ID jamming is also provided as comparison. It can be observed that AJ-MDFH outperforms the carrier/ordinary bits transmission channel of MDFH significantly under noise jamming. Recall that due to a symmetric kernel, MDFH has zero capacity under the worst case disguised jamming. However, it has positive capacity under noise jamming. It can also be observed that AJ-MDFH has a lager capacity under noise jamming comparing with that under ID jamming. Therefore, noise jamming is not as effective as disguised jamming in terms of using the given jamming power.

4.9 Summary

In this chapter, we analyzed that capacity of MDFH and AJ-MDFH under the worst case disguised jamming. We proved that: (i) For MDFH, the corresponding AVC is symmetric, which implies that the deterministic capacity of MDFH is zero; (ii) For AJ-MDFH, due to shared randomness between the transmitter and receiver provided by the secure ID sequence, the corresponding AVC is nonsymmetrizable, which implies that the deterministic capacity of AJ-MDFH is positive, and equal to the random code capacity. We calculated the capacity of AJ-MDFH and showed that it converges as the ID constellation size goes to infinity. This echoes our result in previous chapter, where we showed that the probability of error of AJ-MDFH converges as the ID constellation size goes to infinity. It can be observed that shared secure randomness between the transmitter and receiver plays a critical role in anti-jamming system design.

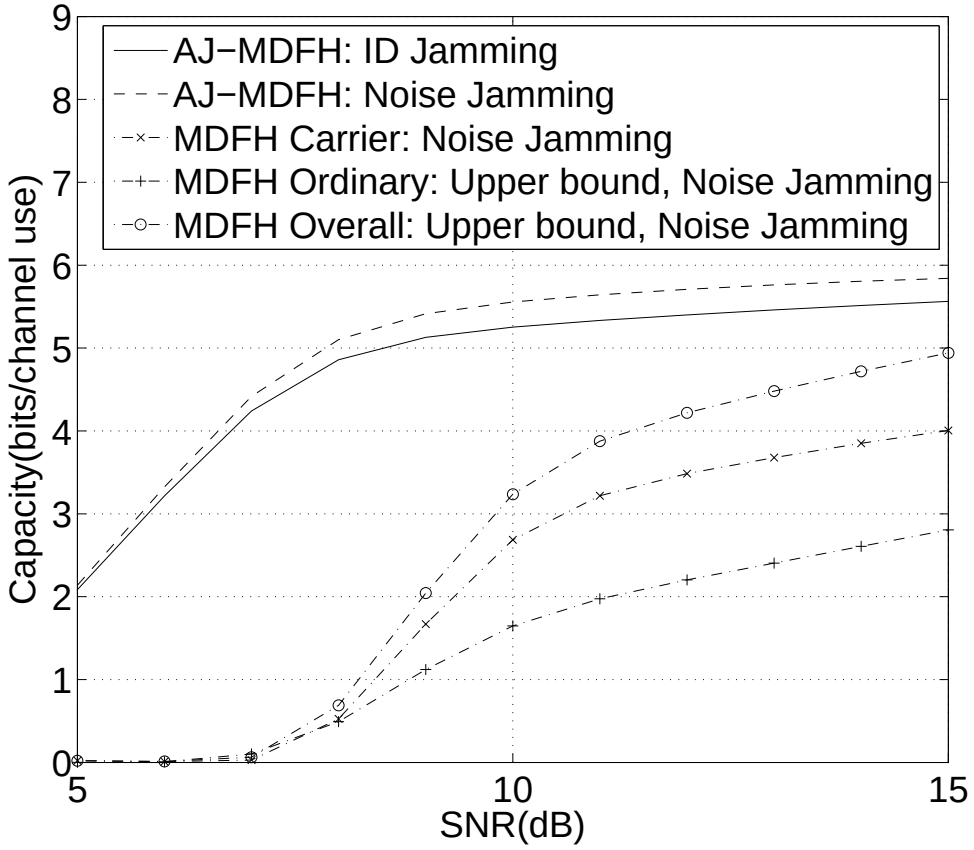


Figure 4.5: Capacity of AJ-MDFH and MDFH under the worst case single band noise jamming. For MDFH, upper bounds for capacity of the ordinary information transmission channel as well as for the overall channel capacity are provided. The number of hops per symbol period is $N_h = 3$.

4.10 Proofs of Chapter 4

4.10.1 Proof of Lemma 3

Proof of Lemma 3: Note that $\mathcal{X}$ can be partitioned into six subsets with respect to $\mathbf{x}_0 = \boldsymbol{\alpha} s$. Define $\mathcal{B}_1 \triangleq \{\boldsymbol{\alpha}\tilde{s}|\tilde{s} \in \Omega\}$, $\mathcal{B}_2 \triangleq \{\boldsymbol{\beta}\tilde{s}|\tilde{s} \in \Omega\}$ and $\mathcal{B}_3 \triangleq \{\boldsymbol{\alpha}_0\tilde{s}|\tilde{s} \in \Omega, \boldsymbol{\alpha}_0 \neq \boldsymbol{\alpha}, \boldsymbol{\beta}\}$. We have $\mathcal{X} = \cup_{i=1}^{3}\mathcal{B}_i$. It then follows from the definition of subset $\mathcal{X}_i$ in (4.42) that $\mathcal{B}_1 = \mathcal{X}_1 \cup \mathcal{X}_2$, $\mathcal{B}_2 = \mathcal{X}_3 \cup \mathcal{X}_4$, $\mathcal{B}_3 = \mathcal{X}_5 \cup \mathcal{X}_6$, and $\mathcal{X} = \cup_{i=1}^{6}\mathcal{X}_i$.

(i) We consider the cases where $\mathbf{y} \in \mathcal{X}_i, i = 1, 3$. When $\mathbf{y} \in \mathcal{X}_1$ ($\mathbf{y} = -\mathbf{x}_0$), the jamming cancels the true signal and the received signal only contains noise, resulting in

$W(\hat{\boldsymbol{\alpha}}_0|\mathbf{x}_0,-\mathbf{x}_0)=\frac{1}{N_c},\forall\hat{\boldsymbol{\alpha}}_0\in\mathcal{A}$. When $\mathbf{y}\in\mathcal{X}_3$ ($\mathbf{y}=\boldsymbol{\beta}s$), the jamming has the same ID symbol as the true signal and the receiver cannot distinguish between the two, resulting in $W(\boldsymbol{\alpha}|\mathbf{x}_0,\boldsymbol{\beta}s)=W(\boldsymbol{\beta}|\mathbf{x}_0,\boldsymbol{\beta}s)$. Hence, $W(\boldsymbol{\alpha}|\mathbf{x}_0,\mathbf{y})=W(\boldsymbol{\beta}|\mathbf{x}_0,\mathbf{y})$ holds in both cases.

(ii) When $\mathbf{y}\in\mathcal{X}_2$, we have $\mathbf{y}=\boldsymbol{\alpha}s_0$ where $s_0\in\Omega, s_0\neq -s$. Assuming $\boldsymbol{\alpha}=v(k)$, the received signal in the ith channel r_i and corresponding Z_i defined in (4.9) can be calculated as

$$r_i=\begin{cases} s+s_0+n_k, & i=k,\\ n_i, & i\neq k,\end{cases}\qquad Z_i=\begin{cases}\dfrac{\|s_0+n_k\|}{\sqrt{\|s+s_0\|^2+\sigma_n^2}}, & i=k,\\ \dfrac{\|n_i-s\|}{\sigma_n}, & i\neq k.\end{cases}\tag{4.135}$$

Then we have

$$\begin{aligned} W(\boldsymbol{\alpha}|\mathbf{x}_0,\mathbf{y}) &= Pr\{Z_k<Z_i,\forall i\in\mathcal{I}_c, i\neq k|\mathbf{x}_0,\mathbf{y}\}\\ &\geq 1-\sum_{i\neq k}Pr\{Z_k\geq Z_i|\mathbf{x}_0,\mathbf{y}\}\\ &= 1-(N_c-1)Pr\{Z_k\geq Z_{i_0}|\mathbf{x}_0,\mathbf{y}\},\end{aligned}\tag{4.136}$$

for any fixed $i_0\neq k$. Since $s_0\neq -s$, we have $\frac{n_{i_0}-s}{\sigma_n}\sim\mathcal{CN}(-\frac{s}{\sigma_n},1)$ and $\frac{s_0+n_k}{\sqrt{\|s+s_0\|^2+\sigma_n^2}}\sim\mathcal{CN}(\frac{s_0}{\sqrt{\|s+s_0\|^2+\sigma_n^2}},\frac{\sigma_n^2}{\sqrt{\|s+s_0\|^2+\sigma_n^2}})$. Define $S_1=\frac{1}{2}\|-\frac{s}{\sigma_n}\|^2=\frac{\gamma}{2}$, $N_1=\frac{1}{2}$ and $S_2=\frac{1}{2}\|\frac{s_0}{\sqrt{\|s+s_0\|^2+\sigma_n^2}}\|^2=\frac{P_s}{\|s+s_0\|^2+\sigma_n^2}$, $N_2=\frac{\sigma_n^2}{2(\|s+s_0\|^2+\sigma_n^2)}$. It then follows from the results in [87] that

$$Pr\{Z_k\geq Z_{i_0}|\mathbf{x}_0,\mathbf{y}\}=Q_1(\sqrt{C},\sqrt{D})-\frac{N_1}{N_1+N_2}e^{-\frac{C+D}{2}}I_0(\sqrt{CD})<Q_1(\sqrt{C},\sqrt{D}),\tag{4.137}$$

where $C=\frac{2S_2}{N_1+N_2}=\frac{2P_s}{\|s+s_0\|^2+2\sigma_n^2}$ and $D=\frac{2S_1}{N_1+N_2}=\frac{2P_s(\|s+s_0\|^2+\sigma_n^2)}{\sigma_n^2(\|s+s_0\|^2+2\sigma_n^2)}$. Since $D>C$, $Pr\{Z_k\geq Z_{i_0}|\mathbf{x}_0,\mathbf{y}\}\leq e^{-\frac{(D-C)^2}{2}}$ [103]. It then follows from (4.136) and $\|s+s_0\|\geq d_{\min}$ that

$$W(\boldsymbol{\alpha}|\mathbf{x}_0,\mathbf{y})>1-(N_c-1)\exp[-2(\frac{\gamma d_{\min}^2}{d_{\min}^2+2\sigma_n^2})^2],\tag{4.138}$$

and

$$W(\boldsymbol{\beta}|\mathbf{x}_0,\mathbf{y})=\frac{1}{N_c-1}[1-W(\boldsymbol{\alpha}|\mathbf{x}_0,\mathbf{y})]<\exp[-2(\frac{\gamma d_{\min}^2}{d_{\min}^2+2\sigma_n^2})^2].\tag{4.139}$$

Hence, we have

$$W(\boldsymbol{\alpha}|\mathbf{x}_0,\mathbf{y}) - W(\boldsymbol{\beta}|\mathbf{x}_0,\mathbf{y}) > 1 - N_c \exp[-2(\frac{\gamma d_{\min}^2}{d_{\min}^2 + 2\sigma_n^2})^2]. \tag{4.140}$$

Under the condition

$$\gamma > \sqrt{\frac{1}{2}\ln N_c} \text{ and } \frac{d_{\min}^2}{\sigma_n^2} > \frac{2\sqrt{\ln N_c}}{\sqrt{2}\gamma - \sqrt{\ln N_c}}, \tag{4.141}$$

$W(\boldsymbol{\alpha}|\mathbf{x}_0,\mathbf{y}) - W(\boldsymbol{\beta}|\mathbf{x}_0,\mathbf{y}) > 0$.

(iii) When $\mathbf{y} \in \mathcal{X}_4$, we have $\mathbf{y} = \boldsymbol{\beta} s_0$ where $s_0 \in \Omega, s_0 \neq s$. Note that $W(\boldsymbol{\alpha}|\mathbf{y},\mathbf{x}_0) = W(\boldsymbol{\beta}|\mathbf{x}_0,\mathbf{y})$. Since $\|s_0 - s\| \geq d_{\min}$, it follows from Proposition 2 that

$$W(\boldsymbol{\alpha}|\mathbf{x}_0,\mathbf{y}) - W(\boldsymbol{\beta}|\mathbf{x}_0,\mathbf{y}) \geq 1 - e^{-\frac{d_{\min}^2}{2\sigma_n^2}} - 2\epsilon. \tag{4.142}$$

Under the condition

$$\epsilon < \frac{1}{2} \text{ and } \frac{d_{\min}^2}{\sigma_n^2} > 2\ln\frac{1}{1-2\epsilon}, \tag{4.143}$$

$W(\boldsymbol{\alpha}|\mathbf{x}_0,\mathbf{y}) - W(\boldsymbol{\beta}|\mathbf{x}_0,\mathbf{y}) > 0$.

(iv) When $\mathbf{y} \in \mathcal{X}_5$, we have $\mathbf{y} = \boldsymbol{\alpha}_0 s$ where $\boldsymbol{\alpha}_0 \in \mathcal{A}, \boldsymbol{\alpha}_0 \neq \boldsymbol{\alpha}, \boldsymbol{\beta}$. It follows from Lemma 2 that $W(\boldsymbol{\alpha}|\mathbf{x}_0,\mathbf{y}) \geq \frac{1}{2} - \epsilon$. Note that $W(\boldsymbol{\alpha}|\mathbf{x}_0,\mathbf{y}) = W(\boldsymbol{\alpha}_0|\mathbf{x}_0,\mathbf{y})$, we have

$$W(\boldsymbol{\beta}|\mathbf{x}_0,\mathbf{y}) = \frac{1}{N_c - 2}[1 - 2W(\boldsymbol{\alpha}|\mathbf{x}_0,\mathbf{y})] \leq \frac{2\epsilon}{N_c - 2}. \tag{4.144}$$

Hence, we have

$$W(\boldsymbol{\alpha}|\mathbf{x}_0,\mathbf{y}) - W(\boldsymbol{\beta}|\mathbf{x}_0,\mathbf{y}) \geq \frac{1}{2} - \frac{N_c\epsilon}{N_c - 2}. \tag{4.145}$$

Under the condition

$$\epsilon < \frac{N_c - 2}{2N_c}, \tag{4.146}$$

$W(\boldsymbol{\alpha}|\mathbf{x}_0,\mathbf{y}) - W(\boldsymbol{\beta}|\mathbf{x}_0,\mathbf{y}) > 0$.

(v) When $\mathbf{y} \in \mathcal{X}_6$, we have $\mathbf{y} = \boldsymbol{\alpha}_0 s_0$ where $\boldsymbol{\alpha}_0 \in \mathcal{A}, \boldsymbol{\alpha}_0 \neq \boldsymbol{\alpha}, \boldsymbol{\beta}$ and $s_0 \in \Omega, s_0 \neq s$. It follows from Lemma 2 that

$$W(\boldsymbol{\alpha}|\mathbf{x}_0,\mathbf{y}) \geq 1 - \frac{1}{2}e^{-\frac{\|s_0 - s\|^2}{2\sigma_n^2}} - \epsilon. \tag{4.147}$$

Assuming $\boldsymbol{\alpha} = v(k)$ and $\boldsymbol{\alpha}_0 = v(k_0)$, it follows from Lemma 1 that

$$\begin{aligned} W(\boldsymbol{\alpha}_0|\mathbf{x}_0, \mathbf{y}) &\geq Pr\{Z_{k_0} < Z_k|\mathbf{x}_0, \mathbf{y}\} - (N_c - 2)Pr\{Z_{k_0} \geq Z_{i_0}|\mathbf{x}_0, \mathbf{y}\} \\ &= \frac{1}{2}e^{-\frac{\|s_0 - s\|^2}{2\sigma_n^2}} - \epsilon. \end{aligned} \tag{4.148}$$

Then we have

$$W(\boldsymbol{\beta}|\mathbf{x}_0, \mathbf{y}) = \frac{1}{N_c - 2}[1 - W(\boldsymbol{\alpha}|\mathbf{x}_0, \mathbf{y}) - W(\boldsymbol{\alpha}_0|\mathbf{x}_0, \mathbf{y})] \leq \frac{2\epsilon}{N_c - 2}. \tag{4.149}$$

Hence, we have

$$W(\boldsymbol{\alpha}|\mathbf{x}_0, \mathbf{y}) - W(\boldsymbol{\beta}|\mathbf{x}_0, \mathbf{y}) \geq 1 - \frac{1}{2}e^{-\frac{d_{\min}^2}{2\sigma_n^2}} - \frac{N_c\epsilon}{N_c - 2}. \tag{4.150}$$

Under the condition

$$\epsilon < \frac{N_c - 2}{N_c} \text{ and } \frac{d_{\min}^2}{\sigma_n^2} > -2\ln 2(1 - \frac{N_c\epsilon}{N_c - 2}), \tag{4.151}$$

$W(\boldsymbol{\alpha}|\mathbf{x}_0, \mathbf{y}) - W(\boldsymbol{\beta}|\mathbf{x}_0, \mathbf{y}) > 0$.

Next, we will show that the conditions in (4.141), (4.143), (4.146) and (4.151) can be reduced into the two conditions

$$\gamma > f^{-1}(\frac{1}{2N_c}) \text{ and } \frac{d_{\min}^2}{\sigma_n^2} > \max(\frac{2\sqrt{\ln N_c}}{\sqrt{2}\gamma - \sqrt{\ln N_c}}, 2\ln\frac{1}{1 - 2\epsilon}), \tag{4.152}$$

as presented in Lemma 3.

Step 1: Recall that $f(x) = \frac{1}{x+2}\exp\{-\frac{x(x+1)}{x+2}\}$, then

$$f'(x) = -\frac{x^2 + 5x + 4}{(x+2)^3}e^{-\frac{x(x+1)}{x+2}}. \tag{4.153}$$

Note that the SNR $\gamma > 0$, hence $f'(\gamma) < 0$, which implies that $f(\gamma)$ is a monotonically decreasing function. Therefore, when $\gamma > f^{-1}(\frac{1}{2N_c})$, we have $f(\gamma) < \frac{1}{2N_c}$, which implies that

$$\epsilon = \frac{N_c - 2}{\gamma + 2}\exp\{-\frac{\gamma(\gamma+1)}{\gamma+2}\} = (N_c - 2)f(\gamma) < \frac{N_c - 2}{2N_c}. \tag{4.154}$$

Step 2: We now show that $\epsilon < \frac{N_c-2}{2N_c}$ implies the following four conditions: $\epsilon < \frac{1}{2}$, $\epsilon < \frac{N_c-2}{N_c}$, $\gamma > \sqrt{\frac{1}{2}\ln N_c}$ and $\frac{d^2_{\min}}{\sigma_n^2} > -2\ln 2(1-\frac{N_c\epsilon}{N_c-2})$. First, when $\epsilon < \frac{N_c-2}{2N_c}$, it is obvious that $\epsilon < \frac{1}{2}$ and $\epsilon < \frac{N_c-2}{N_c}$. Next, we will show that when $\epsilon < \frac{N_c-2}{2N_c}$, we also have $\gamma > \sqrt{\frac{1}{2}\ln N_c}$. Consider $N_c > 2$ (i.e., $N_c \geq 3$). Note that $f(\gamma)$ is a monotonically decreasing function. Hence, $\gamma \geq f^{-1}(\frac{1}{6}) \approx 1.02$, which implies that $\gamma > 1$. Define $h(\gamma) \triangleq e^{2\gamma^2-\gamma} - \frac{\gamma+2}{2}$, then

$$h'(\gamma) = (4\gamma-1)e^{2\gamma^2-\gamma} - \frac{1}{2}, \tag{4.155}$$

$$h''(\gamma) = [(4\gamma-1)^2+4]e^{2\gamma^2-\gamma}. \tag{4.156}$$

Since $h''(\gamma) > 0$, then $h'(\gamma)$ is a monotonically increasing function. When $\gamma > 1$, $h'(\gamma) > h'(1) = 3\cdot e - \frac{1}{2} > 0$, which implies that $h(\gamma)$ is also a monotonically increasing function. Hence, $h(\gamma) > h(1) = e - \frac{3}{2} > 0$, which implies that $\frac{1}{\gamma+2}e^{-\gamma} > \frac{1}{2}e^{-2\gamma^2}$. Then we have

$$\frac{1}{2N_c} > \frac{1}{\gamma+2}e^{-\frac{\gamma(\gamma+1)}{\gamma+2}} > \frac{1}{\gamma+2}e^{-\gamma} > \frac{1}{2}e^{-2\gamma^2}, \tag{4.157}$$

which implies that $\gamma > \sqrt{\frac{1}{2}\ln N_c}$. Therefore, we proved that when $N_c > 2$, $\epsilon < \frac{N_c-2}{2N_c}$ implies $\gamma > \sqrt{\frac{1}{2}\ln N_c}$. Finally, when $\epsilon < \frac{N_c-2}{2N_c}$, we have $-2\ln 2(1-\frac{N_c\epsilon}{N_c-2}) < 0$. Hence, $\frac{d^2_{\min}}{\sigma_n^2} > -2\ln 2(1-\frac{N_c\epsilon}{N_c-2})$ holds automatically.

Hence, when $\gamma > f^{-1}(\frac{1}{2N_c})$ and $\frac{d^2_{\min}}{\sigma_n^2} > \max(\frac{2\sqrt{\ln N_c}}{\sqrt{2}\gamma-\sqrt{\ln N_c}}, 2\ln\frac{1}{1-2\epsilon})$, all the conditions in (4.141), (4.143), (4.146) and (4.151) are satisfied and $W(\boldsymbol{\alpha}|\mathbf{x}_0,\mathbf{y}) - W(\boldsymbol{\beta}|\mathbf{x}_0,\mathbf{y}) > 0$ for any $\mathbf{y} \in \mathcal{X}_i, i = 2,4,5,6$.

For M-PSK constellation with power P_s, we have $s = \sqrt{P_s}e^{j\frac{2\pi m_s}{M}}$ and $b = \sqrt{P_s}e^{j\frac{2\pi m_J}{M}}$ where $m_s, m_J \in [0, M-1]$. It is shown in Section 4.10.2 that $\|b-s\|^2 = 2P_s[1-\cos\frac{2\pi(m_s-m_J)}{M}]$ and $\frac{d^2_{\min}}{\sigma_n^2} = 2\gamma(1-\cos\frac{2\pi}{M})$. For large M, $\cos\frac{2\pi}{M} \approx 1-\frac{1}{2}(\frac{2\pi}{M})^2 = 1-\frac{2\pi^2}{M^2}$ and $\frac{d^2_{\min}}{\sigma_n^2} \approx \frac{4\pi^2}{M^2}\gamma$. Using this approximation, the condition $\frac{d^2_{\min}}{\sigma_n^2} > \frac{2\sqrt{\ln N_c}}{\sqrt{2}\gamma-\sqrt{\ln N_c}}$ can be

rewritten as

$$\gamma^2 - \sqrt{\frac{1}{2}\ln N_c}\gamma - \frac{M^2}{4\pi^2}\sqrt{2\ln N_c} > 0, \tag{4.158}$$

which holds when

$$\gamma > \frac{1}{2}\sqrt{\frac{1}{2}\ln N_c} + \frac{1}{2}\sqrt{\frac{1}{2}\ln N_c + \frac{M^2}{\pi^2}\sqrt{2\ln N_c}}. \tag{4.159}$$

Similarly, the condition $\frac{d_{\min}^2}{\sigma_n^2} > 2\ln\frac{1}{1-2\epsilon}$ can be rewritten as

$$e^{-\frac{2\pi^2}{M^2}\gamma} + \frac{2(N_c-2)}{\gamma+2}\exp\{-\frac{\gamma(\gamma+1)}{\gamma+2}\} < 1. \tag{4.160}$$

Define $f_1(x) \triangleq e^{-\frac{2\pi^2}{M^2}x} + \frac{2(N_c-2)}{x+2}\exp\{-\frac{x(x+1)}{x+2}\}$, then the condition in (4.160) holds when $\gamma > f_1^{-1}(1)$. Therefore, for a given PSK constellation of size M, the condition $\gamma > f^{-1}(\frac{1}{2N_c})$ and $\frac{d_{\min}^2}{\sigma_n^2} > \max(\frac{2\sqrt{\ln N_c}}{\sqrt{2}\gamma - \sqrt{\ln N_c}}, 2\ln\frac{1}{1-2\epsilon})$ can be reduced to one condition on SNR as

$$\gamma > \max[f^{-1}(\frac{1}{2N_c}), \frac{1}{2}\sqrt{\frac{1}{2}\ln N_c} + \frac{1}{2}\sqrt{\frac{1}{2}\ln N_c + \frac{M^2}{\pi^2}\sqrt{2\ln N_c}}, f_1^{-1}(1)]. \ \square \tag{4.161}$$

4.10.2 Calculation of the Probability Matrix W_1

Let $\mathbf{x} = \boldsymbol{\alpha}s$, $\mathbf{J} = \boldsymbol{\beta}b$ with $\boldsymbol{\alpha} = v(k), \boldsymbol{\beta} = v(j)$, and $k, j \in \mathcal{I}_c$, $s, b \in \Omega$. Assume Ω is an M-PSK constellation with power P_s.

(i) When $j = k$, the received signal in the ith channel r_i and corresponding Z_i defined in (4.9) can be calculated as

$$r_i = \begin{cases} s + b + n_k, & i = k, \\ n_i, & i \neq k, \end{cases} \quad Z_i = \begin{cases} \dfrac{\|b + n_k\|}{\sqrt{\|s+b\|^2 + \sigma_n^2}}, & i = k, \\ \dfrac{\|n_i - s\|}{\sigma_n}, & i \neq k. \end{cases} \tag{4.162}$$

Note that $n_1, \ldots, n_{N_c}$ are i.i.d. circularly symmetric Gaussian random variables of zero mean and variance σ_n^2. For any $s, b \in \Omega$, Z_k is a Rician random variable with PDF $p_{Z_k}(z_k) = \frac{z_k}{\sigma^2}e^{-\frac{z_k^2+\nu^2}{2\sigma^2}} I_0\left(\frac{z_k\nu}{\sigma^2}\right)$ for $0 \leq z_k < \infty$, where $\nu = \dfrac{\sqrt{P_s}}{\sqrt{\|s+b\|^2 + \sigma_n^2}}$ and $\sigma =$

$\frac{\sigma_n}{\sqrt{2(\|s+b\|^2+\sigma_n^2)}}$; for $i \neq k$, Z_i's are i.i.d. Rician random variables with PDF $p_{Z_i}(z_i) = \frac{z_i}{\sigma^2} e^{-\frac{z_i^2+\nu^2}{2\sigma^2}} I_0\left(\frac{z_i \nu}{\sigma^2}\right)$ for $0 \leq z_i < \infty$, where $\nu = \frac{\sqrt{P_s}}{\sigma_n}$ and $\sigma = \frac{1}{\sqrt{2}}$. We have

$$\begin{aligned}
W_1 \quad & (k|k,k) \\
= \quad & \frac{1}{|\Omega|^2} \sum_{s\in\Omega} \sum_{b\in\Omega} Pr\{Z_k < Z_i, \forall i \in \mathcal{I}_c, i \neq k | \mathbf{x} = \boldsymbol{\alpha} s, \mathbf{J} = \boldsymbol{\beta} b\} \\
= \quad & \frac{1}{|\Omega|^2} \sum_{s\in\Omega} \sum_{b\in\Omega} \int_0^\infty \prod_{1\leq i\leq N_c, i\neq k} Pr\{Z_i > z_k | \mathbf{x}, \mathbf{J}, z_k\} p_{Z_k}(z_k) dz_k \\
= \quad & \frac{1}{|\Omega|^2} \sum_{s\in\Omega} \sum_{b\in\Omega} \int_0^\infty \left[Q_1\left(\frac{\sqrt{2P_s}}{\sigma_n}, \sqrt{2} z_k\right)\right]^{N_c-1} \frac{2(\|s+b\|^2+\sigma_n^2) z_k}{\sigma_n^2} \\
& \cdot e^{-\frac{(\|s+b\|^2+\sigma_n^2) z_k^2 + P_s}{\sigma_n^2}} I_0\left(\frac{2z_k}{\sigma_n^2}\sqrt{P_s(\|s+b\|^2+\sigma_n^2)}\right) dz_k, \qquad (4.163)
\end{aligned}$$

where Q_1 is the Marcum-Q function and I_0 is the modified Bessel function of the first kind with order zero. For M-PSK constellation with power P_s, we have $s = \sqrt{P_s} e^{j\frac{2\pi m_S}{M}}$ and $b = \sqrt{P_s} e^{j\frac{2\pi m_J}{M}}$ where $m_s, m_J \in [0, M-1]$, then (4.163) can be simplified as

$$\begin{aligned}
W_1(k|k,k) \quad = \quad & \frac{1}{M} \sum_{\kappa=0}^{M-1} \int_0^\infty \left[Q_1\left(\frac{\sqrt{2P_s}}{\sigma_n}, \sqrt{2} z_k\right)\right]^{N_c-1} \\
& \cdot \frac{2[2P_s(1+\cos\frac{2\pi\kappa}{M})+\sigma_n^2] z_k}{\sigma_n^2} e^{-\frac{[2P_s(1+\cos\frac{2\pi\kappa}{M})+\sigma_n^2] z_k^2 + P_s}{\sigma_n^2}} \\
& \cdot I_0\left(\frac{2z_k}{\sigma_n^2}\sqrt{P_s[2P_s(1+\cos\frac{2\pi\kappa}{M})+\sigma_n^2]}\right) dz_k, \qquad (4.164)
\end{aligned}$$

where $\kappa \triangleq (m_s - m_J) \mod M$ is uniformly distributed over $[0, M-1]$. Since Z_i's are i.i.d. $\forall i \in \mathcal{I}_c, i \neq k$, then

$$W_1(i|k,k) = \frac{1}{N_c - 1}[1 - W_1(k|k,k)], \quad \forall i \in \mathcal{I}_c, i \neq k. \qquad (4.165)$$

We have **(P1)**: $W_1(k|k,k)$ and $W_1(i|k,k)$ are fixed values for any $i, k \in \mathcal{I}_c, i \neq k$.

(ii) When $j \neq k$, the received signal r_i and corresponding Z_i can be calculated as

$$r_i = \begin{cases} s + n_k, & i = k, \\ b + n_j, & i = j, \\ n_i, & i \neq j, k, \end{cases} \qquad Z_i = \begin{cases} \dfrac{\|n_k\|}{\sqrt{P_s + \sigma_n^2}}, & i = k, \\ \dfrac{\|b - s + n_j\|}{\sqrt{P_s + \sigma_n^2}}, & i = j, \\ \dfrac{\|n_i - s\|}{\sigma_n}, & i \neq j, k. \end{cases} \tag{4.166}$$

For any $s, b \in \Omega$, Z_k is a Rayleigh random variable with PDF $p_{Z_k}(z_k) = \dfrac{z_k}{\sigma^2} e^{-\frac{z_k^2}{2\sigma^2}}$, where $\sigma = \dfrac{\sigma_n}{\sqrt{2(P_s + \sigma_n^2)}}$; Z_j is a Rician random variable with PDF $p_{Z_j}(z_j) = \dfrac{z_j}{\sigma^2} e^{-\frac{z_j^2 + \nu^2}{2\sigma^2}} I_0\left(\dfrac{z_j \nu}{\sigma^2}\right)$, where $\nu = \dfrac{\|b - s\|}{\sqrt{P_s + \sigma_n^2}}$ and $\sigma = \dfrac{\sigma_n}{\sqrt{2(P_s + \sigma_n^2)}}$; for $i \neq j, k$, Z_i's are i.i.d. Rician random variables with PDF $p_{Z_i}(z_i) = \dfrac{z_i}{\sigma^2} e^{-\frac{z_i^2 + \nu^2}{2\sigma^2}} I_0\left(\dfrac{z_i \nu}{\sigma^2}\right)$, where $\nu = \dfrac{\sqrt{P_s}}{\sigma_n}$ and $\sigma = \dfrac{1}{\sqrt{2}}$. Then, $W_1(k|k, j)$ can be calculated as

$$\begin{aligned} W_1 \quad & (k|k, j) \\ = \quad & \frac{1}{|\Omega|^2} \sum_{s \in \Omega} \sum_{b \in \Omega} Pr\{Z_k < Z_j \text{ and } Z_k < Z_i, \forall i \in \mathcal{I}_c, i \neq k, j | \mathbf{x}, \mathbf{J}\} \\ = \quad & \frac{1}{|\Omega|^2} \sum_{s \in \Omega} \sum_{b \in \Omega} \int_0^\infty Pr\{Z_j > z_k | \mathbf{x}, \mathbf{J}, z_k\} \left[Pr\{Z_i > z_k | \mathbf{x}, \mathbf{J}, z_k\}\right]^{N_c - 2} p_{Z_k}(z_k) dz_k \\ = \quad & \frac{1}{|\Omega|^2} \sum_{s \in \Omega} \sum_{b \in \Omega} \int_0^\infty Q_1\left(\frac{\sqrt{2}}{\sigma_n}\|b - s\|, \frac{z_k \sqrt{2(P_s + \sigma_n^2)}}{\sigma_n}\right) \\ & \cdot Q_1^{N_c - 2}\left(\frac{\sqrt{2P_s}}{\sigma_n}, \sqrt{2} z_k\right) \frac{2 z_k (P_s + \sigma_n^2)}{\sigma_n^2} e^{-\frac{(P_s + \sigma_n^2) z_k^2}{\sigma_n^2}} dz_k, \\ = \quad & \frac{1}{M} \sum_{\kappa = 0}^{M-1} \int_0^\infty Q_1\left(\frac{2}{\sigma_n} \sqrt{P_s \left(1 - \cos\frac{2\pi\kappa}{M}\right)}, \frac{z_k \sqrt{2(P_s + \sigma_n^2)}}{\sigma_n}\right) \\ & \cdot Q_1^{N_c - 2}\left(\frac{\sqrt{2P_s}}{\sigma_n}, \sqrt{2} z_k\right) \frac{2 z_k (P_s + \sigma_n^2)}{\sigma_n^2} e^{-\frac{(P_s + \sigma_n^2) z_k^2}{\sigma_n^2}} dz_k, \end{aligned} \tag{4.167}$$

and

$$
\begin{aligned}
W_1 \quad & (j|k,j) \\
= \quad & \frac{1}{|\Omega|^2}\sum_{s\in\Omega}\sum_{b\in\Omega} Pr\{Z_j < Z_k \text{ and } Z_j < Z_i, \forall i \in \mathcal{I}_c, i \neq j,k | \mathbf{x}, \mathbf{J}\} \\
= \quad & \frac{1}{|\Omega|^2}\sum_{s\in\Omega}\sum_{b\in\Omega}\int_0^\infty Pr\{Z_k > z_j|\mathbf{x},\mathbf{J},z_j\}\left[Pr\{Z_i > z_j|\mathbf{x},\mathbf{J},z_j\}\right]^{N_c-2} p_{Z_j}(z_j)dz_j \\
= \quad & \frac{1}{|\Omega|^2}\sum_{s\in\Omega}\sum_{b\in\Omega}\int_0^\infty e^{-\frac{(P_s+\sigma_n^2)z_j^2}{\sigma_n^2}} Q_1^{N_c-2}\left(\frac{\sqrt{2P_s}}{\sigma_n}, \sqrt{2}z_j\right)\frac{2z_j(P_s+\sigma_n^2)}{\sigma_n^2} \\
& \cdot e^{-(\frac{P_s+\sigma_n^2}{\sigma_n^2}z_j^2 + \frac{\|b-s\|^2}{\sigma_n^2})} I_0\left(\frac{2z_j}{\sigma_n^2}\|b-s\|\sqrt{P_s+\sigma_n^2}\right)dz_j \\
= \quad & \frac{1}{M}\sum_{\kappa=0}^{M-1}\int_0^\infty e^{-\frac{(P_s+\sigma_n^2)z_j^2}{\sigma_n^2}} Q_1^{N_c-2}\left(\frac{\sqrt{2P_s}}{\sigma_n}, \sqrt{2}z_j\right)\frac{2z_j(P_s+\sigma_n^2)}{\sigma_n^2} \\
& \cdot e^{-[\frac{P_s+\sigma_n^2}{\sigma_n^2}z_j^2 + \frac{2P_s}{\sigma_n^2}(1-\cos\frac{2\pi\kappa}{M})]} I_0\left(\frac{2z_j}{\sigma_n^2}\sqrt{2P_s(1-\cos\frac{2\pi\kappa}{M})(P_s+\sigma_n^2)}\right)dz_j. \quad (4.168)
\end{aligned}
$$

Since Z_i's are i.i.d. for any $i \in \mathcal{I}_c, i \neq j,k$, then

$$
W_1(i|k,j) = \frac{1}{N_c-2}[1 - W_1(k|k,j) - W_1(j|k,j)], \quad i \in \mathcal{I}_c, i \neq j,k. \tag{4.169}
$$

We have **(P2)**: $W_1(k|k,j)$, $W_1(j|k,j)$ and $W_1(i|k,j)$ are fixed values for any $i,j,k \in \mathcal{I}_c, j \neq k, i \neq j,k$.

Chapter 5

CONCLUSIONS AND FUTURE WORKS

5.1 Conclusions

This dissertation considered secure and effective communication in wireless networks under hostile jamming attacks. First, we established a framework for the modeling and classification of cognitive jamming. Second, we proposed to enhance the spectral efficiency and security of spread spectrum system by by integrating advanced signal processing techniques and cryptographic techniques into the transceiver design. Finally, we analyzed the capacity of the proposed systems under an effective jamming scenario. More specifically, based on theoretical analysis and simulation results, we had the following conclusions:

On cognitive jamming modeling and classification:

- An innovative two-dimensional time-varying jamming model was proposed to characterize jamming signals in both time and frequency domain. It includes all the existing jamming models as special cases, and can be used to characterize and track time-variant jamming attacks.

- By examining the time-varying autocorrelation function and power spectral density, we introduced the concepts of time-varying jamming coherence time and time-frequency jamming coherence bandwidth. By comparing the jamming coherence time with the signal symbol period, we classified the jamming into fast jamming and slow jamming; By comparing the jamming coherence bandwidth with the signal bandwidth, we classified the jamming into flat jamming and frequency selective jamming.

- Based on relative power and correlation between the signal and the jamming, we introduced the concept of disguised jamming, which is complementary to the traditional strong jamming. It was observed that strong jamming may not always be the worst

case. Disguised jamming, which is highly correlated with the signal and had a similar power level, can be more harmful to the system, as it is more difficult to be detected and eliminated.

- Based on time-frequency analysis and approximation theory, we proposed algorithms for time-varying coherence time and time-frequency coherence bandwidth estimation for both stationary jamming and locally stationary jamming. It enables dynamic jamming pattern detection and is of great significance for adaptive transmission design.

On spectrally efficient anti-jamming system design:

- By embedding part of information into the process of hopping frequency selection, additional information transmission is achieved by MDFH with no extra cost on either bandwidth or power, which increases the system spectral efficiency by multiple times.

- MDFH has distinctive performance under strong jamming and disguised jamming: Under strong jamming, even if the signal is jammed, the power of the jammed signal is enhanced and hence increased the probability of correct detection. As a result, MDFH is particularly robust under *strong jamming* scenarios. When the system experiences *disguised jamming*, it is difficult for the MDFH receiver to distinguish jamming from the true signal, resulting in performance losses.

- To overcome the drawback of MDFH, we proposed the anti-jamming MDFH system, in which a secure ID sequence is transmitted along with the information stream. The ID sequence is generated through a cryptographic algorithm using the shared secret between the transmitter and the receiver, it is then exploited by the receiver for effective signal extraction. It was shown that AJ-MDFH can effectively reduce the performance degradation caused by disguised jamming, while remaining robust under strong jamming. AJ-MDFH also retained the high spectral efficiency of MDFH.

- We investigated ID constellation design and its impact on the performance of AJ-MDFH under both noise jamming and ID jamming. For ID jamming, it was shown that under the ideal case when the system is noise-free, increasing the ID constellation size can increase the ID uncertainty, and hence reduces the probability of error. When noise is present, we proved that the detection error probability converges as the constellation size goes to infinity. In other words, there exists a threshold, increasing the constellation size over the threshold would result in little improvement in error probability. This result justifies the use of practical, finite size constellations in AJ-MDFH.

- Single carrier AJ-MDFH was extended to multi-carrier AJ-MDFH (MC-AJ-MDFH). By exploiting secure group generation algorithm, MC-AJ-MDFH can increase the system efficiency and jamming resistance significantly through jamming randomization and enriched frequency diversity. Moreover, by assigning different carrier groups to different users, MC-AJ-MDFH can also be used as a collision-free multiple access system.

- By incorporating the cryptographic techniques and secure permutation scheme, we proposed a secure ID generation algorithm and a secure group generation algorithm to maximize the security of the proposed AJ-MDFH and MC-AJ-MDFH systems.

On capacity analysis of MDFH based systems under disguised jamming

- Using the AVC model, we showed that the AVC corresponding to MDFH is symmetric, which implies that the deterministic capacity of MDFH is zero.

- For AJ-MDFH, due to the shared randomness between the transmitter and receiver provided by the secure ID sequence, we proved that the corresponding AVC is non-symmetrizable, which implies that the deterministic capacity of AJ-MDFH is positive.

- We calculated the capacity of AJ-MDFH under ID jamming and showed that it converges as the ID constellation size goes to infinity. This echoed our result in AJ-MDFH

system design, where we showed that the probability of error of AJ-MDFH converges as the ID constellation size goes to infinity.

- We extended the capacity analysis to the multiuser AJ-MDFH system (MC-AJ-MDFH) and showed that it outperforms the multiple access scheme for conventional FH (FHMA).
- We observed that shared secure randomness between the transmitter and receiver plays a critical role in anti-jamming system design.

5.2 Future Work

We plan to extend our research in the following two directions.

5.2.0.1 Disguised Jamming Analysis under Different Wireless Systems

In this dissertation, it can be observed that disguised jamming can degrade the performance of MDFH significantly by mimicking the signal of legal user. To prevent the disguised jamming attack to other popular wireless systems such as OFDM and MIMO, it is essential to extend the disguised jamming research to these systems as well. The future research in disguised jamming can be extended to

- Identify and quantitatively characterize disguised jamming for different wireless systems.
- Analyze the performance of these systems under disguised jamming.
- Propose effective methods to combat disguised jamming for these systems.

5.2.0.2 Adaptive Transceiver Design under Cognitive Jamming

Based on the proposed cognitive jamming modeling and classification scheme, we will consider adaptive transceiver design under cognitive jamming. For this purpose, we will conduct

comprehensive performance analysis on DSSS system, collision-free FH system, MDFH system, OFDMA based collision-free FH system. Each system will be tested and analyzed under various jamming attacks. The transmitter can then be adjusted accordingly to achieve optimal jamming mitigation under cognitive jamming. Adaptive transceiver design will include

- Parameter adjustment or reconfiguration of a particular selected anti-jamming system.
- Cognitive switching among different types of anti-jamming systems.

APPENDIX

Appendix A

LIST OF ABBREVIATIONS AND ACRONYMS

3G	Third Generation
AES	Advanced Encryption Standard
AJ-MDFH	Anti-Jamming Message-Driven Frequency Hopping
AWGN	Additive White Gaussian Noise
AVC	Arbitrarily Varying Channel
BER	Bit Error Rate
BPF	BandPass Filter
BPSK	Binary Phase-Shift Keying
CDMA	Code Division Multiple Access
DPSK	Differential Phase-Shift Keying
DS-CDMA	Direct-Sequence Code Division Multiple Access
DSSS	Direct-Sequence Spread Spectrum
E-MDFH	Enhanced Message-Driven Frequency Hopping
FFH	Fast Frequency Hopping
FH	Frequency Hopping
FHMA	Frequency Hopping Multiple Access
FHSS	Frequency Hopping Spread Spectrum
FSK	Frequency-Shift Keying
IFFT	Inverse Fast Fourier Transform
ISI	Inter-Symbol Interference
JSR	Jamming-to-Signal Ratio
LFSR	Linear Feedback Shift Register
MAC	Medium Access Control

MAI	Multiple-Access Interference
MAP	Maximum A Posteriori
MC-AJ-MDFH	Multi-Carrier Anti-Jamming Message-Driven Frequency Hopping
MDFH	Message-Driven Frequency Hopping
MFSK	Multiple Frequency-Shift Keying
ML	Maximum Likelihood
MMSE	Minimum Mean Square Error
MUI	Multiuser Interference
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
QAM	Quadrature Amplitude Modulation
QPSK	Quadrature Phase-Shift Keying
SFH	Slow Frequency Hopping
SINR	Single-to-Interference-Noise Ratio
SNR	Signal-to-Noise Ratio
STFT	Short-Time Fourier Transform
WSS	Wide Sense Stationary

BIBLIOGRAPHY

BIBLIOGRAPHY

[1] G. Stuber, J. Barry, S. Mclaughlin, Y. Li, M. Ingram, and T. Pratt, "Broadband MIMO-OFDM wireless communications," *Proceedings of the IEEE*, vol. 92, no. 2, pp. 271–294, 2004.

[2] H. Sampath, S. Talwar, J. Tellado, V. Erceg, and A. Paulraj, "A fourth-generation MIMO-OFDM broadband wireless system: design, performance, and field trial results," *IEEE Communications Magazine*, vol. 40, no. 9, pp. 143 – 149, Sep. 2002.

[3] A. Ghosh, D. Wolter, J. Andrews, and R. Chen, "Broadband wireless access with WiMax/802.16: current performance benchmarks and future potential," *IEEE Communications Magazine*, vol. 43, no. 2, pp. 129–136, 2005.

[4] T. Teng, F. Sideco, and J. Rebello, "Mobile Handset Market Tracer," iSuppli, Tech. Rep., 2010. [Online]. Available: http://www.isuppli.com/Mobile-and-Wireless-Communications

[5] J. Allen and J. Wilson, "Securing a wireless network," in *Proceedings of the 30th annual ACM SIGUCCS conference on User services*. ACM, 2002, p. 215.

[6] M. Maxim and D. Pollino, *Wireless security*. McGraw-Hill Osborne Media, 2002.

[7] B. Potter, "Wireless security's future," *IEEE Security and Privacy*, vol. 1, no. 4, pp. 68–72, 2003.

[8] P. Ashley, H. Hinton, and M. Vandenwauver, "Wired versus wireless security: the Internet, WAP and iMode for E-Commerce." IEEE Computer Society, 2001, p. 0296.

[9] M. Frater, M. Ryan, and M. Ryan, *Electronic warfare for the digitized battlefield*. Artech House Publishers, 2001.

[10] A. Goldsmith and P. Varaiya, "Capacity of fading channels with channel side information," *IEEE Transactions on Information Theory*, vol. 43, no. 6, pp. 1986 –1992, Nov. 1997.

[11] R. Cheng and S. Verdu, "Gaussian multiaccess channels with ISI: capacity region and multiuser water-filling," *IEEE Transactions on Information Theory*, vol. 39, no. 3, pp. 773 –785, May 1993.

[12] R. Knopp and P. Humblet, "Information capacity and power control in single-cell multiuser communications," in *Proceedings of IEEE International Conference on Communications*, Jun. 1995.

[13] K. Witrisal, Y.-H. Kim, and R. Prasad, "A new method to measure parameters of frequency-selective radio channels using power measurements," *IEEE Transactions on Communications*, vol. 49, no. 10, pp. 1788 –1800, Oct. 2001.

[14] W. Jakes, "Microwave mobile communications," 1975.

[15] D. Godard, "Channel equalization using a kalman filter for fast data transmission," *IBM Journal of Research and Development*, vol. 18, no. 3, pp. 267–273, 1974.

[16] S. Qureshi, "Adaptive equalization," *Proceedings of the IEEE*, vol. 73, no. 9, pp. 1349–1387, 1985.

[17] 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, no. 2, pp. 340–349, 1994.

[18] D. Falconer, S. Ariyavisitakul, A. Benyamin-Seeyar, and B. Eidson, "Frequency domain equalization for single-carrier broadband wireless systems," *IEEE Communications Magazine*, vol. 40, no. 4, pp. 58–66, 2002.

[19] P. Schniter, "Low-complexity equalization of ofdm in doubly selective channels," *IEEE Transactions on Signal Processing*, vol. 52, no. 4, pp. 1002–1011, 2004.

[20] D. Kivanc, G. Li, and H. Liu, "Computationally efficient bandwidth allocation and power control for OFDMA," *IEEE Transactions on Wireless Communications*, vol. 2, no. 6, pp. 1150–1158, 2003.

[21] Q. Spencer, C. Peel, A. Swindlehurst, and M. Haardt, "An introduction to the multi-user MIMO downlink," *IEEE Communications Magazine*, vol. 42, no. 10, pp. 60–67, 2004.

[22] H. Sampath, P. Stoica, and A. Paulraj, "Generalized linear precoder and decoder design for MIMO channels using the weighted MMSE criterion," *IEEE Transactions on Communications*, vol. 49, no. 12, pp. 2198–2206, 2001.

[23] E. Dahlman, *3G evolution: HSPA and LTE for mobile broadband*. Academic Press, 2008.

[24] J. Zyren and W. McCoy, "Overview of the 3GPP long term evolution physical layer," *Freescale Semiconductor, Inc., white paper*, 2007.

[25] M. K. Simon, J. K. Omura, R. A. Scholtz, and B. K. Levitt, *Spread Spectrum Communications Handbook*. McGraw-Hill, 1994.

[26] D. Adamy, *Introduction to electronic warfare modeling and simulation*. Artech House Publishers, 2003.

[27] B. Levitt, "FH/MFSK performance in multitone jamming," *IEEE Journal on Selected Areas in Communications*, vol. 3, no. 5, pp. 627–643, 1985.

[28] 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.

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

[30] 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.

[31] 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.

[32] W. Stark, "Coding for frequency-hopped spread-spectrum communication with partial-band interference-part ii," *IEEE Transactions on Communications*, vol. 33, pp. 1045–1057, Oct. 1985.

[33] 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.

[34] 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.

[35] 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.

[36] A. Viterbi, "Spread spectrum communications: myths and realities," *IEEE Communications Magazine*, vol. 17, no. 3, pp. 11–18, 1979.

[37] R. Peterson, R. Ziemer, and D. Borth, *Introduction to spread-spectrum communications*. Prentice Hall, 1995.

[38] B. Lathi, *Modern digital and analog communication systems*, 3rd ed. Oxford University Press, 1995.

[39] 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, no. 3, pp. 436–446, 1982.

[40] L. Milstein, "Interference rejection techniques in spread spectrum communications," *Proceedings of the IEEE*, vol. 76, no. 6, pp. 657–671, 1988.

[41] S. Zhou, G. Giannakis, and A. Swami, "Digital multi-carrier spread spectrum versus direct sequence spread spectrum for resistance to jamming and multipath," *IEEE Transactions on Communications*, vol. 50, no. 4, pp. 643–655, 2002.

[42] J. Laster and J. Reed, "Interference rejection in digital wireless communications," *IEEE Signal Processing Magazine*, vol. 14, no. 3, pp. 37–62, 1997.

[43] S. Buzzi, M. Lops, and H. Poor, "Code-aided interference suppression for DS/CDMA overlay systems," *Proceedings of the IEEE*, vol. 90, no. 3, pp. 394–435, 2002.

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

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

[46] S. Verdu, *Multiuser detection*. Cambridge University Press, 1998.

[47] A. Duel-Hallen, J. Holtzman, and Z. Zvonar, "Multiuser detection for CDMA systems," *IEEE Personal Communications*, vol. 2, no. 2, pp. 46–58, 1995.

[48] T. Li, Q. Ling, and J. Ren, "A spectrally efficient frequency hopping system," in *Proceedings of IEEE Global Telecommunications Conference*, Nov. 2007, pp. 2997–3001.

[49] Q. Ling and T. Li, "Message-driven frequency hopping: Design and analysis," *IEEE Transactions on Wireless Communications*, vol. 8, no. 4, pp. 1773–1782, Apr. 2009.

[50] Q. Ling, J. Ren, and T. Li, "Spectrally efficient spread spectrum system design: message-driven frequency hopping," *Proceedings of IEEE International Conference on Communications*, pp. 4775–4779, May 2008.

[51] T. Ericson, "Exponential error bounds for random codes in the arbitrarily varying channel," *IEEE Transactions on Information Theory*, vol. 31, no. 1, pp. 42 – 48, Jan. 1985.

[52] R. Ahlswede, "Elimination of correlation in random codes for arbitrarily varying channels," *Probability Theory and Related Fields*, vol. 44, no. 2, pp. 159–175, 1978.

[53] I. Csiszar and P. Narayan, "The capacity of the arbitrarily varying channel revisited: Positivity, constraints," *IEEE Transactions on Information Theory*, vol. 34, no. 2, pp. 181–193, 1988.

[54] N. Pronios and A. Polydoros, "Jamming optimization in fully-connected, spread-spectrum networks," in *Proc. IEEE Military Commun. Conf.* IEEE, pp. 65–70.

[55] 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.

[56] R. Nikjah and N. Beaulieu, "On jamming capacity of general multiuser CDMA systems," in *Proc. IEEE Wireless Commun. Networking Conf.* IEEE, 2007, pp. 191–196.

[57] L. Zhang, H. Wang, and T. Li, "Jamming resistance reinforcement of message-driven frequency hopping," in *Proceedings of IEEE International Conference on Acoustics, Speech and Signal Processing*, Mar. 2010, pp. 3974 –3977.

[58] M. Priestley, "Evolutionary spectra and non-stationary processes," *Journal of the Royal Statistical Society. Series B*, pp. 204–237, 1965.

[59] ——, *Non-linear and non-stationary time series analysis.* Academic Press, 1988.

[60] R. Dahlhaus, "On the kullback-leibler information divergence of locally stationary processes," *Stochastic processes and their applications*, vol. 62, no. 1, pp. 139–168, 1996.

[61] S. Mallat, G. Papanicolaou, and Z. Zhang, "Adaptive covariance estimation of locally stationary processes," *Annals of Statistics*, vol. 26, no. 1, pp. 1–47, 1998.

[62] N. Saito and R. Coifman, "Local discriminant bases and their applications," *Journal of Mathematical Imaging and Vision*, vol. 5, no. 4, pp. 337–358, 1995.

[63] R. Coifman and M. Wickerhauser, "Entropy-based algorithms for best basis selection," *IEEE Transactions on Information Theory*, vol. 38, no. 2, pp. 713 –718, Mar. 1992.

[64] D. Manolakis, V. Ingle, and S. Kogon, *Statistical and adaptive signal processing.* Artech House, 2005, vol. 1.

[65] 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.

[66] A. Viterbi, "A processing-satellite transponder for multlple access by low rate mobile users," *IEEE Journal on Selected Areas in Communications*, Oct. 1978.

[67] M. Simon and A. Polydoros, "Coherent detection of frequency-hopped quadrature modulations in the presence of jamming–part I: QPSK and QASK modulations," *IEEE Transactions on Communications*, vol. 29, pp. 1644–1660, Nov. 1981.

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

[69] 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.

[70] K. Choi and K. Cheun, "Performance of asynchronous slow frequency-hop multiple-access networks with MFSK modulation," *IEEE Transactions on Communications*, vol. 48, no. 2, pp. 298–307, Feb. 2000.

[71] L.-L. Yang and L. Hanzo, "Overlapping M-ary frequency shift keying spread-spectrum multiple-access systems using random signal sequences," *IEEE Transactions on Vehicular Technology*, vol. 48, no. 6, pp. 1984–1995, Nov. 1999.

[72] 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, no. 1, pp. 16–29, Jan. 2000.

[73] J. Cho, Y. Kim, and K. Cheun, "A novel frequency-hopping spread-spectrum multiple-access network using M-ary orthogonal Walsh sequence keying," *IEEE Transactions on Communications*, vol. 51, no. 11, pp. 1885–1896, Nov. 2003.

[74] 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.

[75] Y. Kim, K. Cheun, and K. Yang, "A bandwidth-power efficient modulation scheme based on quaternary quasi-orthogonal sequences," *IEEE Communications Letters*, vol. 7, no. 7, Jul. 2003.

[76] *Advanced Encryption Standard*, FIPS-197, National Institute of Standards and Technology Std., Nov. 2001.

[77] J. Lee and L. Miller, "Error performance analyses of differential phase-shift-keyed/frequency-hopping spread-spectrum communication system in the partial-band jamming environments," *IEEE Transactions on Communications*, vol. 30, no. 5, pp. 943–952, May 1982.

[78] J. Kang and K. Teh, "Performance of coherent fast frequency-hopped spread-spectrum receivers with partial-band noise jamming and AWGN," *IEE Proc. Commun.*, vol. 152, no. 5, pp. 679–685, Oct. 2005.

[79] C. Esli and H. Delic, "Antijamming performance of space-frequency coding in partial-band noise," *IEEE Transactions on Vehicular Technology*, vol. 55, no. 2, pp. 466–476, Mar. 2006.

[80] L. Zhang, J. Ren, and T. Li, "Spectrally efficient anti-jamming system design using message-driven frequency hopping," in *Proceedings of IEEE International Conference on Communications*, Jun. 2009.

[81] T. Li, Q. Ling, and J. Ren, "Physical layer built-in security analysis and enhancement algorithms for CDMA systems," *EURASIP J. Wireless Commun. Networking*, vol. 2007, pp. Article ID 83 589, 7 pages, 2007.

[82] J. G. Proakis and M. Salehi, *Digital Communications*, 5th ed. New York: McGraw-Hill, 2008.

[83] M. Kuczma, *An Introduction to the Theory of Functional Equations and Inequalities: Cauchy's Equation and Jensen's Inequality*, 2nd ed. Springer, 2009.

[84] R. Viswanathan and K. Taghizadeh, "Diversity combining in FH/BFSK systems to combat partial band jamming," *IEEE Transactions on Communications*, vol. 36, no. 9, pp. 1062–1069, Sep. 1988.

[85] J. Lee, L. Miller, and Y. Kim, "Probability of error analyses of a BFSK frequency-hopping system with diversity under partial-band jamming interference–part II: Performance of square-law nonlinear combining soft decision receivers," *IEEE Transactions on Communications*, vol. 32, no. 12, pp. 1243–1250, Dec. 1984.

[86] L. Miller, J. Lee, and A. Kadrichu, "Probability of error analyses of a BFSK frequency-hopping system with diversity under partial-band jamming interference–part III: Performance of a square-law self-normalizing soft decision receiver," *IEEE Transactions on Communications*, vol. 34, no. 7, pp. 669–675, Jul. 1986.

[87] S. Stein, "Unified analysis of certain coherent and noncoherent binary communications systems," *IEEE Transactions on Information Theory*, vol. 10, no. 1, pp. 43–51, Jan. 1964.

[88] L. Zhang, H. Wang, and T. Li, "Anti-jamming message-driven frequency hopping: Part I – system design," *IEEE Transactions on Wireless Communications*, 2011, under review.

[89] D. Blackwell, L. Breiman, and A. Thomasian, "The capacities of certain channel classes under random coding," *The Annals of Mathematical Statistics*, pp. 558–567, 1960.

[90] I. Csiszar and J. Körner, *Information theory: coding theorems for discrete memoryless systems*. Academic press, 1981, vol. 244.

[91] I. Csiszár and P. Narayan, "Arbitrarily varying channels with constrained inputs and states," *IEEE Transactions on Information Theory*, vol. 34, no. 1, pp. 27–34, 1988.

[92] A. Lapidoth and P. Narayan, "Reliable communication under channel uncertainty," *IEEE Transactions on Information Theory*, vol. 44, no. 6, pp. 2148 –2177, Oct. 1998.

[93] A. Sarwate, "Robust and adaptive communication under uncertain interference," Technical Report No. UCB/EECS-2008-86, University of California at Berkeley, Tech. Rep., 2008.

[94] J. Daemen and V. Rijmen, *The Design of Rijndael: AES–the Advanced Encryption Standard*. Springer, 2002.

[95] J. Borden, D. Mason, and R. McEliece, "Some information theoretic saddlepoints," *SIAM journal on control and optimization*, vol. 23, p. 129, 1985.

[96] T. Basar and Y. W. Wu, "Solutions to a class of minimax decision problems arising in communications systems," *J. Optim. Theory Appl.*, vol. 51, pp. 375–404, Dec. 1986.

[97] T. Başar, "The gaussian test channel with an intelligent jammer," *IEEE Transactions on Information Theory*, vol. 29, no. 1, pp. 152–157, 1983.

[98] T. Başar and G. Olsder, *Dynamic noncooperative game theory*. Society for Industrial Mathematics, 1999, vol. 23.

[99] I. Stiglitz, "Coding for a class of unknown channels," *IEEE Transactions on Information Theory*, vol. 12, no. 2, pp. 189 – 195, Apr. 1966.

[100] T. Cover and J. Thomas, *Elements of information theory*. Wiley-Interscience, 2006.

[101] J. Goh and S. Maric, "The capacities of frequency-hopped code-division multiple-access channels," *IEEE Transactions on Information Theory*, vol. 44, no. 3, pp. 1204–1211, 1998.

[102] A. D. Wyner, "Bounds on communication with polyphase coding," *Bell Labs Technical Journal*, pp. 523 –559, Apr. 1966.

[103] M. Simon and M. Alouini, "Exponential-type bounds on the generalized marcum q-function with application to error probability analysis over fading channels," *IEEE Transactions on Communications*, vol. 48, no. 3, pp. 359 –366, Mar. 2000.