Resilient Waveform Design for OFDM-MIMO Communication Systems

Chowdhury M. R. Shahriar

Dissertation Submitted to the Faculty of
Virginia Polytechnic Institute and State University
in Partial Fulfillment of the Requirements for the Degree of

Doctor of Philosophy
in
Electrical Engineering

Thomas C. Clancy, Chair
Luiz A. DaSilva
Wenjing Lou
Jeffrey H. Reed
Yue Wang

September 11, 2015
Arlington, Virginia

Keywords: Physical-Layer Security, Communications Security, OFDM, MIMO, Jamming, Antijam, Equalization Attack, Pilot Attack, LTE, WiMAX

Resilient Waveform Design for OFDM-MIMO Communication Systems

Chowdhury M. R. Shahriar

ABSTRACT

This dissertation addresses physical layer security concerns, resiliency of the Orthogonal Frequency Division Multiplexing (OFDM) and the Multiple Input Multiple Output (MIMO) systems; the 'de-facto' air-interface of most wireless broadband standards including LTE and WiMAX. The major contributions of this dissertation are: 1) developing jamming taxonomy, 2) proposing OFDM and MIMO equalization jamming attacks and countermeasures, 3) developing antijam (AJ) MIMO systems, and 4) designing null space projected overlapped-MIMO radar waveform for spectrum sharing between radar and communications system.

First, we consider OFDM systems under various jamming attacks. Previous research is focused on jamming OFDM data transmissions. We focus on energy efficient attacks that can disrupt communication severely by exploiting the knowledge of target waveform. Specifically, these attacks seek to manipulate information used by the equalization algorithm to cause errors to a significant number of symbols, i.e., pilot tones jamming and nulling. Potential countermeasures are presented in an attempt to make OFDM waveform robust and resilient. The threats were mitigated by randomizing the location and value of pilot tones, causing the optimal attack to devolve into barrage jamming.

We also address the security aspects of MIMO systems in this dissertation. All MIMO systems need a method to estimate and equalize channel, whether through channel reciprocity or sounding. Most OFDM-based MIMO systems use sounding via pilot tones. Like OFDM attacks, this research introduces MIMO channel sounding attack, which attempts to manipulate pilot tones to skew the channel state information (CSI) at the receiver.

We describe methods of designing AJ MIMO system. The key insight is that many of the theoretical concepts learned from transmit beamforming and interference alignment (IA) in MIMO systems can be applied to the field of AJ and robust communications in the presence of jammers. We consider a realistic jamming scenario and provide a 'receiver-only' and a transmitter 'precoding' technique that allow a pair of two-antenna transceivers to communicate while being jammed by a malicious non-cooperative single-antenna adversary.

Finally, we consider designing a collocated MIMO radar waveform, which employs a new MIMO architecture where antenna arrays are allowed to overlap. This overlapped-MIMO radar poses many advantages including superior beampattern and improvement in SNR gain. We combine this radar architecture with a projection-based algorithm that allows the radar waveform to project onto the null space of the interference channel of MIMO communications system, thus enabling the coexistence of radar and communications system.

Dedication

To my loving family,
for unconditional support and encouragement

Acknowledgments

I owe my deepest gratitude to my adviser, Dr. T. Charles Clancy, for giving me the opportunity to work under him. I would like to thank him for his guidance, patience, and instruction. His valuable advice and guidance has helped me throughout my student life at Virginia Tech. This dissertation will not be in the shape as it is now without his constructive feedback.

I am also thankful to my Ph.D. committee members Professor Jeffrey H. Reed, Professor Luiz A. DaSilva, Professor Wenjing Lou, and Professor Yue Wang for their valuable time and feedback. I would also like to thank the post-doc trio (Dr. Shabnam Sodagari, Dr. Ravi Tandon and Dr. Ahmed Abdelhadi) who guided me during my Ph.D. research.

Last but not the least; I am grateful to my parents (Rafiqul Islam Chowdhury and Suraiya Begum), my sibling (Sonia Sohani Chowdhury), my wife (Dr. Mahin Khan), my daughter (Meera Muntaha Chowdhury), my relatives (grandfather Shafi-Uddin Ahmed, grandmother Latifa Begum, grandmother Ambia Khatun, uncle Mizanur Rahman, uncle Mostafizur Rahman, uncle Mahbubur Rahman, uncle Mushfiqur Rahman, aunt Sultana Parvin, and aunt Sabina Yasmin), my past mentors (Matiur Rahman, Zainul Abedin, Prabir Bhattacharya, and Dr. Steven Ellingson), and my bosom friends (Russel, Baki, Manju, Shanto, Tapu, Niaz, Tanvir, Salim, Dale, Amit, Rahat, Kamol, Dr. Fakhrul Alam, Dr. Rushad Faridi, Nighat Jahan Suzana, Mostafa Naquib Ahsan, Bashirul A. Polash, Dr. Shajedul Hasan, Dr. Mahmud Harun) for their patience and continuous support. Without them this work would have never come into reality.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 State of the Art

Modern wireless broadband communication systems require achieving and maintaining extremely high throughput using a limited bandwidth in order to accommodate the ever increasing demand for voice, video, and data. The Orthogonal Frequency Division Multiplexing (OFDM) modulation technique and associated Orthogonal Frequency Division Multiple Access (OFDMA) channel access mechanism have emerged as the frontrunner physical (PHY) layer waveform for modern wireless broadband communication systems. This is due to OFDM's high spectral efficiency, high achievable data rates, robustness to frequency-selective multipath fading, and low computational complexity.

The OFDM modulation scheme and associated OFDMA multiple access technique have become the primary technology used by the latest wireless broadband standards; both fixed and mobile wireless communications. Fixed wireless broadband over a short distance is provided by the standard called Wireless Local Area Network (WLAN), also known as Wi-Fi, which uses OFDM. Almost all the WLAN technologies based on the IEEE 802.11a, 802.11g, 802.11n, 802.11ac, and 802.11ad standards use OFDM. For fixed wireless broadband over

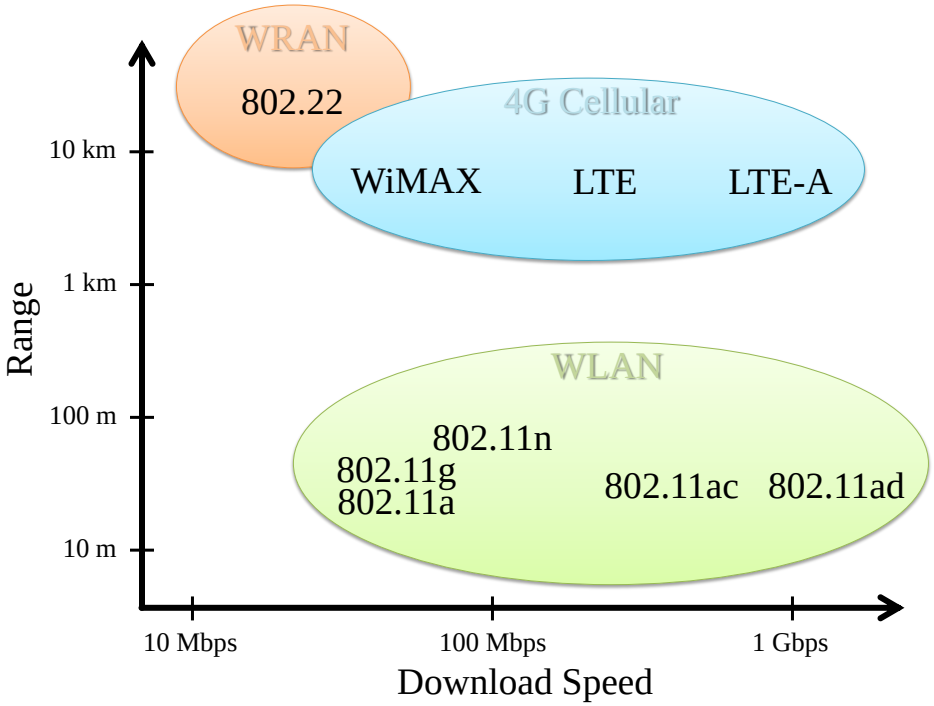

Figure 1.1: OFDM-based wireless broadband technologies, mapped according to typical range and data rate.

long distance, the IEEE 802.22 standard describes an OFDM-based Wireless Regional Area Network (WRAN) which utilizes white spaces in the TV frequency bands (also known as TV White Space). In terms of leading cellular broadband technologies, the most recent generation of mobile broadband standards including Long Term Evolution (LTE), LTE-Advanced and WiMAX (i.e., Metropolitan Area Network (WMAN), IEEE 802.16d, 802.16e, 802.16m) rely on OFDM for their air-interfaces. Figure 1.1 illustrates OFDM-based technologies used to provide wireless broadband over a variety of distances.

LTE is well on its way in becoming the primary commercial standard for mobile wireless broadband. LTE is gaining popularity all over the world because of its high speed communications at a rapidly reducing cost. The LTE standard is extensive and is in a state of continuing improvement by the Third Generation Partnership Project (3GPP). Releases 10 and higher of LTE correspond to the LTE-Advanced technology, which includes additional capabilities such as coordinated multipoint transmission and reception (CoMP), carrier ag-

gregation, self-organizing networks (SON), and more advanced multiple input and multiple output (MIMO) antenna schemes.

In addition to commercial use, LTE is the preferred technology for the United States' nationwide public safety network known as FirstNet, which is presently under development. The FirstNet network will comprise of dedicated LTE infrastructure in the 700 MHz band. In locations where dedicated infrastructure does not yet exist or congested, FirstNet devices will share commercial LTE networks. The use of LTE in FirstNet is an example of how LTE will play a role in mission-critical communications, which is why we should consider the security and information assurance aspects of LTE.

In recent years, MIMO systems have attracted attention in the wireless communications research community as they offer significant increase in capacity and link range without additional bandwidth or transmit power requirements. It achieves this by higher spectral efficiency, spatial multiplexing, and link reliability. Due to the nature of wireless channels, which encompasses multipath fading, MIMO technology is a robust tool toward enhancing the performance and reliability of wireless communications along with OFDM, in terms of throughput and spectral efficiency, by taking advantage of diversity (reduced fading).

In order to achieve the high throughput objective, MIMO systems are equally adopted as OFDM systems in the commercial communications industry. The best part is that they complement each other. The OFDM can be used in conjunction with MIMO transceiver to increase the diversity gain and/or the system capacity by exploiting spatial domain. Because the OFDM system effectively provides numerous parallel narrowband channels, jointly MIMO-OFDM is considered as a key technology in all the emerging high data rate standards mentioned earlier. The research, discussion, results included in this dissertation primarily involve OFDM/OFDMA and MIMO communications system.

1.2 Current Trend in Security

In this section, we discuss the current trend in security. At first we discuss physical (PHY) layer threats, then describe the details of transmission security (TRANSEC) in terms of low probability of detection (LPD), low probability of interception (LPI), and antijam (A/J).

1.2.1 PHY-Layer Threat Model

In this section, we discuss about the threats against communication systems, potential attackers, their goals, and capabilities. Often communication systems become subject of interest to malicious users or adversaries. The threat becomes even more imminent if the systems are used for tactical communications. The conventional notion of 'threat' means the actual destructive devices and systems. However, in electronic warfare (EW) cases, instead of tangible devices/systems, often the signals associated with the threat systems can be seen in action. That is why a signal associated with actual threat is often defined as threat [1]. There are three kinds of adversarial threats available for intervening and disrupting communication – 1) detection of signal, 2) interception of signal, and 3) jamming of signal.

Typically, the PHY-layer of communication systems is designed to be easily detectable, which is essential for user nodes to locate, join, and communicate in the network. The detections are carried out via preamble and/or cyclic prefix. As a result, the communication signals become prone to detection by the adversaries as well. The next level of threat comes from the interception of target signal by the adversary. The last option in EW is signal jamming by the adversary. The purpose of all the jamming is to interfere with target's effective use of electromagnetic spectrum. The basic technique of jamming is to place an interfering signal into target receiver along with desired signal. In jamming situations, the adversaries send high power noise or other modulated/structured signal that can disrupt communication and may result in loss of communication (i.e., denial of services (DoS)) [1–3].

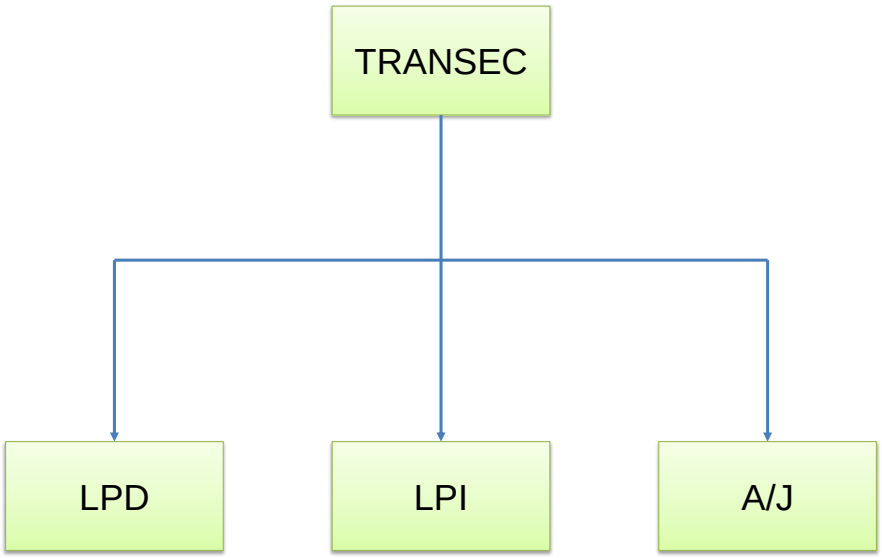

Figure 1.2: Types of transmission securities (TRANSEC) available.

1.2.2 Transmission Security (TRANSEC)

In this section, we discuss transmission security (TRANSEC) in detail and present the common security measures such as low probability of detection (LPD), low probability of interception (LPI), and antijam (A/J) techniques. Figure 1.2 shows types of transmission securities (TRANSEC) available.

1.2.2.1 Low Probability of Detection(LPD)

Classically, the techniques of identifying the presence of energy are known as signal detection theory [4]. According to the theory, there are a number of determiners of how a detection system will detect a signal and where its threshold levels will be. Identifying signal energy is a function of long-term averaging and is easier if the target signal has higher signal-to-noise ratio (SNR). The design goal of *low probability of detection* (LPD) systems is to hide the signal somehow so that a malicious user or adversary finds it difficult to deter-

mine that the signal is even present [3]. Two key approaches for designing signal with *low probability of detection* (LPD) are – 1) designing signal with lower power (wide band), i.e., direct sequence spread spectrum (DS-SS), and 2) designing signal with short duration such as ultra-wideband (UWB) signal. The reason for DS-SS signal to be a LPD signal is that it spreads its energy in wider bandwidth to make it difficult to detect. A third approach would be hiding the signal energy from plain sight or making it look like noise or something else in the environment [2].

1.2.2.2 Low Probability of Interception (LPI)

The definition of 'interception' varies and generally revolves around the answer of the following two questions - 1) can anyone differentiate the energy from noise and/or 2) can anyone synchronize/demodulate the signal? In order to 'intercept' a signal, we need to be able to identify the signal structure and dig into it to begin pulling apart its components [2]. By all means, the first step for ensuring TRANSEC is to make the signal of interest as a LPD one. However, if it cannot be achieved for some reason, the alternate is to make the signal difficult to intercept. This is referred to as *low probability of interception* (LPI). By structure, LPI signals are puzzling to the adversaries attempting to detect them. The basic LPI search techniques always encompass optimization of intercept bandwidth. For the *low probability of interception* (LPI) approach, the signal design objective is to seek a way to pseudo-randomly whiten the signal to make its features statistically difficult to intercept [3]. Typically, both communications and radar signals are considered LPI signals. Most prominent interception avoiding or LPI technologies are frequency hopping spread spectrum (FH-SS) and DS-SS signals [2]. The reason for frequency hopping signal to be a LPI signal is that it frequently hops in time and the amount of time it occupies a specific frequency is too short for an adversary to intercept.

1.2.2.3 Antijam (A/J)

The attempt of degrading and/or denying target communication systems is known as jamming and is a common practice in EW. There are diverse types of jamming threats, especially in tactical communications scenarios. Traditional jammers seek to blindly decrease the SNR of the target, whereas adaptive jammers attempt to manipulate structure in target signals. More recently, a new class of cognitive jammers appeared in the horizon that do so for previously unknown signals. The objective of antijam (A/J) signal is to design a signal that is either impossible or difficult to effectively jam by adversary. The traditional techniques used to achieve A/J signals are the same as those to achieve LPD and LPI, i.e., DS-SS and FH-SS [3].

1.3 Problem Statement

In recent years, the Federal Communications Commission (FCC) has freed up the 700 MHz band (running from $698-806$ MHz) as a result of the *Digital Television* transition and made it available for both commercial wireless and public safety communications [5]. The FCC has allocated portions of the 700 MHz band (24 MHz bandwidth) to establish a nationwide, interoperable wireless broadband communications network that will benefit state and local public safety authorities. The FCC then auctioned licenses to use the remaining 700 MHz band for commercial mobile broadband services for smartphones and other mobile devices. An important element of the 700 MHz public safety spectrum is the establishment of a framework for a 700 MHz public safety/private partnership between the licensee for one of the commercial spectrum blocks and the licensee for the public safety broadband spectrum [6]. Presence of multiple networks will require careful planning and may often become subject of interference from each other. On top of that, both, the dedicated public safety spectrum and the public safety/private partnership, shared commercial spectrum blocks may become

targets of malicious adversaries, making it even more important to look into the security issues of OFDM systems.

While OFDM is often celebrated for its robust performance in noise, fading channel, and uncorrelated interference, it has been shown that the current implementations of OFDM are susceptible to a variety of signal jamming attacks [7–10]. In fact, the United States military prohibits the use of Wireless MAN in such hostile environments [11], prompting development of specific transmission security (TRANSEC) extensions to the standard [12] for such scenarios.

One of the most important prerequisites for communicating using OFDM is synchronization between the transmitter and the receiver. Both, timing and frequency synchronization, are necessary in order to avoid inter-symbol interference (ISI), inter-carrier interference (ICI), and loss of orthogonality among OFDM subcarriers. While there has been research conducted on robustness of OFDM synchronization algorithms [13–22], the majority of this work has been conducted under the assumption of uncorrelated or narrowband interference. Recently, specific adversarial signals are introduced [8, 9], which are highly correlated and designed with the intent of disrupting the OFDM system during the synchronization stage. In his research, the author focused on jamming attacks that prevent a receiver employing OFDM from ever acquiring the proper symbol timing estimate. This work is based on the symbol timing and carrier frequency offset estimation algorithm designed by Schmidl and Cox [23]. This algorithm is the maximum likelihood detector for OFDM, and because of its optimality it is widely used in commercial systems based on OFDM.

When targeting a specific communications protocol, an efficient jamming attack can be realized by interfering with one subsystem of that protocol. This subsystem can take the form of a physical channel or physical signal; several of which are present in OFDM-based protocols. As long as the subsystem is vital to the operation of the link and the jamming signal is received at a high enough jammer-to-signal ratio (JSR), the denial of service (DoS)

is inflicted. Example PHY-layer subsystems include Hybrid Automatic Repeat Request (HARQ) acknowledgements, random access requests, and control channels. By targeting a subsystem that is sparse in both time and frequency (with respect to the entire downlink or uplink signal), an adversary can achieve a low duty cycle, low bandwidth, and low power jamming attack. Further research that involves attacks on protocols can be found in [24,25].

In this research we have explored various adversaries that OFDM communication systems may encounter. The coverage is not all-inclusive; however, most of the common approaches are discussed here. Barrage jamming (or broadband jamming) is the simplest and most intuitive of all the conventional jamming attacks and is also the optimum one when *a priori* knowledge about the target is unavailable [26]. Therefore, barrage jamming is used as the baseline for all the analysis presented in this paper. Another type of jamming attack for OFDM is partial-band jamming in which part of a wideband system is jammed intentionally [27–33]. In [32–36] the impact of partial-band jamming on OFDM-based broadband standards (e.g., Wi-Fi and WiMAX) is investigated. We also attempt to explore the possibilities of other power efficient jamming attack strategies such as 'asynchronous off-tone' jamming attack on OFDM systems.

In OFDM, the channel impulse response is estimated and equalized using known symbols called pilot tones. Various efficient jamming attacks which target these pilot tones used by OFDM communication systems have been derived in [7]. These attacks seek to manipulate information used by the equalization algorithm to cause errors to a significant number of symbols. The two attacks detailed are pilot tone jamming where attack values are independent and identically distributed (i.i.d.) and pilot tone nulling where pilot tone values are assumed to be known and inverted to cause destructive interference. While this is one aspect of OFDM which must be improved, it is not the only area of weakness to a sophisticated adversarial attack. The key aspect of this research is to find out the vulnerabilities of pilot tone-aided OFDM systems and proposing countermeasures to equalization attacks.

All MIMO systems need a method to estimate and equalize their channel, whether through channel reciprocity or sounding. And, most modern OFDM-based MIMO waveforms use sounding via OFDM pilot tones. However, like any communications system, MIMO channels have their own vulnerabilities in the presence of jamming. Previous research has focused on jamming data transmissions. Instead, we focus on jamming channel sounding symbols and introduce the MIMO 'singularity attack', which attempts to reduce the rank of the channel gain matrix estimate by the receiver through transmission of specific jamming signals. More specifically, we introduce and analyze the MIMO 'singularity attack' in which a multi-antenna jammer tries to manipulate pilot tones to skew the channel state information (CSI) obtained at the receiver. We prove singularity jamming can be more destructive than data jamming attacks, such as barrage jamming, by studying its effects on channel bit error rate and capacity. We develop the constraints associated with jamming MIMO sounding channels and further describe how these attacks specifically impact data symbol estimates for data-aided OFDM-MIMO sounding systems. Through simulation we demonstrate efficiency gains over barrage jamming. We also explore another kind anitjam MIMO scheme in this dissertation called 'spatial hiding precoding (SHP)'-based jam resistant MIMO systems.

The remarkable growth of data services via various broadband wireless access (BWA) resulted in scarcity of wireless bandwidth in recent years. This prompted government entities such as FCC and NTIA (National Telecommunications and Information Administration) to explore new options for bandwidth and also reassign underused spectrum. They are interested in sharing formerly used spectrum and reallocating some of the bandwidths that have been allotted to the Department of Defense (DoD) in the past. Recently in its 2010 Fast Track Report, NTIA proposed to share the $3550 - 3650$ MHz band between military radars and commercial BWA communication systems [37]. According to the NTIA report, this band is under-utilized and is favorable for BWA standards such as LTE to coexist with radars. However, the coexistence will require mitigation of electromagnetic interferences (EMI) from one to another. The broadband wireless nodes such as user devices and base-

Table 1.1: Specifications and characteristics of the jamming attacks

Attack	Type	Synch Required?	Strength	Weakness
Barrage Jam	Noise	None	Simplest, optimum in absence of waveform knowledge	Power inefficient, impractical for wideband systems
Pilot Jam	Correlated	Pilot location sych. needed	Power efficient, effective	Sensitive to pilot location
Pilot Null	Correlated	Pilot location sych. needed	Power efficient, effective, Denial of Service (DOS)	Sensitive pilot location, obtaining CSI may be difficult
Channel Sounding Jam	Correlated	Pilot location sych. needed	Power efficient, effective, DOS	Sensitive to pilot location, obtaining CSI may be difficult
CP Jam	Correlated	Frame start timing	Power efficient, effective, DOS	Sensitive to time alignment
off-tone jam	Colored	None	Asynchronous	Power inefficient

stations transmit on the order of microwatts and milliwatts, whereas radar waveform strength is typically in the megawatts! Hence, the coexisting scenario is primarily dominated by the radar EMI. Therefore, the focus of our research is to design radar waveform that reduces EMI to communication systems.

1.4 Contributions

This dissertation seeks to improve upon the state of the art in the OFDM-MIMO systems for wireless broadband communications. The objective is to develop new OFDM-MIMO waveforms that offer resiliency and robustness in the hostile environment.

In this dissertation, we investigate various jamming attacks against OFDM and MIMO communication systems. The objective is to explore the vulnerabilities of OFDM-MIMO systems. The key motivations for this research are: 1) developing various efficient jamming

strategies will enable us to jam OFDM and MIMO systems if they are used by the rival entities and 2) lesson learned from exposing vulnerabilities will enable us to propose modification to the OFDM-MIMO systems to transform them into a robust and resilient one.

In this research, we explore energy efficient jamming attacks against both MIMO and OFDM systems. We propose equalization jamming attacks, cyclic prefix (CP) jamming attacks and asynchronous off-tone jamming attacks. The complete list of jamming attacks introduced in this dissertation are:

- Pilot tone jamming-based equalization jamming attack against OFDM systems.
- Pilot tone nulling-based equalization jamming attack against OFDM systems.
- Channel sounding jamming-based equalization jamming attack against MIMO systems.
- Singularity (a.k.a. nulling)-based equalization jamming attack against MIMO systems.
- CP jamming attack against OFDM systems.
- CP nulling attack against OFDM systems.
- Asynchronous off-tone jamming attack against OFDM systems.

The single most important contribution of this research is equalization jamming attack against OFDM and MIMO systems. It is found that lesser power is needed for equalization attacks to create same BER at the target. For OFDM, it is found that, for 7 dB SJR and 12 dB SNR, the BERs are 0.08, 0.13, 0.42 for barrage jamming, pilot tone jamming and pilot tone nulling respectively. For MIMO channel sounding attacks, we found that channel sounding signal jamming outperforms barrage jamming by 1 dB and singularity attack outperforms barrage jamming by 3 dB at 0.3 BER. Another notable mention is attack of OFDM CP. We observe that, for SJR is 0 and 15 dB, the barrage jamming outperforms both CP jamming and CP nulling at lower SJR, but CP nulling outperforms the other two

at high SJR. With constant signal power, higher SJR implies less jammer power. As the jammer becomes less powerful, CP jamming achieves the upper hand over barrage jamming at high SNR. The Table 1.1 shows specifications and characteristics of the jammers presented in this dissertation.

In this dissertation, we also investigate the countermeasures of various jamming attacks against OFDM and MIMO communication systems. The objective is simple - as we investigate the vulnerabilities of OFDM-MIMO systems in the first half of this research, we now want to develop countermeasures to these attacks, so that the OFDM-MIMO waveform becomes robust and resilient. The key motivations for this research are as follows: 1) this robust and resilient MIMO-OFDM waveform can be used in public safety communication and 2) this robust and resilient MIMO-OFDM waveform can be used by the military in mission critical situations such as ad-hoc battle field communication network.

The mitigation strategies considered are not only limited to the attacks presented in this dissertation, but also covers generic jamming attacks. For example, pilot tone randomization schemes are against specific jamming attack called equalization jamming attack, whereas spatial hiding antijam schemes presented here countermeasures against any existing non-protocol-aware jamming attacks. The randomization of pilot tones and channel sounding signals, and spatial hiding precoding require modification of the transmitted waveform. On the other hand, CP antijamming mechanism and receiver-only spatial hiding method are processed in the receiver chain, the transmitted waveform remain unchanged in these cases. The pilot tone randomization in SISO-OFDM achieves about 10 dB SNR gain for SJR = 0 dB and BER = 0.1. The CP jamming countermeasure results about 6 dB SNR gain for SJR = 0 dB and BER = 0.1. The receiver-only spatial hiding AJ achieves BER = 0.1 for 5 dB SNR and JSR = 3 dB. Lastly, the transmitter percoding spatial hiding AJ achieves about 15 dB SNR gain for JSR = 3 dB dB and BER = 0.1. The Table 1.2 shows specifications and characteristics of the countermeasures presented in this dissertation.

Table 1.2: Specifications and characteristics of the countermeasures

	Pilot Tone Randomize	CP AJ	Spatial Hiding AJ
Against	Equalization attack	CP attack	Uncorrelated attack
Modify	Tx	Rx	Tx & Rx
Need CSI	No	No	Yes
Effect	Save Equalization	Restore CP	Improves BER
Works on	OFDM & MIMO	OFDM	MIMO

Our contributions to this area of research consist of the following elements:

- **Channel Estimation Error Model**: The bit error rate (BER) performance of the communication receiver depends on the quality of channel estimation, which is always subject to error under noise. In existing literature, this error is almost always modeled as zero-mean normal distribution. In this dissertation, we develop an alternate method to model the channel estimation error. In this method, we include two sources of error – 1) error caused by additive noise on pilot tones that propagates during channel interpolation and 2) error caused by channel approximation using finite number of points to visualize a continuous channel function. Chapter 2 (**OFDM Systems**) describes this methodology.

- **Adversarial Model and Jamming Taxonomy**: With the universal accessibility of software defined radio (SDR) technology for wireless communications, the difference between jamming in the electronic warfare (EW) sense and wireless cyber security attacks became ambiguous. In order to demarcate these notions in the quickly expanding arena of transmission security (TRANSEC) and communication security (COMSEC), we propose a jammer taxonomy to classify the theoretical behaviors and characteristics of communications jammers. In contrast to the historical perspective of classifying jammers by specific signal types, in this dissertation we categorize jammers by the information they possess and their capacity to act on it. Key jammer capabilities include whether or not the jammer is time correlated, protocol-aware, uses spoofing, and/or able to learn. Second tier characteristics include jammer parameters such as

relative bandwidth, duty-cycle, modulation, antenna pattern, and whether the antenna is steerable, etc. We then present sample jamming techniques that exist in literature and discuss how they fall into our proposed classification system. The adversarial model and the jamming taxonomy is described in Chapter 3 (**Adversarial Model**).

- **Equalization Jamming Attacks**: The OFDM systems use pilot tones to estimate the channel's frequency response and perform equalization. It is commonly known that jamming pilot tones is more efficient than broadband attacks against an entire OFDM waveform. This dissertation builds on this idea and introduces the pilot tone nulling attack, which is considerably more efficient than simple pilot tone jamming attack, by driving received pilot tone energy as close to zero as possible. In this dissertation, we present our channel and equalizer model and then undertake an analysis of OFDM under these attacks, verifying the assessment through simulation. The analysis of these power efficient jamming attacks and the results are described in Chapter 4 (**OFDM Equalization Jamming Attacks**).

- **Countermeasures to Equalization Jamming Attacks**: In previous research, we explored the concept of pilot tone-based jamming attacks on OFDM systems including pilot tone nulling attacks, which are more power efficient than broadband jamming and can cause severe signal degradation. We built on this idea, and propose approaches to mitigate the effect of such jamming attacks by randomizing pilot tone locations. In the proposed schemes, pilot tone locations are not deterministic, but random variables. We present analysis that show the impact of randomizing pilot tone locations on OFDM equalizer performance. Effective additive noise per symbol for randomized pilot tone location is analytically derived and receiver performance is verified by Monte Carlo simulation. The analysis of these countermeasures and the results are described in Chapter 5 (**OFDM Equalization Jamming Attack Countermeasures**).

- **MIMO Channel Sounding Attacks & Countermeasures**: In recent years, the

MIMO antenna systems attracted attention in wireless communications research community as they offer significant growth in capacity and link range without additional bandwidth or transmit power requirements. The MIMO-OFDM waveform is the 'de-facto' waveform for most of the advanced wireless network standards. We investigated power efficient channel sounding jamming attacks against MIMO-OFDM antenna systems that we named 'singularity attack'. We also explore the effects of such jamming attacks when there are synchronization mismatches. Lastly, we propose countermeasures to this attack. Detailed descriptions are provided in Chapter 6 (**MIMO Channel Sounding Attacks & Countermeasures**).

- **Spatial Hiding Antijam (AJ) Communications**: The transmit beamforming and the interference alignment (IA) in MIMO antenna systems can be applied to the field of antijam (AJ) to develop robust MIMO communication systems. We consider a realistic jamming scenario and provide a 'receiver-only' processing technique and a 'precoding' technique at the transmitter that allow a pair of two-antenna transceivers to communicate while being jammed by a malicious non-cooperative single-antenna adversary. The first method is a receiver-side zero-forcing (ZF) decoder that aligns the received signal to be orthogonal to the jammer. The second method utilizes the most favorable spatial dimension that is also orthogonal to the jammer and requires precoding at the transmitter. The novelty introduced in this work is both the application of transmit spatial beamforming to AJ communications and a specific method that allows a simple implementation to be practically employed. The description of the proposed AJ schemes are given in Chapter 7 (**Spatial Hiding Antijam (AJ) Communications**).

- **New Radar Waveform Design for Spectrum Sharing**: We introduce a new formulation of MIMO radar that we call 'overlapped-MIMO' radar where the transmit array is partitioned into a number of subarrays that are allowed to overlap. We derive an analytical model of the architecture to establish the validity of our proposal.

Through numerical results and simulation, we show that this architecture results in better sidelobe suppression than conventional radars, which improves the coexistence between radar and communication systems. We extend the projection-based spectrum sharing scenario of [38] between MIMO radar and communications system to spectrum sharing between overlapped-MIMO radar and communications system. This extension gives rise to a different coexistence scenario as the overall beampattern of this radar waveform is significantly different from conventional MIMO radar. We also analyze the performance in terms of SNR gain. The design concept is described in Chapter 8 (**Overlapped-MIMO Radar Waveform Design for Spectrum Sharing**).

- **Asynchronous Off-tone Jamming**: In this dissertation, we present a power efficient 'asynchronous off-tone' jamming attacks on OFDM systems. It is known that signal with frequency offset can affect more spectrum than the occupied bandwidth as the signal energy gets smeared into adjacent spectrum while performing FFT operation in the OFDM receiver, and thus create inter-channel interference (ICI). We begin with this idea to build the new asynchronous single off-tone and asynchronous multiple off-tone jamming attacks on OFDM systems. Through analysis and simulation, we show that the off-tone jamming attacks have more adverse effect than jammer aligned with the received signal. The details of this jamming strategy is described in Chapter 3.

- **Cyclic Prefix Jamming Attacks & Countermeasures**: The OFDM systems use Cyclic Prefix (CP) to mitigate inter-symbol interference (ISI) and inter-channel interference (ICI). The use of CP guarantees circular convolution of the channel impulse response with the transmitted symbols. This results in simple one-tap equalization in the receiver by removing ICI. In power constraint situations, CP attacks can be particularly suitable. We also present two methods to counter the CP attacks. The details description of CP attacks and countermeasures are presented in Chapter 4 and Chapter 5, respectively.

1.5 Organization

In Chapter 1, we present a general discussion about the current state of the art, current trend in security, problem statement, and contributions. The rest of this dissertation is organized as follows. Chapter 2 discusses the basic theories of OFDM systems. In Chapter 3, we present theories of existing jamming attacks (i.e., adversarial model), robustness of OFDM systems, and our preliminary investigations required for future research. In Chapter 4, we propose various equalization jamming attacks against OFDM systems such as pilot tone jamming, pilot tone nulling, and cyclic prefix jamming attacks. In Chapter 5, we present countermeasures for OFDM equalization jamming attacks by randomizing pilot tone locations. In Chapter 6, we extend the knowledge gained from SISO-OFDM equalization attacks to MIMO-OFDM domain and tailor singularity jamming attacks as well as mitigation techniques. In Chapter 7, we present an AJ MIMO communications scheme based on spatial hiding precoding. In Chapter 8, we present spectrum sharing strategies between overlapped-MIMO Radar and MIMO communication systems. The findings of this research are summarized in Chapter 9, where suggestions for future work are also identified.

Chapter 2

OFDM Systems

In this chapter, we discuss the basics of the Orthogonal Frequency Division Multiplexing (OFDM) systems. In OFDM systems, many narrowband signals are multiplexed in the frequency-domain, then converted to time-domain and finally transmitted over wireless channel. Pilot tones are inserted in the transmitted signal to estimate and equalize the wireless channel impulse response. In the receiver, signals are converted back to frequency-domain by Fast Fourier Transform (FFT) operation for demodulation. From the frequency-domain signals, channel's frequency response is first estimated and then equalized to remove the effect of the channel using pilot tones over a series of symbols at specific time/frequency locations. The block diagram of an OFDM system and channel model is shown in Figure 2.1.

The remainder of this chapter is organized as follows. In Section 2.1, we describe a typical OFDM transmitter-receiver pair structure. Section 2.2 includes a fading channel model that typical OFDM systems faces. In Section 2.3, a brief description of the OFDM system's synchronization mechanism is presented. Section 2.4 describes the channel estimation and equalization process for the OFDM systems. In Section 2.5, we derive an alternate model for the OFDM channel estimation error. The last section, Section 2.6, is the summary, which sums up the features of the OFDM systems, and notes some possible applications.

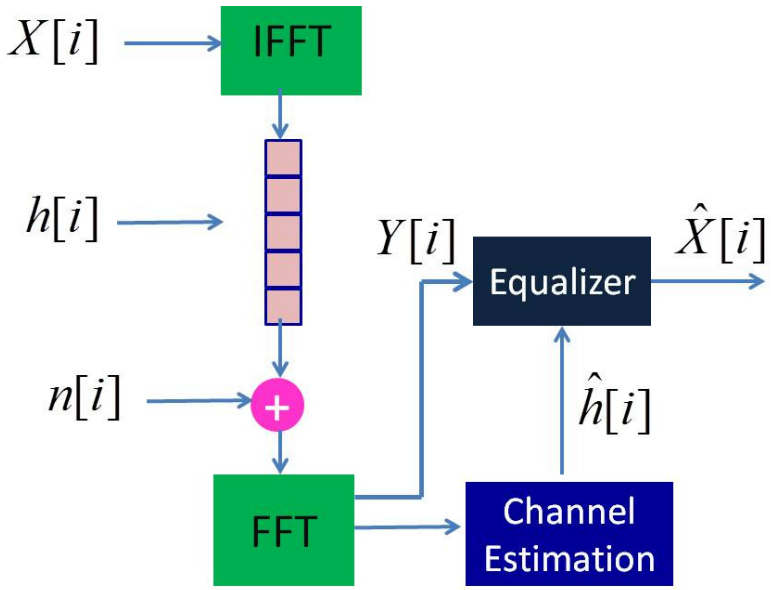

Figure 2.1: System diagram of an OFDM transmitter-receiver pair along with equalizer that is subject to multipath fading channel.

2.1 Transceiver

In an OFDM system, many narrowband signals are multiplexed in the frequency-domain (FD), converted to the time-domain (TD) and finally transmitted. At the appropriate sampling time, the corresponding discrete-time OFDM symbol at the transmitter can be expressed as

$$x_i[n] = \text{IFFT}\{X_i[k]\} = \sum_{k=0}^{N-1} X_i[k] e^{j\frac{2\pi kn}{N}} \quad n \leq N-1 \tag{2.1}$$

where $0 \leq k$ (kth subcarrier) and N is the number of subcarriers.

At the receiver, time-domain received signals are fed to the FFT block to be converted back to the frequency-domain for equalization and demodulation, and can be expressed as

$$Y_i[k] = \text{FFT}\{y_i[n]\} = \sum_{n=0}^{N-1} y_i[n] e^{-j\frac{2\pi kn}{N}}. \tag{2.2}$$

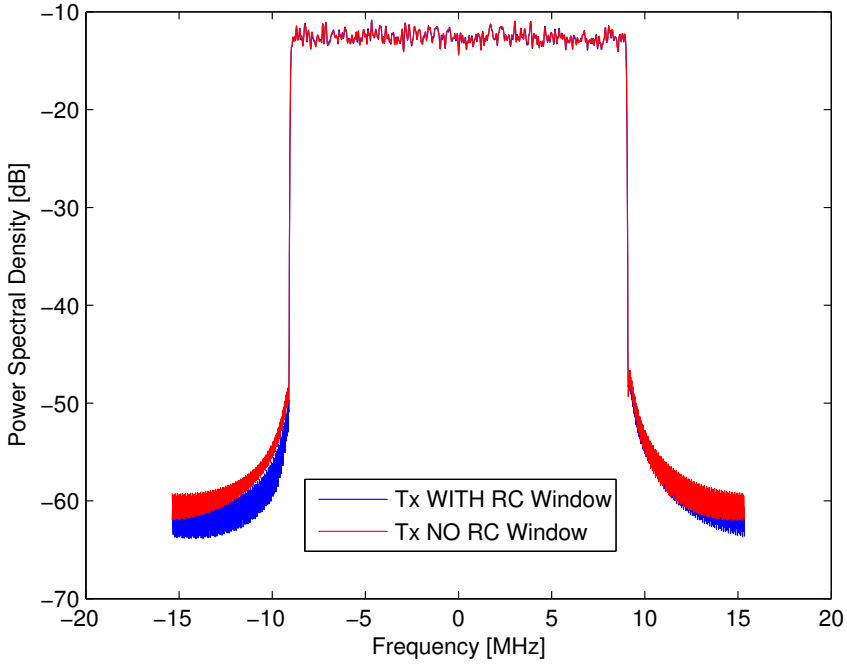

Figure 2.2: An example of a typical OFDM waveform in frequency-domain, which is based on LTE-FDD PHY-layer specification.

Figure 2.2 shows an example of a typical OFDM waveform in frequency-domain, which is based on LTE-FDD PHY-layer specification, where FFT size is 2048, sampling frequency is 30.72 MHz, allocated channel bandwidth is 20 MHz.

2.2 Channel

In this section, we present the OFDM system model in AWGN and fading channel. Though the total channel is a frequency-selective channel, the channel experienced by each subcarrier in an OFDM system is a frequency-flat slow-fading zero-mean AWGN channel with each subcarrier experiencing independent Rayleigh fading. Each individual OFDM subcarrier has a channel bandwidth less than the coherence bandwidth of the channel. Let x_i be the transmitted OFDM signal and y_i be the received OFDM signal. Then, in time-domain, a

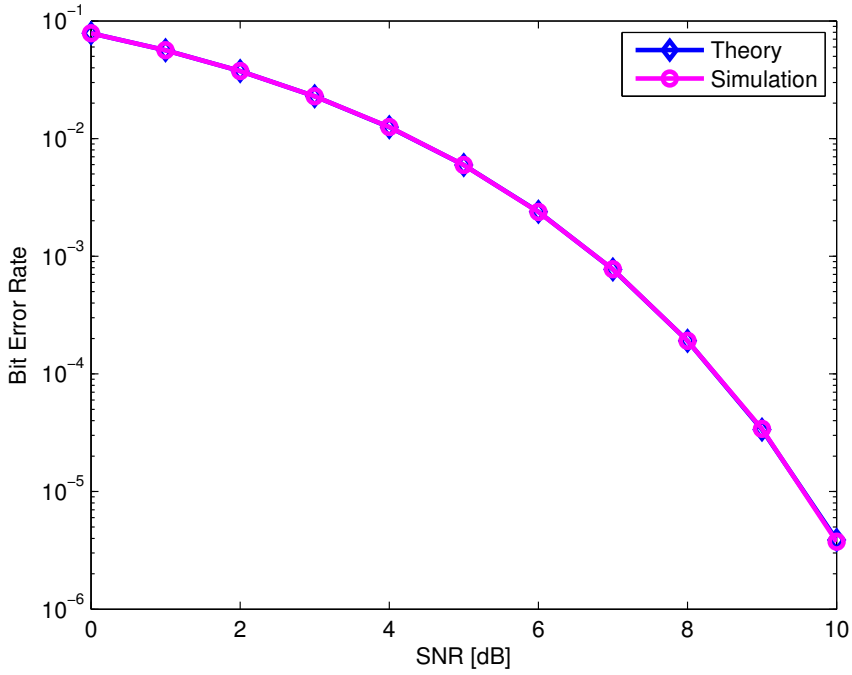

Figure 2.3: Bit error rate (BER) curve for OFDM with QPSK modulation in AWGN channel.

narrowband flat-fading system can be modeled as

$$y_i[n] = h_i[n] * x_i[n] + n_i[n], \tag{2.3}$$

where h_i is the channel impulse response, and n_i is the independent and identically distributed (i.i.d.) additive white Gaussian noise (AWGN) with distribution $\mathcal{N}(0, \sigma_n^2)$.

In OFDM systems cyclic prefix (CP) is used, which refers to the prefixing of a symbol with a repetition of the end. If sufficient length CP is used (i.e., CP greater than channel delay profile), then the effects of inter-symbol interference (ISI) and inter-channel interference (ICI) can be ignored. The use of CP enables OFDM receiver to use point by point linear convolution instead of circular convolution.

Let X_i be the transmitted signal in frequency-domain and Y_i be the received signal in frequency-domain. Then, in frequency-domain, the narrowband flat fading system from

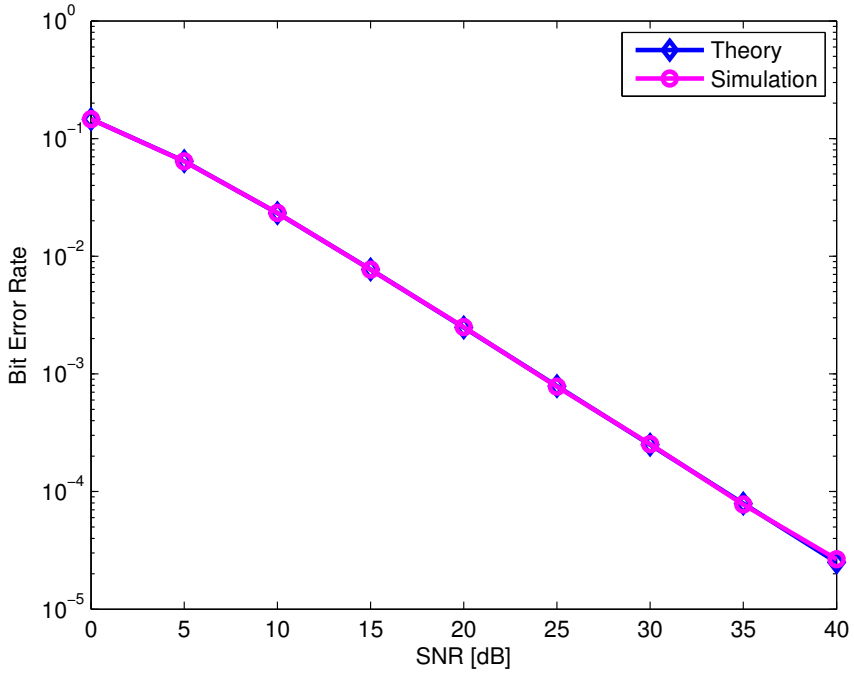

Figure 2.4: Bit error rate (BER) curve for QPSK modulated OFDM in a 6-tap Rayleigh channel.

(2.3) can be modeled as

$$Y_i = H_i X_i + n_i \tag{2.4}$$

where H_i is the frequency response of the channel. Note that the frequency response of a complex Gaussian random variable is also complex Gaussian (and is independent with frequency).

In Figure 2.3 the bit error rate (BER) performance of OFDM system with QPSK modulation in AWGN channel is shown. Figure 2.4 shows the BER performance of the QPSK modulated OFDM system in a frequency-flat Rayleigh slow-fading channel. Notice that the BER performance becomes much worse in fading channel than AWGN channel.

2.3 Synchronization

In this section, we describe common synchronization mechanism of OFDM Systems. There are a number of classic OFDM synchronization algorithms [18–23, 39, 40]. In general, these algorithms rely on the correlation between a training symbol and some copy of itself in order to perform timing acquisition and carrier frequency offset estimation. Notice that there is a similarity of these algorithms. However, for the sake of brevity, the topics covered in this section are described and outlined mathematically in reference [23].

The synchronization method proposed in [23] has three main stages – symbol timing estimation, fine carrier frequency offset estimation and correction, and coarse carrier frequency offset estimation. This algorithm is based on the use of specific *preamble* symbols, transmitted at the beginning of every frame. Due to the nature of this synchronization algorithm, the preamble symbols have a very specific structure.

It is important to note the structure of these symbols and the reasoning behind the structuring. The first symbol is constructed from a pseudo-random (PN) sequence of in-phase/quadrature (IQ) symbols in the frequency domain which is half the length of the number of subcarriers used. In order to mitigate interference with other users, as well as to avoid distortion from frequency down conversion, a guard band of empty subcarriers is used on both the upper and lower frequency edges of each OFDM symbol.

This symbol can be constructed by either populating every other subcarrier in the frequency domain before taking the IFFT to create the time domain OFDM symbol, or by taking a half-length IFFT of the PN sequence then repeating the symbol twice in time. Once the time domain symbol is created, the cyclic prefix is appended in the time domain.

The second preamble symbol is constructed from a PN sequence the length of all of the subcarriers. Each of the subcarriers is populated in the frequency domain, so that there is no repetition of the symbol in the time domain. The IFFT of the PN sequence is taken and

the cyclic prefix is generated in the time domain, as in the previous symbol. The first and second symbol are essentially glued together in time and transmitted as one preamble.

Timing recovery is performed using only the first symbol, but frequency recovery employs the differential PN sequence of the subcarriers that the first and second symbols both use. This sequence is just the division of the PN sequence on the corresponding frequencies from half of the second symbol (even or odd), and the PN sequence from the first symbol. It therefore has the length of half of the number of subcarriers used, and is the rotation on each of the IQ symbols from the first PN sequence to the second. The structure of the preamble and this last PN sequence make up the knowledge that the receiver has about the preamble symbol. This will allow the receiver to both detect the preamble symbol and determine the timing and frequency offset between with the transmitter.

The first step in the synchronization process is the estimation of symbol timing, performed on the complex baseband samples of the RF down converted signal. A sliding window of L samples is used to search from the preamble, where L is equal to the length of half of the first preamble symbol excluding the cyclic prefix. Two terms are computed for timing estimation. The first according to

$$P(d) = \sum_{m=0}^{L-1} (r^*_{d+m} r_{d+m+L}) \tag{2.5}$$

and the second according to

$$R(d) = \sum_{m=0}^{L-1} |r_{d+m+L}|^2 \tag{2.6}$$

where d is the time index which corresponds to the first sample taken in the window and r is the length-L vector of received symbols. These two terms are used to compute the timing metric $M(d)$ according to

$$M(d) = \frac{|P(d)|^2}{R(d)^2} \tag{2.7}$$

whose maximum value determines the symbol timing. Once this is performed, the receiver

will need to correct for the carrier frequency error between the transmitter and the receiver.

Carrier frequency offset estimation is the final step of the synchronization process. There are actually two sub-stages within frequency correction. The first is fine frequency correction and the second is coarse frequency correction. The fine frequency correction Δf is estimated using

$$\Delta f = \text{angle}(P(d))/\pi T \tag{2.8}$$

where T is the period of a single preamble symbol without its cyclic prefix and d is taken from anywhere along the timing metric plateau.

This term provides the fractional frequency offset only. The symbols can then be multiplied by a complex exponential to correct for the fine frequency error. In the frequency domain this represents the subcarriers being properly aligned in to bins.

The coarse frequency error estimation is the final step in the synchronization process, and finally employs the use of the second preamble symbol and the differentially modulated PN sequence. First, FFTs – the length of the symbol period without the cyclic prefix – of each of the symbols are taken. A coarse frequency metric is then computed to determine the number of bins that the symbols are shifted in either direction.

$$B(g) = \frac{|\sum_{k\in\mathcal{X}} x^*_{1,k+2g} v^*_k x_{2,k+2g}|^2}{2(\sum_{k\in X} |x_{2,k}|^2)^2} \tag{2.9}$$

For this equation, the set $\mathcal{X}$ represents all of the subcarrier bins which are occupied by both preamble symbols (either even or odd). The term g spans the range of the possible frequency offsets (there must be some bounds on the frequency errors between the transmitter and receiver). The point $g_{\max}$ at which the function $B(\cdot)$ is maximized represents the coarse frequency offset. The overall frequency offset is

$$\hat{\Delta f} = \text{angle}(P(d))/\pi T + 2g_{\max}/T \tag{2.10}$$

Once the overall frequency offset between the transmitter and the receiver has been determined, the signal acquisition process is complete and symbols can be demodulated.

2.4 Channel Estimation and Equalization

In this section, we describe data-aided (a.k.a. pilot tone based) channel estimation and equalization process for OFDM systems. In conventional OFDM systems, equal power and equally spaced pilot tones are inserted in the transmitted signal to estimate and equalize the channel's response. It is known from the previous research that equally spaced and equal powered pilot tone arrangement in OFDM symbols yields optimum performance under frequency-selective Rayleigh block fading [41–43]. Additionally, it has been proven that pilot tones are separable, that is the training data they convey can be in subcarriers independent of data [44]. In practice, standardized, commercial systems such as WiMAX [45] and LTE [46] follow this approach.

Given N_p known pilot tones and L unknown tap values in the channel impulse response, the equalizer's goal is to use this known information to solve for the unknown. As long as $N_p \geq L$, the receiver enjoys enough degrees of freedom and it has been proven that the channel impulse response can be precisely recovered when no noise is present in the system [41]. When noise is present, there are numerous Maximum Likelihood Estimator (MLE) and Maximum Mean-Squared Estimator (MMSE) approaches that can be utilized, which yield asymptotically similar performance [47].

The goal of this research is not to detail these approaches (see aforementioned references for a full analysis) but instead looks at how frequency-domain equalization is performed in typical OFDM systems. Assume there are N_p pilot tones and N_d data subcarriers in an OFDM frame, resulting total subcarriers in the frame $N_f = N_p + N_d$. The index 'i' and index 'j' represents the ith subcarriers in N_f and jth pilot-tone respectively. In this case, let

$\{k_1, k_2, \ldots, k_{N_p}\}$ are the locations of the pilot tones and $\{k_1, k_2, \ldots, k_{N_f}\}$ are the locations of the total subcarriers. For pilot tones located in $\{k_1, k_2, \ldots, k_{N_p}\}$, the Least Square (LS) estimate of the frequency response of channel at pilot tone location can be expressed as

$$\begin{aligned} \hat{H}_{k_i} &= \frac{Y_{k_i}}{p_i} \\ &= \frac{H_{k_i} p_i + n_{k_i}}{p_i} \\ &= \underbrace{H_{k_i}}_{\text{Channel}} + \underbrace{\frac{n_{k_i}}{p_i}}_{\text{Error}} \end{aligned} \tag{2.11}$$

where $\hat{H}$ is the LS estimate. Note that if the transmitted pilot tone p_i is unit energy, then channel frequency response error at the pilot tone is simply the additive noise.

In OFDM systems, the receiver interpolates between pilot tones to estimate intermediate values of channel frequency response. A number of methods for performing interpolation are available in literature, such as one degree polynomial (or linear) interpolation, higher-order polynomial interpolation, fractal, and spline etc. [48]. Some systems use higher-order polynomial interpolation. However, the use of higher-order polynomial interpolation does not offer significant additional performance in most of the time. We assume linear interpolation for the remainder of this work which is polynomial interpolation of one degree.

For linear interpolation, where $k_j \leq i \leq k_{j+1}$, we have

$$\begin{aligned} \hat{H}_i &= \frac{\hat{H}_{k_j}(k_{j+1} - i) + \hat{H}_{k_{j+1}}(i - k_j)}{k_{j+1} - k_j} \\ &= \frac{1}{k_{j+1} - k_j} \left(\hat{H}_{k_j}(k_{j+1} - i) + \hat{H}_{k_{j+1}}(i - k_j) \right). \end{aligned} \tag{2.12}$$

Notice that all the analysis presented in this work are based on linear interpolation for frequency-domain channel estimation (Equation 2.12). The linear interpolation approach is not optimum. As mentioned earlier, when the number of the pilot tones is not smaller than

the number of channel taps and there is no noise, the channel can be recovered without error. On the other hand, the time-domain channel can be reconstructed by solving a linear system. Therefore, it would be logical to use this method for better performance. However, the analysis will become more complicated and derivation will be challenging. Hence, despite of sub-optimal performance of linear interpolation for frequency-domain channel estimation, we restrict using this approach in this work. This will enable us to clearly quantify the impact of the pilot tone jamming attacks and countermeasures, and will yield clear-cut intuitive analytical model.

The channel equalization is executed after acquiring the channel frequency response $\hat{H}_i$ by computing

$$\begin{aligned} \hat{X}_i &= \frac{Y_i}{\hat{H}_i} \\ &= X_i \frac{H_i}{H_i + \epsilon_i} + \frac{n_i}{H_i + \epsilon_i} \end{aligned} \tag{2.13}$$

where ϵ_i is the overall error of channel estimation.

The overall effective additive noise per symbol, α_i is

$$\begin{aligned} \alpha_i &= \hat{X}_i - X_i \\ &= \frac{n_i - X_i \epsilon_i}{H_i + \epsilon_i}. \end{aligned} \tag{2.14}$$

Notice that suboptimum least square (LS) estimation and zero forcing (ZF) equalization methods are used here for the derivations instead of MLE or MMSE or other types that yield better performance and are used widely in real-life communications. The reason is simple – this provides clear intuitive insight on pilot tone jamming and countermeasure and enables to derive more tractable closed-form expressions. Regardless of estimation/equalization technique, the increased noise on the pilot tones due to jamming will deteriorate the communi-

cation system's quality.

Also a number of pilot tone mapping patterns are available, such as block type (a.k.a. frequency-domain), comb type (a.k.a. time-domain), and combined type (both dimensions), depending on channel characteristics. The derivations used are limited to pilot tone mapped in frequency. The rationale is to use a simple reference mapping and show the impact of proposed jamming attacks and mitigation strategies, rather than showing impact of various mapping patterns. The knowledge gained can be intuitively translated to the other cases. We expect that the attacks/countermeasures will follow the same trend for all the pilot tone mapping patterns for OFDM and OFDMA. On top of it, the time-domain channel can be reconstructed by solving a linear system, which can provide better estimation. But the analysis will become more complicated and derivation will be challenging as well.

The BER performance for QPSK modulated OFDM in Rayleigh fading channel is shown in Figure 2.5. The fading channel shown here is a 6-tap frequency-flat, Rayleigh slow-fading zero-mean AWGN channel, just like ITU Pedestrian B channel model. Notice that there is slightly heightened BER for pilot tone aided channel estimation. This increase in error is caused by the use of finite number of pilot tones to estimate the channel. We model this estimation error in detail in the next section.

2.5 Channel Estimation Error

In this section, we derived an analytical model for channel estimation error, ϵ_i. The overall error, ϵ_i, can be expressed as $\epsilon_i = \epsilon_i^n + \epsilon_i^a$. Here, ϵ_i^n and ϵ_i^a represent error from additive noise on pilot tones that impacts the channel estimation at pilot tones and linear interpolation, and error from the use of finite points to approximate the channel frequency response function respectively. Figure 2.6 shows both of these errors graphically.

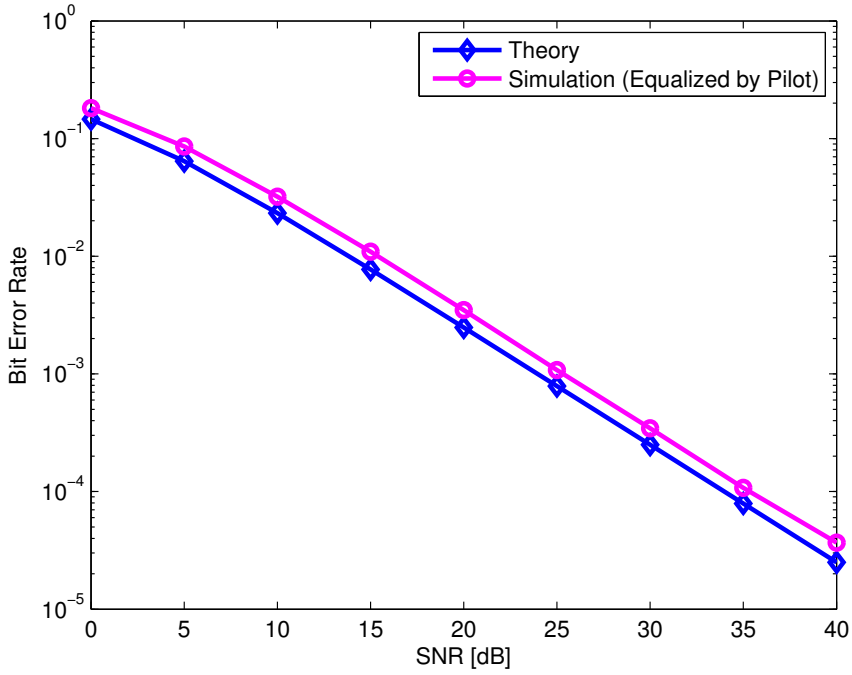

Figure 2.5: Bit error rate (BER) curve for QPSK modulated OFDM in a 6-tap Rayleigh channel, where channel is estimated by 8 pilot tones (pilot tone density of 8).

2.5.1 Channel Noise Error

The additive noise on pilot tone is liable for the erroneous channel estimation at pilot tone, which further spreads during the linear interpolation. From (2.12) and (2.13), for $k_j \leq i \leq k_{j+1}$, the linear interpolation can be expressed separately for channel and error as

$$\tilde{H}_i = \frac{1}{k_{j+1} - k_j} \left(H_{k_j} \left(k_{j+1} - i \right) + H_{k_{j+1}} \left(i - k_j \right) \right) \tag{2.15}$$

and

$$\epsilon_i^n = \frac{1}{k_{j+1} - k_j} \left(\frac{n_{k_j}}{p_j} \left(k_{j+1} - i \right) + \frac{n_{k_{j+1}}}{p_{j+1}} \left(i - k_j \right) \right) \tag{2.16}$$

where $\tilde{H}_i$ is the channel response for linear interpolation that depends on the linear combination of $\hat{H}_{k_j}$ and $\hat{H}_{k_{j+1}}$. Note that $\tilde{H}_i$ is not the true frequency response at subcarrier i. However, the common practice is to assume $\tilde{H}_i \cong H_i$.

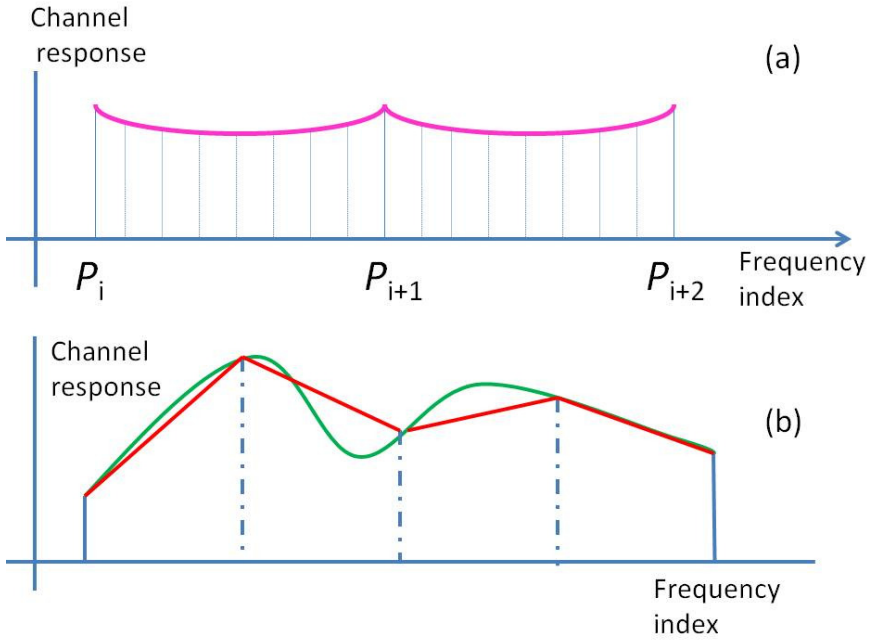

Figure 2.6: The graphical representation of the overall channel estimation error during estimation/equalization process consisting two sources: (a) channel noise error due to the additive white noise on the pilot tones propagating during interpolation, and (b) channel approximation error due to measuring continuous channel function with finite number of points at pilot locations.

If the pilot tones are unit-power, then the error becomes

$$\epsilon_i^n = \frac{1}{k_{j+1} - k_j} \Big(n_{k_j} \left(k_{j+1} - i \right) + n_{k_{j+1}} \left(i - k_j \right) \Big). \tag{2.17}$$

From (2.17), the interpolation error ϵ_i^n is the linear combination of two i.i.d. random variables n_{k_j} and $n_{k_{j+1}}$ with each having distribution $\mathcal{N}(0, \sigma_n^2)$, and therefore, itself is Gaussian with zero mean and variance

$$\sigma^2_{\epsilon_i^n} = \frac{\left(k_{j+1} - i \right)^2 + \left(i - k_j \right)^2}{\left(k_{j+1} - k_j \right)^2} \sigma_n^2. \tag{2.18}$$

Hence, the error, ϵ_i^n, has the following distribution

$$\epsilon_i^n \sim \mathcal{N}\left(0, \left(\frac{(k_{j+1}-i)^2 + (i-k_j)^2}{(k_{j+1}-k_j)^2}\right)\sigma_n^2\right). \tag{2.19}$$

The variance depends on i, taking its maximum value at the extrema $\sigma^2_{\epsilon^n_{k_j}} = \sigma_n^2$ and its minimum at the midpoint $i = (k_{j+1}+k_j)/2$ where $\sigma^2_{\epsilon^n_{k_j}} = \sigma_n^2/2$. The mean variance is estimated by integrating across all the possible values, if i is between k_j and k_{j+1}. Then the average over i is given by

$$\begin{aligned}\overline{\sigma}^2_{\epsilon_i^n} &= \frac{1}{k_{j+1}-k_j}\sum_{i=k_j}^{k_{j+1}-1}\sigma^2_{\epsilon_i^n} \\ &= \frac{1}{d_k}\sum_{i=0}^{d_k-1}\frac{(d_k-i)^2+i^2}{d_k^2}\sigma_n^2 \\ &= \left(\frac{2}{3}-\frac{1}{3d_k^2}\right)\sigma_n^2\end{aligned} \tag{2.20}$$

where $d_k = k_{j+1}-k_j$, and for large d_k the variance can be approximated as $\overline{\sigma}^2_{\epsilon_i^n} \backsimeq \frac{2}{3}\sigma_n^2$.

Hence, the distribution of average error, $\overline{\epsilon}_i^n$, due to channel noise can be expressed as

$$\overline{\epsilon}_i^n \sim \mathcal{N}\left(0, \frac{2}{3}\sigma_n^2\right) \tag{2.21}$$

where σ_n^2 is the variance of i.i.d. AWGN distribution.

2.5.2 Channel Approximation Error

It is well known that if the sum/integral of the time domain channel impulse response $h(t)$ is finite, the frequency response $H(f)$ is continuous everywhere in the (continuous frequency) domain, $f \in \mathbb{R}$. The use of finite points to approximate a continuous function causes error, which is exactly the case here, as channel is estimated with finite number of pilot tones.

Here linear interpolation is used to approximate values of channel frequency response function $H(f)$ using two known values of that function at other points. Let $P(f)$ be the linear interpolation polynomial, defined as

$$P\left(f\right) = H\left(f_{k_j}\right) + \frac{H\left(f_{k_{j+1}}\right) - H\left(f_{k_j}\right)}{f_{k_{j+1}} - f_{k_j}}\left(f - f_{k_j}\right) \tag{2.22}$$

where f_{k_j} and $f_{k_{j+1}}$ denotes frequency at location k_j and k_{j+1} respectively. Notice that even though our channel frequency response H_i is discrete function (sampled) in this work, the assumption that the original $H(f)$ is continuous still holds, and would yield same result.

Then the error of this approximation is defined as

$$E\left(f\right) = H\left(f\right) - P(f). \tag{2.23}$$

If the original function $H(f)$ is continuous in some arbitrary region $[a, b]$ and differentiable up to $(n + 1)$ degrees, then the point-wise estimation error is

$$E\left(f\right) = \frac{H^{(n+1)}(f)}{(n+1)!}\left(\prod_{i=0}^{n}(f - f_i)\right) \; for \; f \in [a, b]. \tag{2.24}$$

For linear interpolation, $n = 1$, $H(f)$ must have second derivative in region $[a, b]$ and the error becomes

$$E\left(f\right) = \frac{1}{2}H^{''}\left(f\right)\left(f - f_{k_j}\right)\left(f - f_{k_{j+1}}\right) \; for \; f \in [a, b]. \tag{2.25}$$

If we consider a single interval $[k_j, k_{j+1}]$ or $\left[f_{k_j}, f_{k_{j+1}}\right]$, then the error can be assumed positive. Taking k_m as midpoint between interval, the error becomes

$$\begin{aligned} E\left(f_{k_m}\right) &= \left|\frac{1}{2}H^{''}\left(f\right)\left(f - f_{k_j}\right)\left(f - f_{k_{j+1}}\right)\right| \\ &= \frac{1}{2}\left|\left(f - f_{k_j}\right)\left(f - f_{k_{j+1}}\right)\right|\left|H^{''}\left(f\right)\right| \end{aligned} \tag{2.26}$$

$$
\begin{aligned}
&= \frac{1}{8}\left(f_{k_{j+1}} - f_{k_j}\right)^2 \left|H^{''}(f)\right| \\
&= \frac{1}{8} d_f^2 \left|H^{''}(f)\right| \; for\; f \in \left[f_{k_{j+1}}, f_{k_{j+1}}\right]
\end{aligned}
$$

where $d_f = \left(f_{k_{j+1}} - f_{k_j}\right)$ is the distance in frequency between pilot tones at k_j and k_{j+1}.

The maximum error occurs at midpoint for linear interpolation. So upper bound (or maximum) for the absolute value of approximation error, $|\epsilon_i^a| = |E(k_{j+1}, k_j)| = \left|E(f_{k_{j+1}}, f_{k_j})\right| = E\left(f_{k_m}\right)$, over two adjacent pilot tones located in k_j and k_{j+1} can be obtained by Chebyshev Infinity Norm and Rolle's Theorem [49] as

$$
\begin{aligned}
|\epsilon_i^a| &\leq \left[\frac{1}{8} \max_{f_{k_j} \leq f \leq f_{k_{j+1}}} \left|H^{''}(f)\right|\right] d_f^2 \\
&\leq \left[\frac{1}{8} \max_{k_j \leq i \leq k_{j+1}} \left|H^{''}(f)\right|\right] d_f^2 \\
&\leq K d_f^2
\end{aligned} \tag{2.27}
$$

where $K = \frac{1}{8} \max_{k_j \leq i \leq k_{j+1}} \left|H^{''}(f)\right|$ is constant for $k_j \leq i \leq k_{j+1}$.

As this is an absolute error (and maximum error as well), a two-sided approximation error can be assumed uniformly distributed between $[-Kd_f^2, Kd_f^2]$

$$
\epsilon_i^a \sim U\left[-Kd_f^2, Kd_f^2\right] \tag{2.28}
$$

with mean, $E\left[\epsilon_i^a\right] = 0$ and variance, $\sigma_{\epsilon_i^a}^2 = \frac{1}{3}K^2 d_f^4$. This assumption results in the worst case bound for the approximation error. Equation (2.28) gives us approximation error for equal pilot tone spacing with total N_p pilot tones within specific band, where pilot tone space d_f is deterministic.

2.6 Summary

In this chapter, we introduced OFDM waveform and described the basics of OFDM systems; we presented the transceiver structure as well as the channel models for AWGN and Rayleigh fading. Then we went along to describe the common synchronization mechanism of OFDM Systems. Afterwords, we described data-aided (a.k.a. pilot tone based) channel estimation and equalization process for OFDM systems. We derived an alternate analytical model for channel estimation error in terms of – 1) channel noise error and 2) channel approximation error. This alternative channel estimation error model is one of the key contributions of this research.

Along with the mathematical models, a set of simple but informative plots are presented to gain better understanding of the OFDM systems. The very first plot is a block diagram of the OFDM system transmitter-receiver pair along with equalizer that is subject to multipath fading channel. An example of a typical OFDM waveform in frequency-domain, which is based on LTE-FDD PHY-layer specification, is provided next. Two plots for bit error rate (BER) performance of QPSK modulated OFDM systems are presented that are subject to AWGN channel and a 6-tap Rayleigh channel, where channel is equalized by 1) perfect channel information and 2) pilot tone assisted estimated channel information. It is found that the fading channel elevates the BER of the communications systems and further error is introduced due to the estimation of the channel.

Chapter 3

Adversarial Model

In this chapter, we discuss the robustness of OFDM systems, conduct a survey of the interferences on OFDM systems, present the adversarial model, classify the jamming taxonomy, describe existing jamming attacks on OFDM systems, and analyze the performance of OFDM systems under various existing jamming strategies. We also present a novel jamming method against OFDM systems that we call 'asynchronous off-tone' jamming attack.

The remainder of this chapter is organized as follows. We start with a general discussion about the robustness of the OFDM systems in Section 3.1. Then we move on to explore the current state of interferences on OFDM systems in Section 3.2. In Section 3.3 we present an adversarial model that is valid for all the communications systems, including OFDM systems. In Section 3.4 we attempt to classify various types of jammers and propose a comprehensive communications jamming taxonomy. Current states of OFDM jamming attacks available to open literature are discussed in Section 3.5. In Section 3.6, we present various noise jamming attacks on OFDM systems, which are considered as more conventional methods of jamming. In Section 3.7, we introduce a novel power efficient noise jamming method against OFDM systems that we named 'asynchronous off-tone' jamming attack. We summarize the contributions of this chapter in Section 3.8.

3.1 Robustness of OFDM Systems

In this section, we discuss the robustness of OFDM systems. One of the key strengths of OFDM systems is its ability to handle multipath propagation. It is capable of combating multipath fading with greater robustness and less complexity. The inter-symbol interference (ISI) caused by multipath propagation is less of a problem with OFDM systems because low data rates are carried by each carrier (also called subcarriers). Since low symbol rate modulation schemes (i.e., where the symbols are relatively long compared to the channel time characteristics) suffer less from ISI, it is advantageous to transmit a large number of low rate streams in parallel instead of a single high rate stream. Since the duration of each symbol is long, it is feasible to insert a guard interval (GI) between the symbols. Using a cyclic prefix (CP) greater than the coherence bandwidth during the GI ensures eliminating most ISI. However, it comes at the price of spectral efficiency [50, 51].

The OFDM systems, due to the avoidance of ISI, can easily adapt to severe channel conditions without the need for complex channel equalization algorithms being employed [50, 51]. For example, frequency-selective fading caused by multipath propagation can be considered as constant (flat) over an OFDM sub-channel if the sub-channel is sufficiently narrow-banded. This makes frequency-domain equalization possible at the OFDM receiver, which is simpler than the time-domain equalization used in the conventional single-carrier modulation.

The OFDM waveforms are also resilient when combating narrowband co-channel interference (CCI). As an OFDM waveform is composed of many narrowband tones, a narrowband interferer can degrade only a limited portion of the signal, leaving the rest of the subcarriers intact. In addition, wireless broadband standards such as LTE include adaptive rate modulation, which allows subcarriers under poor conditions to fall back to a lower order modulation scheme, such as QPSK [52].

Conventional OFDM systems have shorter subcarrier spacing, which can be vulnerable to

Doppler shift observed in high mobility situations. *Doppler* shift can cause significant inter-channel interference (ICI). Luckily, the ICI mitigation strategies can compensate to a certain extent. Another drawback of OFDM systems is their sensitivity to timing and frequency synchronization; a mismatch at the receiver can cause serious ICI and ISI [52].

3.2 Interferences on OFDM Systems

In this section, we explore the current state of interferences on OFDM systems deployed as part of various wireless communications standards. We also discuss the impact of these interferences on OFDM systems. Notice that unwanted structured (or colored) signals are known as interferences in the literature. Interferences can be either intentional or unintentional. Only the unintentional interferences are referred as interferences, whereas the intentional interferences are termed as interference jamming attacks (or simply jamming attacks). In reality, most of the time, we observe unintentional interferences from co-channel and/or adjacent channel communications. For example, baby monitors at the 700 MHz band or the TV channel 51 next to 700 MHz band may cause unintentional colored interferences to OFDM-based waveforms in the 700 MHz band [6].

One source of interference on OFDM-based LTE is TV broadcasting. In [53,54] the authors discussed the potential interferences between TV white space and DSA-enabled cellular communications. Channel 51 TV broadcasting spectrum, which is next to the lower 700 MHz that 3GPP put into their specification, has received some attention recently [55]. In [55], the authors discussed the interference levels (-40 dBm to -20 dBm) that can impact LTE performance. Based on both lab and field test results, it is found that Channel 51 and E Block signals interfere with Band 12 networks using the B and C blocks and Band 17 devices, and can cause significant degradation of throughput (usually measured in block error rate) in large geographic areas, including urban areas. In addition, E-Block transmissions cause

two form of interferences: (1) adjacent channel interference, and (2) reverse intermodulation interference to consumer devices (i.e., LTE-compatible devices) seeking to receive a 5 MHz signal on the C Block or a 10 MHz signal on the B and C Blocks of lower 700 MHz.

There are other cases like this in the records for the Advanced Wireless Services (AWS) band. The FCC plans to reallocate mobile wireless services to 600 MHz spectrum that is currently used for over-the-air broadcast TV services [56, 57]. The impact of 600 MHz TV station interference on the new bands for LTE in the soon-to-be auctioned 600 MHz band is discussed in [56]. A central feature of the FCCs proposed framework is an unusually large duplex gap between the downlink and uplink frequencies combined with the placement of TV stations in that duplex gap. Placing very high power TV stations in the duplex gap would create adjacent channel interference in the 600 MHz devices downlink bands, which could also degrade the receiver performance. Second, the FCCs proposed framework would result in harmonic signals that could interfere with PCS and BRS/EBS mobile downlink spectrum. Third, the FCCs design for uplink spectrum would likely result in co-channel interference (CCI) caused by TV stations operating in nearby geographic areas.

Another potential category of interference for OFDM systems would be the various kinds of radars operating nearby. In [58], the authors consider a scenario where low-frequency radars such as Synthetic Aperture Radar (SAR) interferes with the Digital Terrestrial Television (DTT) standard such as DBV-T that employs an OFDM-based waveform. The low-frequency radar operating at VHS (currently) and UHF (in near future) may cause outages to 20% of DVB-T users operating in the $585 - 806$ MHz band (primarily in Europe). The authors concluded with observations that the interferences from radar can be reduced by flattening the radar spectrum or by increasing FFT size of the channel (which increases the OFDM symbol period). Other notable scenarios where radar interferes with LTE would be weather radar and airport surveillance radar. Both of these radars operate at $2.7 - 2.9$ GHz band, which is a proposed band for LTE.

Apart from these, OFDM based standards like LTE may face interference from Tactical Targeting Network Technology (TTNT) proposed by the Defense Advance Research Project Agency (DARPA). The TTNT proposal consists of researching new waveforms for use in air-to-air networks of high-speed aircraft at $1755 - 1850$ MHz band, which is currently used by commercial cellular users [59]. Even though the Department of Defense (DoD) is planning to relocate TTNT from $1755 - 1850$ MHz band to $2025 - 2110$ MHz band in ten years, it will remain a clear and present danger for LTE systems operating at nearby bands until then.

While most of the examples provided here involve unintentional interferences, we should keep in mind that malicious user nodes or adversaries can intentionally transmit structured (colored) signals to cause communication disruption; especially when they are used against public safety communications or other mission-critical situations. We can classify these intentional structured emissions as interference jamming attacks. In general, interference jamming attacks are ones that may be structured but are not dependent on the target signal. Alternatively, interference jamming attacks can be defined as colored noise where adversaries can have modulated signals that have zero correlation with the target signal, i.e., center frequency of target. Interference jamming attacks are much easier to execute because the adversary does not need to observe and obtain any level of synchronization with the target signal. For example, the adversary may intentionally start its own communication in the band where the target is operating. Any such transmission can interfere with the target and therefore, degrade/disrupt the targets' ability to communicate.

3.3 Adversarial Model for OFDM Systems

In this section, we discuss intention, objective, and capability of the hostile interferences (also known as jamming) on OFDM systems and present the adversarial model. In Figure 3.1, the block diagram of an OFDM transmitter-receiver pair, which is subject to jamming attack,

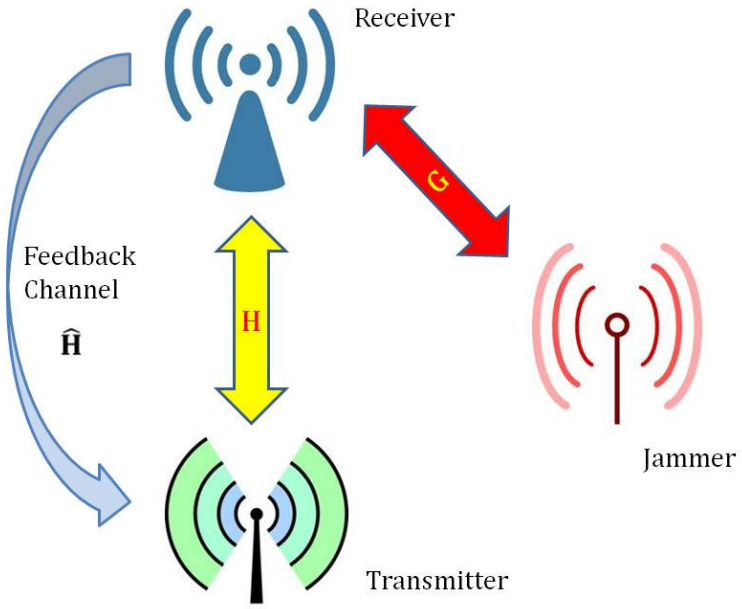

Figure 3.1: System diagram for an OFDM transmitter-receiver pair subject to jamming attack; where **H** is the channel between transmitter and receiver (communication channel) and **G** is the channel between jammer and target receiver (jamming channel).

is shown, where **H** and **G** are the communication and jamming channel, respectively.

It is assumed that each individual OFDM subcarrier channels are a flat-faded Rayleigh fading channel where individual subcarriers have channel bandwidth less than the coherence bandwidth of the channel. Let x_i be the transmitted signal and y_i be the received signal. Then, in the presence of a jammer j_i, a narrowband flat-fading system can be modeled as

$$y_i[n] = h_i[n] * x_i[n] + g_i[n] * j_i[n] + w_i[n], \tag{3.1}$$

where h_i and g_i are channel impulse response of transmitted signal and jammer's signal respectively, and w_i is independent and identically distributed (i.i.d.) additive white Gaussian noise (AWGN) with distribution $\mathcal{N}(0, \sigma_n^2)$.

3.4 Jamming Taxonomy for OFDM Systems

In this section, we attempt to classify various types of jammers and propose a comprehensive communications jamming taxonomy. Typically jammers seek to disrupt communications, and have a variety of strategies that they are capable of. Some techniques are more effective and efficient than others, and a successful strategy depends on the particular type of target employed. Here we present a discussion on communication jamming taxonomy in general, with OFDM systems in mind. The primary delineation of the taxonomy is by jammer capabilities that define the fundamental behavior of the jammer. A secondary refinement of the taxonomy by parameters is presented next [60].

A jammer can have one or more of the following major capabilities:

1. Correlated
2. Protocol-Aware
3. Ability to Learn
4. Signal Spoofing

Figure 3.2 shows how the jammer capabilities are interrelated. These four capabilities are chosen based on a survey of jammer models that exist in literature, with an emphasis on complex forms of jamming.

A jammer can perform following steps prior to execute jamming attacks:

1. **Signal Awareness:** sensing and detecting signals across the spectrum of interest
2. **Threat Assessment:** a decision must be made whether or not signals will be jammed
3. **Attack Selection:** for each signal to be jammed, the best attack must be selected

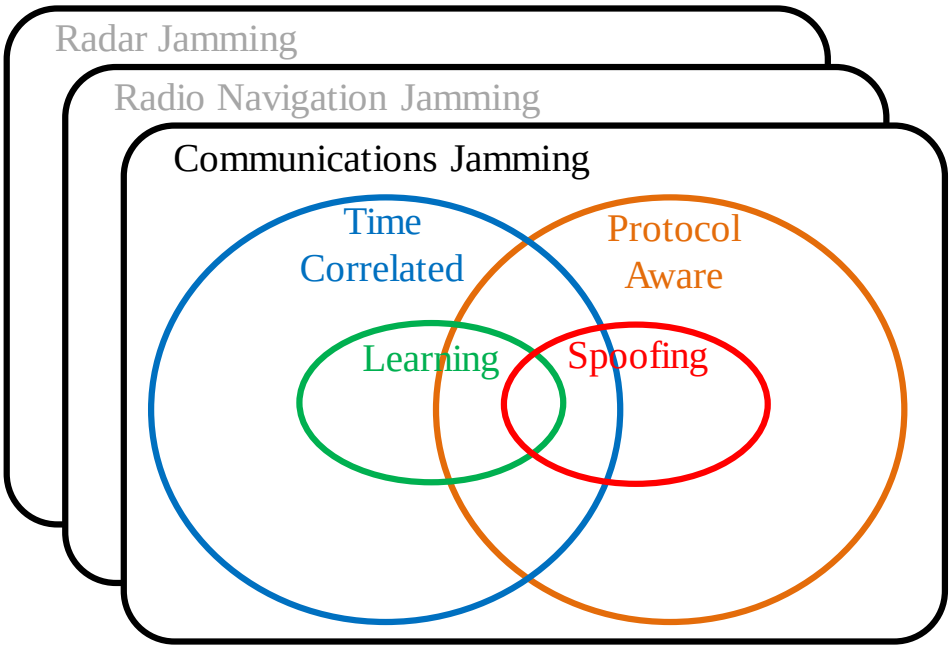

Figure 3.2: Key capabilities of a jammer and how they relate.

3.4.1 Correlated

A correlated jammer implies the jammer can listen to the transmitter's signal, leading to the geometrical configuration shown in Figure 3.3. Correlated jamming attacks are very serious and capable of causing damage to transmissions using minimal power. These attacks are typically very sophisticated and can involve detailed synchronization and knowledge of the target signal, in order to increase effectiveness. A simple example of correlated jamming involves only transmitting a jamming signal when there is energy on the channel. Commercial waveforms are designed with specific structures such as reference signals to perform symbol timing estimation, pilot tones to estimate and equalize channel effects, and control channels to embed various control information. Such waveforms are susceptible to the threat of correlated jamming. This class of jammer could take on a wide range of specific models. While correlated jamming is a very broad category of jamming, it acts as a good characteristic to quickly identify the complexity of the jammer, as a correlated jammer must have some form of a receiver. Because there is significant engineering that goes along with receiving capability

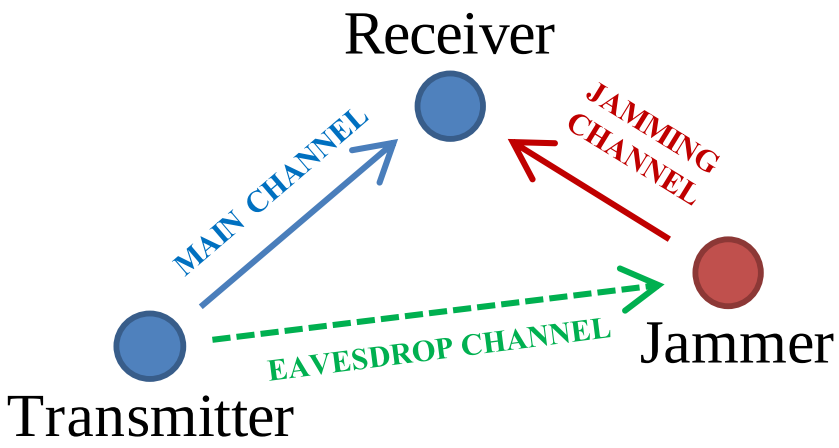

Figure 3.3: Geometrical configuration of a correlated jamming scenario, showing the three channels involved.

(e.g., a full RF chain, sampling, processing), any correlated jamming attack corresponds to a more complex attack.

3.4.1.1 Time Correlated

A jammer is categorized as time correlated jammer if that jammer transmits a jamming signal that is correlated to the target signal in time, in some manner. This category of jammer is also known as *reactive jammer* in some literature. The time correlation capability comes into play during the actual **Attack Selection** step, not the **Signal Awareness** step. Obtaining signal awareness surely requires receiving capability, but a time correlated attack consists of the jammer being tightly synchronized to the target signal. We discuss correlation in the time domain specifically, because it is implicit that a jammer's signal needs to have some correlation in the frequency-domain with the victim's desired signal to be successful (i.e., at least be aware of the spectrum being used by the victim and thereby perform jamming attacks over this spectrum).

3.4.2 Protocol-Aware

The protocol-aware jamming attacks are advanced jamming mechanisms in which the jammers have advance knowledge of the protocol used by the targets, and exploit this knowledge to increase jamming effectiveness. In the protocol-aware jamming attacks, the adversary obtain information about the target signal's protocol during the **Signal Awareness** step and then use it in the **Attack Selection** decision-making. For example, if a jammer knows that the target signal is a Wi-Fi signal, then it could transmit periodic pulses with a period equal to the IEEE 802.11 Extended Inter-frame Space (EIFS). Notice that due to the open nature of Wi-Fi or LTE or any other communications standard specifications, the jammer gets to know almost everything about the PHY and MAC layers of the target. This strategy has been shown to lead to an effective jamming attack utilizing an extremely low duty cycle [61]. A jammer could use *a priori* knowledge of the protocol to exploit weaknesses in the protocol, and launch a jamming attack that is more effective and may be harder to detect than non-protocol-aware jamming. Moreover, a signal does not have to belong to a specific technology to be open to a protocol-aware attack. For example, the jammer may only know a signal uses pilot tone assisted OFDM waveform where pilot tones are in certain locations, which would be considered protocol-aware if it knew exactly where the pilot tones are placed. Recently, pilot tone-based OFDM jamming is introduced [7], where the jammer seeks to jam pilot tones in order to jeopardize equalization. OFDM synchronization jamming attacks are introduced in [8, 9], where the adversary either jams the acquisition signal or misguides the target receiver to synchronize into erroneous time and frequency.

The concept of protocol-aware jamming can be applied to most of the jamming techniques discussed throughout this research. According to the discussion found in the open literature, if a jammer is aware that the specific protocol being used, it can intensify the effectiveness by jamming a PHY or MAC layer mechanism instead of data payload directly. In most wireless protocols, the data payload takes up the largest portion of time and frequency

resources. Thus, if a jammer targets something besides the data payload, it will likely result in an attack that uses much less power and is harder to detect (as long as the targeted mechanism is essential for communications). Possible mechanisms that could be targeted in a protocol-aware attack (taken from open literature) include:

- Control channels/subchannels
- Control frames or packets (e.g., ACKs)
- Pilots (a.k.a. reference symbols)
- Synchronization signals
- Cyclic prefix in OFDM

A survey of protocol-aware jamming attacks against Wi-Fi and LTE can be found in [62] and [24], respectively.

3.4.3 Ability to Learn

In this section, we delineate the term 'learning' in the Machine Learning (ML) sense. Typically they are the systems that can learn from data, rather than follow only explicitly programmed instructions. In the jammers perspective, they are the jammers that are capable of learning as well able to modify their behavior in real-time in retort to its experiences (i.e., instances of successful or unsuccessful jamming actions/decisions) [63]. However, we should remain careful about distinguishing the learning jammer from the adaptive jammer. An adaptive jammer is usually limited to following a pre-programmed sequence of change in response to target, whereas learning jammer goes beyond simply detecting the target's waveform type and choosing from a pre-programmed set of jamming waveforms. A jammer that learns may detect that the target has initiated an antijam strategy, and then the jammer

can explore different strategies of its own to circumvent this antijam defense. The learning jammer can evolve its behavior in response to a target's behavior and adaptation.

The jammers that belong to this category are the most complex ones as they have relatively high computational complexity during training (i.e., supervised learning algorithms such as the popular Support Vector Machine (SVM) or artificial neural networks (ANNs) have complex learning algorithms). Also note that it may be difficult for the jammer to determine the success as it may not have access to the channel feedback information.

Often the ability to learn leads to the tag of 'cognitive'. However, a cognitive jammer that is capable of learning should not be confused with 'cognitive radio jamming', i.e., a jammer designed to deny a cognitive radio network (e.g., primary user emulation (PUE) attack [64]). In some cognitive radio jamming literature, the term 'cognitive jammer' is used, even though the PUE attack rarely involves learning and often is not even correlated.

In some circumstances, a jammer capable of learning may target radios that are also capable of learning, such as cognitive radios presented by Mitola [65] (as opposed to dynamic spectrum sharing radios). The jammer can exploit this fact using a belief manipulation attack thereby causing the targeted system's adaptation processes to seek a poor operating point [66]. This can give rise to a jamming game situation where both adversary and target attempt to maximize its benefit knowing the existence of each-other.

In terms of how presence of learning is related to the other key capabilities, a jammer capable of learning is almost surely correlated as learning comprises observing the target signal. However, we categorize learning capability and protocol-awareness as two independent features, leading to the relationship shown in Figure 3.2.

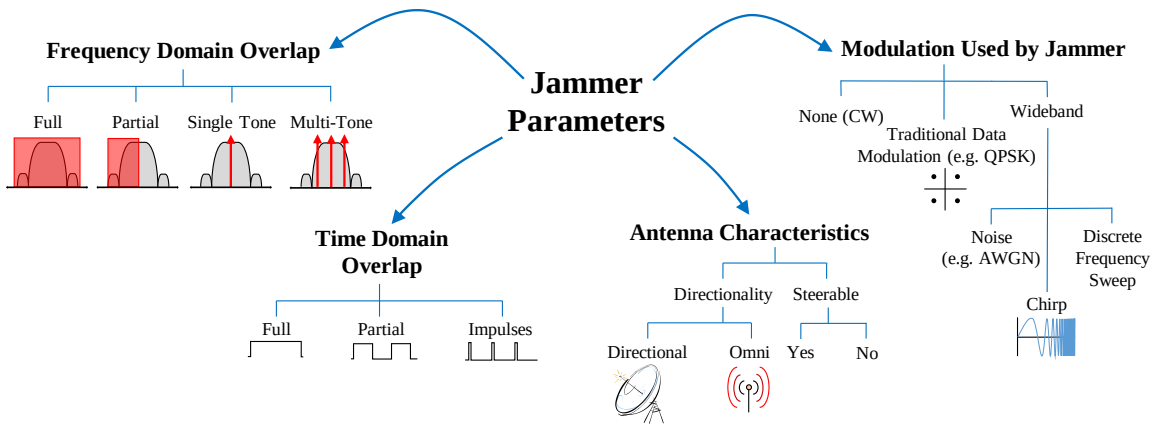

Figure 3.4: Jammer parameters organized into trees.

3.4.4 Spoofing (a.k.a. Protocol Emulation)

Spoofing is generally defined as a situation in which malicious entity successfully masquerades as target entity by falsifying data and/or signals in order to gain an illegitimate advantage. In spoofing, the adversary typically targets a PHY-layer mechanism by emulating a signal. Determining whether a given adversary is spoofing is rather simple. One must check whether it is transmitting noise, or transmitting something that looks legitimate to the target's PHY layer.

Spoofing may or may not be correlated, although in literature it is more often *not* correlated. Also the protocol-aware jamming attacks may or may not be spoofing. On the other hand, spoofing is almost surely protocol-aware, because in this case the jammers need to know what to spoof. Spoofing can be either PHY-layer or higher layer. In higher layer spoofing the jammer transmit information that looks like a valid packet or frame.

The primary user emulation (PUE) attacks are used in cognitive radio technologies, which can be considered as spoofing depending on the specific waveform the jammer transmits. In PUE attacks, the jammer transmit a signal that looks like the primary user's signal (e.g., the pilot tones associated with a radio station), in which case it is PHY-layer spoofing.

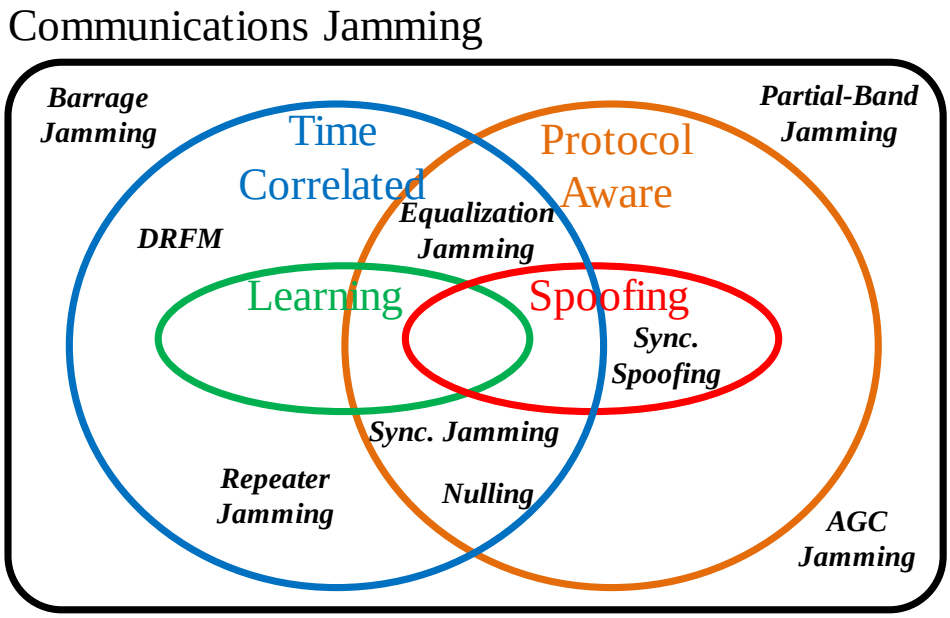

Figure 3.5: Specific jamming techniques discussed in literature, mapped according to key jammer capabilities.

3.4.5 Jammer Parameters

In the previous sections we defined the major categories of jammer capabilities. Here we introduce the concept of jamming taxonomy on the basis of jammer parameters, which serves as second tier refinement in the jamming taxonomy. It comes from the choice of physical parameter values of the jammers. They are less important characteristics as they are not as significant in defining the overall behavior of the jammer.

The jammer parameters are organized in trees in Figure 3.4 where example parameters include frequency, time overlap with jamming target, antenna directionality, and the jammer's waveform or modulation. In this way, jammer types that, in early literature, are treated as distinct technologies can be understood now as minor variations on a common algorithm.

Throughout this dissertation we discussed various jamming attacks against OFDM systems – some of them are conventional and some of them are introduced as part of this research. In Figure 3.5 we classified these attacks with respect to the taxonomy we have developed.

3.5 Current States of OFDM Jamming Attacks

In this section, we explore the current status of jamming attacks on OFDM systems and present a survey on various jamming attacks that can be found in the open literature. The coverage is not all-inclusive; however, most of the common approaches are addressed here.

The most common jamming type that deserves first attention is the noise jamming. In noise jamming, the jamming carrier signal is modulated with a random noise waveform with an intent to disrupt the communication by injecting noise into the receiver. The noise is generally assumed to be Gaussian. A number of papers is available where research is conducted on OFDM systems under barrage jamming attack [7, 29, 33, 67]. A noteworthy mention would be [29], where Lou *et al.* derived the bit error rate (BER) of OFDM under barrage jamming. A jamming game on OFDM setting is explored by Renna *et al.* in [67]. Another major class of noise jamming on OFDM is the partial-band jamming, in which part of a wideband system is jammed intentionally [27–33]. In [28,32–36,68,69] the impact of noise jamming on OFDM-based broadband standards (e.g., Wi-Fi and WiMAX) are explored.

There has been considerable research on OFDM synchronization in the past twenty years. Classical synchronization methods are presented in [23, 39, 40]. In addition, there are a plethora of other methods – some of them specialized, slightly modified, or system specific – examples of which are presented in [18–22]. Previous research encompasses both symbol timing acquisition as well as carrier frequency offset estimation due to the fact that they can be performed jointly or separately.

While there has been research conducted on robustness of OFDM synchronization algorithms [13–22, 70], the majority of this work has been conducted under the assumption of uncorrelated or narrowband interference. Some of these works also include interference detection and mitigation strategies. Recently, specific adversarial signals are introduced [8, 9] which are highly correlated and designed with the intent of disrupting the OFDM system

during the synchronization stage. In those research, the authors focus on jamming attacks that prevent a receiver employing OFDM from ever acquiring the proper symbol timing estimate. This work is based on the symbol timing and carrier frequency offset estimation algorithm designed by Schmidl and Cox [23], which is the maximum likelihood detector for OFDM, and because of its optimality it is widely used in commercial systems based on OFDM, the WiMAX standard being the most recognizable instance.

In OFDM systems, the channel impulse response is estimated and equalized using known symbols, called pilot tones [50, 51, 71]. Clancy *et al.* [72] discussed possibility of jamming the channel estimation procedure as an efficient type of attack. It is suggested that targeting the channel sounding or accuracy of channel state information (CSI) estimation not only requires less power, but also more efficient than barrage jamming. Following [72], jamming of channel estimation and equalization are studied for SISO-OFDM communications [7, 10] and MIMO-OFDM channels [73, 74]. The impact of jamming pilot tones and disrupting equalization process of OFDM systems can also be found in [68, 75–78].

Literature related to control channel jamming attacks on modern wireless broadband technologies is limited. The authors of [79] investigate the extent to which LTE is vulnerable to intentional jamming, by analyzing the components of the LTE downlink and uplink signals. This includes the jamming vulnerability of each control channel in LTE. A survey of the security of LTE availability is given in [80]. The authors of [81] analyze PHY and MAC layer vulnerabilities in WiMAX. While all of these papers focus on the specific PHY and MAC layer channels within each technology, they can be termed as the random access channel attack and the resource allocation attack.

3.6 Noise Jamming Attacks on OFDM Systems

In this section, we briefly discuss various noise jamming attacks on OFDM systems that can be found in open literature such as barrage jamming, partial-band jamming, single-tone jamming and multi-tone jamming etc.

3.6.1 Barrage Jamming

The barrage jamming is the most basic jamming of all the jamming attacks. Conceptually it is also the simplest one, requires no additional information. The other name of the barrage jamming is wideband jamming. In barrage jamming attack, entire transmission bandwidth of the target is blanketed with white Gaussian noise with 100% duty cycle in time. Thus, it is non-correlated and non-protocol-aware attack. It has been shown game theoretically and information theoretically to be the optimal jamming strategy in the absence of any *a priori* knowledge of the target signal [26]. Thus barrage jamming is often treated as the baseline for comparing other jamming attacks.

The objective of barrage jamming is to jam entire transmission with Gaussian noise that increases the noise floor and reduces the signal-to-noise ratio (SNR) at target receiver. The consequence of such jamming is elevated noise n_i and noise error ϵ_i^n, thus resulting higher noise variance, σ_n^2. We use this as the baseline when evaluating other jamming attacks discussed in this dissertation, including pilot tone jamming and pilot tone nulling attacks.

3.6.2 Partial-band Jamming

In partial-band noise (PBN) jamming, a certain fraction of the occupied bandwidth is jammed with Gaussian noise. If the jamming power is constant, then the performance of the PBN depends on the fraction between jamming bandwidth and signal bandwidth. The

jammer-to-signal power ratio (JSR) is given by $\frac{P_{PBN}}{P_{Sig}}$ and the jammer-to-signal bandwidth fraction ratio (JFR) is given by $\rho = \frac{W_{PBN}}{W_{Sig}} \leq 1$, are important values when considering PBN jamming. Here P_{PBN} is the jamming power, P_{Sig} is the target signal power, W_{PBN} is the jamming signal bandwidth, and W_{Sig} is the target signal bandwidth [29]. The power spectral density (PSD) of the PBN is [29]

$$PSD_{PBN} = \frac{P_{Sig}}{\rho} = \frac{P_{PBN}}{W_{Sig}}.\frac{W_{Sig}}{W_{PBN}} = \frac{P_{PBN}}{W_{PBN}}. \tag{3.2}$$

In PBN, the target signal has two frequency bands – i) a jammed band and ii) an unjammed band. If the average PSD of PBN is N_{PBN}, then the effective PSD of PBN in the jammed bands becomes $\frac{N_{PBN}}{\rho}$. Taking this in consideration, we can get the BER for QPSK modulated OFDM system under PBN as [29, 50]

$$P_b(\rho) = \rho.\mathbf{Q}\left(\sqrt{\frac{2E_b}{N_0 + \frac{N_{PBN}}{\rho}}}\right) + (1-\rho).\mathbf{Q}\left(\sqrt{\frac{2E_b}{N_0}}\right). \tag{3.3}$$

The PBN is usually considered a non-correlated jamming attack because the jammer transmits continuously in time. Launching PBN jamming attack against an OFDM waveform is not very effective strategy because strong forward error correction could allow the data to be reconstructed from the unjammed subcarriers.

3.6.2.1 Single-tone Jamming (STJ)

Single-tone jamming (STJ) is a special kind of partial-band jamming where a single high powered tone is transmitted to jam the system of interest. This tone can be of any form and shape. However, the most common ones are impulse, rectangular and Gaussian noise shape.

For OFDM systems, a single-tone jammer is considered to be the one that jams a single

subcarrier. The time-domain single-tone jamming signal for OFDM subcarrier is

$$J(t) = A_J \cos(2\pi f_J t) = \sqrt{2J} \cos(2\pi f_J t), \tag{3.4}$$

where A_J is the amplitude of jamming tone, J is the power of the tone, and f_J is the jamming center frequency [29]. STJ is often used to corrupt the target's automatic-gain-control mechanism; indirectly jamming the rest of the subcarriers.

3.6.2.2 Multi-tone Jamming (MTJ)

Multi-tone jamming (MTJ) is a special kind of partial-band jamming, where multiple equal powered tones in certain frequencies are transmitted to jam the system of interest. As the jammer is power limited, the number of tones is inversely proportional to the power of individual tones. Let J_T be the total jamming power and N_T be the number of tones present in the multi-tone jammer, then the multi-tone jamming power distribution in frequency domain can be expressed as

$$J(k) = \begin{cases} A_k = \frac{J_T}{N_T} & f_L \leq k \leq f_H \\ 0 & \text{otherwise} \end{cases} \tag{3.5}$$

where A_k represents the amplitude of the k-th frequency bin (or subcarrier in the case of OFDM) and frequency index, $k = \{f_L, f_{L+1}, \ldots f_{H-1}, f_H\}$ [29, 82].

For OFDM systems, a multi-tone jammer is considered to be the one that jams multiple subcarriers. Every jamming tone can be modeled as

$$J(t) = A_J \sum_{k=1}^{N_T} \cos(2\pi f_k t) = \sqrt{\frac{2J_T}{N_T}} \sum_{k=1}^{N_T} \cos(2\pi f_k t), \tag{3.6}$$

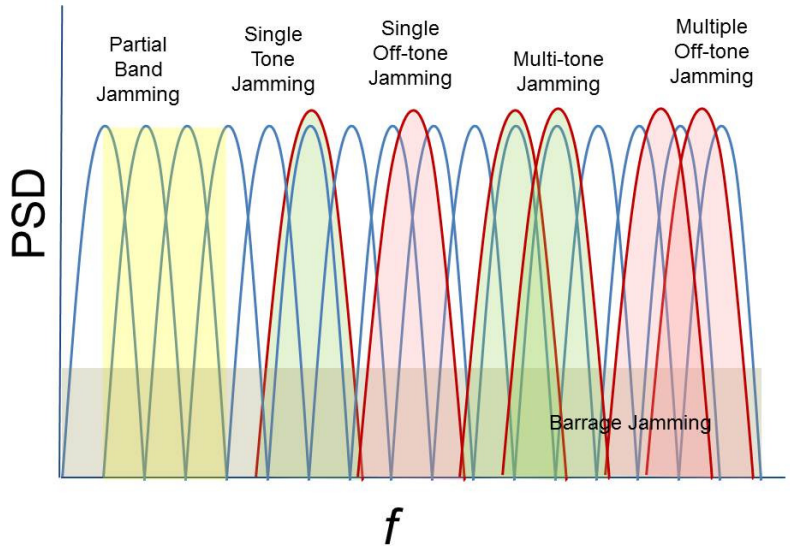

Figure 3.6: Different jamming attacks on OFDM subcarriers.

where A_J is the amplitude of jamming tone, J is the power of the tone, and f_k is the jamming center frequency of k-th subcarrier [82]. MTJ might be used to conserve power while still causing denial of service. Apart from the aforementioned ones, we can find other type of noise jamming attacks such as pulsed and sweeping jamming attack [69].

3.7 Asynchronous Off-tone Jamming Attack

In this section, we introduce and investigate new 'asynchronous off-tone' jamming attacks on OFDM waveforms. Figure 3.6 shows different jamming attacks on OFDM subcarriers.

3.7.1 Asynchronous Off-tone Jamming

The Barrage jamming is optimum when jammer lacks target information. However, wide-band systems such as OFDM require a lot of energy to jam. Researchers attempted to invent various partial-band jammings that require lot less power. Conventional partial-band

jamming attacks are not efficient against OFDM. Synchronized single-tone and multi-tone jamming can successfully jam individual subcarriers, but require knowledge of target's carrier frequencies to align with them, which is difficult in real world scenarios. Here, we propose 'asynchronous off-tone' partial-band jamming that does not need knowledge of target's carrier frequencies and is capable of doing more harm to the target signal.

The OFDM receiver performs FFT operation to convert time-domain signal to frequency-domain signal. Forward FFT takes a signal, multiplies it successively by complex exponential over a range of frequencies, sums each product and plots results as a coefficient of that frequency. However, if the input signal is not perfectly periodic in the sample window or have offset at sampling frequencies, then the energy gets smeared from the true frequency into adjacent frequency bins that eventually creates ICI on the OFDM waveforms at the receiver [83]. Besides this, the tail or side-lobes of a signal, i.e., *sinc function*, not aligned with the orthogonal OFDM subcarriers due to frequency offset can have non-zero components at the sampling period that can be a source of ICI as well. Figure 3.7 shows ICI effect on the OFDM subcarriers due to off-tone jamming attacks. These are the two key incentives of designing jamming signal that is non-periodic by nature and has frequency offset with the target receive signal. On top of these, such jamming attacks does not even need frequency matching with target signal. Moreover, the off-tone jammer can work without knowing the CSI between transmitter to target receiver and jammer to target receiver.

In the proposed scheme, the jammer is off-tone or not synchronous with the target signal. The ith element of the time-domain jamming signal, $j_{\text{off},i}[n]$, can be expressed as

$$j_{\text{off},i}[n] = \frac{1}{N} \sum_{k=0}^{N-1} J_i[k] e^{j\frac{2\pi(k+\varepsilon)n}{N}}, \tag{3.7}$$

where $J[k]$ is the jamming signal in frequency-domain, the power of which equals $\frac{\|J[k]\|^2}{2}$, and ε is the normalized center frequency offset (CFO). If target's subcarrier spacing is Δf_{SC}, and

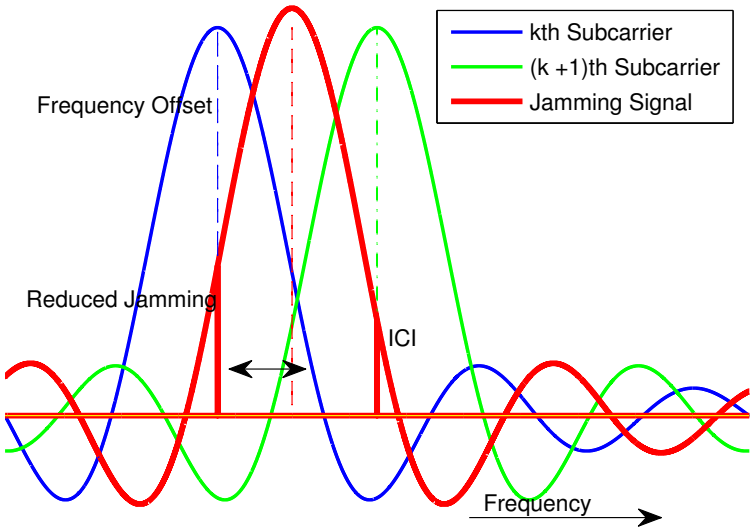

Figure 3.7: ICI at OFDM subcarriers due to 'asynchronous' off-tone jamming attacks.

jamming CFO from target's center frequency is f_{offset}, then the normalized CFO ε is

$$\varepsilon = \frac{f_{\text{offset}}}{\Delta f_{\text{SC}}}. \tag{3.8}$$

For the time-domain jamming signal $j[n]$, a CFO of ε causes a phase offset of $2\pi n\varepsilon$, that is, proportional to the CFO ε and time index n. Note that it is equivalent to a frequency shift of $-\varepsilon$ in the frequency-domain jamming signal $J[k]$.

Let ε_i and ε_f denote the integer part (IFO) and fractional part (FFO) of normalized CFO ε, respectively, therefore,

$$\varepsilon = \varepsilon_i + \varepsilon_f, \tag{3.9}$$

where $\varepsilon = \lfloor \varepsilon_i \rfloor$.

Due to the IFO, the transmitted jamming signal $J[k]$ is cyclic shifted by ε_i in the receiver, and thus producing $J[k-\varepsilon_i]$ in the kth subcarrier. However, the orthogonality among target subcarrier and jamming signal components is not destroyed and thus, ICI does not occur

like FFO ε_f. Hence, we omit IFO here, i.e., $\varepsilon_i = 0$ and go with FFO only so that $\varepsilon = \varepsilon_f$.

Apart from the off-tone, the jamming signal can be any form or shape. However, ensuring non-periodic samples in target's sampling period and selecting signals with strong side-lobes may increase the effectiveness of the jammer. Like STJ and MTJ, the proposed off-tone jammer can be both single off-tone jamming (SOTJ) or multiple off-tone jamming (MOTJ).

The equalized received signal in frequency-domain in the presence of asynchronous off-tone jamming with normalized CFO of ε can be written as follows

$$
\begin{aligned}
\widetilde{Y}_i[k] &= \sum_{n=0}^{N-1} \frac{1}{N} \sum_{m=0}^{N-1} \frac{H_i[m]X_i[m]}{\hat{H}_i[m]} e^{\frac{j2\pi mn}{N}} e^{\frac{-j2\pi kn}{N}} + \sum_{n=0}^{N-1} \frac{1}{N} \sum_{m=0}^{N-1} \frac{G_i[m]J_i[m]}{\hat{H}_i[m]} e^{\frac{j2\pi(m+\varepsilon)n}{N}} e^{\frac{-j2\pi kn}{N}} \\
&\quad + \sum_{n=0}^{N-1} \frac{w_i[n]}{\hat{h}_i[m]} e^{\frac{-j2\pi kn}{N}} \\
&= \frac{H_i[k]}{\hat{H}_i[k]} X_i[k] + \frac{1}{N} \frac{1 - e^{j2\pi\varepsilon}}{1 - e^{\frac{j2\pi\varepsilon}{N}}} \frac{G_i[k]J_i[k]}{\hat{H}_i[k]} + \frac{1}{N} \sum_{m=0, m\neq k}^{N-1} \frac{G_i[m]J_i[m]}{\hat{H}_i[m]} \frac{1 - e^{j2\pi(m-k+\varepsilon)}}{1 - e^{\frac{j2\pi(m-k+\varepsilon)}{N}}} \\
&\quad + \frac{W_i[k]}{\hat{H}_i[k]} \\
&= \underbrace{\frac{H_i[k]}{\hat{H}_i[k]} X_i[k]}_{\text{Signal}} + \underbrace{e^{\frac{j\pi\varepsilon(N-1)}{N}} \left[\frac{\sin(\pi\varepsilon)}{N \sin\left(\frac{\pi\varepsilon}{N}\right)} \right] \frac{G_i[k]}{\hat{H}_i[k]}}_{\text{Scaling of jammer for frequency offset}} J_i[k] \\
&\quad + \underbrace{e^{\frac{j\pi\varepsilon(N-1)}{N}} \sum_{m=0, m\neq k}^{N-1} \frac{\sin(\pi(m-k+\varepsilon))}{N \sin\left(\frac{\pi(m-k+\varepsilon)}{N}\right)} \frac{G_i[m]J_i[m]}{\hat{H}_i[m]} e^{\frac{j\pi(m-k)(N-1)}{N}}}_{\text{ICI caused by off-tone jammer}} + \frac{W_i[k]}{\hat{H}_i[k]}
\end{aligned}
\tag{3.10}
$$

From Equation 3.10 we can see that intentional off-tone jammer has two fold effects: jamming signal scaling and ICI. The first term represents the amplitude and phase change of jamming signal's frequency component that results a scaling of jamming signal. Meanwhile, ICI from the other off-tone jamming signal components implies that the orthogonality among jammer and target is not maintained any longer due to offset. The net result is an enhancement of jammer's effectiveness [84].

3.7.2 Simulation and Results

Here, we develop Monte-Carlo simulations based on OFDM channel model as shown in Figure 2.1 to validate the impact of off-tone jamming attacks. In the receiver, Quadrature Phase Shift Key (QPSK) modulated data and pilot tones are passed through an inverse discrete Fourier transform and then sent over an 8-tap random channel (i.e., Rayleigh Channel) and then AWGN was added. The OFDM modulation used here deploys a 256-point FFT with a cyclic prefix length of 1/8.

Standard OFDM systems use equal power and equally-spaced pilot tones. The model used here has every 8th subcarrier as a pilot tone. The attack signal is added to the received signal after being passed through a channel with different filter tap coefficients. Jammer is assumed to be in the middle of two adjacent OFDM subcarriers, i.e., $\varepsilon = 0.5$. In the receiver, combined target and jamming signal are received, passed through Fourier transform, and equalized using linear interpolation method based on pilot tones. Simulations are run for 5,000 iterations with variable signal-to-noise ratio (SNR), and signal-to-jamming ratio (SJR).

At first we begin with the conventional jamming strategies. In Figure 3.8 we have looked into the performance of OFDM system under barrage, partial band, single-tone, and multi-tone jamming attack. It is found that, for a target operating at 5 dB SNR and 0 dB SJR, BJ has BER of 0.3, PBJ has BER of 0.2, STJ has BER of 0.12, and MTJ has BER of 0.06. This result is expected as all these conventional jammers work in the same way – they just jam individual subcarriers. Hence, their impacts entirely depend on the number of subcarriers they can occupy.

Next, we focus on our proposed 'asynchronous off-tone' jamming attacks. Figure 3.9 compares the impact of both conventional single-tone and single off-tone jamming attacks. Interestingly, the proposed SOTJ has about 3 dB more SJR loss for a target operating at 5 dB SNR, whereas, this ICI impact subsides as SJR increases, meaning jamming signal

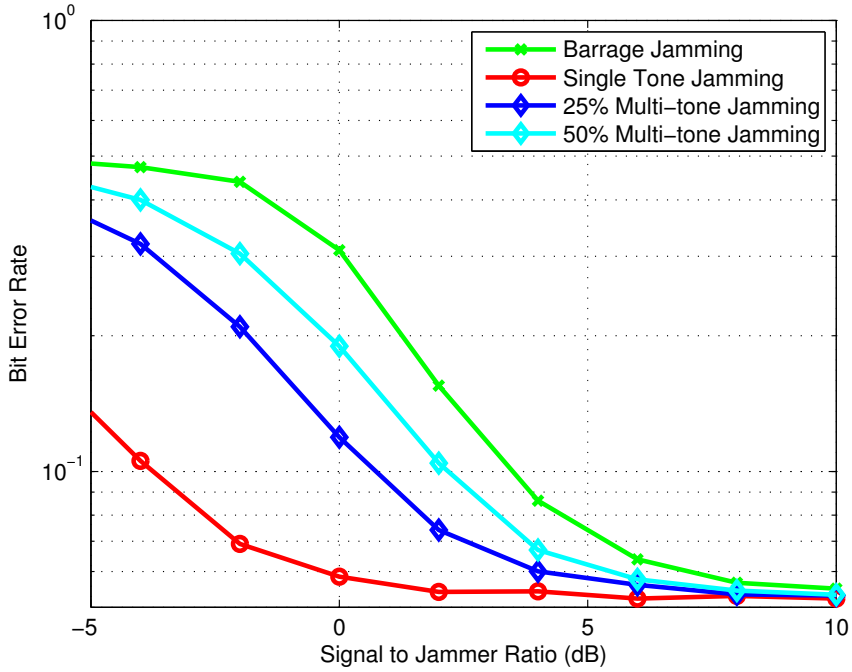

Figure 3.8: Performance of conventional jamming attacks as a function of SJR.

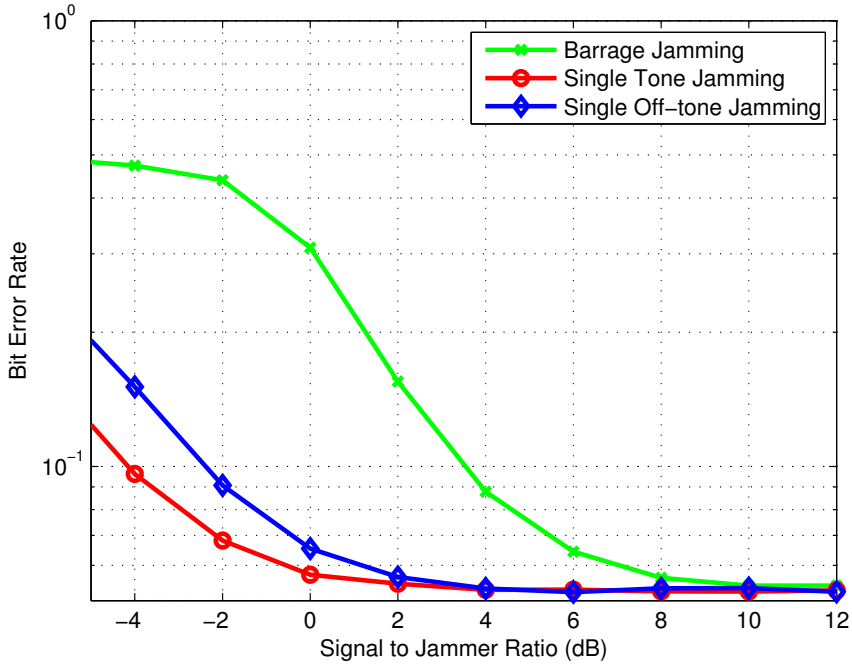

Figure 3.9: Performance of single off-tone jamming attack at 5 dB SNR as a function of SJR.

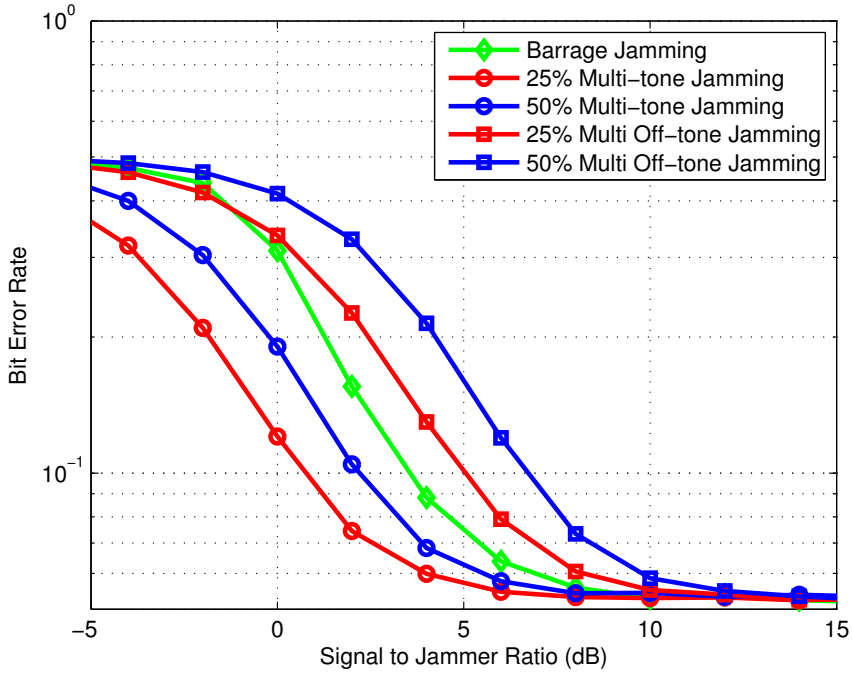

Figure 3.10: Performance of multiple off-tone jamming attack at 5 dB SNR as a function of SJR.

becomes weak enough to make any difference. In Figures 3.10 and 3.11 we compared the impact of both conventional multi-tone and multiple off-tone jamming attacks and found similar trend. In fact, the ICI effect from jammer's frequency offset is so profound that the MOTJ surpasses the barrage jamming for both 5 dB and 10 dB SNR target signal with as few as 25% bandwidth occupation by MOTJ.

Our second objective is to explore the performance behavior pattern of MOTJ with different strength. In Figure 3.10 and Figure 3.11 we found that MOTJ with 50% subcarrier jamming has BER of 0.32 and MOTJ with 25% subcarrier jamming has BER of 0.22 for a target operating at 5 dB SNR and 3 dB SJR.

Next, we compared the impact of MOTJ for target signal with different SNR levels – 5 dB and 10 dB SNR. Typically, the impact of jammer reduces with the increase of target signal strength. However, for MOTJ, the BER increases slightly or remain unchanged with

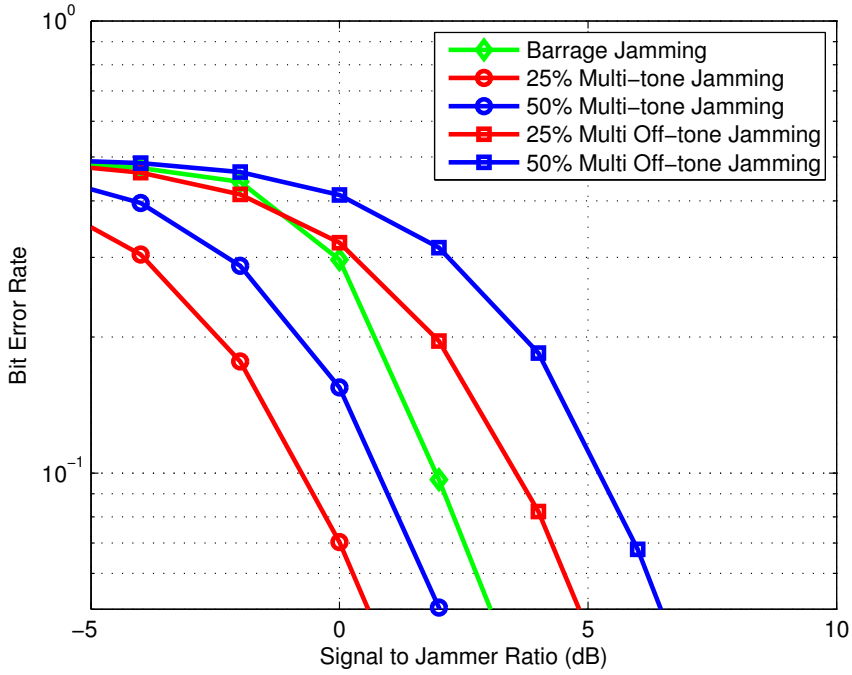

Figure 3.11: Performance of multiple off-tone jamming attack at 10 dB SNR as a function of SJR.

increase of target signal's SNR due to the accumulated ICI effect.

Lastly, we compared the impact of off-tone jamming attack under channel estimation error at the jammer in Figures 3.12 and 3.13. At 5 dB SNR and BER of 0.1, 20% CSI error causes SOTJ lose 1.5 dB and MOJT lose 1 dB. However, they are still more effective than STJ and MTJ, respectively.

3.8 Summary

In this chapter, we discussed the robustness of OFDM systems in wireless environment, looked insight of the current sources of interferences that are faced by OFDM-based communications systems. We modeled the OFDM channel under adversarial attacks and also presented a survey on existing jamming attacks.

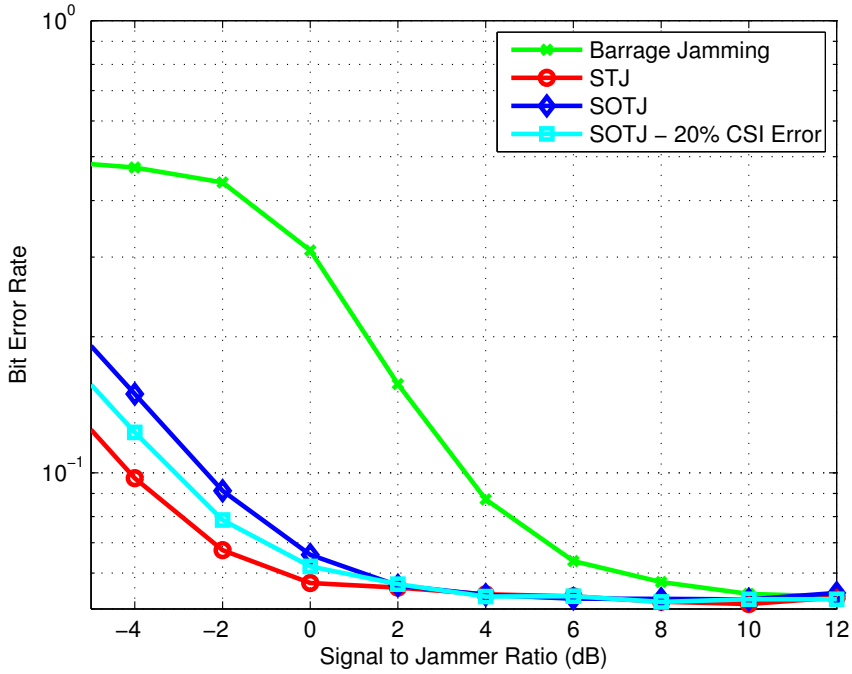

Figure 3.12: Performance of single off-tone jamming attack at 5 dB SNR as a function of SJR with CSI error.

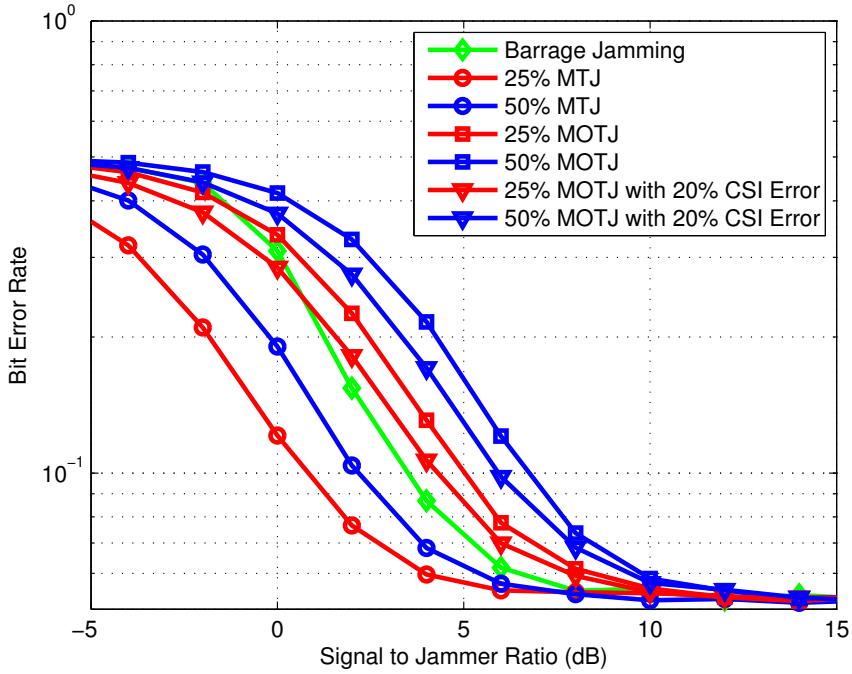

Figure 3.13: Performance of multiple off-tone jamming attack at 5 dB SNR as a function of SJR with CSI error.

In this chapter, we introduced a comprehensive communications jamming taxonomy. The jammer taxonomy presented here structures the organization of jammer classes by what information they possess and their capacity to act on that information. This new vision of jammers emerged naturally from the way contemporary wireless technology relies so extensively on software-driven behavior. In addition, understanding the vital capabilities that distinguish major classes of jamming, as well as the multidimensional parameter space, can benefit in the correct application of antijam strategies.

In this chapter, we introduced a new 'asynchronous off-tone' jamming attack on OFDM systems. We also investigated both the aligned and the off-tone jamming attacks on OFDM systems under various situations. Eventually the impact of all these attacks are compared with simple barrage jamming, which is considered as the optimum jamming in the absence of any knowledge about the target signal. It is found that while partial-band, single-tone, and multi-tone jamming attacks are more power efficient than barrage jamming, they have less impact than barrage jamming which essentially jams the entire bandwidth of the OFDM waveform. However, we have found that the impact of single-tone and multi-tone jamming attacks can be stretched out in spectrum and cause greater damage by transmitting jamming signals that have frequency offsets with the received signal. The key advantage of such attacks is that it does not require any synchronization with the target signal. Details of quantitative analysis are presented, which are eventually backed up by simulation.

Chapter 4

OFDM Equalization Jamming Attacks

In this chapter, we propose and investigate various power efficient equalization jamming attacks against OFDM systems, which include pilot tone jamming and pilot tone nulling attack. Signals known *a priori*, called pilot tones, are employed in the conventional OFDM systems to estimate the channel response and perform equalization. Attacks against these pilot tones can hamper equalization and degrade target's performance. This chapter begins with noise-based pilot tone jamming attack and then moves onto target waveform correlated pilot tone nulling attack. The chapter presents mathematical model of effective noise per symbol and simulation results for OFDM systems under such attacks. The chapter concludes that the noise-based pilot-tone attacks are power efficient than conventional attacks and the pilot nulling is capable of doing the most damage, but in the expense of additional channel state information (CSI). Figure 4.1 shows the subcarriers and channel estimation/interpolation process of OFDM systems under equalization (a.k.a. pilot tone) jamming attack.

The remainder of this chapter is organized as follows. In Section 4.1, barrage jamming is explained, which is used as baseline for comparing all other jamming attacks. Section 4.2 presents pilot tone jamming attack against OFDM. In Section 4.3, we introduce novel pilot tone nulling attack against OFDM. Section 4.4 undertakes an assessment on the CSI avail-

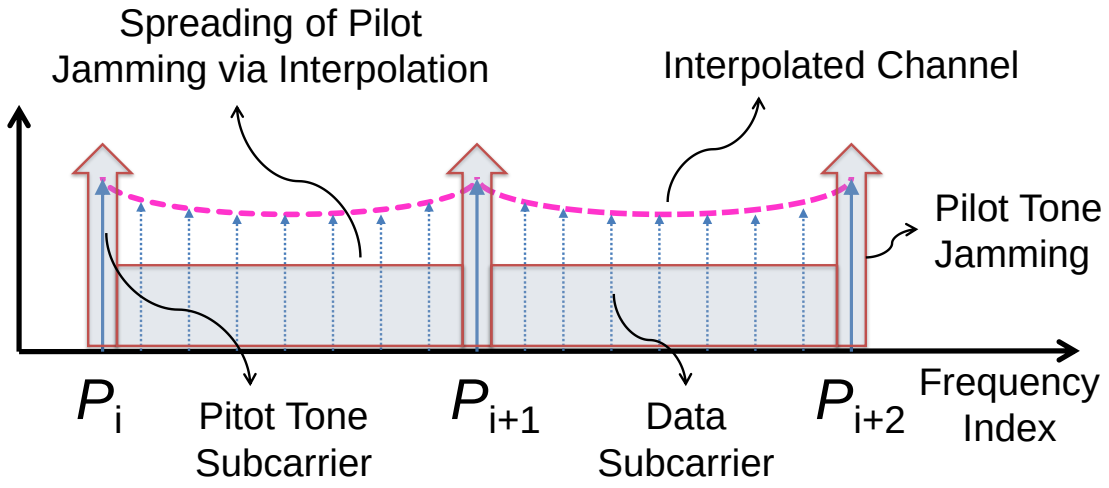

Figure 4.1: Subcarriers and channel estimation/interpolation process of OFDM systems under equalization (a.k.a. pilot tone) jamming attack.

ability, accuracy and impact for the equalization jamming attacks. Section 4.5 discusses the preliminary assumptions and limitations of the proposed attacks. We compare the efficacy of the equalization attacks among themselves and with other protocol-aware attacks in Section 4.6. In Section 4.7, we derive the bit error probability of the OFDM sysmtes under jamming attacks. Section 4.8 analyzes the impact of synchronization mismatch between jammer and target receiver. Section 4.9 provides simulations and analysis of results and finally, Section 4.11 provides a summary of this chapter.

4.1 Barrage Jamming Attack

The barrage jamming is the most basic jamming of all the jamming attacks. Conceptually it is also the simplest one, requires no additional information. The other name of the barrage jamming is wideband jamming. In barrage jamming attack, entire transmission bandwidth of the target is blanketed with white Gaussian noise. It has been shown game theoretically and information theoretically to be the optimal jamming strategy in the absence of any *a*

priori knowledge of the target signal [26]. Thus barrage jamming is often treated as the baseline for comparing other jamming attacks.

The objective of barrage jamming is to jam entire transmission with white Gaussian noise that increases the noise floor and reduces the signal-to-noise ratio (SNR) at target receiver. The consequence of such jamming is elevated noise n_i and noise error ϵ_i^n, thus resulting higher noise variance, σ_n^2. We use this as the baseline when evaluating the pilot tone jamming and pilot tone nulling attacks.

4.2 Pilot Tone Jamming Attack

Pilot tone jamming attack is the first of two equalization attacks we proposed here. In pilot tone jamming, user with malicious intent (or adversary) attempts to increase the noise floor of the targets' pilot tones by transmitting Gaussian noise only at the pilot tone frequencies of the target transmitter-receiver pair and thus disrupt the equalization process. The fundamental assumption here is that the jammer has knowledge about the targets' pilot tone frequencies and is synchronized with the target signal through observation of communication between parties in the network. In this case, the jammer can unleash pilot tone jamming attack by transmitting signal vector, $Z_i = q_i = qn_i^{PJ}$ for targets' pilot tones, where q is the received jamming power, and n_i^{PJ} is i.i.d. zero mean Gaussian noise with distribution $\mathcal{N}(0, \sigma_{PJ}^2)$, and signal vector, $Z_i = 0$ for non-pilot tone subcarriers (data payload).

Note that the family of normal distributions is closed under linear transformations. That is, if some $q_i = qn_i^{PJ}$ is normally distributed with mean μ_{PJ} and variance σ_{PJ}^2, then a linear transform $a_{PJ}n_i + b_{PJ}$ (for real numbers a_{PJ} and b_{PJ}) is also normally distributed with $a_{PJ}n_i^{PJ} + b_{PJ} \sim \mathcal{N}\left(a_{PJ}\mu_{PJ} + b_{PJ}, a_{PJ}^2\sigma_{PJ}^2\right)$. For $\mu_{PJ} = 0$, $b_{PJ} = 0$, $a_{P_J} = q$, q_i is i.i.d. Gaussian with distribution $\mathcal{N}(0, q^2\sigma_{PJ}^2)$.

Note that for all pilot tone based attacks, we assume attack energy is evenly distributed

between all pilot tone subcarriers, for the same reasons that it was determined optimal for pilot tone energy to be evenly distributed between all pilot tone subcarriers [43].

The impact is that the error term ϵ_i^{PJ} under pilot tone jamming attack is dominated by the jammer power, and becomes the linear combination of the jammed energy. For i.i.d. pilot tone jamming, the mean distribution can be expressed as

$$\bar{\epsilon}_i^{PJ} \sim \mathcal{N}\left(0, \frac{2}{3} q^2 \sigma_{PJ}^2\right). \tag{4.1}$$

The received pilot tone at target subject to pilot tone jamming is

$$Y_{k_i}^{PJ} = H_{k_i} p_i + G_{k_i} q_i + n_{k_i} \tag{4.2}$$

where G_{k_i} is the Jx to Rx channel. Assuming $\sigma_n = \sigma_{PJ}$, mean distribution for i.id. jamming follows the distribution

$$\bar{\epsilon}_i^{PJ} \sim \mathcal{N}\left(0, \frac{2}{3} G_i^2 q^2 \sigma_n^2\right). \tag{4.3}$$

Notice that if the same Gaussian noise sequence is coherently transmitted on all pilot tones simultaneously, then noise is not averaged out for linear combinations. That is why jamming pilot tones with coherent signal maximizes damage. Thus it is beneficial to coherently jam pilot tones, and in this case, the overall per-symbol error term, $\alpha_i^{PJ} = \hat{X}_i - X_i$, becomes

$$\alpha_i^{PJ} = \frac{n_i - X_i \left(\bar{\epsilon}_i^{PJ} + \epsilon_i^n + \epsilon_i^a\right)}{H_i + \left(\bar{\epsilon}_i^{PJ} + \epsilon_i^n + \epsilon_i^a\right)}. \tag{4.4}$$

4.3 Pilot Tone Nulling Attack

Pilot tone nulling has the starkest consequence on the OFDM equalizer, which attempts to annul the pilot tones of OFDM systems. The goal of this attack is to transform $\hat{H}_i$ to

asymptotically close to zero, so that when $\hat{X}_i$ is calculated from $\hat{X}_i = Y_i/\hat{H}_i$, it causes a division by zero (or near zero) that results in arbitrarily large $\hat{X}_i$.

Initiation of pilot tone nulling attack depends on the assumption of adversary having the knowledge of its own channel to target receiver, $\hat{G}_{k_i}$ and the channel between transmitter and target receiver, $\hat{H}_{k_i}$. The jammer transmits signal J, which can be defined as

$$J_{k_i} = \left(\frac{\hat{H}_{k_i}}{\hat{G}_{k_i}}\right) e^{j\pi} p_i = -\left(\frac{\hat{H}_{k_i}}{\hat{G}_{k_i}}\right) p_i \tag{4.5}$$

which is channel-corrected, π-radian phase shifted pilot tone.

The received pilot tone subject to nulling attack is then

$$Y_{k_i}^N = H_{k_i} p_i - G_{k_i}\left(\frac{\hat{H}_{k_i}}{\hat{G}_{k_i}}\right) p_i + n_{k_i} \tag{4.6}$$

If the estimated channel state information (CSI) at the jammer is close to the actual value, then target will see noise only, meaning $Y_{k_i}^N$ will be close to n_{k_i}. If the residue term is assumed as δ_i, then it can be defined as

$$\delta_i = H_{k_i} - G_{k_i}\left(\frac{\hat{H}_{k_i}}{\hat{G}_{k_i}}\right) \tag{4.7}$$

then $Y_{k_i}^N = \delta_i p_i + n_{k_i}$ and

$$\hat{H}_{k_i}^N = \delta_i + \frac{n_{k_i}}{p_i}. \tag{4.8}$$

If $\overline{\delta}_i$ is assumed to be the linearly-combined error for non-pilot tones, where $\overline{\delta}_i$ is also a normally distributed random variable with distribution $\mathcal{N}(0, \sigma_{\overline{\delta}_i}^2)$, then the overall channel noise error due to residue term and AWGN is normally distributed as well

$$\epsilon_i^N \sim N\left(0, \sigma_N^2\right) \tag{4.9}$$

where $\sigma_N^2 = \sigma_{\overline{\delta}_i}^2 + \frac{2}{3}\sigma_n^2$.

If the remaining derivation is carried through, then the symbol error, $\alpha_i^N = \hat{X}_i - X_i$, can be obtained

$$\alpha_i^N = \frac{n_i - X_i\left(\overline{\delta}_i + (\epsilon_i^n + \epsilon_i^a) - H_i\right)}{\overline{\delta}_i + (\epsilon_i^n + \epsilon_i^a)}. \tag{4.10}$$

4.4 CSI Availability, Accuracy and Impact

For both barrage and pilot tone jamming cases, the jammer transmits Gaussian noise. On the other hand, pilot tone nulling tries to null the pilot tones utilizing the knowledge of CSI. Therefore, the jammer requires CSI between the jammer and the target receiver, $\mathbf{G}$, and CSI between the transmitter and the target receiver, $\mathbf{H}$, where $\mathbf{G} = [G_1, G_2, \cdots]$ and $\mathbf{H} = [H_1, H_2, \cdots]$. Absence or inaccurate CSI can result rapid loss of effectiveness of the pilot tone nulling attacks.

The first step is to estimate $\mathbf{G}$, the channel between the jammer and the target receiver. The jammer can estimate $\mathbf{G}$ if the forward and backward channels are assumed to be reciprocal, like the time division duplex. The next step is estimating $\mathbf{H}$, the channel gain between the transmitter and the target receiver. Even though this estimation is condition-dependent, enough real-life examples can be found where it is possible. For example, well developed methods can be found in the literature that discusses about the estimation of $\mathbf{H}$ for MIMO and OFDM systems [85]. However, in this case, jammer faces uncooperative target nodes. In this situation, blind techniques are needed to be adopted by the jammer. For example, jammer can simply listen to the feedback CSI from the receiver to the transmitter. However, most of these methods are valid only when the channel is static or quasi-static.

4.5 Assumptions and Limitations of Attacks

The effective implementation of pilot tone nulling attack requires accurate CSI of channel **G** and **H**. Absence or inaccurate CSI can result in rapid loss of effectiveness of the attacks. Occasionally estimating **G** can be delicate as this depends on target receivers transmission policies and in some cases target receiver may not be transmitting anything. Also the methods for estimating **H** are valid only when the channel is static or quasi-static. On top of that, effective pilot tone jamming and pilot tone nulling attacks demand time and frequency synchronization with the target receiver. Mismatch of any kind guarantees degradation in jamming efficacy, which is further discussed in the forthcoming sections.

4.6 Attack Comparison

In this section, we compare the efficacy of the equalization attacks among themselves and with other protocol-aware attacks.

4.6.1 Comparison Among Equalization Attacks

As both barrage and pilot tone jamming use Gaussian noise, they both dismay target in the same way and achieve similar results. However, the pilot tone jamming requires significantly less power to achieve same amount of performance degradation at the target. The reason is simple – jammer transmits only at the target receivers' pilot tones, since only pilot tones need to be jammed. In this case, the jamming power smears across all the subcarriers and thus, the channel noise error ϵ_i^{PJ} is distributed across all subcarriers.

Pilot tone nulling, then again, has the starkest effect as the impact becomes greater due to the fact that H_i moves from denominator to numerator of the error term, making its impact

greater. When $\hat{\delta}_i$, the channel estimation error, is significantly small, this term is significant.

The effect of these jamming attacks on bit error rate (BER) performance is thoroughly investigated, both analytically and simulation-wise, in subsequent sections.

4.6.2 Comparison with Protocol-aware Attacks

Unlike Section 4.6, other protocol-aware attacks presented in [86,87] and [24] are compared here with the proposed ones. In [86], Physical Broadcast Channel (PBCH) message eavesdropping is proposed that relates to 'cell searching procedure' in LTE. As attacks against cellular networks, downlink and uplink smart jamming, and rogue base-station attacks are investigated. In [24], vulnerabilities physical channel and PHY-layer signals are presented. As physical channel vulnerability user data attacks, uplink and downlink control channel attacks are introduced. As PHY-layer attack primary and secondary synchronization signal, and downlink reference signal attacks are discussed. Also in [87], attacks against synchronization mechanism like 'Schmidl and Cox' is discussed, which precedes equalization.

The key advantage of pilot tone nulling is that it can be very effective and generic to any standard that uses OFDM. But it has very strong requirements, such as full time-frequency synchronization, knowledge of CSI, propagation delay of the target, etc. The OFDMA attacks overviewed in [86,87] and [24] have fewer requirements as, in some cases, they target some specific signaling tones in the UL such that the entire cell is blocked. On the other hand, the attacks are less generic in the sense that they are specifically crafted against LTE communication systems.

4.7 Bit Error Probability Calculation

In this section, we calculate the bit error probability (BEP) of OFDM systems under jamming attacks. The BEP is the expectation value of the bit error rate (BER) and equivalent to BER assuming i.i.d. and for a long time interval and a high number of bit errors. Assuming overall channel estimation error, ϵ_i is linear combination of noise error, ϵ_i^k, and approximation error, ϵ_i^a, we get

$$\begin{aligned} \epsilon_i &= \hat{H}_i - H_i \\ &= \left(H_i + \left(\epsilon_i^k + \epsilon_i^a\right)\right) - H_i \\ &= \epsilon_i^k + \epsilon_i^a \end{aligned} \tag{4.11}$$

where $k = \{n, J, N\}$ for no jamming and/or barrage jamming, pilot tone jamming, and pilot tone nulling respectively. If both ϵ_i^k and ϵ_i^a are independent random variables, then the cumulative distribution of overall channel estimation error is

$$\begin{aligned} F_{\epsilon_i}(\epsilon_i) &= P\left[\epsilon_i^k + \epsilon_i^a \leq \epsilon_i\right] \\ &= \int_{\infty}^{\infty} \int_{-\infty}^{\epsilon_i - \epsilon_i^a} f_{\epsilon_i^k, \epsilon_i^a}(\epsilon_i^k, \epsilon_i^a) d\epsilon_i^k d\epsilon_i^a \end{aligned} \tag{4.12}$$

and the probability density function (pdf) is

$$\begin{aligned} f_{\epsilon_i}(\epsilon_i) &= \frac{d}{d\epsilon_i} F_{\epsilon_i}(\epsilon_i) \\ &= \int_{-\infty}^{\infty} f_{\epsilon_i^k, \epsilon_i^a}(\epsilon_i - \epsilon_i^a, \epsilon_i^a) d\epsilon_i^a \\ &= \int_{-\infty}^{\infty} f_{\epsilon_i^k}(\epsilon_i - \epsilon_i^a) f_{\epsilon_i^a}(\epsilon_i^a) d\epsilon_i^a. \end{aligned} \tag{4.13}$$

For noise error, $\epsilon_i^k \sim N(0, \sigma_k^2)$ and approximation error $\epsilon_i^a \sim U(-Kd^2, Kd^2)$, we get the pdf of the overall channel estimation error

$$\begin{aligned} f_{\epsilon_i}(\epsilon_i) &= \int_{-Kd^2}^{Kd^2} \frac{1}{\sqrt{2\pi\sigma_k^2}} \exp^{-\frac{(\epsilon_i - \epsilon_i^a)^2}{2\sigma_k^2}} U(-Kd^2, Kd^2) d\epsilon_i^a \\ &= \frac{1}{2}\left(\mathbf{erf}\left(\frac{\epsilon_i + Kd^2}{\sqrt{2\sigma_k^2}}\right) - \mathbf{erf}\left(\frac{\epsilon_i - Kd^2}{\sqrt{2\sigma_k^2}}\right)\right) \end{aligned} \tag{4.14}$$

with the mean, $E[\epsilon_i] = 0$ and the variance, $\sigma_{\epsilon_i}^2 = \int_{-Kd^2}^{Kd^2} \epsilon_i^2 f_{\epsilon_i}(\epsilon_i) U(-Kd^2, Kd^2)\, d\epsilon_i$.

The BER in slow-fading Rayleigh channel for BPSK at data subcarrier, taking account estimation error, is given by [88]

$$P_{b,BPSK} = \frac{1}{2}\left(1 - \frac{1}{\sqrt{1 + \frac{\sigma_{\epsilon_i}^2 + \frac{\sigma_n^2}{E_b}}{1 - \sigma_{\epsilon_i}^2}}}\right) \tag{4.15}$$

and for QPSK

$$P_{b,QPSK} = \frac{1}{2}\left(1 - \frac{1}{\sqrt{1 + \frac{2\sigma_{\epsilon_i}^2 + \frac{\sigma_n^2}{E_b}}{1 - \sigma_{\epsilon_i}^2}}}\right) \tag{4.16}$$

where $E_b = E_s / \log_2 M$ (M is M-ary modulation).

The average BER (or BEP) can be obtained by averaging P_b for all subcarriers in a symbol and all the symbols in a OFDM block. Notice that letting $\sigma_\epsilon \to 0$ produces well-known result for coherent BPSK and QPSK in Rayleigh channel [83].

4.8 Impact of Synchronization Error

The damage due to pilot-based jamming attack is maximum when the jammer is fully synchronized with the target [7]. However, maintaining perfect synchronization in all the parameters is a difficult task in reality, often we may observe mismatched jamming. The impact of mismatches are the subject of discussion in this section.

4.8.1 Time Offset

When the jamming signal is not aligned with received signal at the target receiver, the timing mismatch/offset occurs. Absence of common time reference, hardware clock imperfections, and changes in propagation time are the key reasons for time synchronization loss of the jamming signal. Figure 4.2(a) visually depicts the synchronization mismatch due to the jamming signal time offset. The time-domain signal, $j\,[n]$, with delay/advance of τ can be represented as $j_{to}\,[n] = j\,[n \pm \tau]$.

When the jamming signal is delayed, then the OFDM symbol is affected by part of the jamming signal. In this case, the jamming signal within the FFT interval for the current OFDM symbol can be expressed as

$$\begin{aligned} J_{to}\,[k] &= \frac{1}{N}\sum_{n=0}^{N-1} j\,[n+\tau]\, e^{-\frac{j2\pi nk}{N}} \\ &= \frac{1}{N}\sum_{n=0}^{N-1}\left\{\sum_{p=0}^{N-1} J\,[p]\, e^{\frac{j2\pi(n+\tau)p}{N}}\right\} e^{-\frac{j\pi nk}{N}} \\ &= \frac{1}{N}\sum_{p=0}^{N-1} J\,[p]\, e^{\frac{j2\pi p\tau}{N}} \sum_{n=0}^{N-1} e^{\frac{j2\pi(p-k)n}{N}} \\ &= J\,[k]\, e^{\frac{j2\pi k\tau}{N}} \end{aligned} \tag{4.17}$$

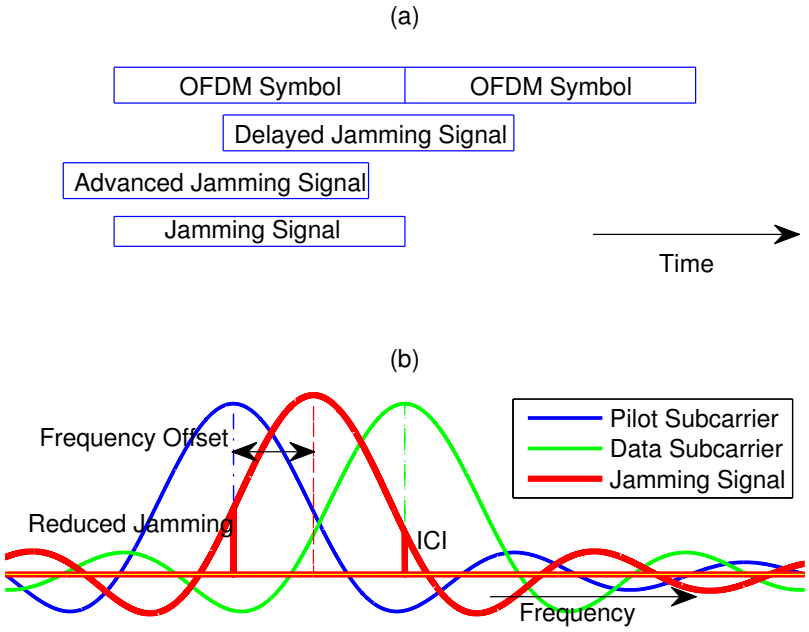

Figure 4.2: Visual description of mismatched synchronization for to a) timing offset and b) frequency offset.

where $J[k] = J$ on the pilot tones and $J[k] = 0$ on data SCs, and using following identity:

$$\sum_{n=0}^{N-1} e^{\frac{j2\pi(p-k)n}{N}} = e^{\frac{j\pi(p-k)(N-1)}{N}} \frac{\sin[\pi(k-p)]}{\sin\left[\frac{\pi(k-p)}{N}\right]} \tag{4.18}$$
$$= \begin{cases} N & \text{for } k = p \\ 0 & \text{for } k \neq p. \end{cases}$$

The Equation (4.17) infers that the orthogonality among all the subcarriers remained unchanged. However, an τ offset in the time-domain creates $\frac{2\pi k\tau}{N}$ phase rotation in the frequency-domain [84]. If the jamming signal is too delayed, then jamming signal may affect the cyclic prefix of the next OFDM symbol, which introduces inter-symbol interference (ISI) and inter-channel interferences (ICI) in that signal. In this case, the subcarrier s' orthogonal arrangement gets shattered by the ISI (from previous symbol) and additionally ICI arises.

When the jamming signal arrives earlier, then the current OFDM symbol is affected by part of current jamming signal and jamming signal for the next OFDM symbol. In this case, the jamming signal within the FFT interval for the current OFDM symbol becomes

$$\begin{aligned} J_{to}[k] &= \sum_{n=0}^{N-1-\tau} j_i[n+\tau]\, e^{-\frac{j2\pi nk}{N}} \\ &+ \sum_{n=N-\tau}^{N-1} j_{i+1}[n+2\tau-N_g]\, e^{-\frac{j2\pi nk}{N}} \\ &= \sum_{n=0}^{N-1-\tau} \left(\frac{1}{N} \sum_{p=0}^{N-1} J_i[p]\, e^{\frac{j2\pi p(n+\tau)}{N}} \right) e^{-\frac{j2\pi nk}{N}} \\ &+ \sum_{n=N-\tau}^{N-1} \left(\frac{1}{N} \sum_{p=0}^{N-1} J_{i+1}[p]\, e^{\frac{j2\pi p(n+2\tau-N_g)}{N}} \right) e^{-\frac{j2\pi nk}{N}} \\ &= \frac{N-\tau}{N} J_i[p]\, e^{\frac{j2\pi p\tau}{N}} \\ &+ \sum_{p=0, p\neq k}^{N-1} J_i[p]\, e^{\frac{j2\pi p\tau}{N}} \sum_{n=0}^{N-1-\tau} e^{\frac{j2\pi(p-k)n}{N}} \\ &+ \frac{1}{N} \sum_{p=0}^{N-1} J_{i+i}[p]\, e^{\frac{j2\pi p(2\tau-N_g)}{N}} \sum_{n=N-\tau}^{N-1} e^{\frac{j2\pi(p-k)n}{N}} \end{aligned} \tag{4.19}$$

considering the following identity:

$$\sum_{n=0}^{N-1-\tau} e^{\frac{j2\pi(p-k)n}{N}} = e^{\frac{j\pi(p-k)(N-1-\tau)}{N}} \frac{\sin\left[\frac{\pi(N-\tau)(k-p)}{N}\right]}{\sin\left[\frac{\pi(k-p)}{N}\right]} \tag{4.20}$$

$$= \begin{cases} N-\tau & \text{for } k=p \\ Nonzero & \text{for } k\neq p \end{cases} \tag{4.21}$$

where N_g is the guard interval length, the second term in the last line of Equation (4.19) represents the ICI, resulting the destruction of the orthogonality, and the last term suggests the emergence of ISI in the received signal [84].

The advanced/delayed arrival of jamming signal results change of jamming signal energy

at the target, which yields a different residue, δ_{to}. For pilot tone nulling (Equation (4.10)), the additive symbol error becomes

$$\alpha_{i,to}^{N} = \frac{n_i - X_i\left(\overline{\delta}_{i,to} + (\epsilon_i^n + \epsilon_i^a) - H_i\right)}{\overline{\delta}_{i,to} + (\epsilon_i^n + \epsilon_i^a)}. \tag{4.22}$$

4.8.2 Frequency Offset

The jammer can be subject to frequency offset due to *Doppler Shift* during propagation. The local oscillator at the transmitter and jammer can be unstable, which can create frequency offset in terms of phase distortion that can be modeled as zero-mean Wiener random process [84]. Also ICI can be created at the target receiver during FFT operation, if the jamming signal has offset at sampling frequencies and/or is aperiodic in the sample window. The offset and/or aperiodicity spread the jamming signal energy from the actual frequency bin to the neighboring frequency bins is the main reason for this ICI [83, 89]. Figure 4.2(b) shows two neighboring OFDM subcarriers and a frequency mismatched jamming signal that overlaps with both of these subcarriers. Notice that the mismatched jamming signal overlaps with both of these subcarriers.

Taking the FFT of pilot tone jamming signal $j\,[n]$ for ith OFDM symbol at the target receiver, the frequency-domain jamming signal can be written as

$$\begin{aligned} J_{fo}\,[k] &= \sum_{n=0}^{N-1} j\,[n]\, e^{-\frac{j2\pi kn}{N}} \\ &= \sum_{n=0}^{N-1} \frac{1}{N} \sum_{m=0}^{N-1} G\,[m]\, J\,[m]\, e^{\frac{j2\pi(m+\lambda)n}{N}} e^{-\frac{j2\pi kn}{N}} \\ &= \frac{1}{N} \frac{1 - e^{j2\pi\lambda}}{1 - e^{\frac{j2\pi\lambda}{N}}} G\,[k]\, J\,[k] \\ &\quad + \sum_{m=0, m\neq k}^{N-1} \frac{1 - e^{j2\pi(m-k+\lambda)}}{1 - e^{\frac{j2\pi(m-k+\lambda)}{N}}} G\,[m]\, J\,[m] \end{aligned} \tag{4.23}$$

$$= G[k]\, J[k] \Bigg(\underbrace{e^{\frac{j\pi\lambda(N-1)}{N}} \frac{\sin(\pi\lambda)}{N \sin\left(\frac{\pi\lambda}{N}\right)}}_{Scaling} + \underbrace{e^{\frac{j\pi\lambda(N-1)}{N}} \sum_{m=0, m\neq k}^{N-1} \frac{\sin(\pi(m-k+\lambda))}{N \sin\left(\frac{\pi(m-k+\lambda)}{N}\right)}}_{ICI} \Bigg)$$

where $J[k] = J$ on the pilot tones and $J[k] = 0$ on data subcarriers, λ is normalized carrier frequency offset (CFO) defined as $\lambda = \frac{f_{FO}}{f_{SC}}$, f_{SC} is subcarrier spacing, and f_{FO} is frequency offset. The λ normalized CFO creates $2\pi n\lambda$ phase offset in the time-domain, which is proportional to time index n and CFO. This is also equivalent to $\pm\lambda$, $J[k \pm \lambda]$ frequency shift in frequency-domain signal, $J[k]$. The deviated jamming signal is scaled at target pilot tone, but introduces ICI on data subcarriers.

An altered residue δ_{fo} for frequency offset can be obtained by plugging the offset jamming signal into (4.7). The effective additive symbol error for pilot tone nulling (Equation (4.10)) is given by

$$\alpha_{i,fo}^{N} = \frac{n_i - X_i\left(\overline{\delta}_{i,fo} + (\epsilon_i^n + \epsilon_i^a) - H_i\right)}{\overline{\delta}_{i,fo} + (\epsilon_i^n + \epsilon_i^a)}. \tag{4.24}$$

4.9 Simulation and Results

4.9.1 Simulation Methodology

In this section, we carried out rigorous simulation and analysis to verify the analytical outcomes of the jamming schemes that we presented. The Signal to Noise Ratios (SNRs) and the Signal to Jamming Ratios (SJRs) are varied throughout the experiments to collect the bit error rate (BER) at target receiver. Fixed WiMAX (802.16d) based OFDM waveform is generated here that employs 256-point FFT, 192 data subcarriers, pilot density of 8, 1/8-length cyclic prefix (CP), and QPSK modulation. The remaining subcarriers are null/guard-

bands. Like ITU Pedestrian B channel model, a 6-tap frequency-flat, Rayleigh slow-fading zero-mean AWGN channel is used. Normalized powered equalization attacks are synthesized and transmitted over own channel and added at the target receiver.

4.9.2 Result and Analysis

The first experiment is about quantifying the BER impact of SNR and SJR for three jamming attacks. It is found that lesser power is needed for equalization attacks to create same BER at the target. Figure 4.3 shows target's BER as function of SNR for a fixed 7 dB SJR. At 12 dB SNR, the BERs are 0.08, 0.13, 0.42 for barrage jamming, pilot tone jamming and pilot tone nulling respectively. Notice that due to pilot tone jamming, the ZF equalizer at the detector fails to eliminate ISI within a block and produces irreducible error floor. Figure 4.4 shows target's BER as function of SJR for a fixed 5 dB SNR received signal. Interestingly pilot jam and pilot null required 4 dB and 12 dB less power than barrage jam to cause 0.3 BER. Here, this 0.3 BER is taken as the baseline causing signal denial, meaning it will be difficult for error correction code to reliably yield error-free OFDM frames for the medium access control (MAC) layer.

A noteworthy observation is that the equalization attacks are not as effective as one might presume. When the pilot tone density is 1/8, only 1/8 of the target subcarriers are required to be jammed for equalization attack, the expected efficiency gain should be always 9 dB. But the effect of jamming is diluted by the linear arrangement across pilot tones. Whereas, in barrage jam, data subcarriers are under attacks from both direct jamming and equalization error that propagated, which enhanced the overall effect.

The second experiment is designed to analyze the impact of CSI quality for pilot tone nulling attacks. The performance of target under pilot tone nulling attacks are observed for situations where the adversary had (i) accurate estimation of both jamming channel

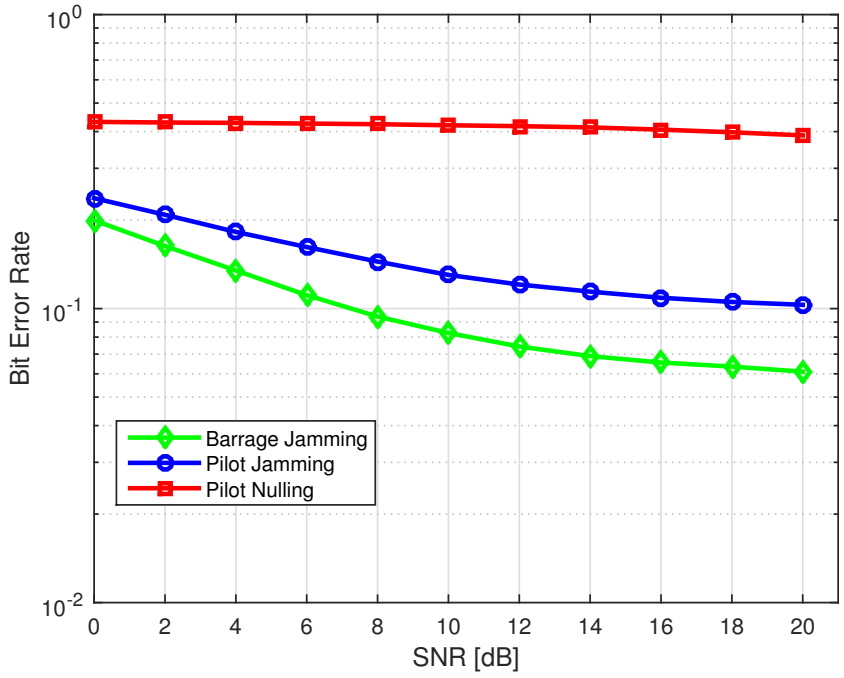

Figure 4.3: The bit error rate of target's receiver as function of SNR, under three jamming attacks, for fixed 7 dB SJR.

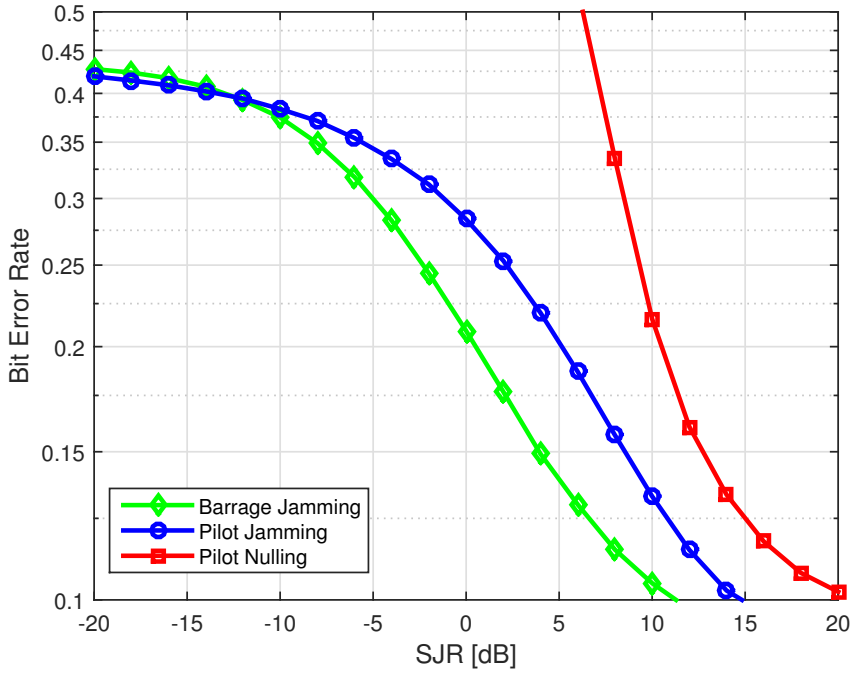

Figure 4.4: The bit error rate of target's receiver as function of SJR, under three jamming attacks, for fixed 5 dB SNR.

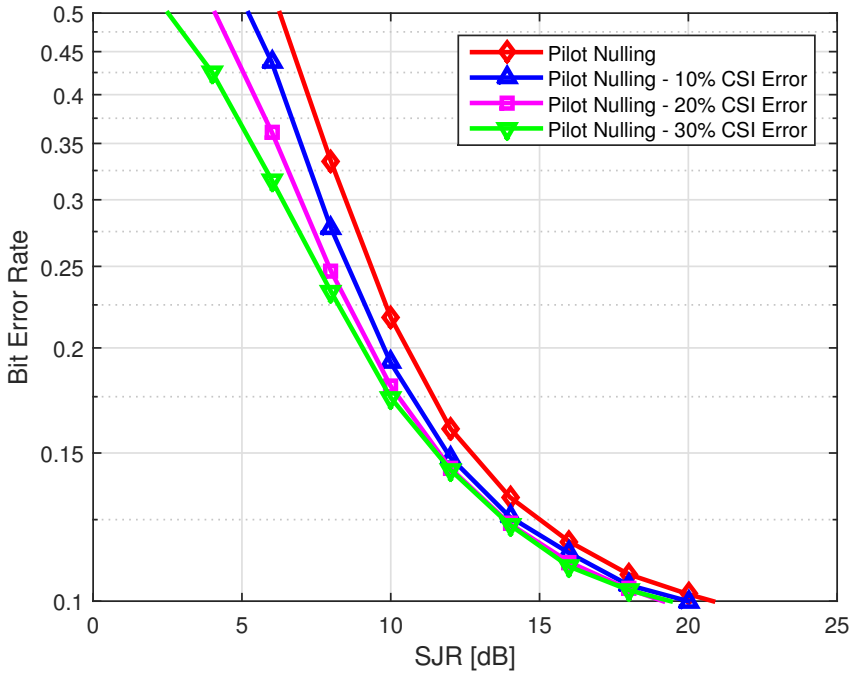

Figure 4.5: The bit error rate of target's receiver as function of SJR, under pilot nulling with various CSI Error, for 5 dB SNR.

and communication channel and (ii) accurate estimation of jamming channel only, shown in Figure 4.5. For perfect CSI knowledge at jammer and for 5 dB SNR, full denial (BER = 0.5) is achieved at 7 dB SJR. At BER 0.5, for 10%, 20%, and 30% estimation error, jammers efficiencies are reduced by 1 dB, 2 dB, and 3 dB respectively.

The next experiment is designed to investigate the impact of synchronization mismatch between jamming and target signal. In Figure 4.6, simulations are presented that varies time and frequency offsets to collect the BER for pilot nulling attacks, where transmitter-receiver pair SNR is set to 5 dB. Even though, offsets caused jammer's effectiveness degradation, the equalization attacks remained more efficient.

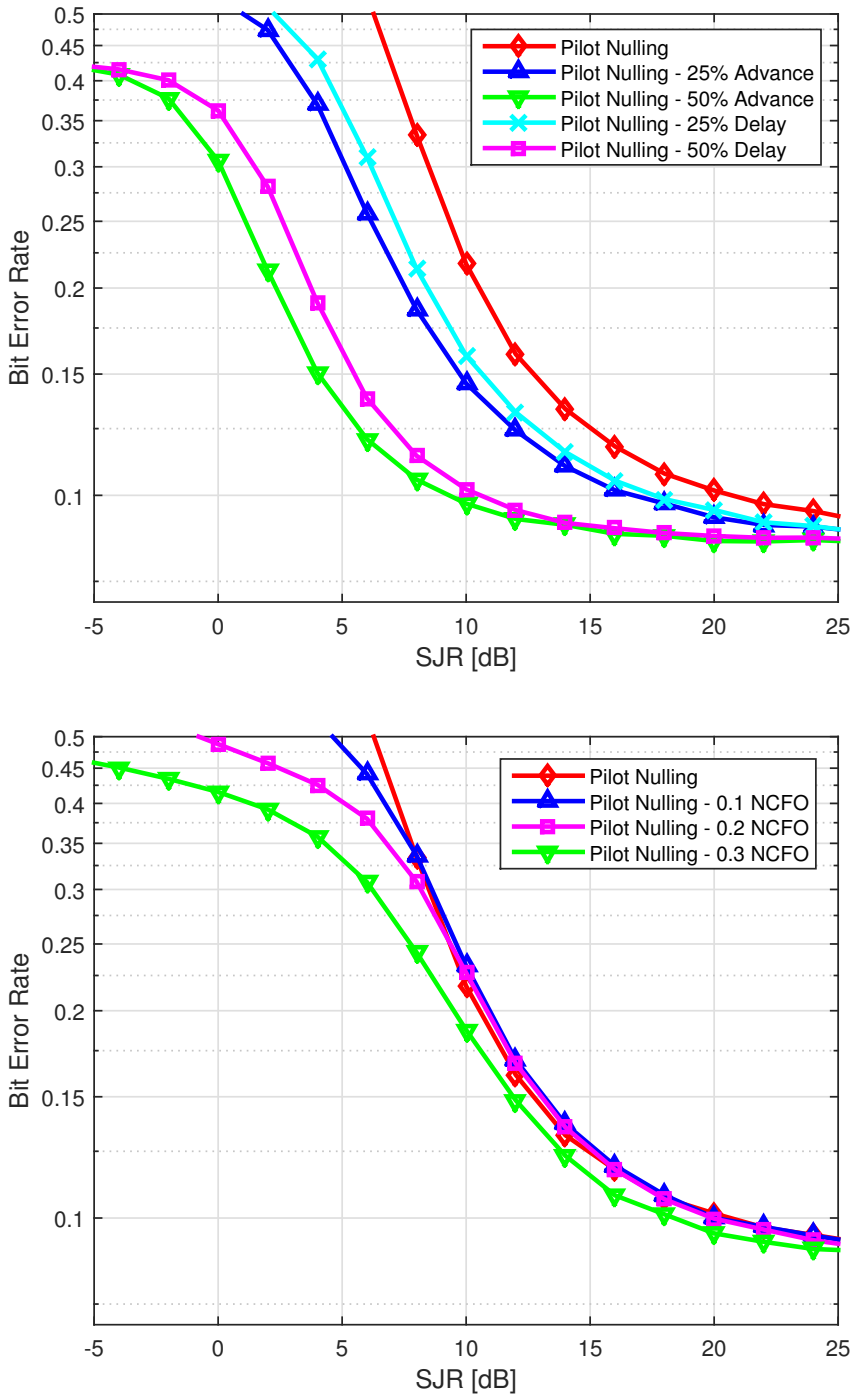

Figure 4.6: The bit error rate of target's receiver as function of SJR, under pilot nulling with different synchronization errors: (a) timing offset (b) frequency offset, for 5 dB SNR.

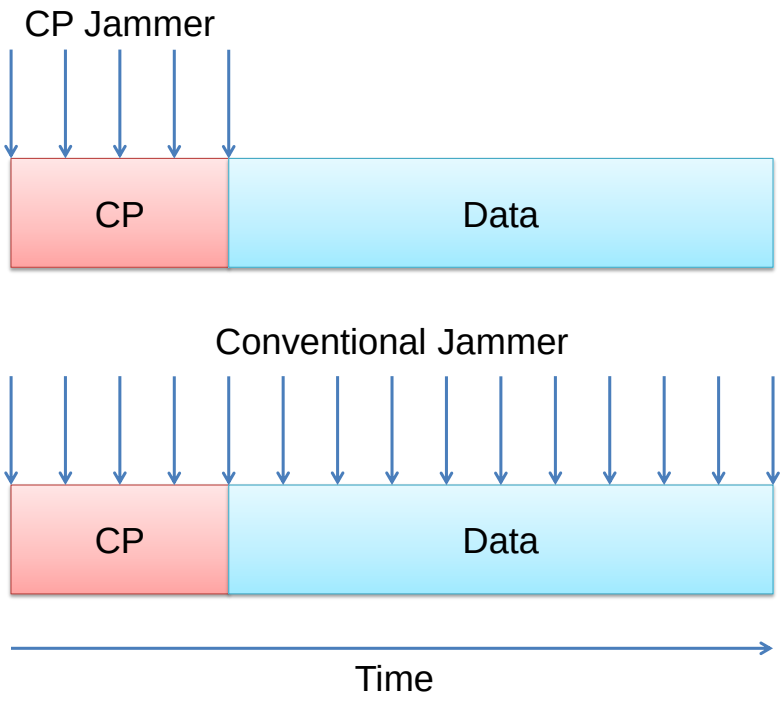

Figure 4.7: The OFDM signal under jamming attack – jamming only the cyclic prefix (CP) of the OFDM signal versus jamming on all the subcarriers of the OFDM signal.

4.10 Cyclic Prefix Jamming Attack

In OFDM, a cyclic prefix (CP) is almost always used, which refers to the prefixing of a symbol with a repetition of the end [50, 51]. It is known that frequency-domain equalization (FDE) depends on the CP to take advantage of the DFT operations in frequency-domain. The convolution-multiplication property of the DFT states that circular convolution of two signals in time is equivalent to multiplication of two signals in frequency. Circular convolution requires the input sequence to be periodic. In practice, OFDM symbols are made to look like periodic sequences by adding the CP. Therefore, at the receiver, a simple linear equalization can be used to recover the transmitted data symbols. Moreover, the CP serves as a guard interval, which eliminates the interference from the previous symbol and allows for simple frequency-domain processing, which is used for channel estimation [50, 51, 90, 91].

The analysis in this section is more focused on the operation of CP. Let us assume that G is CP length and L is channel impulse response (CIR) length. For $G \geq L$, in order to mitigate ISI, the CP, i.e., the first G samples are discarded at the receiver. Without CP, the received symbol vector, $\mathbf{r}[k] = [r_0[k], r_1[k], \cdots, r_{N-1}[k]]^T$ can be expressed as

$$\mathbf{r}[k] = \underbrace{\begin{bmatrix} x_0[k] & x_{N-1}[k] & \cdots & x_{N-L+1}[k] \\ x_1[k] & x_0[k] & \cdots & x_{N-L+2}[k] \\ \vdots & \ddots & \ddots & \vdots \\ x_{N-1}[k] & x_{N-2}[k] & \cdots & x_{N-L}[k] \end{bmatrix}}_{\bar{\mathbf{C}}[k]^{N\times L}} \mathbf{h}[k] + \tilde{\mathbf{n}}[k] \tag{4.25}$$

where $\tilde{\mathbf{n}}[k] = [n_G[k], n_{G+1}[k], \cdots, n_{N+G-1}[k]]^T$ is noise, $x_i[k]$ is OFDM subcarrier in time-domain, and $\mathbf{h}[k]$ is channel vector. The above equation shows that part of the CP would still remain in the received symbol vector even after the removal of CP. Note that the red samples are from the CP of the current OFDM symbol block, and the black samples are from the non-CP part of the current OFDM symbol block [92].

By adding $(N - L)$ zeros to the channel vector, the signal matrix can be extended without changing the output vector $\mathbf{r}[k]$ as follows

$$\mathbf{r}[k] = \mathbf{C}[k]\,\tilde{\mathbf{h}}[k] + \tilde{\mathbf{n}}[k] \tag{4.26}$$

where $\tilde{\mathbf{h}}[k]^{N\times 1} = [h_0[k], h_1[k], \cdots, h_{L-1}[k], 0, \cdots, 0]^T$. The matrix $\mathbf{C}[k]$ is circulant and its Fourier transform is diagonal with eigenvalues given by the DFT of its first column. So, the structure of circulant matrix $\mathbf{C}[k]$ is shown in (4.27).

$$\mathbf{C}[k] = \begin{bmatrix} x_0[k] & x_{N-1}[k] & \cdots & x_{N-L+1}[k] & x_{N-L}[k] & \cdots & x_1[k] \\ x_1[k] & x_0[k] & \cdots & x_{N-L+2}[k] & x_{N-L+1}[k] & \cdots & x_2[k] \\ \vdots & \ddots & \ddots & \ddots & \ddots & \vdots & \\ x_{N-1}[k] & x_{N-2}[k] & \cdots & x_{N-L}[k] & x_{N-L+1}[k] & \cdots & x_0[k] \end{bmatrix} \tag{4.27}$$

With the mathematical analysis and detailed operations of CP described above, it is obvious that CP plays a critical role for effective detection of OFDM symbols at the receiver. The two major purposes served by the CP are – 1) elimination of ISI, and 2) translation of linear convolution into circular convolution and thus making equalization simpler by removing ICI.

4.10.1 CP Jamming and Nulling

In this section, we describe different types of jamming attacks on CP of OFDM system. All the jammers are generated in time domain as CP is in time domain. We assume that the jammer is synchronized with the target signal and the attack energy is evenly distributed among the target discrete-time samples. Here, we consider two kinds of CP jamming attacks – 1) CP jamming attack and 2) CP nulling attack. Figure 4.7 shows a CP jamming versus a conventional barrage jamming model on a typical OFDM symbol.

In CP jamming attack, the jammer transmits Gaussian noise to only the CP of each OFDM symbol. The objective of CP jamming attack is to raise the noise floor in the CP. Under CP jamming attack, the circulant matrix $\mathbf{C}[k]$ can be written as

$$\mathbf{C}_{\text{jam}}[k] = \begin{bmatrix} x_0[k] & x_{N-1}[k]+j_{N-1}[k] & \cdots & x_{N-L+1}[k]+j_{N-L+1}[k] & x_{N-L}[k] & \cdots & x_1[k] \\ x_1[k] & x_0[k] & \cdots & x_{N-L+2}[k]+j_{N-L+2}[k] & x_{N-L+1}[k] & \cdots & x_2[k] \\ \vdots & \vdots & \ddots & \ddots & \ddots & \vdots & \\ x_{L-2}[k] & \cdots & \cdots & x_{N-1}[k]+j_{N-1}[k] & x_{N-2}[k] & \cdots & x_{L-1}[k] \\ x_{L-1}[k] & \cdots & \cdots & x_0[k] & x_{N-1}[k] & \cdots & x_L[k] \\ \vdots & \vdots & \ddots & \ddots & \ddots & \vdots & \\ x_{N-1}[k] & x_{N-2}[k] & \cdots & x_{N-L}[k] & x_{N-L+1}[k] & \cdots & x_0[k] \end{bmatrix} \tag{4.28}$$

In CP nulling attack, the adversary attempt to null the CP [7], which results unmodulated subcarriers for the duration of CP. The efficacy of CP nulling attack depends on the accuracy of the estimation of channels between the two transceivers, and the jammer's own channel to the target. CP nulling also demands *a priori* knowledge of the target signal structure. Under CP nulling attack, the circulant matrix $\mathbf{C}[k]$ can be written as

$$\mathbf{C}_{\text{null}}[k] = \begin{bmatrix} x_0[k] & 0 & \cdots & 0 & x_{N-L}[k] & \cdots & x_1[k] \\ x_1[k] & x_0[k] & \cdots & 0 & x_{N-L+1}[k] & \cdots & x_2[k] \\ \vdots & \vdots & \ddots & \ddots & \ddots & \vdots & \\ x_{L-2}[k] & \cdots & \cdots & 0 & x_{N-2}[k] & \cdots & x_{L-1}[k] \\ x_{L-1}[k] & \cdots & \cdots & x_0[k] & x_{N-1}[k] & \cdots & x_L[k] \\ \vdots & \vdots & \ddots & \ddots & \ddots & \vdots & \\ x_{N-1}[k] & x_{N-2}[k] & \cdots & x_{N-L}[k] & x_{N-L+1}[k] & \cdots & x_0[k] \end{bmatrix} \tag{4.29}$$

Even though $\mathbf{C}[k]$ is a circulant matrix, both $\mathbf{C}_{\text{jam}}[k]$ as shown in (4.28) under CP jamming

Table 4.1: Simulation assumptions and parameters for OFDM

Parameters	Values
System bandwidth	5 MHz
Sampling rate	5 Msps
Cyclic prefix, CP	20 samples
Transmitter IFFT size, N	512
Equalization	ZF
Data modulation	QPSK
Channel estimation	Perfect

and $\mathbf{C}_{\text{null}}[k]$ as shown in (4.29) under CP nulling attack are not circulant anymore. Guard period is still there to absorb ISI but circular convolution is no longer accomplished in the channel with consequent presence of ICI [93]. As a result, point-wise simple equalization technique is not applicable anymore. This ineffective equalization will fail to remove the distortion introduced by the channel. The ICI and failure of channel equalization would introduce irreducible error floors in the BER plots. As CP jammers attempt to disrupt only parts of digital signal, focusing only on the portions necessary to disrupt or deny communications, they are extremely power efficient. Note that we use barrage jamming as a baseline to evaluate CP jamming and nulling attacks.

4.10.2 Simulation Results

OFDM link-level simulations are carried out in MATLAB. The overall channel is assumed to be frequency-selective time-invariant. As the subcarrier spacing is assumed to be less than the coherence bandwidth of the channel, the channel is frequency-flat for each subcarrier. For the multipath channels, we have considered the ITU Vehicular A channel [92] between the two transceivers while a variation of ITU Vehicular A channel between the jammer and the target. Table 4.1 summarizes the other parameters. The CP length is chosen to be longer than the channel delay spread.

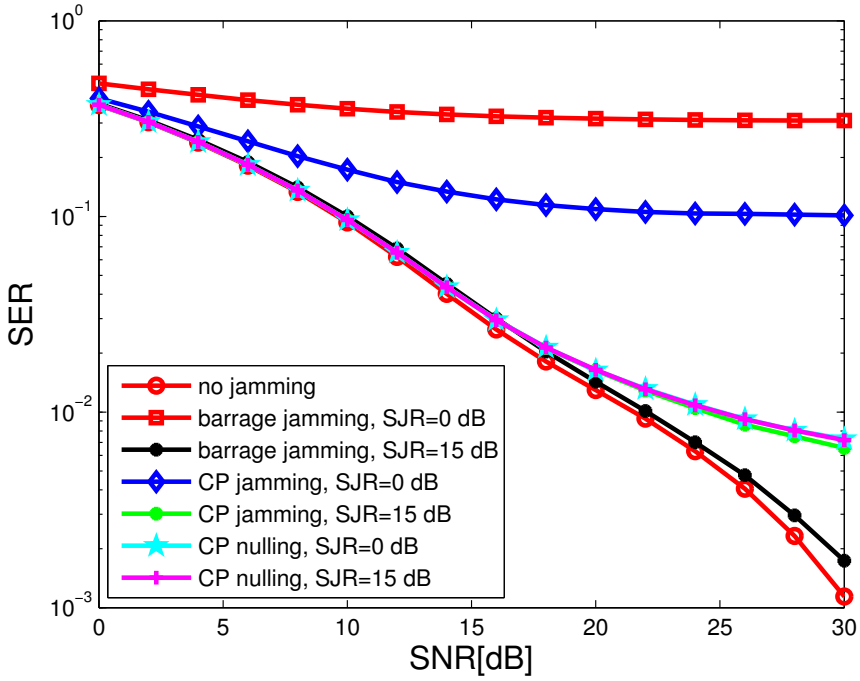

Figure 4.8: Performance of the CP jamming techniques in terms of Symbol Error Rate (SER) versus SNR curves for SJR = 0, 15 dB. ZF equalization is used.

Figure 4.8 shows the performance of the two CP jamming techniques in terms of Symbol Error Rate (SER) and compare them with no-jamming case. Zero Forcing (ZF) equalization is employed at the target and the SJR is 0 and 15 dB. We observe that the barrage jamming outperforms both CP jamming and CP nulling at lower SJR, but CP nulling outperforms the other two at high SJR. With constant signal power, higher SJR implies less jammer power. As the jammer becomes less powerful, CP jamming achieves the upper hand over barrage jamming at high SNR. This is due to the fact that CP jamming requires significantly less power than barrage jamming, since only CP portion rather than the entire symbol needs to be jammed. At low SJR, CP jamming has caused higher degradation in SER performance than CP nulling. Both CP jamming and nulling follow the no-jamming curve at low SNR, but tend to deviate from no-jamming curve as well as from each other at higher SNR. As optimal CP nulling is independent of jammer energy, it is same at both SJRs. All of the attacks have been able to introduce irreducible SER error floors at high SNR due to ICI

caused by the failed circular convolution in the channel and channel distortion which is not mitigated by the disrupted one-tap equalization at the receiver.

4.11 Summary

In this chapter, we proposed various equalization attacks against OFDM and OFDMA systems. These attacks targets to jam the equalization process of OFDM waveform and thus, create elevated error during demodulation. The two major types equalization attacks presented in the paper are pilot tone jamming attack and pilot tone nulling attack. In pilot tone jamming attack, Gaussian noise-like jamming signals are transmitted by the malicious users at the locations where target's pilot tones are employed in intent to raise the noise level at pilot tones. In pilot tone nulling, the adversary simply transmits jamming signal that consists inverted pilot tones in order to cancel the pilot tones at the target, thus making channel equalization dysfunctional.

Both pilot tone jamming and pilot tone nulling attacks performances are compared to each other and with the barrage jamming, which serves as reference point. Along with targets BER degradation, power required by each types of jamming is considered. In this chapter we also discussed some of the non-ideal scenarios where jammer has time and frequency mismatch with the target receiver. It is found that the attack performance is proportional to the jammer's knowledge of the CSI, the timing and the frequency mismatches. It is also found that jammer's knowledge of CSI plays important role in pilot tone nulling, and even with imperfect synchronization, jammer can outperform the barrage jamming.

Chapter 5

OFDM Equalization Jamming Attack Countermeasures

In this chapter, we describe countermeasures against OFDM equalization jamming attacks by randomizing the pilots tones. In last chapter power efficient jamming attacks against OFDM equalization process are introduced. The key idea of these attacks is jamming the pilot tones of the OFDM waveforms, which are known *a priori* to all the interested parties. Hence, a natural intuitive solution to this vulnerability is to make the locations of the pilot tones random so that the adversaries fail to locate the pilot tones and thus, fail to launch such jamming attacks. Even though this randomization mitigates equalization attack threat, it creates further implications. For example, it is known that the conventional orientation of pilot tones provides minimum channel estimation error; and altering that arrangement will result a change in the quality of channel estimation and equalization. Therefore, it is necessary to investigate the effect of pilot tone randomization. We have carried out this study in this chapter. Another relevant concern would be – how one can share this new pilot tone arrangement among the trusted users. Here we proposed a Pseudorandom Keystream mechanism to solve this crisis.

The remainder of this chapter is organized as follows. Section 5.1 briefly discusses jamming detections strategies for OFDM equalization jamming attacks. In Section 5.2 we introduce the countermeasures against OFDM equalizations attacks by randomizing the locations of the pilots tones. Here we propose two specific mitigation strategies. In the first strategy, we randomize the pilot tones that follows binned uniform distribution and in the second one, the pilot tones follows unbinned uniform distribution. In Section 5.3 we discuss an idea about sharing the new random locations of the pilot tones among the trusted users via Pseudorandom Keystream. In Section 5.4 the complexities related to the implementation of the mitigation strategies are discussed. Section 5.5 consists a comparative study, where proposed methods are compared with other existing methods. In Section 5.6 simulations and analysis of results are presented. Section 5.7 describes the countermeasures to CP jamming and finally, Section 5.8 provides a summary of this chapter.

5.1 Jamming Detection

The very first step to mitigate the OFDM equalization jamming attacks is to detect that the jamming had taken place. In this section we briefly discus about the detection of OFDM equalization jamming attacks. Notice that we will face three scenarios when the equalization jammers are active – 1) pilot tone being jammed with white noise, 2) pilot tone being nulled, and 3) pilot tone being jammed with variable amount of noise that maximizes error. Next we elaborate strategies to detect the first two kinds of scenarios mentioned above as they are the direct outcome of pilot tone jamming and pilot tone nulling attacks.

Detecting the presence of signal (be it friendly or hostile) can be performed by various kinds of detectors [4, 94]. However, we chose the simplest one – the energy detector with a 'threshold'. We can detect the white noise jamming (or pilot tone jamming) by adding ceiling threshold for pilot tone noise at the receiver. If that threshold is being crossed, we

will assume that pilot tone jamming has taken place. One risk of such algorithm is that it may turn 'false alarm' ON when no jamming occurred but the SNR is low (meaning nose is high). Setting a simple threshold floor for pilot tone noise can be enough to detect pilot tone nulling. However, deep fading can be a problem in such case, which can provide a false sense of pilot tone nulling. The third scenario is jamming power maximization, which can change the pattern of the channel and is left out of this dissertation. However, it can be a subject of future research where we would like to find out how to recognize the channel pattern anomaly due to this kind of jamming power allocation in the pilot tones.

5.2 Jamming Mitigation by Pilot Randomization

In this section, strategies to mitigate the threat from equalization jamming attacks are presented. Pilot tone nulling attacks can be avoided by transmitting pilot tones whose values are unknown to the attackers. In the absence of knowledge about pilot tone values, pilot tone nulling becomes as effective as pilot tone jamming. Then, by randomizing the pilot tone locations, pilot tone jamming can be completely exterminated. As countermeasure we propose two approaches of randomization of the pilot tones of OFDM systems and the approaches are:

1. Pilot tone randomization pattern follows Uniform distribution within neighboring pilot tones of an OFDM symbol; and

2. Pilot tone randomization pattern follows Poisson distribution within an OFDM symbol and/or resource block.

In this scenario, when the pilot tone locations are randomly assigned, the distance between two adjacent pilot tones can be treated as random variable (RV). If this RV is defined as X,

where $X = (x_{i+1} - x_i)$, then from (2.27), the absolute error can be expressed as

$$|E(x_1, x_0)| \leq \left[\frac{1}{8} \max_{a \leq x \leq b} |f(x)|\right] (X)^2. \tag{5.1}$$

Let us define $Y = X^2$. As X is a random variable, Y is a random variable too and we get

$$\begin{aligned} |E(x_1, x_0)| &\leq \left[\frac{1}{8} \max_{a \leq x \leq b} |f(x)|\right] Y \\ &\leq KY. \end{aligned} \tag{5.2}$$

Notice that the random variable Y will have different distribution than X. Using random variable transformation theorem [95], the distribution of Y can be found.

If $y \geq 0$, then $x^2 \leq y$ for $-\sqrt{y} \leq x \leq \sqrt{y}$. Hence

$$\begin{aligned} F_Y(y) &= P\left[-\sqrt{y} \leq x \leq \sqrt{y}\right] \quad for\, y > 0 \\ &= F_X(\sqrt{y}) - F_X(-\sqrt{y}). \end{aligned} \tag{5.3}$$

If $y < 0$, then there are no values of x for $x^2 \leq y$. Hence

$$\begin{aligned} F_Y(y) &= P\left[\emptyset\right] \quad for\, y < 0 \\ &= 0. \end{aligned} \tag{5.4}$$

By direct differentiation of $F_Y(y)$, we get

$$f_Y(y) = \begin{cases} \frac{1}{2\sqrt{y}} \left[f_X\left(\sqrt{y}\right) + f_X\left(-\sqrt{y}\right)\right] & \text{if } y > 0 \\ 0 & \text{otherwise} \end{cases} \tag{5.5}$$

where $f_Y(y)$ and $f_X(x)$ are the distribution of Y and X respectively.

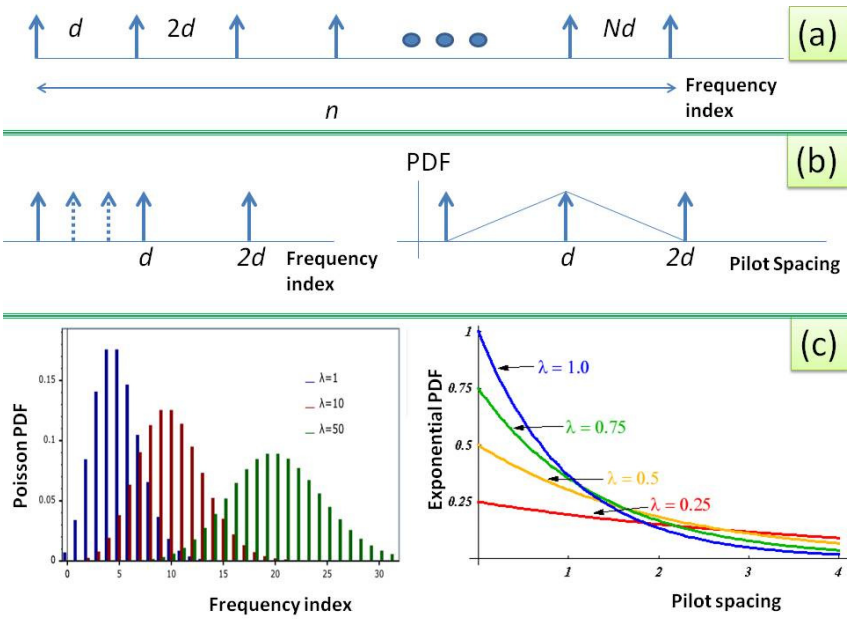

Figure 5.1: Three different orientation for pilot tone locations and their corresponding pdf for: (a) conventional equal spaced, (b) uniformly distributed confined within a bin, and (c) completely random arrangement with exponential distribution.

As we have developed general understanding about the distributions of pilot tone spacing, let's look further into proposed schemes and attain the channel approximation error, ϵ_i^a due to irregularities in approximation points (i.e., due to the change in the distance of the pilot tones within an OFDM symbol). Note that the other source of error, the interpolation error due to noise, ϵ_i^n, remains unchanged. The reason is obvious as the change in pilot tone distance does not impact the noise and they are completely independent parameters.

5.2.1 Scenario 1: Binned Uniform Distribution

In the first scheme, we propose that the pilot tones are uniformly distributed within a bin. The key advantage is that it has same average density like conventional equal space tones, yet it is random. Moreover, the equalizer performance is similar to optimum deterministic scheme as the pilot tones are constrained by distance. In this case, we assume that the i-th

pilot tone k_i, is located anywhere among subcarriers $\{(i-1)d+1, (i-1)d+2, \cdots, id\}$ for $i = \{1, \cdots, N_p\}$, uniformly distributed. Here d is the distance between two adjacent pilot tone used in conventional scheme. For example, if the pilot tone x_i is located at idth location index, then new location of pilot tone x_{i+1} is going to be anywhere within the frequency bin between id to $(i+1)d$, which means $id \leq k_{i+1} \leq (i+1)d$.

The distance between two adjacent pilot tones, X, will have triangular distribution (see Figure 5.1(b)). Using (5.1) and (5.5), we get the distribution of Y as (taking i = 0)

$$f_Y(y) = \frac{1}{2\sqrt{y}}\left(\frac{\sqrt{y}}{d^2} + \frac{2d-\sqrt{y}}{d^2}\right) \; for\; a < x < b \tag{5.6}$$

where the mean is

$$\begin{aligned} E(Y) &= \int_0^{4d^2} y f_Y(y) dy \\ &= \int_0^{4d^2} \frac{y}{2\sqrt{y}}\left(\frac{\sqrt{y}}{d^2} + \frac{2d-\sqrt{y}}{d^2}\right) dy \\ &= \int_0^{d^2} \frac{y\sqrt{y}}{2d^2\sqrt{y}} dy + \int_{d^2}^{4d^2} \frac{y(2d-\sqrt{y})}{2d^2\sqrt{y}} dy \\ &= \frac{7}{6}d^2 \end{aligned} \tag{5.7}$$

and the second moment is

$$\begin{aligned} E(Y^2) &= \int_0^{4d^2} y^2 f_Y(y) dy \\ &= \int_0^{(2d)^2} \frac{y^2}{2\sqrt{y}}\left(\frac{\sqrt{y}}{d^2} + \frac{2d-\sqrt{y}}{d^2}\right) dy \\ &= \int_0^{d^2} y^2 \frac{1}{2\sqrt{y}} \frac{\sqrt{y}}{d^2} dy + \int_{d^2}^{4d^2} y^2 \frac{1}{2\sqrt{y}} \frac{2d-\sqrt{y}}{d^2} dy \\ &= \frac{36}{15}d^4 \end{aligned} \tag{5.8}$$

and the variance is

$$\begin{aligned}\sigma_y^2 &= E\left[Y^2\right] - \left(E\left[Y\right]\right)^2 \\ &= \frac{36}{15}d^4 - \left(\frac{7}{6}d^2\right)^2 \\ &= \frac{561}{540}d^4.\end{aligned} \tag{5.9}$$

Hence, two-sided approximation error can be upper bounded by uniform distribution between $[-\frac{7}{6}Kd^2, \frac{7}{6}Kd^2]$ whose pdf is

$$\epsilon_i^a \sim U\left[-\frac{7}{6}Kd^2, \frac{7}{6}Kd^2\right] \tag{5.10}$$

with mean, $E\left[\epsilon_i^a\right] = 0$ and variance,

$$\begin{aligned}\sigma_{\epsilon_i^a}^2 &= \frac{49}{108}K^2E\left[d^4\right] \\ &= \frac{49}{108}K^2\left(\frac{36}{15}d^4\right) \\ &= \frac{49}{45}K^2d^4.\end{aligned} \tag{5.11}$$

5.2.2 Scenario 2: Unbinned Uniform Distribution

In this scheme, the locations of pilot tones are assigned completely random fashion and they are not confined within any bin like the previous case. However, the lone restriction imposed here is that the total number of pilot tones, N_p, will remain unchanged within an OFDM symbol. Such an event can be modeled as Poisson process which ensures the average number of events occurs within a finite interval. Therefore, the distribution associated with it is going to have Poisson distribution [95].

In this case, X, the distance between two adjacent pilot tones, is exponentially distributed

as shown in Figure 5.1(c). Using (5.1) and (5.5), we get the distribution of Y as

$$f_Y(y) = \frac{1}{2d\sqrt{y}} e^{-\frac{\sqrt{y}}{d}} \; for \; a = 0 < x < b = N \tag{5.12}$$

under the assumption that $N \ggg d \ggg 1$, that is $1 \lll N_P \lll N$ and where the mean is

$$\begin{aligned} E(Y) &= \int_0^{d^2} y f_Y(y) dy \\ &= \int_0^{d^2} y \frac{1}{2d\sqrt{y}} e^{-\frac{\sqrt{y}}{d}} dy \\ &= 2d^2 \end{aligned} \tag{5.13}$$

and the second moment is

$$\begin{aligned} E(Y^2) &= \int_0^{d^2} y^2 f_Y(y) dy \\ &= \int_0^{d^2} y^2 \frac{1}{2d\sqrt{y}} e^{-\frac{\sqrt{y}}{d}} dy \\ &= 24d^4 \end{aligned} \tag{5.14}$$

and the variance is

$$\begin{aligned} \sigma_y^2 &= E\left[Y^2\right] - \left(E\left[Y\right]\right)^2 \\ &= 24d^4 - \left(2d^2\right)^2 \\ &= 20d^4. \end{aligned} \tag{5.15}$$

Hence, two-sided approximation error can be upper bounded by uniform distribution be-

tween $[-2Kd^2, 2Kd^2]$ and defined as

$$\epsilon_i^a \sim U\left[-2Kd^2, 2Kd^2\right] \tag{5.16}$$

with mean, $E\left[\epsilon_i^a\right] = 0$ and variance,

$$\begin{aligned} \sigma^2_{\epsilon_i^a} &= \frac{4}{3}K^2 E\left[d^4\right] \\ &= \frac{4}{3}K^2\left(24d^4\right) \\ &= 32K^2d^4. \end{aligned} \tag{5.17}$$

5.3 Pseudorandom Keystream

In order to make the proposed countermeasures functional, the locations of the randomized pilot tones must be informed to the legitimate nodes within the network in advance, but obstructed from the malicious users (i.e., attackers) or from the nodes that are out of the trust circle. Any equalization clues given to allow new users would also give information away to adversaries, unless cryptographically protected in some way.

Employing Pseudorandom Keystream (PK) generator that will specify information about the locations and values of pilot tones is one approach that we are going to elaborate here. This keystream will be shared with the legitimate users, and in every OFDM frame. This is seeded by a shared secret known to members of the network, and an initialization vector changed every frame. Automated key management could be performed at higher protocol layers, but this still requires all devices to be provisioned with the current pilot tone key in order to join the network. This may not be feasible in many deployment scenarios.

Specifically, a time-based initialization vector synchronization approach will be derived. Assuming the following parameters:

- Shared secret K common to all provisioned devices
- Initialization vector V based on the current clock
- Clock accurate to within N_c seconds
- Downlink frames transmitted every D seconds
- Automated key management updates K every L seconds

The pseudorandom keystream generator used to provide randomness to each frame requires an initialization vector with $[\log_2(L/D)]$ bits of resolution to avoid roll-over during the key lifetime. As an example, for a 5 ms frame time and key updates every 24 hours, V must be at least 25 bits long.

New devices attempting to synchronize to the base station will require timing synchronization to recover the initialization vector state. The device will need to exhaust over $[\log_2(N_c/D)]$ bits search space for N_c seconds clock accuracy. For a clock accurate to within 5 minutes, this is 16 bits.

To synchronize, a device knowing K will observe a frame and record the observed time T, exhaust over the time-limited search space $[T - N_c/2; T + N_c/2]$ of V , using the pilot tone locations identified by the pseudorandom output. If equalization is successful for a particular $\hat{V}$, the device will compute a relative clock correction $\hat{V} - T$ and then join the network with the proper initialization vector state. If exhausting over 16 bits, and it takes 100 μs to attempt equalization, state synchronization require 3.3 seconds, on average.

A major area for future research is public-key approaches for managing keys used to protect PHY-layer properties associated with TRANSEC. Note that these cryptographic keys require in-depth study and extensive research and therefore, can be out of the scope of this dissertation and can be explored in future as part of independent research.

5.4 Complexity of Implementation

In this section, we briefly discuss about the complexities related to the implementation of proposed mitigation strategies. The major limitation of this security enhancement is the requirement for a global partnership of all the legitimate user nodes. However, new users may find this inconvenient to join in the network as they now lack information about the pilot tone locations. Any mechanism to provide hint to the new users about equalization can also expose it to the adversaries, and only way to avoid it is to protect it via cryptography. One feasible way for various deployment scenarios would be managing key automatically at higher protocol and current pilot tone key will be shared with all the devices to join the network. Other than that, PHY-layer would not face any more complexities as the pilot-tones are used in the same way for channel estimation regardless of the pilot tone arrangements.

5.5 Comparison with Other Methods

In this section, we perform a comparative study where the proposed methods are compared with other existing AJ methods. Among the most prominent countermeasures [76, 76–78], and [86], are compared here with the proposed algorithm. In [78], employing boosted pilot-tones (i.e., transmitting pilot tones with higher energy) and using jamming side information to expunge the pilot tones jammed are proposed. In [77] and [76], an improved detection algorithm is presented to remove the jammed pilot tones by calculating the variances of each pilot tones, then setting a threshold, $\Lambda = \max\{Var[H_{Pilot}]\} - \min\{Var[H_{Pilot}]\} > \eta$, to tag jammed pilot tones and excise them from channel estimation. Both of these solutions provide better performance at the cost of additional energy, but fail to mitigate pilot tone attacks, unlike pilot tone randomization. Hence, randomization of pilot tones is not only superior against equalization attacks, but also energy efficient. On the other hand, in [96],

a jam resistant subcarrier assignment for OFDMA is presented where at each hop each user generates a new set of subcarriers based on pseudorandom code using 32-bit linear feedback shift register, where different users use different nonoverlapping set of subcarriers. Like ours, this algorithm follows shifting subcarrier locations and hence are expected to perform similarly against pilot tone attacks. However, it proposes to shift all the subcarriers (both data and pilot-tone) including pilot-tones, unlike ours. In [86], spread-spectrum transmission with scrambling is proposed as countermeasure to protocol-aware attacks.

5.6 Simulation and Results

To further explore the efficacy and the impact of the proposed mitigation strategies against equalization attacks by pilot tone randomization, we carried out simulation based on the OFDM channel model shown in Figure 2.1. Fixed WiMAX (802.16d) based OFDM is generated that comprises Quadrature Phase Shift Keyed (QPSK) data and pilot-tones. The OFDM modulation uses a 256-point FFT with a cyclic prefix (CP) length of 1/8, 192 data subcarriers, every 8th subcarrier is a pilot tone (for standard deterministic scheme), and remaining subcarriers are null/guard-bands. The signals are passed through an inverse Fast Fourier Transform (IFFT), and then sent over a 6-tap random channel (i.e., frequency-flat, Rayleigh slow-fading Channel), and finally AWGN is added. The normalized powered equalization attack signal is generated and passed through a channel with different filter tap coefficients, and added to the received signal at the target receiver. The result is passed through an FFT and equalized via linear interpolation.

The simulations are run for 10000 Monte-Carlo iterations for different SNRs and Signal-to-Jamming Ratios (SJRs). For each, the target signal's BER is measured. Attack signals are constructed in the frequency domain, passed through an inverse FFT, and had their power normalized in the time domain to meet SJR requirements. The channel between transmitter

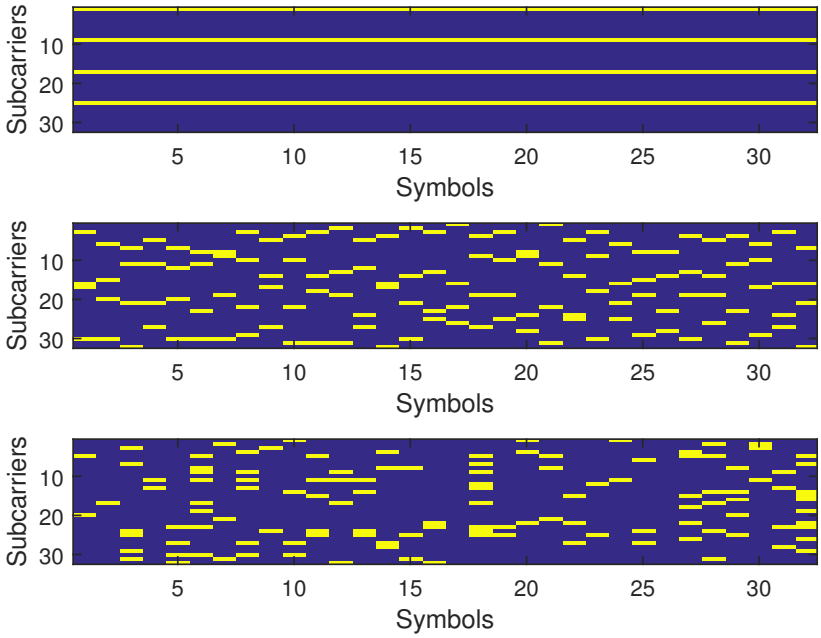

Figure 5.2: Pilot tone locations in an OFDM frame for three different pilot tone space arrangements: (a) conventional equal spaced, (b) uniformly distributed confined within a bin, and (c) completely random arrangement with exponential distribution.

and target as well as jammer's own channel are assumed to be known fully at the jammer (unless otherwise told) to ensure maximum impact of the jamming attack.

The performances of equalization attack mitigation strategies by randomizing pilot tones are validated next. In Figure 5.2, an OFDM frame is shown, where pilot tones are arranged in three configurations: (a) conventional equally-spaced (deterministic), (b) uniformly distributed confined within a bin, and (c) completely random with exponential distribution.

In Figure 5.3, we compare the performance of the three pilot tone arrangements in absence and presence of pilot tone jamming to understand the advantage of pilot tone randomization. When jamming signal is not present, the conventional arrangement provides best BER performance, which is followed by confined bin and random pilot tone arrangement, and is consistent with prior findings [41, 43]. When pilot tones are jammed by noise, the conventional scheme produces severe equalization error. The situation becomes even worse as

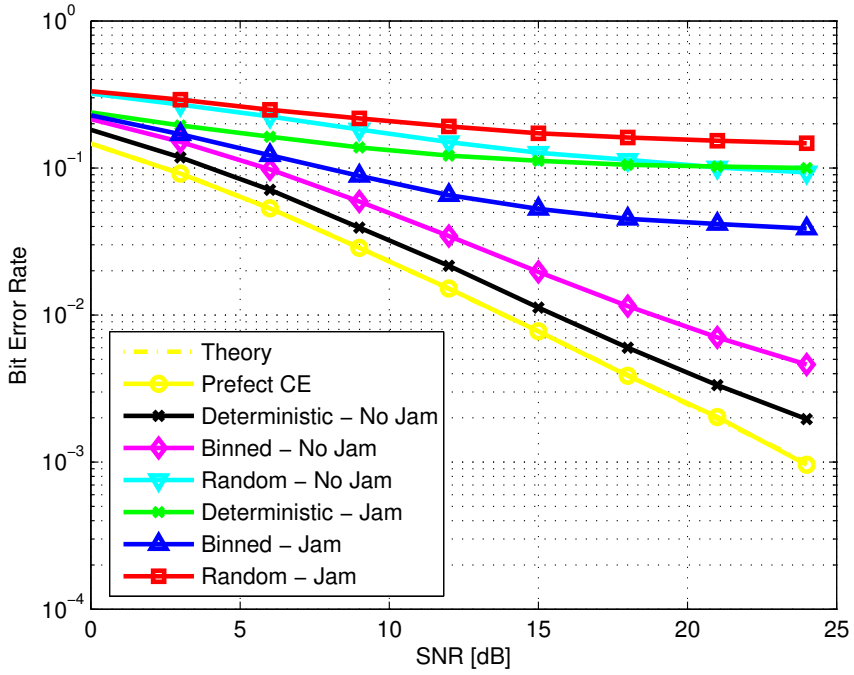

Figure 5.3: The bit error rate of target as function of SNR, for three pilot tone arrangements, when jammer is NOT operational and when pilot tone jamming is in action, for 7 dB SJR.

this error further propagates through interpolation. Consequently, both confined bin and random pilot tone arrangements produces higher BER than conventional one under pilot tone jamming attack.

As last experiment, we investigate various pilot tone arrangements by varying SJR to find the impact of jammer's strength. We observe that when jamming is strong (low SJR), the confined bin produces least BER performance. Even the random arrangements of the pilot tones perform better than the conventional one (from targets perspective). In Figure 5.4, at -10 dB SJR and 5 dB SNR, the conventional arrangement's BER is 0.4, confined bin's BER is 0.2, and random arrangements BER is 0.3. However, when jamming power is low (high SJR), the BER curve look much like the no-jamming scenario. At 20 dB SJR, the conventional, confined bin, and random arrangement's BER are 0.09, 0.15, and 0.25 respectively.

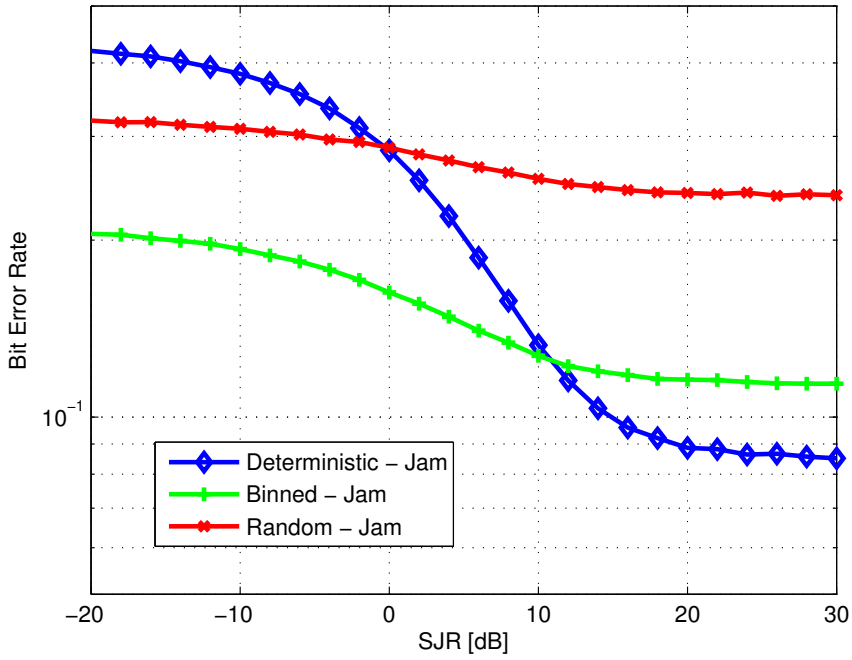

Figure 5.4: The bit error rate of target as function of SJR, for three pilot tone arrangements, under pilot tone jamming and 5 dB SNR.

5.7 CP Jamming Attack Countermeasures

In this section, we develop two approaches to countermeasure the CP jamming attacks. These mitigation strategies take advantage of the CP at receiver rather than neglecting it. First, we start with CP nulling attack mitigation, then move on to CP jamming attack. We assume that the AWGN is negligible during the analysis in section.

5.7.1 Countermeasures

Under CP nulling attack, after the removal of CP, the received symbol vector can be written as

$$\mathbf{r}_{\text{null}}[k] = \bar{\mathbf{C}}_{\text{null}}[k]\,\mathbf{h}[k] \tag{5.18}$$

$$= \underbrace{\begin{bmatrix} h_0[k] & 0 & 0 & 0 & 0 \\ h_1[k] & h_0[k] & 0 & 0 & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ h_{L-1}[k] & \cdots & \cdots & h_0[k] & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & h_{L-1}[k] & \cdots & h_0[k] \end{bmatrix}}_{\mathbf{H}_{\text{null}}[k]^{N\times N}} \mathbf{x}[k]_{nocp}$$

where $\bar{\mathbf{C}}$ denotes the corresponding signal matrix $\mathbf{C}$ without extension. In the above equation, $\mathbf{H}_{\text{null}}[k]$ is a lower triangular Toeplitz matrix, which is invertible as long as $h_0[k] \neq 0$ [97]. Hence, $\mathbf{H}_{\text{null}}[k]$ can be easily built from the channel estimates. For multipath channel, $h_0[k] = 1$. $\mathbf{x}[k]_{nocp}$ can be recovered as follows

$$\mathbf{x}[k]_{nocp} = \mathbf{H}_{\text{null}}[k]^{-1}\,\mathbf{r}_{\text{null}}[k] \tag{5.19}$$

The strategy to counter the CP jamming attack would be converting $\bar{\mathbf{C}}_{\text{jam}}[k]$ into $\bar{\mathbf{C}}_{\text{null}}[k]$ and then employing the approach mentioned in CP nulling countermeasure. Mathematically,

$$\bar{\mathbf{C}}_{\text{null}}[k]\,\mathbf{h}[k] = \bar{\mathbf{C}}_{\text{jam}}[k]\,\mathbf{h}[k] - \bar{\mathbf{C}}_{noise}[k]\,\mathbf{h}[k] \tag{5.20}$$

where $\bar{\mathbf{C}}_{noise}[k]$ is $\bar{\mathbf{C}}_{\text{jam}}[k]$ with the black samples replaced with zeros. The contaminated $(L-1)$ distinct samples of $\bar{\mathbf{C}}_{noise}[k]$ can be reproduced at the receiver by utilizing the contaminated CP of the received symbol vector. The details approaches can be found in [98].

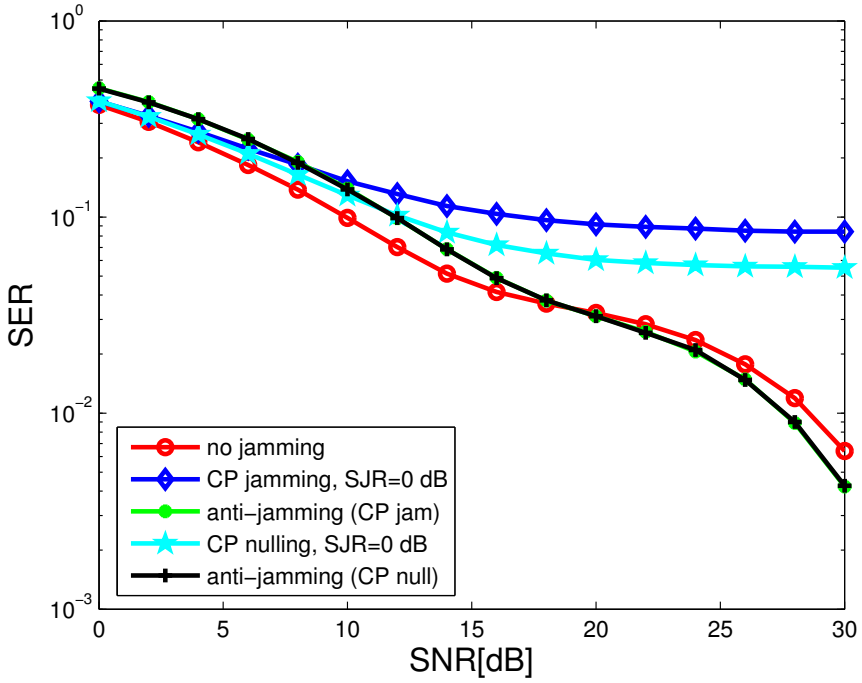

Figure 5.5: The SER of target as function of SNR, for two antijam techniques against CP jam with 0 dB SJR.

5.7.2 Simulation Results

Like the simulations in Section 4.10, OFDM link-level simulations are carried out here. For the multipath channels, we have considered the ITU Vehicular A channel [92] between the two transceivers while a variation of ITU Vehicular A channel between the jammer and the target. As the subcarrier spacing is assumed to be less than the coherence bandwidth of the channel, the channel is frequency-flat for each subcarrier. The CP length is chosen to be longer than the channel delay spread and perfect channel estimation is used.

Figure 5.5 shows the SER performance of target receiver as function of SNR for two above mentioned antijam techniques against CP jamming for SJR = 0 dB. It can be seen that the AJ strategies successfully able to restore the CP of the OFDM waveform.

5.8 Summary

In this chapter, we described the countermeasures against OFDM equalization jamming attacks, which involves randomizing pilot tone locations. Here we proposed two pilot tone randomization schemes to mitigate pilot tone based jamming attacks 1) binned pilot tone arrangement and 2) completely random pilot tone arrangement. We compared these random arrangements of pilot tones with the conventional equally spaced pilot tone scheme. The conventional deterministic scheme outperforms both random schemes in the absence of jamming. However, in pilot tone jamming attacks, both binned scheme and completely random scheme outperform deterministic scheme at low SJR. At high SJR, the deterministic scheme outperforms other two schemes as jamming power becomes too low to have any influence on the target signal. Even though the completely random scheme lags behind in performance than the other two schemes and may not look attractive in an adversary-free network, it can provide significant jamming resistance in hostile situation where adversary is deliberately attempting to disrupt communication by launching equalization jamming attacks.

Performance of this scheme can be improved by increasing the number of pilots. Even though a higher number of pilot tones may reduce throughput, it may very well be a viable option for mission critical environment.

One major drawback of randomization is that it makes equally difficult for the legitimate users to rip the benefit of using pilot tones. As suggested, pseudorandom key can be a solution this problem. However, further knowledge on cryptographic techniques for key management is needed, which can be subject to future research.

Chapter 6

MIMO Channel Sounding Attacks & Countermeasures

In this chapter, we investigate efficient channel sounding jamming attacks against multiple input multiple output (MIMO) antenna systems and explore the effects of such attacks when there are synchronization mismatches. In recent years MIMO attracted attention in wireless communications research community as they offer significant growth in capacity and link range without additional bandwidth or transmit power requirements. MIMO achieves these by higher spectral efficiency, spatial multiplexing, and link reliability or diversity (reduced fading) [85]. Here, we address efficient jamming attacks against MIMO-enabled systems. However, we do not discuss merely MIMO systems; rather we investigate MIMO-OFDM systems. MIMO-OFDM waveform is the 'de-facto' waveform for most advanced wireless network standards because it achieves the greatest spectral efficiency and, therefore, delivers the highest capacity and data throughput. MIMO multiplies capacity by transmitting different signals over multiple antennas, and OFDM divides a radio channel into a large number of closely spaced subchannels to provide more reliable communications at high speeds. Hence, in a way combining MIMO with OFDM is natural and they complement each-other [84].

The remainder of this chapter is organized as follows. Section 6.1 briefly discusses relevant researches that investigated jamming attacks against MIMO channels. Section 6.2 describes the MIMO channel and equalization/channel sounding model. In Section 6.3 and Section 6.4, we introduce the concept of channel sounding attack and singularity attack. In Section 6.5, we discuss the capacity of MIMO systems under various channel sounding attacks. Section 6.7 analyzes the impact of synchronization mismatch between jammer and target receiver. In Section 6.8, we briefly introduce countermeasure strategies against previously introduced channel sounding attacks. Section 6.9 provides simulations and analysis of results and finally, Section 6.10 provides a summary of this chapter.

6.1 Related Literature on Attacks

Attacks against MIMO channels are not rare; a number of scholarly articles are available that dealt with this problem from communication theory and information theory perspective. However, attacks against channel sounding process are limited. Miller *et al.* [99, 100] discussed jamming attacks that target the exactitude of channel state information (CSI) estimation of MIMO channels. In [99], the authors showed attacks against the Alamouti Code, a space-time code based MIMO system, which is widely employed in standards including 802.11. Various types of attacks on the channel sounding process in MIMO channels in the low and the high SNR regimes and their effects on the constellation management are investigated in [100]. As a result, authenticating the channel estimation procedure is an effective countermeasure against this type of attack [101]. Notice that in [100], channel rank attack is briefly mentioned, which is somewhat similar to our work in one sense. From another point of view, our approach is different as our approach introduces attack on CSI estimation and perception of the channel response matrix from a very different angle and present an exhaustive analysis and formulation on attack algorithm, its effect on the MIMO channel capacity. Wang *et al.* [102] explore cooperative jamming schemes for MIMO channels, where

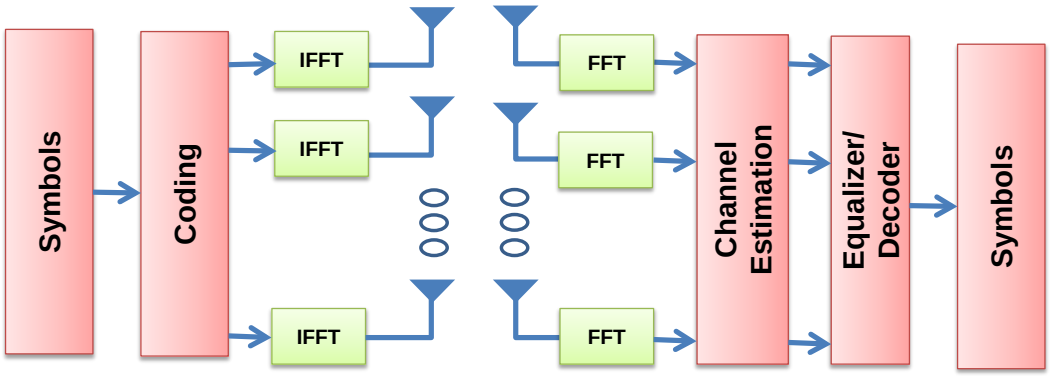

Figure 6.1: A system diagram for an MIMO-OFDM transmitter and receiver pair subject to a multipath channel.

they state that jamming signals avoid interfering legitimate users via cooperative discussion.

6.2 System Model

OFDM-based systems deploying MIMO are of interest here. We assume the channel is a flat faded Rayleigh channel that ensures individual OFDM subcarriers have bandwidth less than the coherence bandwidth of the fading channel. A narrowband flat fading MIMO system is modeled as

$$\mathbf{y} = \mathbf{H}\mathbf{x} + \mathbf{n}, \tag{6.1}$$

where $\mathbf{x}$ is M-length transmit symbol vector, $\mathbf{y}$ is N-length receive symbol vector, $\mathbf{H}$ is $N \times M$ pairwise Rayleigh channel gain matrix and $\mathbf{n}$ is N-length i.i.d. AWGN vector with distribution $\mathcal{N}(0, \sigma^2)$. Figure 6.1 shows a MIMO-OFDM transmitter-receiver pair of our interest.

At the receiver, channel is first estimated and then equalized to negate the effect of the channel by transmitting known data (called channel sounding symbols) over a series of

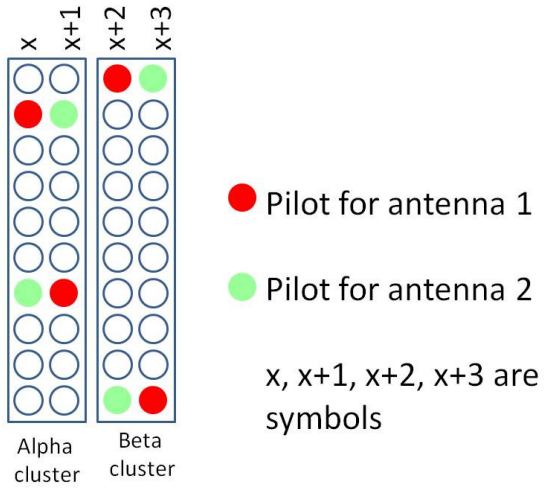

Figure 6.2: The pilot configuration in WiMAX standard for matrix B.

symbols at specific space, time and frequency locations. This process is known as *channel sounding* process for MIMO communications. For example, in OFDM-based systems using MIMO, the OFDM pilot tones are usually employed for this purpose, e.g., specific pilot tones are embedded in specific antennas at specific times/frequencies to estimate the CSI.

Let $\mathbf{P}$ be sounding symbol matrix with $M \times M$ matrix dimension. Each column signifies values transmitted on a certain antenna, and each row signifies values transmitted at certain orthogonal spectral-temporal channel. For any single-carrier modulation schemes, these are different symbols, and for multi-carrier modulation schemes, these are different subcarriers. For MIMO-OFDM, the channel sounding symbols are equally spaced and contains equal power for optimum configuration [42]. In SISO-OFDM symbol, a fraction of the subcarriers are utilized as pilot tones. Pilot tones are used to calculate the frequency response of the channel across all subcarriers, and in MIMO-OFDM, each pilot tone is only used by a single transmit antenna. For example, in a system with two transmit antennas, even pilot tones might carry pilot data for Antenna 1, while odd pilot tones might carry pilot data for Antenna 2. Figure 6.2 shows *Matrix B* mode of Mobile WiMAX (IEEE 802.16e), which employs 2×2 MIMO without space-time coding. Note that this pattern combines both

space-time and space-frequency pilot tone insertion in MIMO-OFDM discussed in [103,104]. The transmitter antennas 1 and 2 send pilot tones P_1 and P_2 respectively at different times and frequencies, i.e., for a specific pilot tone frequency, signals $(P_1, 0)$ and $(0, P_2)$ are sent from antennas in two different subcarriers and/or symbols.

Let us denote the estimated values of $\mathbf{x}$ and $\mathbf{H}$ by $\hat{\mathbf{x}}$ and $\hat{\mathbf{H}}$, respectively. For SISO-OFDM systems, $\mathbf{H}$ is a vector, whereas for MIMO-OFDM system with pilot tone signals, $\mathbf{H}$ is 2×2 matrix. At the receiver, the coefficients of 2×2 matrix $\hat{\mathbf{H}}$ are calculated for a specific frequency. As this channel sounding procedure is repeated, we get different 2×2 channel coefficient matrices, each for a different pilot tone frequency.

The estimate of channel for 2×2 MIMO-OFDM system with pilot tone signals, $\mathbf{H}$ can be expressed as

$$\hat{\mathbf{H}} = \begin{bmatrix} \hat{h}_{11}^{P_m} & \hat{h}_{12}^{P_m} \\ \\ \hat{h}_{21}^{P_m} & \hat{h}_{22}^{P_m} \end{bmatrix}. \tag{6.2}$$

The receiver linearly interpolates between pilot tones to estimate intermediate values of channel frequency response by

$$\hat{h}_{ij}^{f} = \frac{\hat{h}_{ij}^{P_m}(P_{m+1} - f) + \hat{h}_{ij}^{P_{m+1}}(f - P_m)}{P_{m+1} - P_m}. \tag{6.3}$$

For equalization, and in case channel noise and MIMO channel distributions are unknown, the channel matrix can be estimated by least square (LS) estimator as

$$\hat{\mathbf{H}}_{\text{LS}} = \mathbf{Y}\mathbf{P}^*(\mathbf{P}\mathbf{P}^*)^{-1}, \tag{6.4}$$

where $(\cdot)^*$ denotes the conjugate transpose.

After calculating the estimation of $\mathbf{H}$ denoted by $\hat{\mathbf{H}}$, channel equalization is performed by

$$\begin{aligned} \hat{\mathbf{x}} &= \hat{\mathbf{H}}^{-1}\mathbf{y} \\ &= \hat{\mathbf{H}}^{-1}(\mathbf{H}\mathbf{x}+\mathbf{n}) \\ &= \hat{\mathbf{H}}^{-1}\mathbf{H}\mathbf{x}+\hat{\mathbf{H}}^{-1}\mathbf{n} \\ &= (\mathbf{H}+\boldsymbol{\epsilon})^{-1}\mathbf{H}\mathbf{x}+(\mathbf{H}+\boldsymbol{\epsilon})^{-1}\mathbf{n}, \end{aligned} \tag{6.5}$$

where $\boldsymbol{\epsilon}$ is the matrix of measurement error due to channel noise and inaccuracies in interpolation of channel response to pilot tones.

The overall effective noise per symbol vector $\boldsymbol{\alpha} = \hat{\mathbf{x}} - \mathbf{x}$ is

$$\boldsymbol{\alpha}^T = (\mathbf{n}^T - \mathbf{x}^T\boldsymbol{\epsilon})(\mathbf{H}+\boldsymbol{\epsilon})^{-1}. \tag{6.6}$$

6.3 Channel Sounding Attack

In this section, we introduce a new kind of jamming attack that we call channel sounding jamming attack and compare it with barrage jamming. Figure 6.3 shows a simple 2×2 MIMO system under jamming attack. Barrage jamming is the simplest and the baseline of all the attacks, in which entire bandwidth of the target is jammed by transmitting AWGN. This increases the noise amount and the error $\boldsymbol{\epsilon}$, thus degrading signal to noise ratio (SNR) of the target.

In channel sounding jamming attack, assuming the jammer is synchronized with the target, jammer transmits signal $\mathbf{J}$, where $J_i = 0$ for data payload and $J_i = q_i$ for channel sounding symbols, where q_i is i.i.d AWGN with distribution $N(0, \sigma_J^2)$. The impact is that the error term ϵ under coherent channel sounding jamming attack is dominated by jammer power and thus the target SNR is severely degraded.

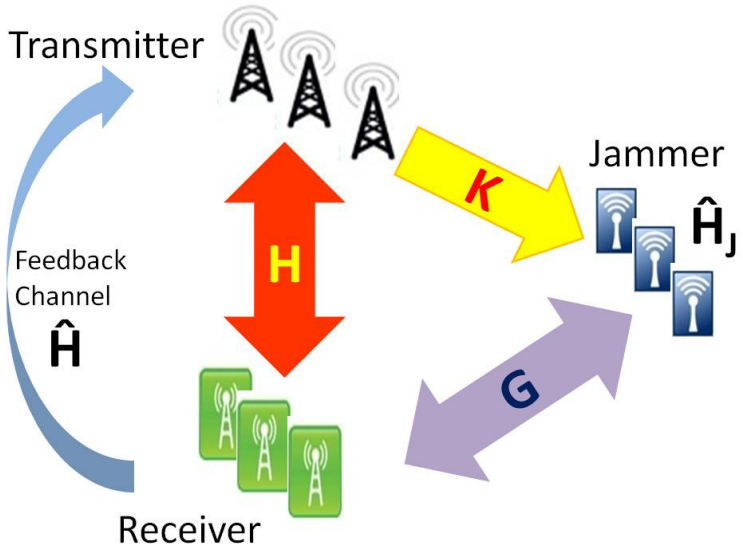

Figure 6.3: The channel sounding jamming attack on MIMO Systems. **H**, **K**, and **G** denote the channels between transmitter-receiver, transmitter-jammer, and receiver-jammer, respectively. $\hat{\mathbf{H}}$ is receiver's estimated CSI of **H**, which is fed back to the transmitter.

Both barrage jamming and channel sounding jamming inject AWGN in the target and therefore, degrade SNR by increasing noise. However, channel sounding jamming is more energy efficient from jammer's perspective, as it jams the channel sounding signal only and distributes the MIMO channel estimation error $\boldsymbol{\epsilon}$ across all the subcarriers during equalization, using interpolated channel frequency response.

6.4 Singularity Attack

In this section, we introduce the *singularity attack*, where the jammer seek to null the channel singular value. Another way to explain this attack would be saying that the employed jammer attempts to manipulate the channel matrix estimation at the receiver by turning it into a singular matrix. The rationale behind this idea is such that the noise term asymptotically approaches infinity and transmitted signal will be buried in noise at the receiver.

Let us assume $\mathbf{J}$ is a $K \times M$ matrix of attack symbols using K transmit antennas over the same M orthogonal spectral-temporal channels as used by the transmitter. Let us also assume that $\mathbf{G}$ is the $N \times K$ matrix of channel gains between the K-antenna jammer and N-antenna receiver. Also note that the sounding matrix $\mathbf{P}$ is already defined as $M \times M$ matrix in previous section.

As an efficient jammer, the adversary seek to influence the estimate of $\mathbf{H}$ and accordingly its singular values. This way the transmitter assigns wrong water-filled power levels to channel Eigen-modes, due to its miss-estimation of eigenvalues, resulting in degraded capacity.

For aforementioned purpose, let us consider a jamming scenario where a jammer have approximate estimates of h_{ij}, the elements of channel matrix $\mathbf{H}$, and adjusts its transmitted signal $\mathbf{J}$ through channel $\mathbf{G}$, the MIMO channel between jammer and receiver antennas, such that the overall channel matrix appearing to receiver antennas becomes singular with no inverse. Hence, the receiver will not be able to estimate what $\mathbf{x}$ was transmitted. The rationale here is to make $\hat{\mathbf{H}}$ asymptotically zero or close to zero so that in equalization phase, i.e., $\hat{\mathbf{x}} = \hat{\mathbf{H}}^{-1}\mathbf{y}$, the inverse has very large terms. The underlying assumption here is that the adversary has the knowledge about the channel $\mathbf{H}$ between the target transmitter and receiver and his own channel to the target $\mathbf{G}$.

In singularity atack, the jammer transmits the signal $\mathbf{J}$, which is defined as

$$\mathbf{J} = -\mathbf{G}^{-1}\mathbf{H}\mathbf{P} \tag{6.7}$$

where $\mathbf{G}^{-1}$ is the Moore-Penrose pseudoinverse of channel matix $\mathbf{G}$.

The received pilot-tones (or sounding signals) $\mathbf{S}$ under jamming attack is an $N \times M$ matrix and is equal to

$$\mathbf{S} = \mathbf{H}\mathbf{P} + \mathbf{G}\mathbf{J} + \mathbf{N} \tag{6.8}$$

where $\mathbf{N}$ is additive white Gaussian noise (AWGN).

The target receiver estimates the channel gain matrix $\hat{\mathbf{H}}$ by computing

$$\begin{aligned}\hat{\mathbf{H}} &= \mathbf{S}\mathbf{P}^{-1} \\ &= (\mathbf{H}\mathbf{P} + \mathbf{G}\mathbf{J} + \mathbf{N})\mathbf{P}^{-1} \\ &= \mathbf{H} + \mathbf{G}\mathbf{J}\mathbf{P}^{-1} + \mathbf{N}\mathbf{P}^{-1}\end{aligned} \tag{6.9}$$

If the CSI estimates at the jammer are perfect or near perfect, the term $\mathbf{H} + \mathbf{G}\mathbf{J}\mathbf{P}^{-1}$ is small and we are left with only noise term. Also note that if the noise term is ignored, then the goal of the jammer is to select $\mathbf{J}$ that minimizes rank$(\mathbf{H} + \mathbf{G}\mathbf{J}\mathbf{P}^{-1})$. As the rank of $\mathbf{H}$ cannot surpass its dimensionality, if $K \geq \min(M, N)$, the jammer retains enough degrees of freedom to arbitrarily change $\hat{\mathbf{H}}$, subject to the constraints of the AWGN term. Notice that the equation (6.7) represents the overdetermined case where $K \geq \min(M, N)$. On the other hand, the adversarys ability to affect the rank of $\hat{\mathbf{H}}$ is limited for underdetermined case. In general, it can reduce the rank of $\hat{\mathbf{H}}$ to $\max(0, \min(M, N) - K)$ assuming $\mathbf{G}$ and $\mathbf{H}$ are full-rank.

6.5 Capacity Under Attack

In this section, we look into the MIMO channel under jamming attack from information-theoretic perspective. The MIMO channel capacity in bits/s/Hz can be written as

$$C = \log_2 \left(\det \left(\mathbf{I} + \frac{\rho}{M} \mathbf{H}\mathbf{H}^* \right) \right), \tag{6.10}$$

where ρ is average SNR per channel. The singular value decomposition (SVD) for $\mathbf{H}$ can be computed as $\mathbf{H} = \mathbf{U}\Sigma\mathbf{V}^*$, which yields $\mathbf{H}\mathbf{H}^* = \mathbf{U}\Sigma^2\mathbf{V}^*$. The channel capacity of MIMO

systems can be expressed in terms of singular value by

$$C = \sum_{i=1}^{\min(M,N)} \log_2 \left(\mathbf{I} + \frac{\rho}{M} \sigma_i^2 \right), \tag{6.11}$$

where σ_i^2 is i-th singular value and $\min(M, N)$ is the rank of $\mathbf{H}$, which can be denoted as R_H. An alternate form of the equation (6.11) can be written as

$$C = \sum_{i=1}^{R_H} (\log(\mu \sigma_i))^+, \tag{6.12}$$

where the function $(x)^+ = \max\{x, 0\}$ and μ is the waterfill level, which is chosen such that $\sum_{i=1}^{R_H} P_i = P$. Here P_i is the power allocated to each parallel non-interfering channels acquired by the singular value decomposition of channel $\mathbf{H}$, and P is the average power constraint across all transmitter antennas.

The channel sounding jammer attempts to influence $\hat{\mathbf{H}}$, the estimate of $\mathbf{H}$ at the receiver to minimize its singular value, resulting a decrease in the capacity [105]. If the receiver's perception of $\mathbf{H}$ under attack is denoted as $\breve{\mathbf{H}}$, then under jamming attack equation (6.12) can be written as

$$\begin{aligned}
C &= \sum_{i=1}^{R_{\breve{H}}} (\log(\mu \breve{\sigma}_i^2))^+ \\
&\leq R_{\breve{H}} \log \mu + \sum_{i=1}^{R_{\breve{H}}} \log \breve{\sigma}_i^2 \\
&= R_{\breve{H}} \log \mu + \log \prod_{i=1}^{R_{\breve{H}}} \breve{\sigma}_i^2 = R_{\breve{H}} \log \mu + \log(\det(\breve{\mathbf{H}} \breve{\mathbf{H}}^*)) \\
&= R_{\breve{H}} \log \mu + \log(\det(\breve{\mathbf{H}}) \det(\breve{\mathbf{H}}^*)) \\
&= R_{\breve{H}} \log \mu + \log(\det(\breve{\mathbf{H}})(\det(\breve{\mathbf{H}}))^*) \\
&= R_{\breve{H}} \log \mu + \log(|\det(\breve{\mathbf{H}})|^2) \\
&= R_{\breve{H}} \log \mu + 2 \log(|\det(\breve{\mathbf{H}})|),
\end{aligned} \tag{6.13}$$

where $|\det(\breve{\mathbf{H}})|$ denotes the magnitude of determinant of matrix $\breve{\mathbf{H}}$. The equation (6.13) implies that we need to have knowledge of the rank and the determinant of matrix $\breve{\mathbf{H}}$ to calculate the MIMO capacity under jamming attack.

6.6 Impact of Channel Estimation Error

In ideal scenario, an attacker expects to obtain error free estimation of CSI. However, inaccuracies are most likely unavoidable in $\hat{\mathbf{H}}_J$, which is the estimation of channel $\mathbf{H}$ at the jammer, due to noise and the attacker's distance from transmitter and receiver. In other words,

$$\hat{\mathbf{H}}_J = \boldsymbol{\alpha}\mathbf{H} + \boldsymbol{\beta}, \tag{6.14}$$

where β is the noise vector $\beta \sim \mathcal{N}(0, \sigma^2)$ and α is the relative error [105].

When $\mathbf{P} = \mathbf{I}p$, its inverse $\mathbf{P}^{-1} = \mathbf{I}/p$ and the jammer estimates the channel response by

$$\begin{aligned} \hat{\mathbf{H}} &= \left[(\boldsymbol{\alpha}\mathbf{H} + \boldsymbol{\beta})\,\mathbf{P} + \mathbf{N}\right]\mathbf{P}^{-1} \\ &= \boldsymbol{\alpha}\mathbf{H} + \boldsymbol{\beta} + \mathbf{N}/p \\ &= \boldsymbol{\alpha}\mathbf{H} + (\boldsymbol{\beta} + \mathbf{N}/p)\,, \end{aligned} \tag{6.15}$$

where $(\boldsymbol{\beta} + \mathbf{N}/p) \sim \mathcal{N}\left(0, \sigma^2\left(\frac{p^2+1}{p^2}\right)\right)$.

In the fully informed case, meaning $\alpha = \mathbf{I}$ or identity matrix.

$$\mathbf{J} = -\mathbf{G}^{-1}\,(\mathbf{H} + \boldsymbol{\beta})\,\mathbf{P}. \tag{6.16}$$

The received signal then becomes

$$\begin{aligned} \mathbf{S} &= \mathbf{HP} + \mathbf{GJ} + \mathbf{N} \\ &= \mathbf{HP} - \mathbf{GG}^{-1}\left(\mathbf{H} + \boldsymbol{\beta}\right)\mathbf{P} + \mathbf{N}. \end{aligned} \tag{6.17}$$

Notice that the received signal becomes $\mathbf{S} = \mathbf{N}$ in the fully informed scenario, i.e., dominated by noise that defuses the influence of pilot-tones at the receiver.

Otherwise, we have estimate residue $\boldsymbol{\delta}$, that can be defined as

$$\boldsymbol{\delta} = \mathbf{H} + \mathbf{GJP}^{-1} \tag{6.18}$$

Let $\overline{\boldsymbol{\delta}}$ be the linearly-combined error for non-pilot tones. The symbol error $\boldsymbol{\alpha} = \hat{\mathbf{x}} - \mathbf{x}$ is then

$$\boldsymbol{\alpha}^T = \left(\mathbf{n}^T - \mathbf{x}^T\left(\overline{\boldsymbol{\delta}} + \boldsymbol{\epsilon} - \mathbf{H}\right)\right)\left(\overline{\boldsymbol{\delta}} + \boldsymbol{\epsilon}\right)^{-1}, \tag{6.19}$$

where $(.)^T$ denotes the matrix transpose operation. We verify the validity of above observations via simulations in Section 6.9.

6.7 Impact of Synchronization Error

Channel sounding jamming attacks achieve maximum jamming when the jammer is synchronized with the target [73]. To maintain perfect synchronization, jammer needs prior knowledge about the channel, carrier frequency, and propagation time etc. In reality, it is difficult to maintain perfect synchronization over all these parameters. In this section, we analyze the effect of synchronization error on the performance of channel sounding attacks.

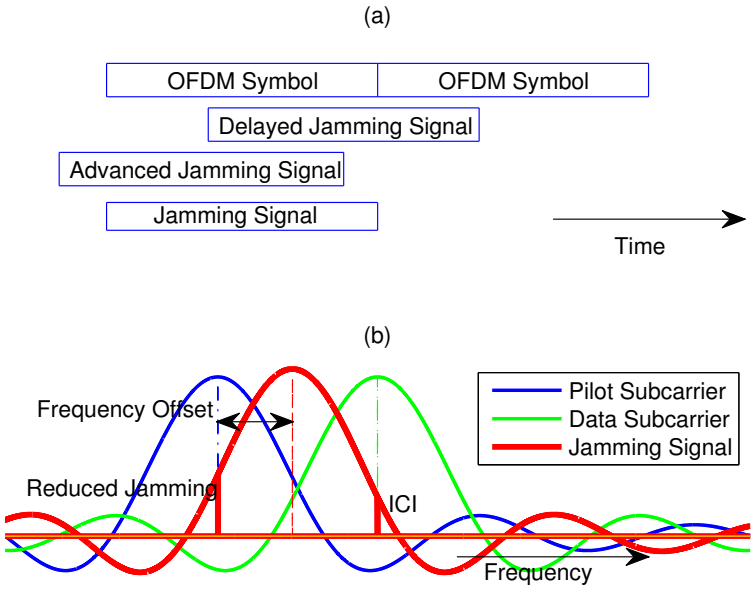

Figure 6.4: Synchronization mismatch in MIMO-OFDM jamming due to a) time offset b) frequency offset.

6.7.1 Time Offset

Time offset occurs when jammer and target symbol are not aligned at the target receiver. Absence of common time reference, hardware clock imperfections, and changes in propagation time are the key reasons for time synchronization loss of the jamming signal at the target receiver. Figure 6.4(a) shows time offset in the jamming signal with delay and advance. The time domain signal, $j(n)$, with delay of τ can be represented as $j_{to}[n] = j[n+\tau]$. Time offset of τ in the time domain gives rise to phase rotation of $\frac{2\pi k\tau}{N}$ in the frequency domain [84]. Hence, in the frequency-domain, the signal $J_o[k]$ can be represented as

$$J_{to}[k] = J[k]e^{\frac{j2\pi k\tau}{N}}. \tag{6.20}$$

Advanced or delayed arrival of jamming signal results loss of jamming signal energy at the target and this energy loss in jamming signal reduces the effectiveness of the attack. The effect of energy loss is further quantified with simulation in Section 6.9.

Plugging this changed jamming signal to equation (6.9), we can get estimation residue $\boldsymbol{\delta}_{\text{to}}$ for time offset

$$\boldsymbol{\delta}_{\text{to}} = \mathbf{H} + \mathbf{G}\mathbf{J}_{\mathbf{to}}\mathbf{P}^{-1}. \tag{6.21}$$

The symbol error $\boldsymbol{\alpha} = \hat{\mathbf{x}} - \mathbf{x}$ is then

$$\boldsymbol{\alpha}^{\,T} = \left(\mathbf{n}^{\,T} - \mathbf{x}^{\,T}\left(\overline{\boldsymbol{\delta}}_{\text{to}} + \boldsymbol{\epsilon} - \mathbf{H}\right)\right)\left(\overline{\boldsymbol{\delta}}_{\text{to}} + \boldsymbol{\epsilon}\right)^{-1}. \tag{6.22}$$

6.7.2 Frequency Offset

Frequency offset is defined as the difference between the actual carrier frequency at the target (receiver) and the jammer. Even though the jammer assumes to have initial knowledge about the carrier frequencies of the target, both target and jamming signal can be subject to distortion. Instability of the local oscillator used to generate carrier signal at the transmitter, receiver and jammer can give rise to frequency offset in terms of phase distortion, which can be modeled as a zero-mean Wiener random process [84]. Frequency offset can also be caused by *Doppler shift* in the channel.

Let us define the normalized carrier frequency offset (CFO), λ, as the ratio of f_{FO}, to f_{SC} or subcarrier spacing $\lambda = \frac{f_{FO}}{f_{SC}}$.

Then the time-domain jamming signal can be written as

$$j_{fo}[n] = j[n]e^{\frac{j2\pi n\lambda}{N}}. \tag{6.23}$$

In the time domain, normalized CFO of λ causes phase offset of $2\pi n\lambda$, that is, proportional to the CFO and time index n and is equivalent to frequency shift of $\pm\lambda$, $J[k \pm \lambda]$ on the frequency domain signal, $J[k]$. Figure 6.4(b) shows a MIMO-OFDM symbol with 3 subcarriers, where the first waveform represents target pilot tone, i.e., the left most one.

The right most one is the target data subcarrier and the one in the middle is the jamming subcarrier. Notice that jamming signal is not aligned with pilot tone and is overlapped with both pilot and data subcarriers. The deviated jamming signal has reduced magnitude on the target pilot tone and therefore loses its effectiveness accordingly. On the contrary, it introduces ICI type effect to the data symbol subcarrier that causes some BER degradation in data signal. As the pilot tones are located far apart, any data subcarrier sees this effect only from nearest one or two jamming tones. The accumulated effect of this is minor compared to actual impact of jamming attack and omitted here for simplicity.

Note that, if ICI effect from jamming is neglected, then $J[k \pm \lambda]$ is just amplitude scaled down version of the original jamming signal (see Figure 6.4). Let this scaling factor be defined as s, which is a direct function of λ, then

$$J_{fo}[k] = J[k \pm \lambda] \approx sJ[k]. \tag{6.24}$$

Plugging this changed jamming signal into equation (6.9), we can get estimation residue $\boldsymbol{\delta}_{\text{fo}}$ for frequency offset

$$\begin{aligned} \boldsymbol{\delta}_{\text{fo}} &= \mathbf{H} + \mathbf{G}\mathbf{J}_{\mathbf{fo}}\mathbf{P}^{-1} \\ &= \mathbf{H} + \mathbf{G}\mathbf{J}\mathbf{P}^{-1}s. \end{aligned} \tag{6.25}$$

The symbol error $\boldsymbol{\alpha} = \hat{\mathbf{x}} - \mathbf{x}$ is then

$$\boldsymbol{\alpha}^{\,T} = \left(\mathbf{n}^{\,T} - \mathbf{x}^{\,T}\left(\overline{\boldsymbol{\delta}}_{\text{fo}} + \boldsymbol{\epsilon} - \mathbf{H}\right)\right)\left(\overline{\boldsymbol{\delta}}_{\text{fo}} + \boldsymbol{\epsilon}\right)^{-1}. \tag{6.26}$$

6.8 Attack Countermeasures

In this section, we briefly discuss about possible countermeasure against MIMO-enabled attacks presented earlier in this chapter. Notice that these attacks are somewhat similar to OFDM equalizer attacks. Hence the mitigation strategies are going to be similar too. Therefore, to mitigate the 'singularity attack', the Tx-Rx pair should make it difficult for a untrusted third party to have access to their CSI and pilot tone locations. In other words, the communications between the transmitter and receiver should appear to have an unrecognizable structure from outside. Like OFDM strategies, we can randomize the channel sounding tones to avoid jamming power on them and then share the location information among the trusted nodes via pseudorandom codes.

6.9 Simulation and Results

In this section, we develop simulations based on 2×2 MIMO-OFDM (known as WiMAX *Matrix B*) channel model of Figure 6.1 to explore the efficacy of pilot tone jamming. The quadrature phase shift keyed (QPSK) data and pilot tones are passed through an inverse fast Fourier transform (IFFT) and then sent over an 8-tap random channel with AWGN. The OFDM modulation used here deploys a 256-point FFT with a cyclic prefix length of 1/8 and every 4th subcarrier is a pilot tone (shown in Figure 6.2). The attack signal from a 2 antenna jammer is added to the received signal after being passed through a channel with different filter tap coefficients. In the receiver, combined target and jamming signal is received, passed through FFT, and equalized using the linear interpolation method based on pilot tones. We have also simulated the 4×4 MIMO-OFDM configuration as well. Simulations were run for 1000 Monte-Carlo iterations with variable SNR and SJR. We also varied different levels of channel estimation capability by the jammer and used target BER as a measure of attack

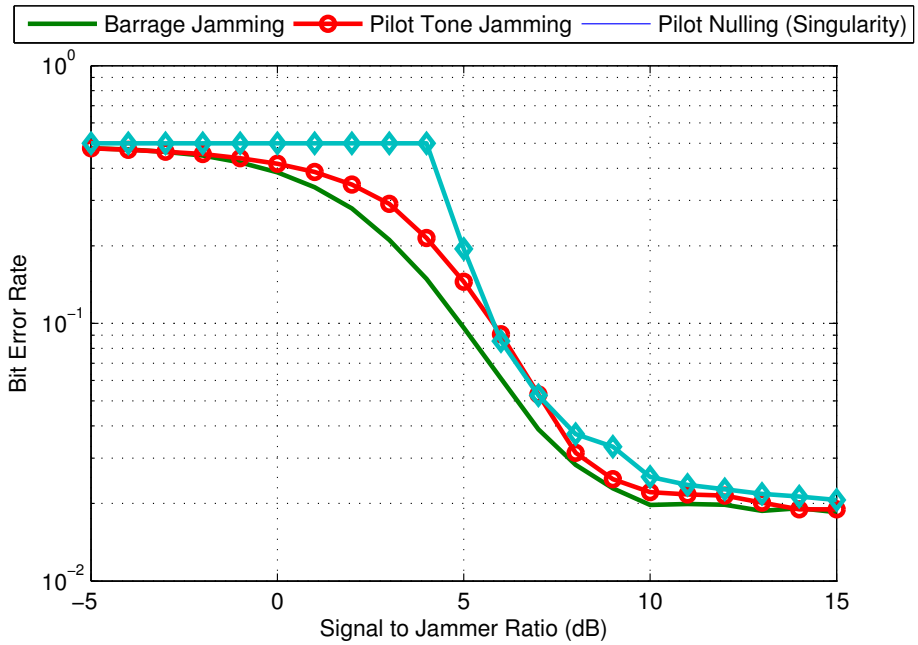

Figure 6.5: Performance of three jamming methods with 50% Time Offset (TO) as a function of SJR at WiMAX MIMO-OFDM *Matrix B* system for target signal operating at 10 dB SNR and with perfect knowledge of CSI.

efficiency.

Figure 6.5 shows effects of varying SJR on BER for different pilot tone jamming at 50% symbol time offset. At 0.3 BER, pilot tone jamming outperforms barrage jamming by 1 dB and singularity attack by 3 dB. Figure 6.6 compares MIMO singularity attack for different CSI errors and time offset vs. SJR for target signal operating at 10 dB SNR. At 0.5 BER, 25% time offset degrades the jamming performance by about 0.5 dB, compared to 1 dB with 50% time offset. Therefore, time offset is the cause of loss in performance and the loss rate increases sharply with increase in time offset. However, the difference in performance in both cases tends to decrease and ultimately converges with perfect time synchronization at higher SJR, around 2 dB and up. Notice that the effect of erroneous CSI at the jammer has greater impacts than the time offset. At 0.5 BER 20% CSI error causes about 0.25 dB jamming performance loss with 50% time offset compared to 25% time offset. Therefore, even when

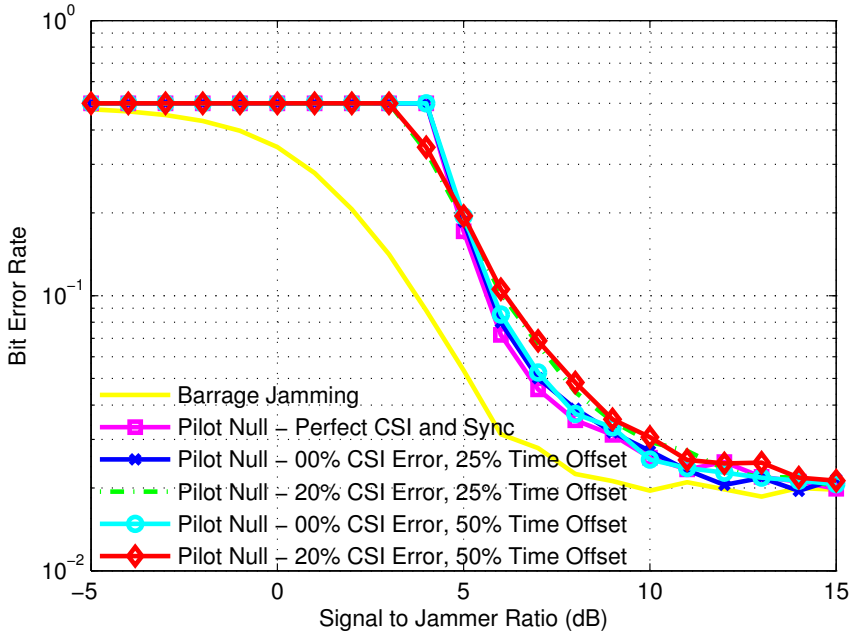

Figure 6.6: Performance of singularity jamming operating at target signal SNR of 10 dB, for different levels of CSI knowledge and varying Time Offset (TO).

the attacker has no perfect information about channels and loses some attack energy due to imperfect time synchronization, we still observe that singularity attack outperforms barrage jamming in almost all cases.

Figure 6.7 shows the effect of varying SJR on BER for different pilot tone jamming strategies at 0.5 normalized frequency offset (NCFO). At 0.3 BER, pilot tone jamming outperforms barrage jamming by 1 dB and singularity by 3 dB. Figure 6.8 compares singularity attack efficiency for different NCFO and different CSI. At 0.5 BER, 0.2 NCFO causes 0.5 dB and 0.5 NCFO causes 1 dB loss in jamming performance, compared to frequency synchronized singularity and 20% CSI error causes about 1 dB performance loss.

Figure 6.9 shows the capacity of a 4×4 WiMAX system under jamming attacks. The capacity shown in Figure 6.9 is averaged over all pilot tones. The jammer also has 4 antennas and the jammer-to-signal ratio (SJR) is assumed to be 10 dB.

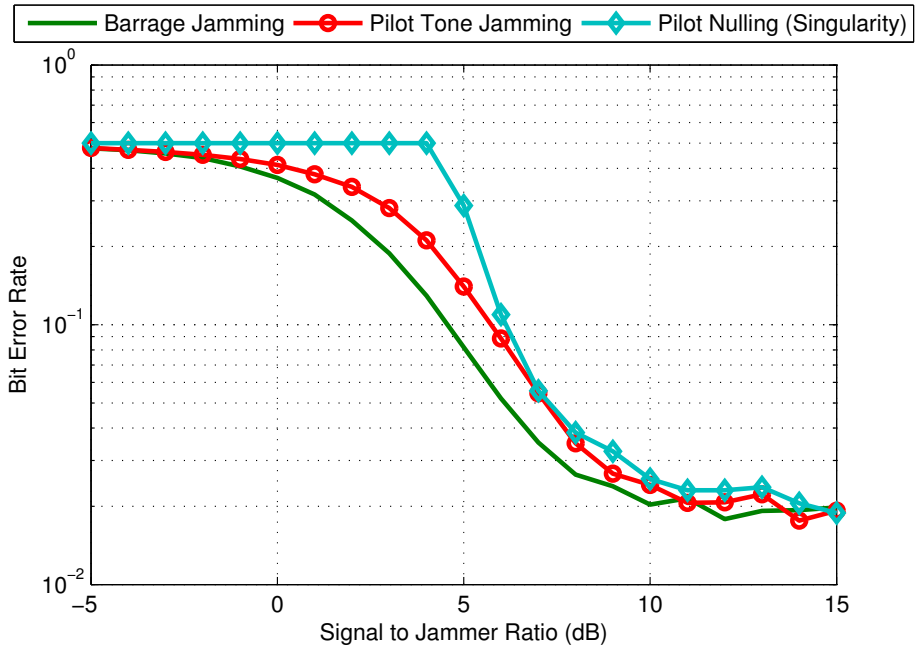

Figure 6.7: Performance of three jamming attack methods with normalized frequency offset (NCFO) equal to 0.5 as a function of SJR at WiMAX MIMO-OFDM Matrix B system for target signal operating at 10 dB SNR and with perfect knowledge of CSI.

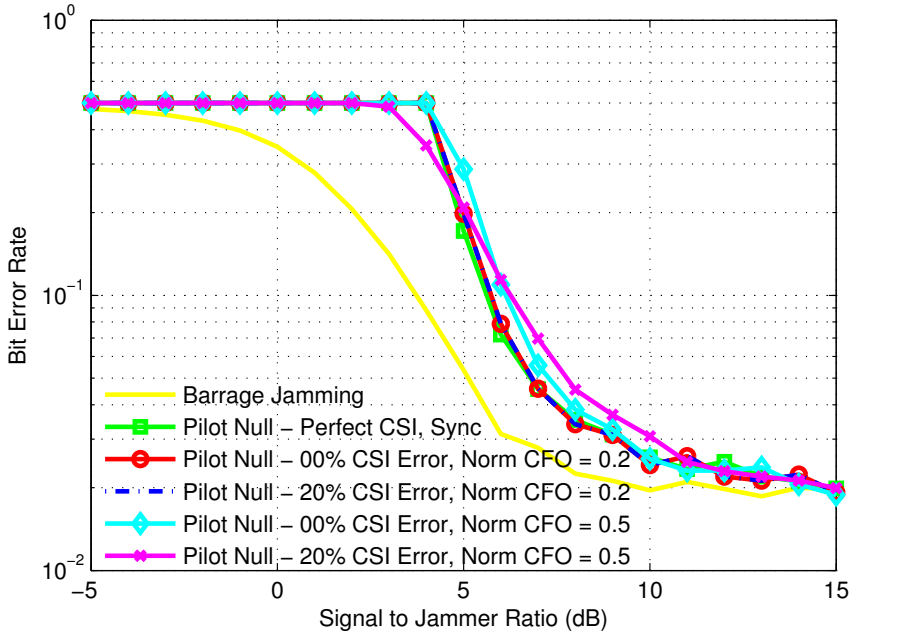

Figure 6.8: Performance of pilot singularity jamming operating at target signal SNR of 10 dB, for different levels of CSI knowledge and varying normalized frequency offset (NCFO).

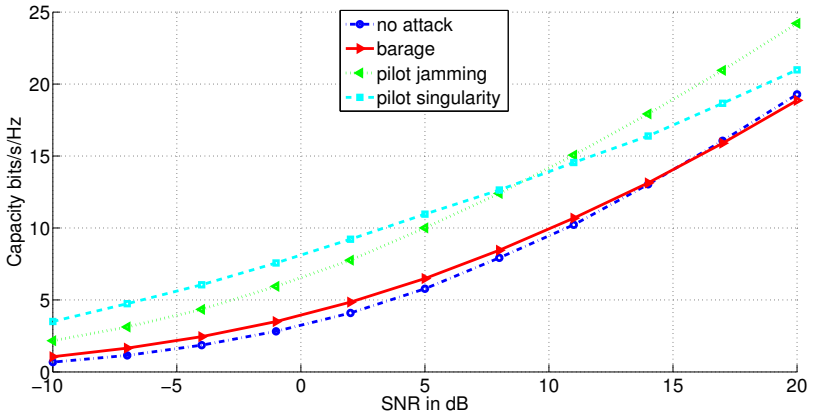

Figure 6.9: Comparison of perceived MIMO capacity in a 4×4 WiMAX vs. SNR with and without different jamming strategies (20% error in jammer's CSI estimation).

6.10 Summary

In this chapter, we addressed an efficient attacks against MIMO-enabled communications systems. We introduced a new type of attack on MIMO channels, which we termed as the 'singularity attack'. In this attack, the malicious node tries to manipulate the perception of CSI at the receiver and accordingly at the transmitter (when the feedback channel exists from receiver to transmitter). The jammer executes this by sending signals synchronous with pilot tones and adjusting them in a way that they cancel out the received pilot tones. As such, the receiver is misled in estimating the MIMO channel response resulting in higher BER. When this miss-estimated CSI is fed back to the transmitter, the MIMO channel capacity perception of the transmitter is also skewed, which results in water-filling with falsified eigenvalue information. This in turn, worsens the overall throughput. We showed singularity attack can be more effective than barrage jamming, pilot tone jamming and pilot tone singularity attacks in terms of BER degradation and deceptive channel capacity perception.

Eventually the efficiency of all these pilot tone attacks were compared with simple barrage jamming, which can be considered as optimum jamming in the absence of any knowledge

about the target signal. It is found that efficiency of the attacks decreases with the increase of time and frequency offsets, which is somewhat intuitive; however, intuition is backed up with specific quantitative results. Here we have simulated *Matrix B*, a specific MIMO-OFDM based WiMAX system. The simulation results indicate that even with imperfect time and frequency synchronization, pilot tone jamming, pilot tone nulling and singularity attacks outperform barrage jamming. However, the performance of the jammer depends on estimation accuracy of jammers knowledge of CSI between transmitter and target receiver.

As was shown in the analysis carried out here, the more accurate the jammer's estimation of the responses of the two MIMO channels, i.e. transmitter/receiver and jammer/receiver, the worse the effects of the attack. Therefore, to mitigate the singularity attack, the Tx-Rx pair should make it difficult for a third party to have access to their CSI. In other words, the communications between the transmitter and receiver should appear to have an unrecognizable structure from outside.

Chapter 7

Spatial Hiding Antijam (AJ) Communications

In this chapter, we describe a new method of designing an antijam (AJ) communications system. The key insight is that many of the theoretical concepts learned from transmit beamforming and interference alignment (IA) in multiple input multiple output (MIMO) antenna systems can be applied to the field of AJ and robust communications in the presence of intentional jammers. We consider a realistic jamming scenario and provide both a 'receiver-only' processing technique and a 'precoding' technique at the transmitter that allow a pair of two-antenna transceivers to communicate while being jammed by a malicious non-cooperative single-antenna adversary. The first method is a receiver-side zero-forcing (ZF) decoder that aligns the received signal to be orthogonal to the jammer. The other method utilizes the most favorable spatial dimension that is also orthogonal to the jammer and requires precoding at the transmitter. The transmit precoding technique uses a small amount of channel state information (CSI) that is fed back from the receiver to shape the signal to appear orthogonal to the jammer at the receiver. This allows a performance gain over the traditional receiver-only spatial hiding technique. The novelty introduced in this

work is both the application of transmit spatial beamforming to AJ communications and a specific method that allows a simple implementation to be practically employed.

The remainder of this chapter is organized as follows. In Section 7.1, motivation behind the work, as well as related literature surveys are presented. Section 7.2 describes the system model, sets up the basic assumptions, and notations used in the work. Section 7.3 explains both 'receiver-only' and 'precoding' processing techniques used to achieve a practical AJ system. In Section 7.4, the impact of imperfect communications CSI and jamming CSI on AJ schemes are investigated. A lower bound for jammer's interference as a function of the jamming CSI estimation error is also derived here. Section 7.5 provides simulated plots of BER performance results for the spatial hiding techniques in the context of an AJ system with various jammer-to-signal levels. The last section, Section 7.6, is the summary, which sums up the contributions, discusses limitations, and notes some possible applications.

7.1 Motivation and Related Works

The motivation for this work comes from the intuition that the innovative concepts from the nascent field of interference alignment [106–109] can be applied to the more mature field of data communication secrecy and robustness in the presence of intentional interferers, or jammers. The techniques examined in this work have previously been applied to wireless networks in scenarios where the RF interference is coming from legitimate adjacent co-channel users, such as nearby base stations in a cellular network. It provides a new fundamental technique for hiding a signal in the spatial domain, similar to the mature techniques of frequency hopping or direct sequence spread spectrum [110] that have been used for half a century to hide signals in the frequency domain.

This work examines a simple technique for defeating a high-powered jammer by using spatial beamforming at the transmitter and/or the receiver. Spatial nulling techniques at

the receiver have been used in practice for many years [111]. The idea of using the extra spatial dimensions provided by a MIMO channel in an AJ context is similar to the work done in [112] where users have different numbers of antennas and new transmitters attempt to use the same spectrum while avoiding the incumbent users by coding their signal to align in a non-interfering spatial dimension. It has also been mentioned in [113] where the two regimes of interference cancellation and array gain are employed to achieve a higher throughput. A good theoretical examination of a similar scenario to the one considered in this work is given in [114], where a jamming signal is intentionally added to improve the secrecy of a communications link. The major difference between this work and previous interference alignment work is the context of the problem – in AJ and cognitive radio scenarios, the other node is not a cooperative member that will willingly modify its signal or provide an estimate of its pilot symbols or channel estimation to other users. This work provides a precoding strategy at the transmitter side. This work also shows a simple receiver with ZF decoder that can achieve the same performance of spatial nulling with slightly less effort. A MIMO-based jamming resilient communication in wireless networks is presented in [115].

However, the key limitation of these methods is that their performance heavily depends on the availability and quality of the CSI. In practice, CSI estimation is always subject to error due to the presence of noise, statistical characteristics' of wireless channel, and limitations of hardware [116]. One of the most difficult aspects of utilizing spatial hiding techniques is acquiring the high quality CSI. This work describes several simple ways to do this for a particularly practical scenario – the 2×2 communications system in the presence of a single-antenna uncooperative jammer and discusses impact of CSI imperfection on the AJ communications system.

7.2 System Model

The system of interest involves a MIMO setup in the presence of a jammer. This work describes a scenario that has uni-directional communication, but the same techniques can be employed in the reverse direction of communications as well. There are three types of nodes in the scenario – a Transmitter, a Receiver, and a Jammer. The specific scenario analyzed in this work is the simplest application of the spatial hiding AJ technique that the author can envision. To keep the system simple, the MIMO system presented here is kept limited to a two-antenna Transmitter, a two-antenna Receiver, and a single-antenna Jammer. This sets up a two-dimensional space (2×2 MIMO) for the transmitter and receiver to utilize, while the jammer is restricted to a single dimension due to its single antenna. Note that it can be extended to higher order MIMO systems as well, but at the expense of increased computational complexity.

Figure 7.1 illustrates the high level block diagram of a 2×2 MIMO system in the presence of a single-antenna jammer. This system function can be modeled as

$$\mathbf{r} = \mathbf{H_{Tot}}\mathbf{v}^T + \mathbf{n} \tag{7.1}$$

where $\mathbf{r}$ is a 2×1 signal vector received at the two receiver antennas, $\mathbf{v}$ is a 1×3 signal vector that comprises signals sent from the two transmitter antennas and the jammer antenna, $\mathbf{H_{Tot}}$ is a 2×3 channel gain matrix whose elements are communication channel gains (i.e., channels between Tx-Rx pair) and jamming channel gains (i.e., channels between Jx-Rx pair), and $\mathbf{n}$ is a 2×1 vector of the two i.i.d additive complex Gaussian noise samples caused by the receiver thermal noise. Each component of $\mathbf{n}$ has a two-sided power spectral density of $\frac{N_o}{2}$.

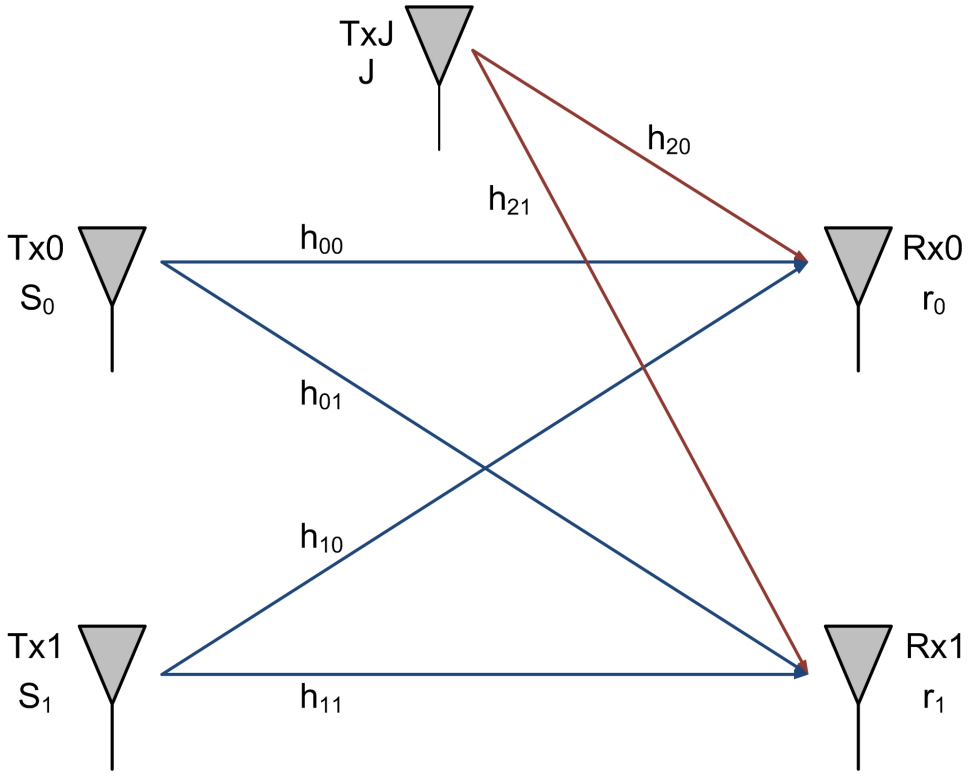

Figure 7.1: The block diagram of a simple 2×2 MIMO communications system in the presence of a single-antenna jammer.

Note that here $\mathbf{v}$ is the vector of all the transmitted signals and is given by

$$\mathbf{v} = \Big(S_0,\ S_1,\ J \Big) \tag{7.2}$$

where S_0 and S_1 are the signals transmitted from the two transmitter antennas and J is the signal transmitted by the jammer.

The channel gain matrix, $\mathbf{H_{Tot}}$ is given by

$$\mathbf{H_{Tot}} = \begin{pmatrix} h_{00} & h_{10} & h_{20} \\ h_{01} & h_{11} & h_{21} \end{pmatrix} \tag{7.3}$$

where each component is an independently drawn Rayleigh random variable. Therefore, each h_{ij} is a complex random variable with a uniformly distributed phase and a magnitude

with $E[h_{ij}^2] = 1$ and a Rayleigh amplitude distribution.

The jamming analysis in this chapter is from the perspective of the victim, or jamming target, receiver. The jammer power is defined as that which is received at the detector at the same point in the receiver that $\frac{E_b}{N_o}$ analysis normally occurs. Thus, the jammer transmit power necessary to achieve a certain jammer receive power will depend on where the jammer is located with respect to a receiver and the channel conditions between them. A jamming-to-signal ratio (JSR) parameter, α, is defined as $\alpha = \frac{E_j}{E_s}$, the ratio of jamming power at the receiver to intended signal power.

7.3 Two AJ Methods to Orthogonalize Intended Signal From Jammer

In this section, we consider a realistic jamming scenario and formulate two methods to orthogonalize intended signal from jammer – one is receiver-only processing technique and the other one is a precoding technique at the transmitter that allows a pair of two-antenna transceivers to communicate while being jammed by a malicious single-antenna jammer.

7.3.1 Receiver Only Antijam Communications

In order to understand the problem in the context of jamming, let us break the channel matrix, $\mathbf{H_{Tot}}$, into two components – communication channel matrix and jamming channel matrix. Here, the communication channel matrix, $\mathbf{H}$, refers to a 2×2 matrix between transmit antennas and receiver antennas and the jamming channel matrix, $\mathbf{H_j}$, refers to a 2×1 matrix between the jammer and receiver antennas.

The first step of the AJ process is to estimate the channel $\mathbf{H}$. All MIMO techniques require some level of channel information, so there are well developed methods in the literature [85]

to estimate $\mathbf{H}$. However, in the context of AJ systems there is the added complexity of an uncooperative jammer potentially being present. There are a number of ways to determine $\mathbf{H}$ during jamming and a few are listed here. One way is to assume that there are periods when the jammer sends a constant value over a few symbol intervals, making it possible to send some known pilot symbols and assemble enough linearly independent equations to solve for $\mathbf{H}$ at either the transmitters or receivers. It could also be the case that the jammer power is low enough at the transmitters that an estimate of $\mathbf{H}$ is available there. Another possibility is that the jammer is not constantly active and thus there are times when channel sounding can be performed to estimate $\mathbf{H}$ when no jammer is present. The practical problem of channel estimation in the presence of a jammer is scenario dependent, but there are plenty of cases where it is possible.

The next step is to estimate $\mathbf{H_j}$, the channel gains between the jammer and the two receiver antennas. $\mathbf{H_j}$ is the last column of $\mathbf{H_{Tot}}$. The receiver-only AJ technique will NOT require both h_{20} and h_{21} individually. It is really only necessary to find the ratio of $\frac{h_{20}}{h_{21}}$ to perform receiver only processing. The precoding technique will require both h_{20} and h_{21} individually. To get this ratio, just refrain from sending any symbols at the transmitters while listening at the receivers to the jamming signal:

$$\begin{aligned} r_0 &= Jh_{20} + n_0 \\ r_1 &= Jh_{21} + n_1 \end{aligned} \tag{7.4}$$

It can be assumed that the jammer energy J is large in relation to the thermal noise n_i so that the ratio of $\frac{r_0}{r_1}$ now reduces to $\frac{h_{20}}{h_{21}}$, which is independent of the jammer signal J assuming that it is received at the two antennas at roughly the same time. If the antennas are spaced one foot apart for example, the worst case time difference between the received J at r_0 and r_1 is approximately one nanosecond. So, as long as the jammer is not using more than 1 GHz of bandwidth, it is safe to assume that the two J values are nearly equivalent.

Many jammers utilize a bandwidth narrower than 1 GHz.

Now, it is possible to use this jamming CSI ratio to create a vector that is orthogonal to the jammer and use this vector, $\mathbf{Q}$, as a ZF decoder. The vector $\mathbf{Q}$, looks like

$$\mathbf{Q} = \left[1, -\left(\frac{h_{20}}{h_{21}}\right)\right] \tag{7.5}$$

Now, S_0 and S_1 , which is the data vector portion of $\mathbf{v}$ that is sent from the two antennas, can be fixed as $[1, 0]X$, where X is the one-dimensional data stream that we can send in the presence of the jammer signal J. The total received signal is now a sum of three distinct parts (from left to right): the precoded data affected by the 2X2 MIMO channel $\mathbf{H}$, the jammer signal affected by a 2X1 SIMO channel $\mathbf{H_j}$, and the additive Gaussian noise.

$$\mathbf{r} \quad = \mathbf{H}[1, 0]X + J\mathbf{H_j} + \mathbf{n} \tag{7.6}$$

The simplest decoder for this received signal is a ZF decoder that aligns the received vector $\mathbf{r}$ in the dimension of $\mathbf{Q}$ (i.e. orthogonal to the $\mathbf{H_j}$ dimension). The ZF decoder (which in this simple 2×1 case is a dot product operation along the dimension of $\mathbf{Q}$) correlates with the intended data, X, while being orthogonal to the jammer, J. The thermal noise $\mathbf{n}$ is now sampled in the direction of the $\mathbf{Q}$ vector, but since the noise is assumed to be circularly symmetric, the noise power in this dimension is equal to its value in the original unrotated dimension (i.e. it is still $\frac{N_o}{2}$). The output of the decoder will look like

$$\begin{aligned} Y &= \mathbf{Q} \cdot \mathbf{r} \\ &= \mathbf{Q}^T\mathbf{r} \\ &= \mathbf{Q}^T\Big[\mathbf{H}[1, 0]X + J\mathbf{H_j} + \mathbf{n}\Big] \\ &= \mathbf{Q}^T\mathbf{H}[1, 0]X + J\mathbf{Q}^T\mathbf{H_j} + \mathbf{Q}^T\mathbf{n} \end{aligned} \tag{7.7}$$

$$
\begin{aligned}
&= \left[1, -\left(\frac{h_{20}}{h_{21}}\right)\right]^T \mathbf{H}[1,0]X + J\left[1, -\left(\frac{h_{20}}{h_{21}}\right)\right]^T \mathbf{H_j} + \left[1, -\left(\frac{h_{20}}{h_{21}}\right)\right]^T \mathbf{n} \\
&= \left[1, -\left(\frac{h_{20}}{h_{21}}\right)\right]^T \mathbf{H}[1,0]X + J\left[1, -\left(\frac{h_{20}}{h_{21}}\right)\right]^T \left[h_{20}, h_{21}\right] + \left[1, -\left(\frac{h_{20}}{h_{21}}\right)\right]^T \left[n_0, n_1\right] \\
&= \left[1, -\left(\frac{h_{20}}{h_{21}}\right)\right]^T \mathbf{H}[1,0]X + J\left[h_{20} - \frac{h_{20}h_{21}}{h_{21}}\right] + \left[n_0 - n_1\left(\frac{h_{20}}{h_{21}}\right)\right] \\
&= \left[1, -\left(\frac{h_{20}}{h_{21}}\right)\right]^T \mathbf{H}[1,0]X + J\left[h_{20} - h_{20}\right] + \left[n_0 - n_1\left(\frac{h_{20}}{h_{21}}\right)\right] \\
&= \left[1, -\left(\frac{h_{20}}{h_{21}}\right)\right]^T \mathbf{H}[1,0]X + 0 + \left[n_0 - n_1\left(\frac{h_{20}}{h_{21}}\right)\right] \\
&= \underbrace{\gamma X}_{\text{Signal}} + \underbrace{0}_{\text{Jammer}} + \underbrace{w}_{\text{Noise}}
\end{aligned}
$$

where the superscript T stands for transpose, $\gamma = \left[1, -\left(\frac{h_{20}}{h_{21}}\right)\right]^T \mathbf{H}[1,0]$ is the scaling factor, and $w = \left[n_0 - n_1\left(\frac{h_{20}}{h_{21}}\right)\right]$ is the combined noise. The performance for one stream (X) of information in this channel is the same as it would have been with no jammer present. To get the transmitted data, X, multiply the result of Equation 7.7 by γ^* and make a hard decision. Both γ and w are random variables whose probability density function (pdf) are dependent on the pdf's of communication channel gains (i.e., h_{00}, h_{01}, h_{10}, and h_{11}), jamming channel gains (i.e., h_{20} and h_{21}), and additive white Gaussian noises (i.e., n_1 and n_2). Note that the pdf of each of these independent random variables are zero mean complex Gaussian.

Once $\mathbf{H_j}$ has been successfully estimated, the channel gains between the transmitter and receiver, $\mathbf{H}$, can be estimated at the receiver just as any typical communication system would estimate the channel (e. g. see [85]), such as with a short known preamble synchronization sequence.

Notice that the 'receiver only' antijam algorithm described above is shown in algorithm (1).

Algorithm 1 Receiver Only AJ Algorithm

loop
At time t_0, receive jamming signal $r_0 = Jh_{20} + n_0$ at receive antenna Rx_0.
At time t_0, receive jamming signal $r_1 = Jh_{21} + n_0$ at receive antenna Rx_1.
Form the received jamming CSI ratio $\frac{r_0}{r_1} \approx \frac{h_{20}}{h_{21}}$ at receiver.
Construct $\mathbf{Q}$, where $\mathbf{Q} = \left[1, -\frac{h_{20}}{h_{21}}\right]$.
At time t_1, receive total signal $\mathbf{r} = \mathbf{H}[1,0]X + J\mathbf{H_j} + \mathbf{n}$.
At receiver, perform ZF decoding as $Y = \mathbf{Q} \cdot \mathbf{r} = \mathbf{Q}^T\mathbf{r} = \gamma X + 0 + w$.
Make hard decision by multiplying Y with γ^*, where $\gamma = \left[1, -\left(\frac{h_{20}}{h_{21}}\right)\right]^T \mathbf{H}[1,0]$.
end loop

7.3.2 Transmitter Precoding Antijam Communications

One way to increase the throughput performance of system is to precode the data at the transmitter to take advantage of the dominant eigenmode of the combined transceiver and jammer channel. Here we introduce a spatial hiding precoding technique. Let us define a 2×2 projection operator that is orthogonal to the jammer channel as $\bar{\mathbf{P}}$.

$$\bar{\mathbf{P}} \quad = \left(\mathbf{I} - \frac{\mathbf{H_j}\mathbf{H_j}^\dagger}{\mathbf{H_j}^\dagger\mathbf{H_j}}\right) \tag{7.8}$$

where $\mathbf{I}$ is the 2×2 identity matrix and the $\dagger$ stands for the transpose conjugate operation.

The precoding vector should be the dominant right singular vector of $\bar{\mathbf{P}}\mathbf{H}$, which is the projection in the direction orthogonal to the jamming channel upon the transceiver channel. Let us call this dominant right singular vector $\mathbf{v}$. Then the 2×1 precoding vector is given by $\mathbf{v}X$, where X is the one-dimensional data stream as defined earlier.

The received signal is now:

$$\mathbf{r} = \mathbf{H}[v_0, v_1]X + J\mathbf{H_j} + \mathbf{n} \tag{7.9}$$

The ZF receiver will then be $\mathbf{u}^\dagger\bar{\mathbf{P}}$, where $\mathbf{u}$ is the dominant left singular vector of $\bar{\mathbf{P}}\mathbf{H}$.

$$\begin{aligned}\mathbf{u}^\dagger\bar{\mathbf{P}}\mathbf{r} &= \mathbf{u}^\dagger\bar{\mathbf{P}}(\mathbf{H}\mathbf{v}X + J\mathbf{H_j} + \mathbf{n}) \\ &= \mathbf{u}^\dagger\bar{\mathbf{P}}\mathbf{H}\mathbf{v}X + 0 + \mathbf{u}^\dagger\bar{\mathbf{P}}\mathbf{n} \\ &= \lambda X + 0 + \mathbf{u}^\dagger\bar{\mathbf{P}}\mathbf{n}\end{aligned} \tag{7.10}$$

where λ is the largest singular value of $\bar{\mathbf{P}}\mathbf{H}$. Since the norm of $\mathbf{u}^\dagger\bar{\mathbf{P}}$ is one, the thermal noise $\mathbf{n}$ is now sampled in the direction of $\mathbf{u}^\dagger\bar{\mathbf{P}}$, but since the noise is assumed to be circularly symmetric, the noise power in this direction is equal to its value in the original unrotated direction (i.e. it is still $\frac{N_o}{2}$).

This method of precoding in the dominant spatial direction of the combined transceiver and jammer channel leads to a large performance gain over the case where there is no precoding and only receiver spatial nulling is performed. It is intuitive that some type of gain should be expected because in this case, unlike the previous case with receiver-only processing, both transmitter antennas are being used by sending v_0X on one and v_1X on the other. The BER results in Section 7.5 highlight how the precoding technique can offer a performance gain.

In both of these spatial hiding methods – receiver only and combined transmit and receive – the communications signal is now orthogonal to the jammer signal J at the receiver. This means that the effective signal-to-noise ratio at the receiver is independent of the jammer-to-signal ratio, α. This is quite an extraordinary quality for an AJ radio to have – a signal quality that is not affected by the amount of power in the jammer's signal! The drawback to this method is that it does assume perfect channel information for $\mathbf{H_j}$. However, because only one complex value ($\frac{h_{20}}{h_{21}}$) must be estimated in the receiver-only beamforming method and only two complex values (h_{20}, h_{21}) are estimated in the transmitter beamforming method, it is practical to implement such a scheme under a wide variety of scenarios. The necessity of feedback to the transmitter does limit the speed of adaptation that the precoding will be able to handle. If the channel conditions of $\mathbf{H_j}$ vary at such a speed that the feedback required

Algorithm 2 Transmitter Precoding AJ Algorithm

loop
At time t_0, receive jamming signal $r_0 = Jh_{20} + n_0$ at antenna Rx_0, assume $r_0 \approx h_{20}$.
At time t_0, receive jamming signal $r_1 = Jh_{21} + n_0$ at antenna Rx_1, assume $r_1 \approx h_{21}$.
Construct projection operator orthogonal to jamming channel, where $\bar{\mathbf{P}} = \left(\mathbf{I} - \frac{\mathbf{H_j}\mathbf{H_j}^\dagger}{\mathbf{H_j}^\dagger\mathbf{H_j}}\right)$.
Construct precoder $\mathbf{v}$, which is right sigular vector of $\bar{\mathbf{P}}\mathbf{H}$.
At time t_1, receive total signal $\mathbf{r} = \mathbf{H}[v_0, v_1]X + J\mathbf{H_j} + \mathbf{n}$.
At receiver, perform ZF decoding as $Y = \mathbf{u}^\dagger\bar{\mathbf{P}}\mathbf{r} = \lambda X + 0 + \mathbf{u}^\dagger\bar{\mathbf{P}}\mathbf{n}$.
Make hard decision by multiplying Y with λ^* where $\lambda = \mathbf{u}^\dagger\bar{\mathbf{P}}\mathbf{H}\mathbf{v}$.
end loop

for the precoding cannot keep up with the current set of values for $\mathbf{H_j}$, then the performance of this AJ technique will degrade significantly. This would be the case, for example, if the jammer were moving at a high speed. In this case, it is more practical to do the receiver only processing method of Equation 7.7.

The sensitivity of these AJ communications methods to channel estimation errors is investigated in the next section, and it is found that for moderate α's the precoding will still be valuable even with the channel estimation errors inherent in real systems 7.4. Analysis and simulations showed that the BER degradation for a 5% and 10% channel estimation error was manageable for values of $\alpha < 10$.

Notice that the spatial hiding precoding (SHP) antijam algorithm described above is shown in algorithm (2).

7.4 Impact of Imperfect Channel State Information

In this section, we investigate the impact of imperfect communication and jamming CSI on spatial hiding AJ communications. Note that estimating the channel always results in some estimation error due to the presence of AWGN, wireless channel discrepancies, hardware limitations etc. Hence, it is always necessary to evaluate the impact of such impairment. By modeling the CSI estimation error as independent complex Gaussian random variables,

analytical model for post-processing residual interference is derived in closed-form for both transceiver and jamming CSI estimation error. In addition, a lower bound for jammer's interference as a function of jamming CSI estimation error is derived. Through simulation we demonstrate the effect of imperfect CSI on spatial hiding anti-jam and validate the analytical model as well.

7.4.1 Imperfect CSI: Communication Channel

In this section we investigate the impact of imperfect communication CSI on spatial hiding AJ communications.

If we consider the channel estimation model for MIMO in [85], we can model the communication channel estimate as

$$\hat{\mathbf{H}} = \mathbf{H} + \epsilon\boldsymbol{\Omega} \tag{7.11}$$

where $\epsilon\boldsymbol{\Omega}$ is the estimation error that is uncorrelated with $\mathbf{H}$, the entries of $\boldsymbol{\Omega}$ are i.i.d zero mean unit variance complex Gaussian and ϵ is the measure of how accurate the channel estimation is.

Suppose $\mathbf{G} = \mathbf{H^{-1}}$, then

$$\hat{\mathbf{G}} = \hat{\mathbf{H}}^{-\mathbf{1}} = (\mathbf{H} + \epsilon\boldsymbol{\Omega})^{-\mathbf{1}} \tag{7.12}$$

Assuming $\epsilon << 1$, then the inverse of the estimated channel matrix can be approximated by the linear part of the Taylor expansion as

$$\hat{\mathbf{G}} \cong \mathbf{H}^{-\mathbf{1}}(\mathbf{I}_{\mathbf{N_r}} - \epsilon\boldsymbol{\Omega}\mathbf{H}^{-\mathbf{1}}) \tag{7.13}$$

where I_{N_r} is the identity matrix of size $N_r \times N_r$, with N_r being the number of received antennas [116].

For communication channel estimation error, the received signal, for receiver only scheme,

right after the receiver post-processing, can be written as (excluding jamming signal and AWGN) [117]

$$\begin{aligned} S &= \mathbf{Q} \cdot \mathbf{r} \\ &= \mathbf{Q}^T \mathbf{r} \\ &= \left[1, -\left(\frac{h_{20}}{h_{21}}\right)\right]^T (\mathbf{H} + \epsilon\mathbf{\Omega})[1,0]X \\ &= \Bigg[\underbrace{\left[1, -\left(\frac{h_{20}}{h_{21}}\right)\right]^T \mathbf{H}[1,0]}_{Scaled-Signal} + \underbrace{\left[1, -\left(\frac{h_{20}}{h_{21}}\right)\right]^T (\epsilon\mathbf{\Omega})[1,0]}_{Residue}\Bigg] X \end{aligned} \tag{7.14}$$

The post-processing residue noise term due to communication channel estimation error or imperfect CSI can be modeled as

$$N_H = \left[1, -\left(\frac{h_{20}}{h_{21}}\right)\right]^T (\epsilon\mathbf{\Omega})[1,0] \tag{7.15}$$

For communication channel estimation error, the received signal, for precoder scheme, right after the receiver post-processing, can be written as (excluding jamming signal and AWGN) [117]

$$\begin{aligned} S &= \mathbf{u}^\dagger \bar{\mathbf{P}} \mathbf{r} \\ &= \mathbf{u}^\dagger \bar{\mathbf{P}} (\mathbf{H} + \epsilon\mathbf{\Omega})\mathbf{v}X \\ &= \Bigg[\underbrace{\mathbf{u}^\dagger \bar{\mathbf{P}} \mathbf{H} \mathbf{v}}_{Scaled-Signal} + \underbrace{\mathbf{u}^\dagger \bar{\mathbf{P}} \epsilon\mathbf{\Omega}\mathbf{v}}_{Residue}\Bigg] X \end{aligned} \tag{7.16}$$

The post-processing residue noise term due to communication channel estimation error or imperfect CSI can be modeled as

$$N_H = \mathbf{u}^\dagger \bar{\mathbf{P}} \epsilon\mathbf{\Omega}\mathbf{v} \tag{7.17}$$

This is not a big set back as this effect can be undone simply by changing γ^* to perform hard decision. However, the exact amount of error is typically unknown and hence, causes degradation in demodulation performance.

7.4.2 Imperfect CSI: Jamming Channel

Here we investigate the impact of imperfect jamming CSI on spatial hiding AJ communications. Note that estimating the ratio of jamming channels under AWGN results in estimation error.

Let the estimate of jamming channels be $\hat{h}_{20} = h_{20} + \epsilon_{20}$ and $\hat{h}_{21} = h_{21} + \epsilon_{21}$ at time $t = t_0$ (the time when no transmission occurs and receiver sits idle and listens to jammer). Hence, a new variable $\hat{\mathbf{Q}}$, the estimated version of $\mathbf{Q}$, can be defined as

$$\hat{\mathbf{Q}} = \left[1, -\left(\frac{\hat{h}_{20}}{\hat{h}_{21}}\right)\right] \tag{7.18}$$

Along with orthogonality, the initial assumption for AJ scheme was such that the jamming channels are static or quasi-static. Hence, it can be said that the jamming channel at $t = t_1 > t_0$ is $\tilde{h}_{20} \cong h_{20}$ and $\tilde{h}_{21} \cong h_{21}$. The residual noise or interference from the jammer, N_{H_j}, can be written as

$$\begin{aligned} N_{H_j} &= \hat{\mathbf{Q}} \cdot J\tilde{\mathbf{H}}_{\mathbf{j}} \\ &= \hat{\mathbf{Q}}^T J\tilde{\mathbf{H}}_{\mathbf{j}} \\ &= \left[1, -\left(\frac{\hat{h}_{20}}{\hat{h}_{21}}\right)\right]^T \left(J\left[\tilde{h}_{20}, \tilde{h}_{21}\right]\right) \\ &= \left[1, -\left(\frac{\hat{h}_{20}}{\hat{h}_{21}}\right)\right]^T \left(J\left[h_{20}, h_{21}\right]\right) \\ &= Jh_{20} - \frac{(\hat{h}_{20})(Jh_{21})}{\hat{h}_{21}} \end{aligned} \tag{7.19}$$

$$
\begin{aligned}
&= Jh_{20} - \frac{Jh_{21}(h_{20}+\epsilon_{20})}{h_{21}+\epsilon_{21}} \\
&= J\left(\frac{h_{20}\epsilon_{21} - h_{21}\epsilon_{20}}{h_{21}+\epsilon_{21}}\right) \\
&= JI_{H_j}
\end{aligned}
$$

Note that here h_{20}, h_{21}, ϵ_{20}, and ϵ_{21} can be defined respectively as $h_{20} = h_{20}^S(h_{20}^R + ih_{20}^I)$, $h_{21} = h_{21}^S(h_{21}^R + ih_{21}^I)$, $\epsilon_{20} = \epsilon_{20}^S(\epsilon_{20}^R + i\epsilon_{20}^I)$ and $\epsilon_{21} = \epsilon_{21}^S(\epsilon_{21}^R + i\epsilon_{21}^I)$, where h_{20}^S, h_{21}^S, ϵ_{20}^S and ϵ_{21}^S are scaling factors. The superscript 'R' and 'I' stands for real and imaginary part of the complex signal. Note that each of them (real and imaginary) are zero mean and unit variance Gaussian random variables.

$$
\begin{aligned}
I_{H_j} &= \frac{h_{20}\epsilon_{21} - h_{21}\epsilon_{20}}{h_{21}+\epsilon_{21}} \\
&= \frac{h_{20}^S(h_{20}^R + ih_{20}^I)\epsilon_{21}^S(\epsilon_{21}^R + i\epsilon_{21}^I) - h_{21}^S(h_{21}^R + ih_{21}^I)\epsilon_{20}^S(\epsilon_{20}^R + i\epsilon_{20}^I)}{h_{21}^S(h_{21}^R + ih_{21}^I) + \epsilon_{21}^S(\epsilon_{21}^R + i\epsilon_{21}^I)} \\
&= \frac{h_{20}^S\epsilon_{21}^S(h_{20}^R\epsilon_{21}^R - h_{20}^I\epsilon_{21}^I + i(h_{20}^R\epsilon_{21}^I + h_{20}^I\epsilon_{21}^R)) - h_{21}^S\epsilon_{20}^S(h_{21}^R\epsilon_{20}^R - h_{21}^I\epsilon_{20}^I + i(h_{21}^R\epsilon_{20}^I + h_{21}^I\epsilon_{20}^R))}{(h_{21}^S h_{21}^R + ih_{21}^S h_{21}^I) + (\epsilon_{21}^S\epsilon_{21}^R + i\epsilon_{21}^S\epsilon_{21}^I)} \\
&= \frac{h_{20}^S\epsilon_{21}^S(h_{20}^R\epsilon_{21}^R - h_{20}^I\epsilon_{21}^I + i(h_{20}^R\epsilon_{21}^I + h_{20}^I\epsilon_{21}^R)) - h_{21}^S\epsilon_{20}^S(h_{21}^R\epsilon_{20}^R - h_{21}^I\epsilon_{20}^I + i(h_{21}^R\epsilon_{20}^I + h_{21}^I\epsilon_{20}^R))}{(h_{21}^S h_{21}^R + \epsilon_{21}^S\epsilon_{21}^R) + i(h_{21}^S h_{21}^I + \epsilon_{21}^S\epsilon_{21}^I)}
\end{aligned}
\tag{7.20}
$$

Let us define new variables $X = h_{20}^S\epsilon_{21}^S = Constant$, $Y = h_{21}^S\epsilon_{20}^S = Constant$, $A = (h_{20}^R\epsilon_{21}^R - h_{20}^I\epsilon_{21}^I)$, $B = (h_{21}^R\epsilon_{20}^R - h_{21}^I\epsilon_{20}^I)$, $C = (h_{20}^R\epsilon_{21}^I + h_{20}^I\epsilon_{21}^R)$, $D = (h_{21}^R\epsilon_{20}^I + h_{21}^I\epsilon_{20}^R)$, $E = (h_{21}^S h_{21}^R + \epsilon_{21}^S\epsilon_{21}^R)$, and $F = (h_{21}^S h_{21}^I + \epsilon_{21}^S\epsilon_{21}^I)$. Hence

$$
I_{H_j} = \frac{(XA - YB) + i(XC - YD)}{(E + iF)} \tag{7.21}
$$

Note that in each case h_i^j and ϵ_i^j both are standard normal distribution. Hence, the bivariate probability density function (pdf) will be product normal distribution whose pdf

can be expressed as

$$\begin{aligned} P_{h_i^j \epsilon_i^j}(u_k) &= \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} \frac{e^{-(h_i^j)^2/2\sigma^2_{h_i^j}}}{\sigma_{h_i^j}\sqrt{2\pi}} \frac{e^{-(\epsilon_i^j)^2/2\sigma^2_{\epsilon_i^j}}}{\sigma_{\epsilon_i^j}\sqrt{2\pi}} \delta(h_i^j \epsilon_i^j - u_k)\,\mathrm{d}h_i^j \mathrm{d}\epsilon_i^j \\ &= \frac{1}{\pi \sigma_{h_i^j}\sigma_{\epsilon_i^j}} K_0\left(\frac{|u_k|}{\sigma_{h_i^j}\sigma_{\epsilon_i^j}}\right) \\ &= \frac{1}{\pi} K_0(|u_k|) \end{aligned} \tag{7.22}$$

where $\delta(x)$ is a delta function and $K_n(z)$ is a modified Bessel function of the second kind. Note that it's mean $\mu = 0$ and variance, $var\{P\} = var\{h_i^j\}var\{\epsilon_i^j\} = 1$.

So, the combined pdf of I_{H_j} can be expressed as

$$f(I_{H_j}) = \frac{(Xf(A) - Yf(B)) + i(Xf(C) - Yf(D))}{f(E) + if(F)} \tag{7.23}$$

where

$$f(A) = \frac{1}{\pi}\left(K_0(|u_1|) - K_0(|u_2|)\right) \tag{7.24}$$

$$f(B) = \frac{1}{\pi}\left(K_0(|u_3|) - K_0(|u_4|)\right) \tag{7.25}$$

$$f(C) = \frac{1}{\pi}\left(K_0(|u_5|) + K_0(|u_6|)\right) \tag{7.26}$$

$$f(D) = \frac{1}{\pi}\left(K_0(|u_7|) + K_0(|u_8|)\right) \tag{7.27}$$

$$f(E) = \left(K_0(|u_9|) - K_0(|u_{10}|)\right) \tag{7.28}$$

$$f(F) = \left(K_0(|u_{11}|) + K_0(|u_{12}|)\right) \tag{7.29}$$

$$f(E) = N\left(0, (h_{21}^S)^2 + (\epsilon_{21}^S)^2\right) \tag{7.30}$$

$$f(F) = N\left(0, (h_{21}^S)^2 + (\epsilon_{21}^S)^2\right) \tag{7.31}$$

7.4.2.1 A Lower Bound

Here, utilizing the properties of absolute values, we attempt to derive a lower bound for the magnitude of N_{H_j}.

The magnitude of N_{H_j} can be written as

$$\begin{aligned} \left|N_{H_j}\right| &= \left| J\frac{h_{20}\epsilon_{21} - h_{21}\epsilon_{20}}{h_{21}+\epsilon_{21}} \right| \\ &= \frac{|Jh_{20}\epsilon_{21} - Jh_{21}\epsilon_{20}|}{|h_{21}+\epsilon_{21}|} \\ &= \frac{|Jh_{20}\epsilon_{21} - Jh_{21}\epsilon_{20}|}{|h_{21}^S h_{21}^R + ih_{21}^S h_{21}^I + \epsilon_{21}^S \epsilon_{21}^R + i\epsilon_{21}^S \epsilon_{21}^I|} \\ &= \frac{|Jh_{20}\epsilon_{21} - Jh_{21}\epsilon_{20}|}{|(h_{21}^S h_{21}^R + \epsilon_{21}^S \epsilon_{21}^R) + i(h_{21}^S h_{21}^I + \epsilon_{21}^S \epsilon_{21}^I)|} \\ &= \frac{|Jh_{20}\epsilon_{21} - Jh_{21}\epsilon_{20}|}{|R|} \end{aligned} \tag{7.32}$$

where $R = (h_{21}^S h_{21}^R + \epsilon_{21}^S \epsilon_{21}^R) - i(h_{21}^S h_{21}^I + \epsilon_{21}^S \epsilon_{21}^I)$ and J is jamming signal (complex or real number).

Using the property of absolute values, $|a-b| \geq |a| - |b|$, we can derive a lower bound for $\left|N_{H_j}\right|$ as

$$\begin{aligned} \left|N_{H_j}\right| &\geq \frac{|Jh_{20}\epsilon_{21}| - |Jh_{21}\epsilon_{20}|}{|R|} \\ &= \frac{|J|\,|h_{20}|\,|\epsilon_{21}| - |J|\,|h_{21}|\,|\epsilon_{20}|}{|R|} \\ &= |J| \left(\frac{|h_{20}|\,|\epsilon_{21}|}{|R|} - \frac{|h_{21}|\,|\epsilon_{20}|}{|R|} \right) \\ &= |J| \left(\left(\frac{|h_{20}|}{|R|} \right) |\epsilon_{21}| - \left(\frac{|h_{21}|}{|R|} \right) |\epsilon_{20}| \right) \end{aligned} \tag{7.33}$$

Note that $|h_{20}|$, $|h_{21}|$, $|\epsilon_{20}|$ and $|\epsilon_{21}|$ are independent Rayleigh distributed random variables with mean $\mu = \sqrt{\frac{\pi}{2}}$ and variance, $\sigma^2 = \frac{4-\pi}{2}$ [95]. Also note that, the absolute value of the

denominator is a Rayleigh distributed random variable as well. Hence,

$$\begin{aligned} |R| &= \left| \left(h_{21}^S h_{21}^R + \epsilon_{21}^S \epsilon_{21}^R \right) + i \left(h_{21}^S h_{21}^I + \epsilon_{21}^S \epsilon_{21}^I \right) \right| \\ &= |E + iF| \\ &= \sqrt{E^2 + F^2} \end{aligned} \tag{7.34}$$

where the pdf of both E and F are normal distribution with $N\left(0, (h_{21}^S)^2 + (\epsilon_{21}^S)^2\right)$ and $N\left(0, (h_{21}^S)^2 + (\epsilon_{21}^S)^2\right)$ respectively. So, the Rayleigh distribution of $|R|$ can be described with mean $\mu = \left(\sqrt{\frac{\pi}{2}}\right)\left(h_{21}^S + \epsilon_{21}^S\right)$ and variance, $\sigma^2 = \left(\frac{4-\pi}{2}\right)\left((h_{21}^S)^2 + (\epsilon_{21}^S)^2\right)$.

Since all the elements of the final expression are independent Rayleigh random variables, we can easily reproduce $\left|N_{H_j}\right|$ statistically with the combination of multiple pdf's. In fact, this is the key motivation of deriving the lower bound; we may lose the precision, but gain a statistical knowledge about the error caused by imperfect H_j CSI.

$$\left|N_{H_j}\right| \geq |J| \left(\frac{f_h(|h_{20}|) f_\epsilon(|\epsilon_{21}|)}{f_r(|R|)} - \frac{f_h(|h_{21}|) f_\epsilon(|\epsilon_{20}|)}{f_r(|R|)} \right) \tag{7.35}$$

where $f_i(|i|)$ represents the pdf for Rayleigh distribution and i is variable.

Now, let us try to find out the combined probability density function (pdf) of the magnitude N_{H_j}. Before doing that, let us define several new intermediate variables – $u = \frac{h_{20}}{r}$, $v = \frac{h_{21}}{r}$, $p = u\epsilon_{21}$ and $q = v\epsilon_{20}$.

So, the combined pdf of N_{H_j} can be expressed as

$$f_{N_{H_j}}\left(\left|N_{H_j}\right|\right) \geq f_z(z) = f_z\left(\frac{|h_{20}|}{|r|} |\epsilon_{21}| - \frac{|h_{21}|}{|r|} |\epsilon_{20}| \right) \tag{7.36}$$

Alternatively it can be written as for $h_{20} \geq 0,\ h_{21} \geq 0,\ \epsilon_{20} \geq 0,\ \epsilon_{21} \geq 0\ and\ r \geq 0$

$$f_{N_{H_j}}\left(I_{H_j}\right) \geq f_z(z) = f_z\left(\frac{h_{20}}{r}\epsilon_{21} - \frac{h_{21}}{r}\epsilon_{20}\right) \tag{7.37}$$

We know that the ratio of two independent random variables can be written as [95]

$$\begin{aligned} f_{z'}\left(z'\right) &= \int_{-\infty}^{\infty} |y'|\, f_{x'y'}\left(x', y'\right)\ \mathrm{d}y' \\ &= \int_{-\infty}^{\infty} |y'|\, f_{x'y'}\left(y'z', y'\right)\ \mathrm{d}y' \\ &= \int_{-\infty}^{\infty} |y'|\, f_{x'}\left(y'z'\right) f_{y'}\left(y'\right)\ \mathrm{d}y' \\ &= \int_{0}^{\infty} y' f_{x'}\left(y'z'\right) f_{y'}\left(y'\right)\ \mathrm{d}y' \quad for\ x' \geq 0,\ y' \geq 0,\ and\ z' \geq 0 \end{aligned} \tag{7.38}$$

Now, we have already defined two new random variables $u = \frac{h_{20}}{r}$ and $v = \frac{h_{21}}{r}$; hence, the ratio distributions can be defined as

$$\begin{aligned} f_u\left(u\right) &= \int_0^{\infty} r f_{h_{20}}\left(ru\right) f_r\left(r\right) \mathrm{d}r \\ &= \int_0^{\infty} r\left[\frac{ru}{\sigma_{h_{20}}^2} e^{-(ru)^2/2\sigma_{h_{20}}^2}\right] \times \left[\frac{r}{\sigma_r^2} e^{-(r)^2/2\sigma_r^2}\right] \mathrm{d}r \\ &= 2\left(\frac{\sigma_{h_{20}}^2}{\sigma_r^2}\right) \frac{u}{\left(u^2 + \frac{\sigma_{h_{20}}^2}{\sigma_r^2}\right)^2} U\left(u\right) \\ &= 2\frac{\left(\frac{4-\pi}{2}\right)}{\left(\frac{4-\pi}{2}\right)\left((h_{21}^S)^2 + (\epsilon_{21}^S)^2\right)} \frac{u}{\left(u^2 + \frac{\left(\frac{4-\pi}{2}\right)}{\left(\frac{4-\pi}{2}\right)\left((h_{21}^S)^2 + (\epsilon_{21}^S)^2\right)}\right)^2} U\left(u\right) \\ &= 2\frac{1}{\left((h_{21}^S)^2 + (\epsilon_{21}^S)^2\right)} \frac{u}{\left(u^2 + \frac{1}{\left((h_{21}^S)^2 + (\epsilon_{21}^S)^2\right)}\right)^2} U\left(u\right) \\ &= \frac{2u\left((h_{21}^S)^2 + (\epsilon_{21}^S)^2\right)}{\left(u^2\left((h_{21}^S)^2 + (\epsilon_{21}^S)^2\right) + 1\right)^2} U\left(u\right) \quad for\ h_{20} \geq 0,\ r \geq 0,\ and\ u \geq 0 \end{aligned} \tag{7.39}$$

and

$$
\begin{aligned}
f_v(v) &= \int_0^\infty r f_{h_{21}}(rv) f_r(r)\,\mathrm{d}r \qquad (7.40)\\
&= \int_0^\infty r\left[\frac{rv}{\sigma_{h_{21}}^2} e^{-(rv)^2/2\sigma_{h_{21}}^2}\right] \times \left[\frac{r}{\sigma_r^2} e^{-(r)^2/2\sigma_r^2}\right] \mathrm{d}r\\
&= 2\left(\frac{\sigma_{h_{21}}^2}{\sigma_r^2}\right) \frac{v}{\left(v^2 + \frac{\sigma_{h_{21}}^2}{\sigma_r^2}\right)^2} U(v)\\
&= 2\frac{\left(\frac{4-\pi}{2}\right)}{\left(\frac{4-\pi}{2}\right)\left((h_{21}^S)^2 + (\epsilon_{21}^S)^2\right)} \frac{v}{\left(v^2 + \frac{\left(\frac{4-\pi}{2}\right)}{\left(\frac{4-\pi}{2}\right)\left((h_{21}^S)^2+(\epsilon_{21}^S)^2\right)}\right)^2} U(v)\\
&= 2\frac{1}{\left((h_{21}^S)^2 + (\epsilon_{21}^S)^2\right)} \frac{v}{\left(v^2 + \frac{1}{\left((h_{21}^S)^2+(\epsilon_{21}^S)^2\right)}\right)^2} U(v)\\
&= \frac{2v\left((h_{21}^S)^2 + (\epsilon_{21}^S)^2\right)}{\left(v^2\left((h_{21}^S)^2 + (\epsilon_{21}^S)^2\right) + 1\right)^2} U(v) \quad \textit{for } h_{21} \geq 0,\ r \geq 0,\ \textit{and } v \geq 0
\end{aligned}
$$

Now, let us look into the next step, which is multiplying two independent random variables. Let x" and y" be continuous random variables with joint pdf $f_{x",y}(x",y")$. The pdf of $z" = x"y"$ can be written as [95]

$$
\begin{aligned}
f_{z''}(z'') &= \int_{-\infty}^{\infty} \frac{1}{|x''|} f_{x''y''}(x'', y'')\ \mathrm{d}x'' \qquad (7.41)\\
&= \int_{-\infty}^{\infty} \frac{1}{|x''|} f_{x''y''}\left(x'', \frac{z''}{x''}\right)\ \mathrm{d}x''\\
&= \int_{-\infty}^{\infty} \frac{1}{|x''|} f_{x''}(x'') f_{y''}\left(\frac{z''}{x''}\right)\ \mathrm{d}x''\\
&= \int_{0}^{\infty} \frac{1}{x''} f_{x''}(x'') f_{y''}\left(\frac{z''}{x''}\right)\ \mathrm{d}x'' \quad \textit{for } x'' \geq 0,\ y'' \geq 0,\ \textit{and } z'' \geq 0
\end{aligned}
$$

Now, we already defined two new random variables $p = u\epsilon_{21}$ and $q = v\epsilon_{20}$; hence the

product distributions can be defined as

$$\begin{aligned} f_p(p) &= \int_0^\infty \frac{1}{u} f_u(u)\, f_{\epsilon_{21}}\left(\frac{p}{u}\right)\, \mathrm{d}u \quad for\ u \geq 0,\ \epsilon_{21} \geq 0,\ and\ p \geq 0 \\ &= \int_0^\infty \frac{1}{u}\left[\frac{2u\left((h_{21}^S)^2 + (\epsilon_{21}^S)^2\right)}{\left(u^2\left((h_{21}^S)^2 + (\epsilon_{21}^S)^2\right)+1\right)^2}\right] \times \left[\frac{(p/u)}{\sigma_{\epsilon_{21}}^2} e^{-\frac{(p/u)^2}{2\sigma_{\epsilon_{21}}^2}}\right] \mathrm{d}u \\ &= \frac{2\left((h_{21}^S)^2 + (\epsilon_{21}^S)^2\right)}{\sigma_{\epsilon_{21}}^2} \int_0^\infty \frac{p e^{-p^2/2u^2\sigma_{\epsilon_{21}}^2}}{\left(u^2\left((h_{21}^S)^2 + (\epsilon_{21}^S)^2\right)+1\right)^2 u}\, \mathrm{d}u \end{aligned} \tag{7.42}$$

and

$$\begin{aligned} f_q(q) &= \int_0^\infty \frac{1}{v} f_v(v)\, f_{\epsilon_{20}}\left(\frac{q}{v}\right)\, \mathrm{d}v \quad for\ v \geq 0,\ \epsilon_{20} \geq 0,\ and\ q \geq 0 \\ &= \int_0^\infty \frac{1}{v}\left[\frac{2v\left((h_{21}^S)^2 + (\epsilon_{21}^S)^2\right)}{\left(v^2\left((h_{21}^S)^2 + (\epsilon_{21}^S)^2\right)+1\right)^2}\right] \times \left[\frac{(q/v)}{\sigma_{\epsilon_{20}}^2} e^{-\frac{(q/v)^2}{2\sigma_{\epsilon_{20}}^2}}\right] \mathrm{d}v \\ &= \frac{2\left((h_{21}^S)^2 + (\epsilon_{21}^S)^2\right)}{\sigma_{\epsilon_{20}}^2} \int_0^\infty \frac{q e^{-q^2/2v^2\sigma_{\epsilon_{20}}^2}}{\left(v^2\left((h_{21}^S)^2 + (\epsilon_{21}^S)^2\right)+1\right)^2 v}\, \mathrm{d}v \end{aligned} \tag{7.43}$$

Rohatgi's well-known result for determining the distribution of the product of two random variables is straightforward to derive, but difficult to implement.

So, the combined pdf of N_{H_j} can be expressed as for $h_{20} \geq 0,\ h_{21} \geq 0,\ \epsilon_{20} \geq 0,\ \epsilon_{21} \geq 0$ and $r \geq 0$

$$\begin{aligned} f_{N_{H_j}}\left(N_{H_j}\right) \geq f_z(z) &= f_z(p-q) \\ &= \int_{-\infty}^{\infty} f_{pq}(p,q)\, \mathrm{d}p\mathrm{d}q \\ &= \int_{-\infty}^{\infty} f_{pq}(z+q,q)\, \mathrm{d}q \\ &= \int_{-\infty}^{\infty} f_p(z+q) f_q(q)\, \mathrm{d}q \\ &= \int_{0}^{\infty} f_p(z+q) f_q(q)\, \mathrm{d}q \\ &= \int_0^\infty \left[\frac{2\left((h_{21}^S)^2 + (\epsilon_{21}^S)^2\right)}{\sigma_{\epsilon_{21}}^2} \int_0^\infty \frac{(z+q) e^{-(z+q)^2/2u^2\sigma_{\epsilon_{21}}^2}}{\left(u^2\left((h_{21}^S)^2 + (\epsilon_{21}^S)^2\right)+1\right)^2 u}\, \mathrm{d}u\right] \end{aligned} \tag{7.44}$$

$$\times \left[\frac{2\left((h_{21}^S)^2 + (\epsilon_{21}^S)^2\right)}{\sigma_{\epsilon_{20}}^2} \int_0^\infty \frac{q e^{-q^2/2v^2\sigma_{\epsilon_{20}}^2}}{\left(v^2\left((h_{21}^S)^2 + (\epsilon_{21}^S)^2\right)+1\right)^2 v}\, \mathrm{d}v \right] \mathrm{d}q \quad (7.45)$$

$$= \frac{4\left((h_{21}^S)^2 + (\epsilon_{21}^S)^2\right)}{(4-\pi)} \int_0^\infty \left[\int_0^\infty \frac{(z+q) e^{-(z+q)^2/2u^2\sigma_{\epsilon_{21}}^2}}{\left(u^2\left((h_{21}^S)^2 + (\epsilon_{21}^S)^2\right)+1\right)^2 u}\, \mathrm{d}u \right]$$

$$\times \left[\int_0^\infty \frac{q e^{-q^2/2v^2\sigma_{\epsilon_{20}}^2}}{\left(v^2\left((h_{21}^S)^2 + (\epsilon_{21}^S)^2\right)+1\right)^2 v}\, \mathrm{d}v \right] \mathrm{d}q$$

7.5 Simulation Results

In this section, we executed simulations based on the system model shown in Figure 7.1 to validate the theoretical results from the previous section. In the transceiver, the only modulation scheme considered is an anti-podal scheme, like binary phase shift keying (BPSK), with no pulse shaping or error correction coding. The modulated signal is then sent over a random channel (i.e., Rayleigh Channel). The jamming signal is added to the received signal after being passed through the channel. Four different jammer-to-signal ratios, $\alpha = 2, 5, 10, 100$, are tested. Simulations were run for minimum $10,000$ Monte-Carlo samples with variable signal-to-noise ratio (SNR), and jamming-to-signal ratio (JSR), α. We attempted to compare the system using AJ schemes when CSI estimate is perfect, when CSI estimate is imperfect and when system is not using any AJ techniques at all.

Figure 7.2 shows the performance of a zero-forcing (ZF) decoder [85] and a maximum likelihood (ML) detector for 2×2 MIMO on a Rayleigh channel and with NO jammer present. This is the base case for comparison. The ZF decoder does have some degradation compared to an ML decoder and unfortunately, for the AJ schemes presented in this work, a ZF decoder must be employed because the distribution of the jammer signal will not be known a priori, so an ML detector is not possible to use. The comparisons between the cases of using precoding and not using precoding in the presence of a jammer will be compared to the base case of a ZF decoder.

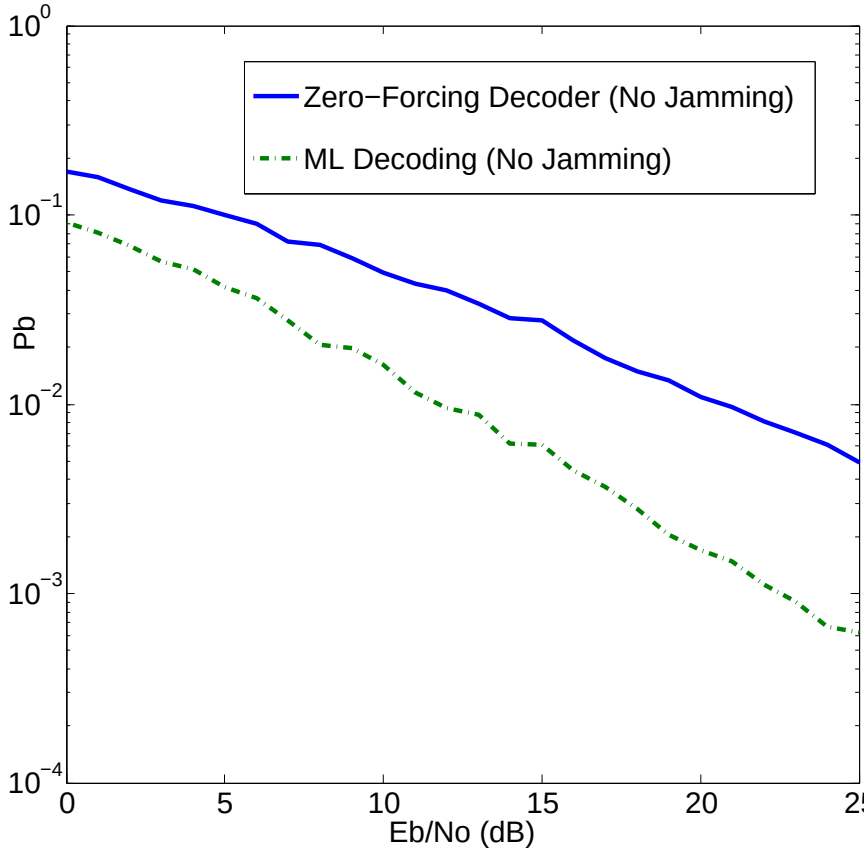

Figure 7.2: Comparison of the performance of Zero-Forcing Decoder (ZF or ZFD) with Maximum Likelihood (ML) decoder on Rayleigh fading channel when NO jammer is present.

First, a comparison between the case of using the orthogonal ZF decoder and using the standard ZF decoder in the presence of a jammer is shown. The theoretical results presented in Section 7.3 make it clear that the spatial hiding techniques orthogonalize the intended signal with respect to the jammer, so the performance results with a jammer present should be identical across all α's. The performance should also be identical to the base case ZF decoder with no jammer present as seen in Figure 7.2. After normalizing the precoded transmit signal by $\frac{1}{\sqrt{2}}$ since only one bit of information is being transmitted at each time interval compared to the base case where two independent streams are being sent, the bit-error rate performance versus $\frac{E_b}{N_0}$ should be the same. Figure 7.3 shows that this is exactly

the case - the jammer, regardless of power level relative to the intended signal - does not degrade the receiver performance at all! The notation in the figure is 'ZFD' (the standard ZF decoder) and 'AJ ZFD' (which is the ZF decoder that projects the received vector into the dimension orthogonal to the jammer). Notice that all three solid lines, corresponding to the AJ decoder performance, are clumped together and are equivalent to the ZFD results in Figure 7.2 where no jammer is present. The unmodified ZFD performance is given by the dashed lines and it has a horrible performance in the presence of the jammer, as would be expected. Its performance is also α dependent and gets better as α decreases and would approach the performance of the AJ decoder case as $\alpha \to 0$.

Next, we try to investigate the impact of communication and jamming CSI error on AJ scheme performance. In Figur 7.4, we looked into the performance of the ZF decoder with and without AJ with 5% communication CSI error (top) and 10% communication CSI error (bottom) on Rayleigh Channel in the presence of a jammer. For $\alpha = 2$, the BER is 0.03 for 5% communication CSI error at 15 dB E_bN_0 and the BER is 0.04 for 10% transceiver CSI error at 15 dB E_bN_0. Next, in Figure 7.5, we looked into the performance with and without AJ with 5% jamming CSI error (top) and 10% jamming CSI error (bottom) on Rayleigh Channel in the presence of a jammer. For $\alpha = 2$, the BER is 0.04 for 5% CSI error at 15 dB E_bN_0 and the BER is 0.05 for 10% jamming CSI error at 15 dB E_bN_0. In both cases, the performance of the AJ scheme degrades with the increase of CSI error. Unlike communication CSI error case, in jamming CSI error case the performance degradation grows alarmingly with the increase of α. For example, at 15 dB SNR and 5% jamming CSI error, the BER is 0.05 for $\alpha = 2$, the BER is 0.1 for $\alpha = 5$, and BER is 0.2 for $\alpha = 10$.

Our next objective is to compare the performance degradation of AJ precoding scheme due to communication CSI error versus that of jamming CSI error. From Figures 7.4 and 7.5, we can see that, for $\alpha = 2$, the BER is 0.03 for 5% communication CSI error at 15 dB E_bN_0 and the BER is 0.04 for 5% jamming CSI error at 15 dB E_bN_0. Therefore, it can be

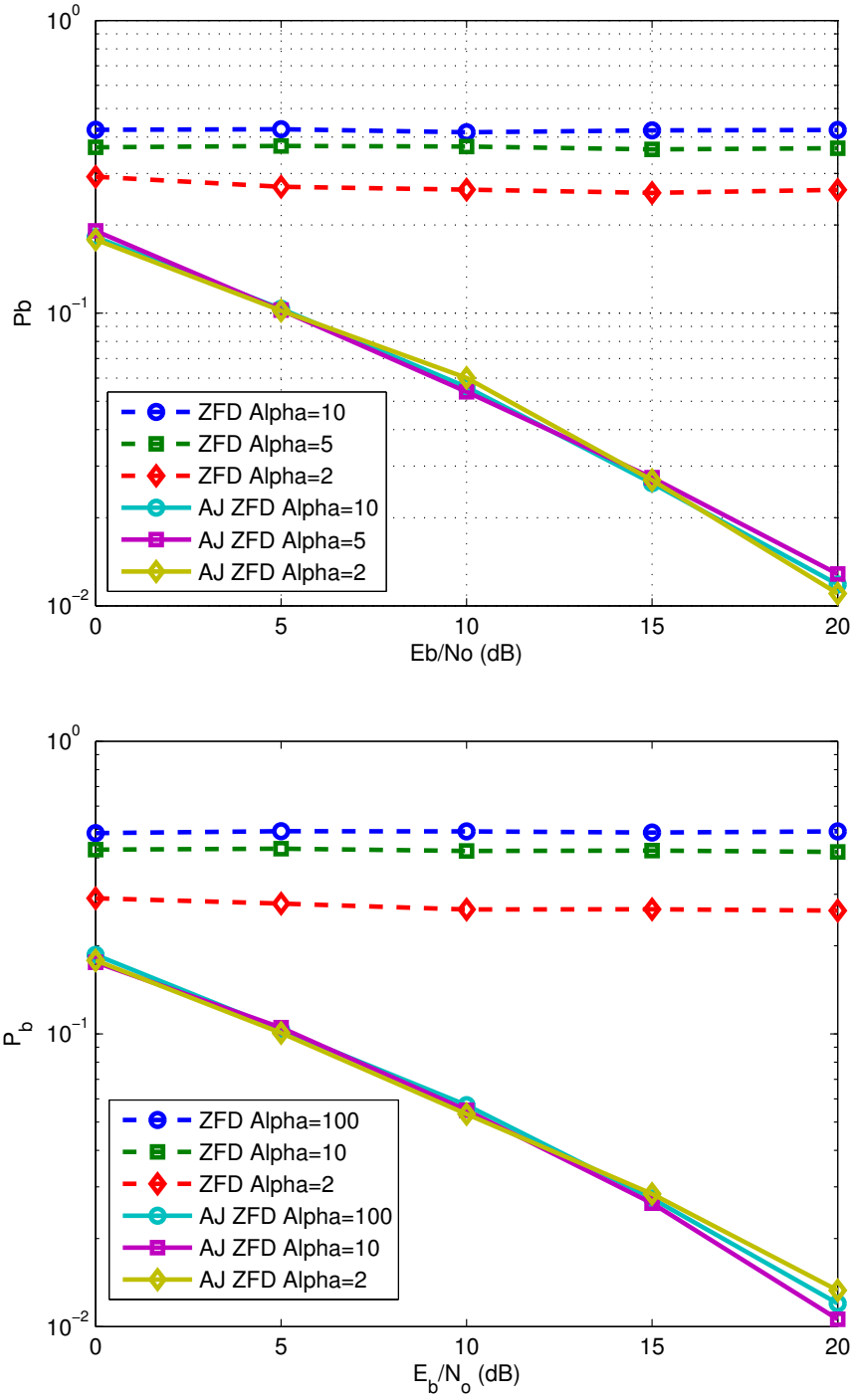

Figure 7.3: A comparison of the performance of Zero-Forcing Decoder (ZFD) and Antijam Zero-Forcing Decoder (AJ ZFD) on Rayleigh fading channel in the presence of a jammer with three different jammer-to-signal ratios (JSR): a) $\alpha = 2, 5, 10$ (top) and b) $\alpha = 2, 10, 100$ (bottom).

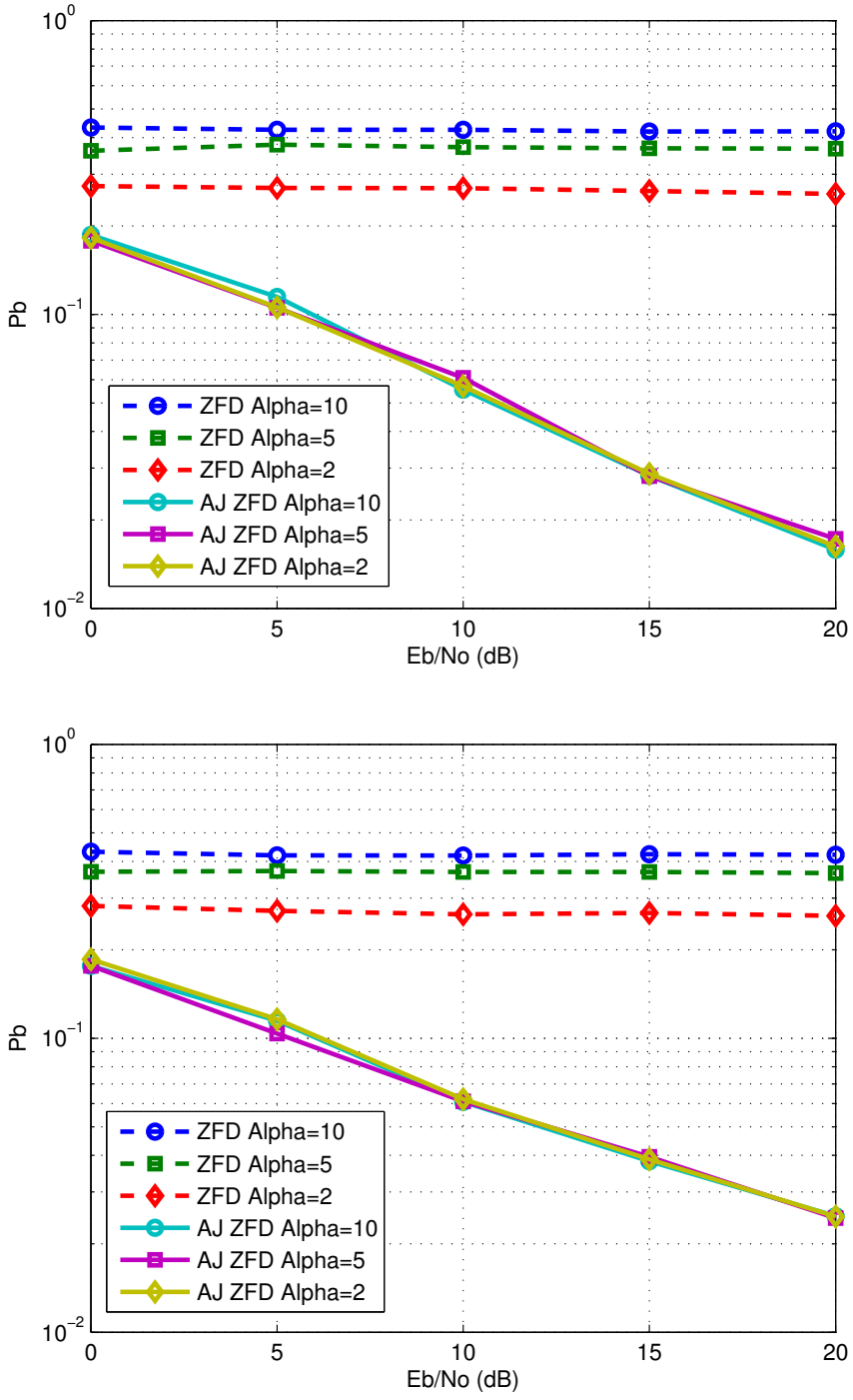

Figure 7.4: A comparison of the performance of Zero-Forcing Decoder (ZFD) and Anti-jam Zero-Forcing Decoder (AJ ZFD) on Rayleigh fading channel in the presence of a jammer with three jammer-to-signal ratios (JSR), $\alpha = 2, 5, 10$ AND $\mathbf{H}$ estimation error: *a*) 5% error (top) and *b*) 10% error (bottom).

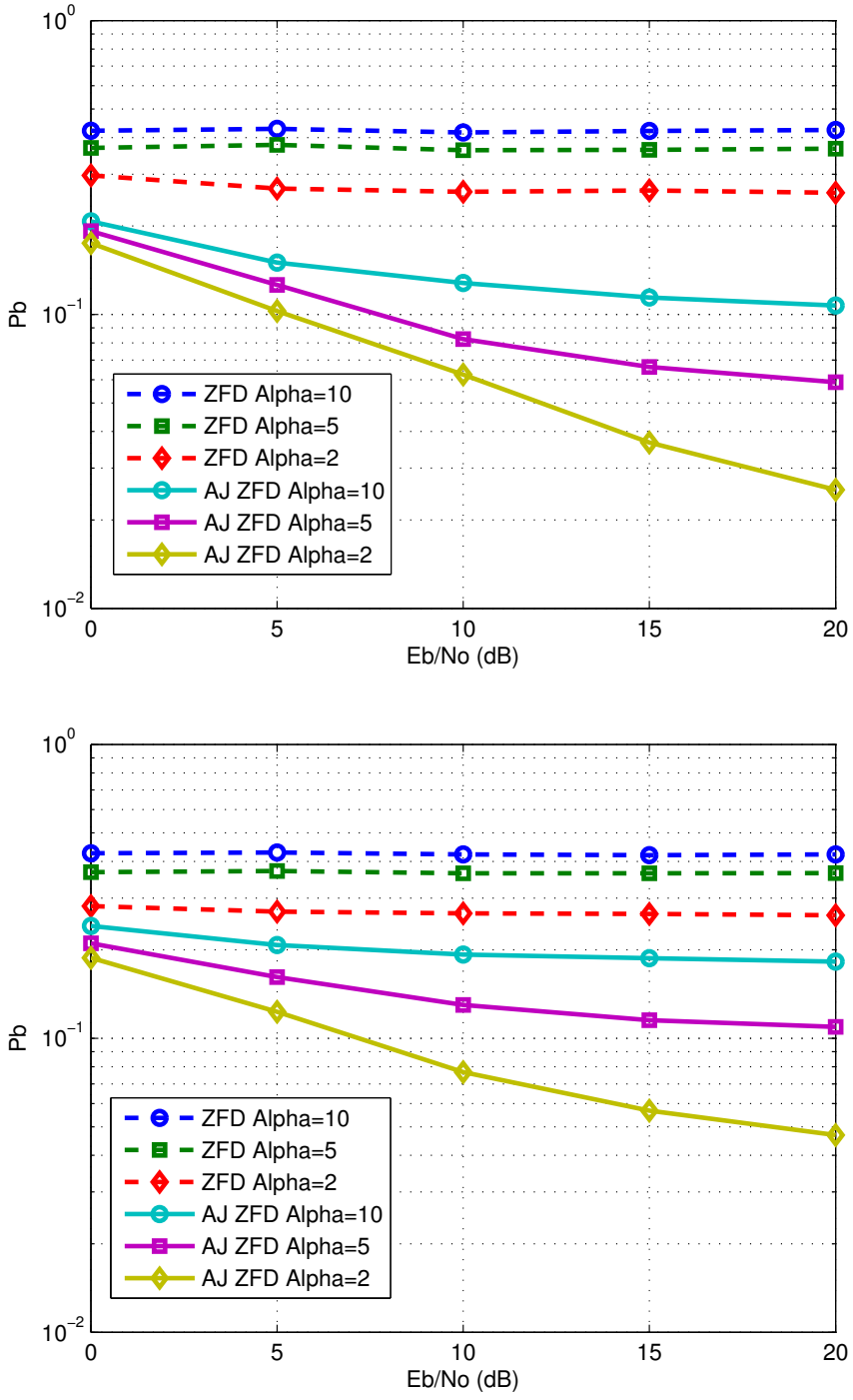

Figure 7.5: A comparison of the performance of Zero-Forcing Decoder (ZFD) and Anti-jam Zero-Forcing Decoder (AJ ZFD) on Rayleigh fading channel in the presence of a jammer with three jammer-to-signal ratios (JSR), $\alpha = 2, 5, 10$ AND $\mathbf{H_j}$ estimation error: *a*) 5% error (top) and *b*) 10% error (bottom).

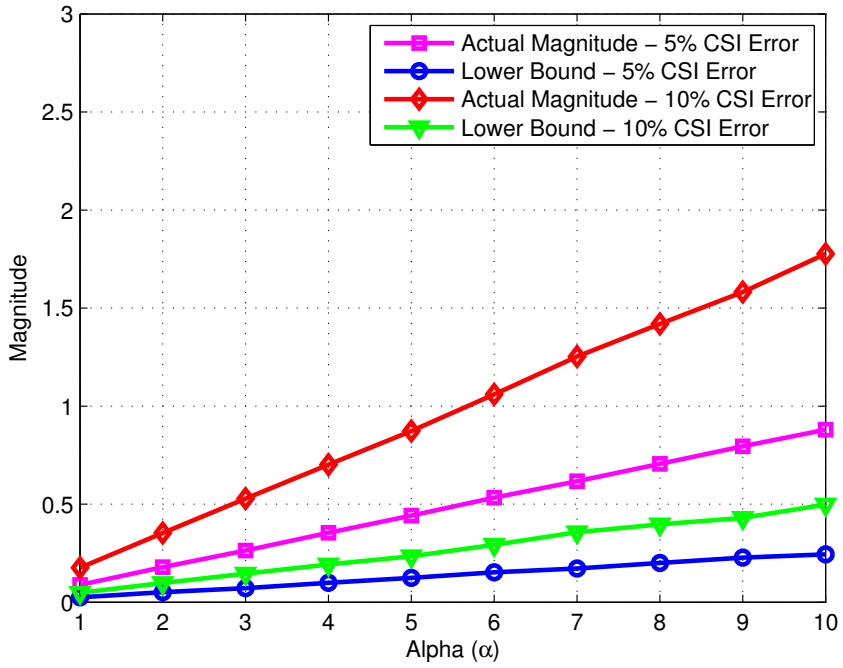

Figure 7.6: Lower bound of $\left|N_{H_j}\right|$ as function of jamming-to-signal ratio (JSR) parameter, α and CSI estimation error, ϵ.

claimed that the jamming CSI error has higher impact than the transceiver CSI error on the performance of anti-jam scheme. Not only that, this performance degradation accelerates as the α increases. Last but not the least, we simulated a plot to compare the lower bound of $\left|N_{H_j}\right|$ with actual distribution with Monte Carlo samples as function of jamming-to-signal ratio parameter, α and CSI estimation error, ϵ. This enables us to quantify the tightness of the lower bound. As we can see in Figure 7.6, for 5% CSI error actual magnitude and lower bound are 0.09 and 0.03 respectively for $\alpha = 1$, the case when jamming power and signal power is same. For 10% CSI error actual magnitude and lower bound are 0.175 and 0.05 respectively for $\alpha = 10$, i.e., when the jamming power is 10 times more than the signal power. We noticed that the difference between the actual magnitude and the lower bound grow higher as the CSI estimation error increases. We also observed that the difference between the actual magnitude with the lower bound increases linearly with the increase of jamming-to-signal power ratio, α.

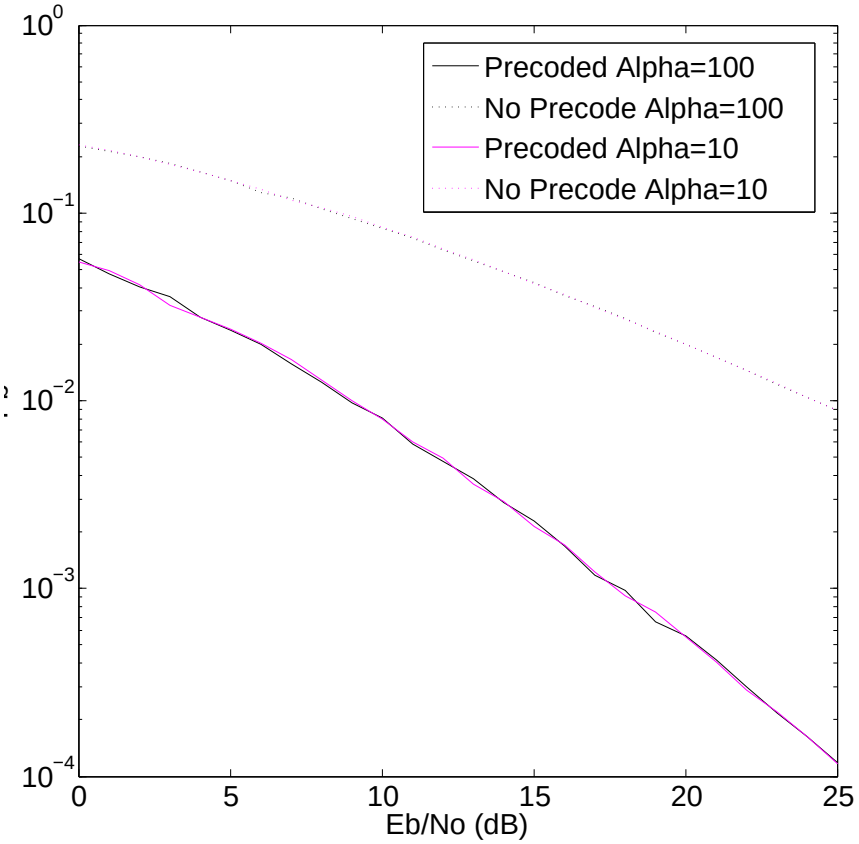

Figure 7.7: Transmitter Precoding on Rayleigh Channel WITH Jammer

Last but not the least, in the final plot in Figure 7.7 shows the gain in performance that can be achieved with proper precoding (beamforming) at the transmitter. There is a roughly 15 dB gain at $P_b = 0.01$ on the Rayleigh channel compared to the case where beamforming processing is performed in the receiver only.

7.6 Summary

In this chapter we introduced two simple AJ techniques that allow a 2×2 MIMO system to practically operate in the presence of a relatively high-powered malicious and uncooperative adversary. These spatial hiding techniques shapes the signal to be orthogonal to the jammer

signal at the receiver, thus making the decoder performance independent of the jammer-to-signal ratio, which paves a way to practically operate in the presence of a relatively high-powered malicious and uncooperative jammer.

A practical scenario with a single malicious node employing a single antenna was discussed. It would be natural to analyze more complex scenarios of one or more $N_T \times N_R$ MIMO systems in the presence of one or more jammer nodes. The work presented here can be extended and applied to more complex modulation schemes such as higher order QAM or OFDMA modulations and it would be an interesting extension of this work to explore these cases.

Closed-form expressions of the performance of spatial hiding AJ schemes for both communication and jamming CSI error were derived. A lower bound for jammer's interference as a function of jamming CSI estimation error was also derived. In addition, the impact of imperfect CSI on the performance of AJ scheme is examined through simulation. The simulation results indicate that even with imperfect CSI, the AJ schemes are capable of mitigating the jamming effect significantly. However, the performance degrades with the increase of CSI estimation error. We also observed that the jamming CSI error had higher impact than the communication CSI error on the performance of AJ scheme. We also observed that the impact of CSI error varies with the JSR and increases with the increase of JSR.

Chapter 8

Overlapped-MIMO Radar Waveform Design

In this chapter, we investigate a collocated overlapped multiple-input multiple-output (O-MIMO) radar design, which is combined with an algorithm to share spectrum through null space projection (NSP) for the coexistence of radar and communications system. In this dissertation, we extend the previous work [38, 118, 119], which consider a coexistence scenario where collocated MIMO radar operates in the same band as MIMO communications system, to a spectrum sharing topology of O-MIMO radar and MIMO communications system. The antenna array of collocated O-MIMO radar is divided into multiple subarrays for transmitting signals in this antenna orientation. The antenna elements are overlapped among the subarrays, where the elements of transmitting subarrays comprise coherent signals and inter-subarray signals are orthogonal to each other.

The proposed antenna design causes lesser interference to communication systems as well as retains the high degree performance of MIMO radar (such as retaining improved sidelobe suppression in the beampattern and achieving higher SNR gain). On the other hand, the radar-centric projection algorithm to share spectrum avoids interference to communications

system by projecting the radar signal onto the null space of the communications channel. Numerical analysis offered here demonstrates the outcome of the proposed orientation in terms of overall beampattern, sidelobe levels of the radar waveform, and SNR gain.

The remainder of this chapter is organized as follows. In Section 8.1 a survey on existing research works is presented. Section 8.2 builds the foundation of spectrum sharing architecture between MIMO radar and MIMO communications system by providing the channel model. Section 8.3 discusses the preliminaries of collocated MIMO radar. Section 8.4 introduces the proposed overlapped-MIMO radar architecture. In Section 8.5, we discuss the performance of the proposed radar architecture in terms of beampattern and SNR gain. Section 8.6 derives the optimum subarray size for collocated O-MIMO radar. Section 8.7 presents the radar-centric spectrum sharing algorithm that is called the null space projection (NSP) algorithm. In Section 8.8 a general discussion on the assumptions and limiting factors of NSP algorithm is presented. Section 8.9 discusses the simulation setup and provides quantitative results along with discussion. Section 8.10 concludes the chapter.

8.1 Related Works

The concepts of MIMO radar are getting attention nowadays as they can have better performance than legacy radar systems to identify targets with higher angular resolution [120]. In MIMO radar, multiple waveforms are transmitted via multiple transmit antenna elements and reflected signals from the targets are received by multiple receive antennas. In [121], authors have proposed a different kind of MIMO radar that they called 'Phased-MIMO' radar. In Phased-MIMO radar, waveforms are transmitted from a MIMO radar where antenna elements are partitioned into multiple subarrays and the elements are allowed to overlap among subarrays. The benefit of this formulation over conventional MIMO radar is its higher coherent processing gain and overall suppressed sidelobes.

The idea of projecting signals onto the null space of an interference channel, in order to avoid interference, is a well-studied topic in the cognitive radio research community [122,123]. An interference channel's null space is calculated at the transmitter either by exploiting channel reciprocity using its second order statistics [122] or by blindly estimating the null space, if no cooperation exists between resource sharing nodes [123]. However, for MIMO radar systems this idea of null space projection (NSP) was first proposed in [38], which was followed by an array of papers [118,119,124] where authors studied the NSP-based spectrum sharing approach for various radar-communications scenarios to avoid interference.

8.2 System Model for Coexistence

In this section, we build the foundation for coexistence of radar and communications system. We start that by describing the model of both radar and communications system. We define the channel model for spectrum sharing too. On top of that, we also state the assumptions made on the interference channel.

8.2.1 Radar Model

The radars assumed to be employed here are the variants of collocated MIMO radar that comprises M_T transmit and M_R receive antenna elements. The antennas of the collocated MIMO radars are uniform linear array (ULA) and elements are spaced at least a half wavelength apart (or at the order of half wavelength). The use of collocated radar is beneficial as this provides superior spatial resolution and target parameter identification than other antenna architecture such as widely-spaced radar [125].

8.2.2 Communications System Model

We assume that the communications system is either wireless broadband or cellular system with MIMO antennas. The MIMO communications system have N_T transmit and N_R receive antennas. The communication nodes can be either base stations or user equipments.

8.2.3 Coexistence Channel Model

Let us now look into the channel model for this spectrum sharing scenario. If we look from the communication systems perspective, then the received signal at the receiver terminal of the communications system can be written as

$$\mathbf{y_C}(t) = \mathbf{H_I}^{N_R \times M_T} \mathbf{x_{Radar}}(t) + \mathbf{H}^{N_R \times N_T} \mathbf{x_C}(t) + \mathbf{n}(t) \tag{8.1}$$

where $\mathbf{x_{Radar}}(t)$ is transmitted radar signal, $\mathbf{x_C}(t)$ is transmitted communications signal, $\mathbf{H_I}$ is $N_R \times M_T$ interference channel between radar and communications system, $\mathbf{H}$ is $N_R \times N_T$ channel between transmitter and receiver of the communications system, $\mathbf{n}(t)$ is AWGN.

The interference channel $\mathbf{H_I}$ can be denoted as

$$\mathbf{H_I} = \begin{bmatrix} h^{(1,1)} & \dots & h^{(1,M_T)} \\ \vdots & \ddots & \vdots \\ h^{(N_R,1)} & \dots & h^{(N_R,M_T)} \end{bmatrix} \quad (N_R \times M_T) \tag{8.2}$$

where $h_i^{(n,m)}$ is the coefficient of the channel between m^{th} antenna element of the MIMO radar to the n^{th} antenna element of the MIMO communications system. The elements of the $\mathbf{H_I}$ are assumed to be independent, identically distributed (i.i.d.) and circularly symmetric complex Gaussian random variables with zero-mean and unit-variance (also known as Rayleigh fading).

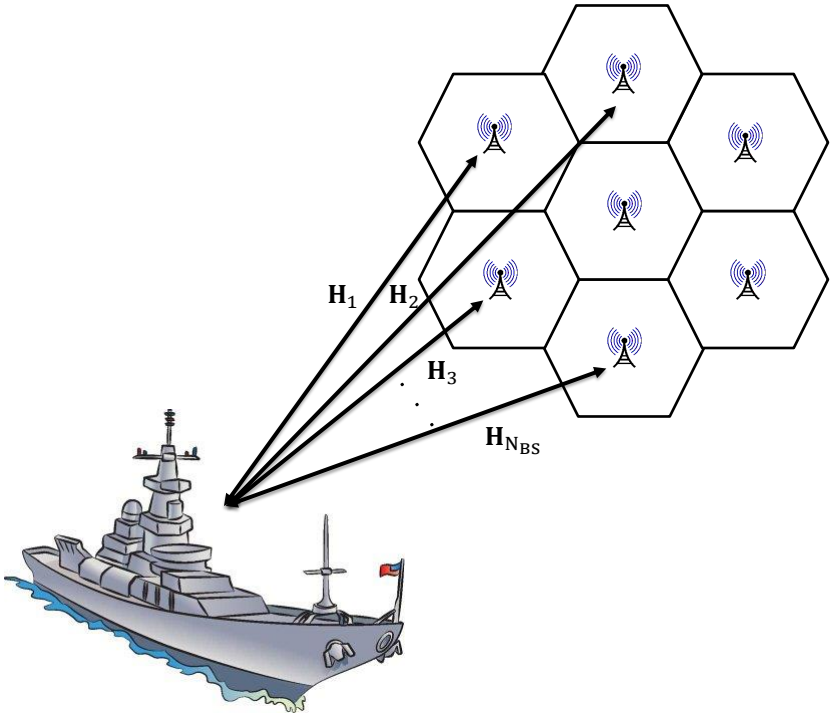

Figure 8.1: A possible spectrum sharing scenario between a radar mounted on a ship and an on shore communications system.

8.2.4 Key Assumptions

We assume that both the radar and communications system are working in a friendly RF environment, cooperating with each other and sharing information various information. Information is shared under an agreement that each system will seek to avoid causing interference to the other. In this research, we investigate a radar-centric design approach. In our radar-centric design, we assume that the interference channel state information (CSI) of the communications system is available at the radar terminal and the goal of the radar is then to develop its own radar waveform that will avoid interference to the communications system. A typical coexistence scenario is shown in Figure 8.1.

On top of that, the following assumptions are used throughout this research to make the analysis tractable and intuitive:

- A point target/source is considered, which is defined for targets/sources having a scatterer with infinitesimal spatial extent.
- Both θ and α are deterministic unknown parameters representing the target's direction of arrival and the complex amplitude of the target, respectively.
- The path loss α is assumed to be identical for all transmit and receive elements, due to the far-field assumption.
- The angle θ is the azimuth angle of the target.

8.3 Collocated MIMO Radar Basics

In this section, we develop the preliminary mathematical foundations of collocated MIMO radar. This derivation will enable us to further understand the proposed overlapped radar architecture in the later sections. The MIMO radar considered in this work is assumed to be collocated. The term 'collocated' refers a radar system where the transmit and the receive antennas are located closely in space (often they are the same array) [120]. In this case, let us assume the number of antenna elements in the transmit and the receive arrays are M_T and M_R respectively. Let θ denote as the location parameter of generic target.

Let $\boldsymbol{\phi}(t)$ be the waveform emitted from collocated MIMO radar, which can be defined as

$$\boldsymbol{\phi}(t) = \begin{bmatrix} \phi_1(t) & \phi_2(t) & \cdots & \phi_{M_T}(t) \end{bmatrix}^T \tag{8.3}$$

where t is the time dimension of a radar pulse, and $(\cdot)^T$ is the transpose of a vector/matrix. The signal $\phi_m(t)$, the mth element of the vector $\boldsymbol{\phi}(t)$, is the waveform emitted by the mth transmit antenna of the MIMO radar. In this MIMO radar case, signal transmitted by each elements are assumed to be orthogonal to each other. As a result, the overall waveform

satisfies the orthogonality principle, which infers

$$\mathbf{R}_x = \int_{T_0} \boldsymbol{\phi}(t)\boldsymbol{\phi}^H(t)dt = \mathbf{I}_{M_T} \tag{8.4}$$

where T_0 stands for the radar pulse width, $(\cdot)^H$ denotes the Hermitian transpose and $\mathbf{I}_{M_T}$ is the $M_T \times M_T$ identity matrix. The orthogonal signal transmission has many advantages. For example, beamforming is possible at transmitter in addition to receiver, improved angular resolution can be achieved, extended array aperture is available in the form of virtual arrays, sidelobes are lower than usual, and the number of resolvable targets are increased.

In the transmitter, the waveform is steered towards the direction of a particular target (or source) during transmission. If the target (or source) direction is assumed to be θ and $M_T \times 1$ transmit steering vector is assumed to be $\mathbf{a}(\theta)$, then for a uniform linear array (ULA), the transmit steering vector $\mathbf{a}(\theta)$ can be expressed as

$$\begin{aligned} \mathbf{a}(\theta) &= \begin{bmatrix} a_1(\theta) & a_2(\theta) & \cdots & a_{M_T}(\theta) \end{bmatrix}^T \\ &= \begin{bmatrix} 1 & e^{-j2\pi d_T \sin\theta} & \cdots & e^{-j2\pi d_T (M_T-1)\sin\theta} \end{bmatrix}^T \end{aligned} \tag{8.5}$$

where the first element of vector $\mathbf{a}(\theta)$ is considered as the reference element, which is set as $a_1(\theta) = 1$, the mth element is set as $a_m(\theta) = e^{-j2\pi d_T (M_T-1)\sin\theta}$, and the inter-element space for array is denoted as d_T, which is measured in terms of wavelength.

Hence, the initial waveform is multiplied (or steered) with the steering vector and final output of the radar transmitter can be expressed in compact vector form as

$$\begin{aligned} \mathbf{x_{Radar}}(t) &= \mathbf{a}(\theta) \odot \boldsymbol{\phi}(t) \\ &= \begin{bmatrix} a_1(\theta)\phi_1(t) & a_2(\theta)\phi_2(t) & \cdots & a_{M_T}(\theta)\phi_{M_T}(t) \end{bmatrix} \\ &= \begin{bmatrix} x_1(t) & x_2(t) & \cdots & x_{M_T}(t) \end{bmatrix} \end{aligned} \tag{8.6}$$

where $\odot$ denotes the Hadamard (element-wise) product.

The snapshot vector of size $M_R \times 1$ received by the collocated MIMO radar receive antenna array can be expressed as

$$\mathbf{y_{Radar}}(t) = \mathbf{y_s}(t) + \mathbf{y_i}(t) + \mathbf{n}(t) \tag{8.7}$$

where $\mathbf{y_s}(t)$ is the signal from the target/source, $\mathbf{y_i}(t)$ is the jamming/interference signal, and $\mathbf{n}(t)$ is the AWGN.

If single point target/source is assumed, then the received signal at the radar becomes

$$\mathbf{y_s}(t) = \beta_s(\mathbf{a}^T(\theta_s)\boldsymbol{\phi}(t))\mathbf{b}(\theta_s) \tag{8.8}$$

where θ_s is the direction of the target/source, β_s is the complex-valued reflection coefficient of the focal point θ_s (that takes account of channel effect and propagation loss), and $\mathbf{b}(\theta)$ is the receive steering vector of size $M_R \times 1$ for the direction θ, which can be expressed as

$$\begin{aligned} \mathbf{b}(\theta) &= \begin{bmatrix} b_1(\theta) & b_2(\theta) & \cdots & b_{M_R}(\theta) \end{bmatrix}^T \\ &= \begin{bmatrix} 1 & e^{-j2\pi d_T \sin\theta} & \cdots & e^{-j2\pi d_T (M_R-1)\sin\theta} \end{bmatrix}^T \end{aligned} \tag{8.9}$$

The signal returned from mth transmitted waveform can be recovered by implementing a matched-filter at the receiver of the radar. The matched-filter would contain each of the waveforms $\{\phi_m(t)\}_{m=1}^{M_T}$ and will be matched with received signal as following

$$\mathbf{y_m}(t) = \int_{T_0} \mathbf{y_{Radar}}(t)\phi_m^*(t)dt \quad m = 1, \cdots, M_T \tag{8.10}$$

One of the key differences of collocated MIMO radar is having more degrees of freedom (DoF) by the emergence of virtual array. Notice that, the transmitting signals from the

single transmitter of the radar are different. As a result, the echo signals can be re-assigned to the source. This in return gives an enlarged virtual receive aperture. Then, the size of the virtual data vector will be $M_T M_R \times 1$ and it can be expressed as

$$\begin{aligned} \mathbf{y_v} &= \left[\mathbf{y}_1^T \mathbf{y}_2^T \cdots \mathbf{y}_{M_T}^T\right]^T \\ &= \beta_s \mathbf{a}(\theta_s) \otimes \mathbf{b}(\theta_s) + \mathbf{y_{i+n}} \end{aligned} \tag{8.11}$$

where $\otimes$ denotes the Kronker product operator and $\mathbf{y_{i+n}}$ denotes the combined component of interference and noise. Hence, the target/source signal component can be written as

$$\mathbf{y_s} = \beta_s \mathbf{v}(\theta_s) \tag{8.12}$$

where $\mathbf{v} = \mathbf{a}(\theta_s) \otimes \mathbf{b}(\theta_s)$ is the virtual steering vector of size $M_T M_R \times 1$, which is associated with a virtual array of $M_T M_R$ elements.

For ULA, the $(m_t M_R + m_r)$th entry of virtual array steering vector $\mathbf{v}(\theta)$ is given by

$$\mathbf{v}_{[m_t M_R + m_r]}(\theta) = e^{-j2\pi(m_t d_T \sin\theta + m_r d_R \sin\theta)} \tag{8.13}$$

where $m_t = 0, \cdots, M_T - 1$ and $m_r = 0, \cdots, M_R - 1$. For $d_T = M_R d_R$, the virtual array steering vector simplifies to [126]

$$\mathbf{v}_{[\varsigma]}(\theta) = e^{-j2\pi\varsigma d_R \sin\theta} \tag{8.14}$$

where $\varsigma = m_t M_R + m_r = 0, 1, \cdots, M_T M_R - 1$, which infers that an $M_T M_R$ effective aperture array can be achieved by employing $M_T + M_R$ antennas [121]. Here, the resulting virtual array is a ULA of $M_T M_R$ elements spaced and d_R wavelength apart. For collocated MIMO radar, aperture size increases due to virtual array, which is resulted from the use of orthogonal signals in the antenna elements. This size extension is referred as *waveform diversity*.

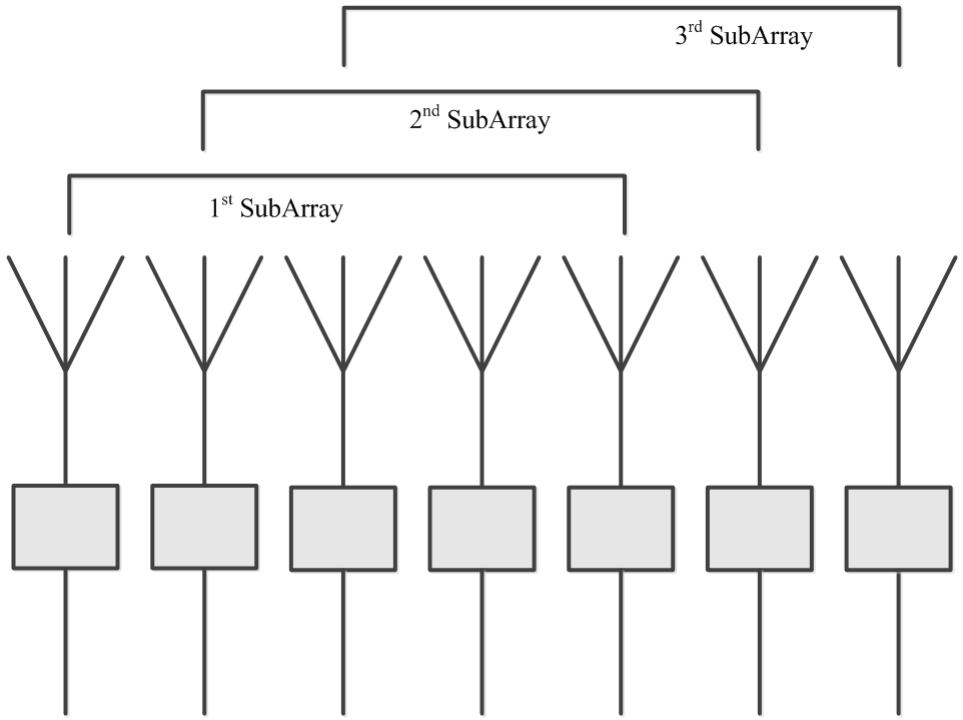

Figure 8.2: A block diagram of the overlapped-MIMO radar formulation.

8.4 Proposed Overlapped-MIMO Radar

In this section, we present a novel formulation of antenna arrays in the MIMO radar that we named 'overlapped-MIMO' radar. In this formulation, the antenna elements of the array are partitioned into multiple overlapped subarrays. Among many, one of the key advantage of this formulation is that it allows to beamform in both transmit and receive arrays. The key idea behind this formulation is to partition the transmit arrays into K subarrays where $1 \leq K \leq M_T$, which are allowed to overlap [121]. The overlapped-MIMO radar formulation is shown in Figure 8.2.

The complex envelope of the signals at the output of the kth subarray can be expressed as

$$s_k(t) = \sqrt{\frac{M_T}{K}}\phi_k(t)\tilde{\boldsymbol{w}}_k \quad k = 1, \cdots, K \tag{8.15}$$

where $\tilde{\boldsymbol{w}}_k$ is a $M_T \times 1$ unit-norm complex vector with M_k beamforming weights corresponding

to the active antenna elements in kth subarray and $M_T - M_k$ zero weights corresponding to the inactive antennas.

As transmitted signal, the frequency spaced signals can be adopted [127], which is orthogonal if the frequency increment $\Delta f = f_{k+1} - f_k$ between the waveform ϕ_{k+1} to ϕ_k satisfies $\Delta f \gg 1/T_0$. The orthogonal waveform $\phi(t)_k$ can be modeled as

$$\phi_k(t) = Q(t)e^{j2\pi k(\Delta f)t} \tag{8.16}$$

where $Q(t)$ is the pulse shape of duration T_0, where $0 < t < T_0$, and $k = 1, \cdots, K$ [128].

The energy of $s_k(t)$ within one radar pulse can be written as

$$E_k = \int_{T_0} s_k^H(t)s_k(t)dt = \frac{M_T}{K} \tag{8.17}$$

which infers that the total transmitted power is equal to M_T.

The reflected signal from the target/source at the direction θ in the far-field can be expressed as

$$\begin{aligned} r(t,\theta) &\triangleq \sqrt{\frac{M_T}{K}}\beta(\theta)\sum_{k=1}^{K}\tilde{\boldsymbol{w}}_k^H\tilde{\boldsymbol{a}}_k(\theta)\phi_k(t) \\ &= \sqrt{\frac{M_T}{K}}\beta(\theta)\sum_{k=1}^{K}\boldsymbol{w}_k^H\boldsymbol{a}_k(\theta)e^{-j\tau_k(\theta)}\phi_k(t) \end{aligned} \tag{8.18}$$

where $\beta(\theta)$ is the reflection coefficient, $\boldsymbol{w}_k$ and $\boldsymbol{a}_k(\theta)$ are the $M_k \times 1$ beamforimng vectors and steering vector, respectively. The $\tilde{\boldsymbol{a}}_k$ is a $M_T \times 1$ vector with M_k steering vector corresponding to the active antenna elements in kth subarray and $M_T - M_k$ zero corresponding to the inactive antennas. Finally, $\tau_k(\theta)$ is the time of propagation required for the wave to travel from the first element to the next element.

The equation (8.18) can be rewritten as

$$r(t,\theta) = \sqrt{\frac{M_T}{K}}\beta(\theta)\left(\mathbf{c}(\theta)\odot\mathbf{d}(\theta)\right)^T\boldsymbol{\phi}_K(t) \tag{8.19}$$

where the waveform vector is $\boldsymbol{\phi}_K(t) \triangleq [\phi_1(t),\cdots,\phi_k(t)]$ with dimension $K\times 1$, the transmit coherent processing vector is $\mathbf{c}(\theta) \triangleq [\mathbf{w}_1^H\mathbf{a}_1(\theta),\cdots,\mathbf{w}_K^H\mathbf{a}_K(\theta)]$ with dimension $K\times 1$, and the waveform diversity vector is $\mathbf{d}(\theta) \triangleq [e^{-j\tau_1(\theta)},\cdots,e^{-j\tau_K(\theta)}]$ with dimension $K\times 1$.

The received complex vector of the array observation can be written as

$$\mathbf{y_{Radar}}(t) = r(t,\theta_s)\mathbf{b}(\theta_s) + \sum_i^D r(t,\theta_i)\mathbf{b}(\theta_i) + \boldsymbol{n}(t) \tag{8.20}$$

where D is the number of interfering signals (or scatterers), $\mathbf{b}(\theta)$ is the receive steering vector of size $M_R\times 1$ associated with direction θ, and $\boldsymbol{n}(t)$ is AWGN.

Following equations (8.10) and (8.11), by match-filtering $\mathbf{y_{Radar}}(t)$ to each of the waveforms $\{\phi_k\}_{k=1}^K$ we can obtain $KM_R\times 1$ virtual data vectors as

$$\begin{aligned}\mathbf{y_v} &= [\mathbf{y^T_{Radar,1}}(t),\cdots\mathbf{y^T_{Radar,K}}(t)]^T \\ &= \sqrt{\frac{M_T}{K}}\beta_s\mathbf{u}(\theta_s) + \sum_i^D\sqrt{\frac{M_T}{K}}\beta_i\mathbf{u}(\theta_i) + \boldsymbol{n}\end{aligned} \tag{8.21}$$

where $\mathbf{u}(\theta) \triangleq [(\mathbf{c}(\theta)\odot\mathbf{d}(\theta))\otimes\mathbf{b}(\theta)]$ is the $KM_R\times 1$ virtual steering vector, $\boldsymbol{\beta}_s = \boldsymbol{\beta}(\theta_s)$ and $\boldsymbol{\beta}_i = \boldsymbol{\beta}(\theta_i)$ are the reflection coefficients of the target/source and interference, respectively. This overlapped subarray formulation collapses to a phased-array when $K = 1$ is chosen. In this case, only one waveform is emitted. On the other hand, when $K = M_T$ is chosen, the formulation becomes a conventional MIMO without array partition.

8.5 Performance Metrics for O-MIMO Radar

In this section, we develop performance metrics of the proposed null space projected overlapped-MIMO radar waveform. We evaluate the performance of the proposed architecture based on beampattern and SNR gain calculation.

We start with calculating the the corresponding beamformer weight vector. In the case of non-adaptive beamforming, the corresponding beamformer weight vectors are given for the kth transmitting subarray as

$$\mathbf{w}_k = \frac{\mathbf{a}_k(\theta_s)}{\|\mathbf{a}_k(\theta_s)\|} = \frac{\mathbf{a}_k(\theta_s)}{\sqrt{M_T - K + 1}} \tag{8.22}$$

where $k = 1, 2, \cdots, K$. The beamforming weight vector of size $KN \times 1$ for the receiving subarrays can be written as

$$\mathbf{w}_d \triangleq \mathbf{u}(\theta_s) = [\mathbf{c}(\theta_s) \odot \mathbf{d}(\theta_s)] \otimes \mathbf{b}(\theta_s). \tag{8.23}$$

8.5.1 Beampattern Improvement

Let $G(\theta)$ be the normalized overall beampattern for overlapped-MIMO

$$G(\theta) = \frac{|\mathbf{w}_d^H \mathbf{u}(\theta)|^2}{|\mathbf{w}_d^H \mathbf{u}(\theta_s)|^2} = \frac{|\mathbf{u}^H(\theta_s)\mathbf{u}(\theta)|^2}{\|\mathbf{u}(\theta_s)\|^4} \tag{8.24}$$

For the special case of a ULA, we have $\mathbf{a}_1^H(\theta)\mathbf{a}_1(\theta_s) = \cdots = \mathbf{a}_K^H(\theta)\mathbf{a}_K(\theta_s)$. Using equation (8.24), the beampattern of the overlapped-MIMO radar for a ULA with overlapped partitioning of K transmit subarrays can be expressed as

$$G_O(\theta) = \frac{\left|\mathbf{a}_K^H(\theta_s)\mathbf{a}_K(\theta)\left[(\mathbf{d}(\theta_s) \otimes \mathbf{b}(\theta_s))^H (\mathbf{d}(\theta) \otimes \mathbf{b}(\theta))\right]\right|^2}{\|\mathbf{a}_K^H(\theta_s)\|^4 \|\mathbf{d}(\theta_s) \otimes \mathbf{b}(\theta_s)\|^4} \tag{8.25}$$

As we know that $\|\mathbf{a}_K(\theta_s)\|^2 = M_T - K + 1$, $\|\mathbf{d}(\theta_s)\|^2 = K$ and $\|\mathbf{b}(\theta_s)\|^2 = M_R$, the beampattern can be rewritten as

$$\begin{aligned} G_O(\theta) &= \frac{\left|\mathbf{a}_K^H(\theta_s)\mathbf{a}_K(\theta)\right|^2}{(M_T-K+1)^2} \cdot \frac{\left|\mathbf{d}^H(\theta_s)\mathbf{d}(\theta)\right|^2}{K^2} \cdot \frac{\left|\mathbf{b}^H(\theta_s)\mathbf{b}(\theta)\right|^2}{M_R^2} \\ &= T_O(\theta) \cdot D_O(\theta) \cdot R(\theta) \end{aligned} \tag{8.26}$$

where the waveform diversity beampattern is $D_O(\theta) \triangleq \frac{\left|\mathbf{d}^H(\theta_s)\mathbf{d}(\theta)\right|^2}{K^2}$, the transmit beampatten is $T_O(\theta) \triangleq \frac{\left|\mathbf{a}_K^H(\theta_s)\mathbf{a}_K(\theta)\right|^2}{(M_T-K+1)^2}$ and the receive beampatten is $R(\theta) \triangleq \frac{\left|\mathbf{b}^H(\theta_s)\mathbf{b}(\boldsymbol{\theta})\right|^2}{M_R^2}$. So, we can see that the overall beampattern of the overlapped-MIMO radar can be expressed in terms of three distinct and independent beampattern.

For MIMO radar, the subarray number is $K = M_T$ and the transmitter beampattern $T_M(\theta) = 1$. Hence, the overall beampattern for MIMO radar can be expressed as

$$G_{MIMO}(\theta) = D_M(\theta) \cdot R(\theta) \tag{8.27}$$

where the waveform diversity beampattern is $D_M(\theta) = \frac{\left|\mathbf{a}^H(\theta_s)\mathbf{a}(\theta)\right|^2}{M_T^2}$. Notice that the overall beampattern of the MIMO radar has only the waveform diversity and receive beampattern.

For phased-array radar, the subarray number is $K = 1$ and the waveform diversity beampattern $D_P(\theta) = 1$. Hence, the overall beampattern for phased-array radar can be expressed as

$$G_{PH}(\theta) = T_P(\theta) \cdot R(\theta) \tag{8.28}$$

where the transmit beampattern is $T_P(\theta) = \frac{\left|\mathbf{a}^H(\theta_s)\mathbf{a}(\theta)\right|^2}{M_T^2}$. Notice that the overall beampattern of the phased-array radar has only transmit and receive beampattern.

8.5.2 SNR Gain Improvement

According to [121], the output SNR of the overlapped-MIMO radar with non-adaptive transmit/receive beamforming can be expressed as

$$SNR_{OMIMO} = M_R M_T \left(M_T - K + 1\right) \frac{\sigma_s^2}{\sigma_n^2} \tag{8.29}$$

where σ_s^2 is the variance of the target/source reflection coefficient, thus $\sigma_s^2 = E\{|\beta|^2\}$ and σ_n^2 is the noise variance.

For MIMO radar, the output SNR can be found by substituting $K = M_T$ at (8.29)

$$SNR_{MIMO} = M_R M_T \frac{\sigma_s^2}{\sigma_n^2} \tag{8.30}$$

For phased-array radar, the output SNR can be found by substituting $K = 1$ at (8.29)

$$SNR_{PH} = M_R M_T^2 \frac{\sigma_s^2}{\sigma_n^2} = M_T \cdot SNR_{MIMO} \tag{8.31}$$

Finally, from (8.29), (8.30), and (8.31), we can express the output SNR of overlapped-MIMO radar as

$$SNR_{OMIMO} = \eta \cdot SNR_{PH} = \eta \cdot M_T \cdot SNR_{MIMO} \tag{8.32}$$

where $\frac{1}{M_T} \leq \eta \triangleq \frac{(M_T - K + 1)}{M_T} \leq 1$ is the ratio between the overlapped-MIMO radar SNR gain and that of the phased-array radar.

We can see that the SNR gain of the MIMO radar is equal to $M_R M_T$ and the SNR gain of the phased-array radar is equal to $M_R M_T^2$ and the SNR gain of the overlapped-MIMO radar is equal to $M_R M_T (M_T K + 1)$. The SNR gain of the phased-array radar is M_T times greater than that of the MIMO radar. The SNR gain of the overlapped-MIMO radar is

$(M_T K + 1)$ times greater than that of the MIMO radar and $\frac{(M_T K+1)}{M_T}$ times greater than that of the phased-array radar. Henc, we can see an overall SNR gain improvement for the overlapped-MIMO architecture.

8.6 Optimum Subarray Size for O-MIMO Radar

In order to maximize the impact of the overlapping subarray architecture presented, we have to select a value for the number of subarrays K that maximizes the virtual array size, M_ϵ. Hence,

$$K = \arg\max_K \left(M_\epsilon\right) \tag{8.33}$$

where $M_\epsilon = \left(M_T - K + 1\right) K$.

The number of subarrays K in the overlapped array can be optimized by

$$\begin{aligned} \frac{\partial}{\partial K}\left(M_\epsilon\right) &= 0 \\ \frac{\partial}{\partial K}\Big(\left(M_T - K + 1\right) K\Big) &= 0 \\ M_T - 2K + 1 &= 0 \\ K &= \left\lfloor \frac{M_T + 1}{2} \right\rfloor \end{aligned} \tag{8.34}$$

where $\lfloor \cdot \rfloor$ stands for the floor operation as K should be an integer. Note that the radar has most significant impact when the number of virtual arrays, M_ϵ , on transmitter side is maximized (see equation (8.34)).

8.7 Radar-Centric Spectrum Sharing Algorithm

In this section, we describe the details of a radar-centric projection algorithm, which projects the overlapped-MIMO radar signal onto the null space of the communication interference channel via null space projection (NSP) technique proposed in [119]. We start with a generic description of the spectrum sharing algorithm and move on to present the mathematical details of the projection matrix.

8.7.1 Null Space Projection (NSP)

This section describes the null space projection (NSP) algorithm, which projects radar signal onto the null space of the interference channel $\mathbf{H_I}$. The NSP algorithm requires the radar to have the interference channel's CSI available in advance, which can be obtained in a number of ways and conveyed to the radar via mutual cooperation between the radar and the communication systems [38, 118, 119].

The proposed algorithm works as follows. At the beginning, the radar receives $\mathbf{H_I}$, which is the CSI between radar and communication node's interference channel. It then calculates the number of null spaces available to project the radar signal by performing singular value decomposition (SVD) on $\mathbf{H_I}$. The dimension of the null space is $M_T - N_R$. It then calculates the projection channel matrix $\mathbf{P}$ and constructs a new radar waveform $\hat{\mathbf{x}}_{\mathbf{Radar}}$. If $\mathbf{H_I}$ is the channel matrix and $\mathbf{P}$ is the projection matrix onto the null space of $\mathbf{H_I}$, then the overlapped-MIMO radar waveform projected onto the null space of $\mathbf{H_I}$ to avoid interference from radar can be written as

$$\hat{\mathbf{x}}_{\mathbf{Radar}}(t) = \mathbf{P}\mathbf{x}_{\mathbf{Radar}}(t). \tag{8.35}$$

Notice that the spectrum sharing algorithm via null space projection (NSP) described above is shown in Algorithm (3).

Algorithm 3 Spectrum Sharing Algorithm via Null Space Projection (NSP)

loop
  Get CSI of $\mathbf{H_I}$ through feedback from 'Communications Node'.
  Send $\mathbf{H_I}$ to inner loop (i.e., NSP Algorithm) for projection matrix $\mathbf{P}$ formation.
  if $\mathbf{H_I}$ received from the outer loop, **then**
    Perform SVD on $\mathbf{H_I}$ (i.e. $\mathbf{H_I} = \mathbf{U\Sigma V}^H$).
    Construct $\widetilde{\mathbf{\Sigma}} = \text{diag}(\widetilde{\sigma}_1, \widetilde{\sigma}_2, \ldots, \widetilde{\sigma}_k)$.
    Construct $\widetilde{\mathbf{\Sigma}}' = \text{diag}(\widetilde{\sigma}'_1, \widetilde{\sigma}'_2, \ldots, \widetilde{\sigma}'_{M_T})$.
    Setup projection matrix $\mathbf{P} = \mathbf{V}\widetilde{\mathbf{\Sigma}}'\mathbf{V}^H$.
    Send $\mathbf{P}$ to the outer loop.
  end if
  Receive the projection matrix $\mathbf{P}$ from inner loop.
  Perform null space projection, i.e., $\hat{\mathbf{x}}_{\mathbf{Radar}}(t) = \mathbf{P}\mathbf{x}_{\mathbf{Radar}}(t)$.
end loop

8.7.2 Projection Matrix

In this section, we introduce the formation of the projection matrix $\mathbf{P}$ and analyze the properties of this projection matrix. Let $\mathbf{H_I}$ be the interference channel between the radar and communications node. We assume that $\mathbf{H_I} \in \mathbf{F}^{N_R \times M_T}$ for $\mathbf{F} = \mathbb{R}$ or $\mathbf{F} = \mathbb{C}$. We want a projection matrix $\mathbf{P} \in \mathbf{F}^{M_T \times M_T}$ of a maximum rank such that it satisfies fowling properties:

- $\mathbf{H_I P} = 0$
- $\mathbf{P}^2 = \mathbf{P}$

The projection matrix $\mathbf{P}$, which satisfies above properties and projects onto the null space of interference channel $\mathbf{H_I}$, can be found by taking the SVD of $\mathbf{H_I}$. The SVD of $\mathbf{H_I}$ is

$$\mathbf{H_I} = \mathbf{U\Sigma V}^H \tag{8.36}$$

where $\mathbf{U}$ and $\mathbf{V}$ are unitary or orthogonal, depending on $\mathbf{F}$, of order N_R and M_T, respectively, and $\mathbf{\Sigma} \in \mathbb{R}^{N_R \times M_T}$ is an $N_R \times M_T$ rectangular diagonal matrix with non-negative real numbers

on the diagonal. Let us define

$$\widetilde{\mathbf{\Sigma}} = \text{diag}\left(\tilde{\sigma}_1, \tilde{\sigma}_2, \cdots, \tilde{\sigma}_k\right) \tag{8.37}$$

where $k = \min\left(N_R, M_T\right)$ and $\tilde{\sigma}_1 \geq \tilde{\sigma}_2 \geq \cdots \geq \tilde{\sigma}_p \geq \tilde{\sigma}_{p+1} = \tilde{\sigma}_{p+2} = \cdots = \tilde{\sigma}_k = 0$ are the singular values of $\mathbf{H_I}$. Let us define

$$\widetilde{\mathbf{\Sigma}}^{'} = \text{diag}\left(\tilde{\sigma}_1^{'}, \tilde{\sigma}_2^{'}, \cdots, \tilde{\sigma}_{M_T}^{'}\right) \tag{8.38}$$

where $\widetilde{\mathbf{\Sigma}}^{'} \in \mathbb{R}^{M_T \times M_T}$ and

$$\tilde{\sigma}_i^{'} = \begin{cases} 0, & \text{if } i \leq p, \\ 1, & \text{if } i > p. \end{cases}$$

Note that $\widetilde{\mathbf{\Sigma}}\widetilde{\mathbf{\Sigma}}^{'} = 0$ and $\left(\widetilde{\mathbf{\Sigma}}^{'}\right)^2 = \widetilde{\mathbf{\Sigma}}^{'}$. Now, one can define the projection matrix as

$$\mathbf{P} = \mathbf{V}\widetilde{\mathbf{\Sigma}}^{'}\mathbf{V}^H \tag{8.39}$$

We can verify that this matrix $\mathbf{P}$ is valid projection matrix by computing the properties mentioned above. The details of this proofs are given below.

Property 1. $\mathbf{P} \in \mathbb{R}^{M_T \times M_T}$ *is an orthogonal projection matrix onto the null space of* $\mathbf{H_I} \in \mathbb{R}^{N_R \times M_T}$*, if and only if* $\mathbf{H_I P} = \mathbf{H_I P}^H = 0$.

Proof. Since $\mathbf{P} = \mathbf{P}^H$ (see property 2), it can be written

$$\mathbf{H_I P} = \mathbf{H_I P}^H = \mathbf{U}\widetilde{\mathbf{\Sigma}}\mathbf{V}^H \times \mathbf{V}\widetilde{\mathbf{\Sigma}}^{'}\mathbf{V}^H = \mathbf{0}. \tag{8.40}$$

The result mentioned above follow from the fact that $\widetilde{\mathbf{\Sigma}}\widetilde{\mathbf{\Sigma}}^{'} = \mathbf{0}$ by construction. □

Property 2. $\mathbf{P} \in \mathbb{R}^{M_T \times M_T}$ *is a projection matrix, if and only if* $\mathbf{P} = \mathbf{P}^H = \mathbf{P}^2$.

Proof. At first, let us prove the 'only if' part, where we will have to show $\mathbf{P} = \mathbf{P}^H$. By taking the Hermitian of equation (8.39), we will get

$$\mathbf{P}^H = \left(\mathbf{V}\widetilde{\mathbf{\Sigma}}'\mathbf{V}^H\right)^H = \mathbf{P}. \tag{8.41}$$

Then, by squaring the equation (8.39) we will get

$$\mathbf{P}^2 = \mathbf{V}\widetilde{\mathbf{\Sigma}}\mathbf{V}^H \times \mathbf{V}\widetilde{\mathbf{\Sigma}}\mathbf{V}^H = \mathbf{P} \tag{8.42}$$

where the equation (8.42) follows from $\mathbf{V}^H\mathbf{V} = \mathbf{I}$ (both of them are orthonormal matrices) and $\left(\widetilde{\mathbf{\Sigma}}'\right)^2 = \widetilde{\mathbf{\Sigma}}'$ (by construction). If we follow the equations (8.41) and (8.42), we will find that $\mathbf{P} = \mathbf{P}^H = \mathbf{P}^2$.

Next, we will show that $\mathbf{P}$ is a projector matrix by proving that if $\mathbf{v} \in$ range $(\mathbf{P})$, then $\mathbf{Pv} = \mathbf{v}$, i.e., for some $\mathbf{w}, \mathbf{v} = \mathbf{Pw}$, then

$$\mathbf{Pv} = \mathbf{P}(\mathbf{Pw}) = \mathbf{P}^2\mathbf{w} = \mathbf{Pw} = \mathbf{v}. \tag{8.43}$$

On top of that, $\mathbf{Pv} - \mathbf{v} \in$ null$(\mathbf{P})$, i.e.,

$$\mathbf{P}(\mathbf{Pv} - \mathbf{v}) = \mathbf{P}^2\mathbf{v} - \mathbf{Pv} = \mathbf{Pv} - \mathbf{Pv} = \mathbf{0}. \tag{8.44}$$

This concludes the proof. □

8.8 Assumptions and Limiting Factors of NSP

In this section, we discuss the assumptions and limiting factors of the NSP algorithm implementation. We consider two spectrum sharing scenario depending upon the number of antenna elements in the radar and communications system.

The key assumption of NSP algorithm implementation is 'cooperation'. There must be some kind of cooperation between the radar and the communication node to effectively project radar signal onto the null space. They must be exchanging the CSI of the inference channel though feedback/feedforward or any other kind of mechanism. It will work only when the channel is static or quasi-static, meaning the CSI will not be changed before the projection takes place. A number mechanisms to exchange CSI between radar and communications system is presented in [129].

Notice that we run into two possible scenarios: 1) the number of antenna elements in radar transmit array is less than equal to that of communications system, $M_T \leq N_R$ and 2) the number of antenna elements in the radar transmit array is greater than that of communications system, $M_T > N_R$. For first scenario where we have $M_T \leq N_R$, we cannot use the NSP method. However, a possible solution to this problem is using overlapped-MIMO as it increases the *effective* number of transmit arrays, thus making NSP possible. In this case, the *effective* transmit array aperture, M_ϵ is equal to $(M_T - K + 1)K$, which is greater than N_R. Note that M_ϵ is essentially the number of the virtual arrays in the transmitter of the radar. Hence, the overlapped-MIMO radar results in a total virtual array of size $((M_T - K + 1)K)\, M_R$. On the other hand, if $M_T > N_R$, then we will have sufficient degrees of freedom (DoF) to make NSP possible for $M_T - N_R$ dimensions. However, even in this case the performance can be increased using overlapped-MIMO since it increases the effective number of transmit arrays.

8.9 Simulation and Results

In this section, we simulate an overlapped-MIMO radar. We assume a ULA with $M_T = 20$ antenna elements at the transmitter. At the receiver, we also assume $M_R = 20$ antennas. In both cases the space between elements is $d_T = 0.5$, meaning adjacent antenna elements are half a wavelength apart. The signal passes through a Rayleigh distributed channel and is subject to AWGN. Each antenna element is omnidirectional. We assume the target of interest is at $\theta_s = 15^o$ and two interfering signals are located at directions -30^o and -10^o. Output SINRs are computed using $10,000$ independent simulations.

Figure 8.3 shows the overall beampattern for four different MIMO radar formulations: (1) overlapped-MIMO radar with $K = 1$ (single subarray or phased-array), (2) overlapped-MIMO radar with $K = 5$, (3) overlapped-MIMO radar with $K = 10$ and (4) MIMO radar with $K = 20$ (MIMO). Here the overlapped-MIMO radars have two different orientations of 5 and 10 overlapped subarrays and each subarray has 11 and 16 antenna elements respectively. We can observe that the overlapped-MIMO with $K = 1$ (phased-array) and MIMO radars have exactly the same overall transmit/receive beampatterns. However, the overlapped-MIMO radar (for $K = 5$ and $K = 10$) has significantly improved sidelobe suppression compared to the beampattern of the MIMO and the phased array radar.

Figure 8.4 shows the overall beampattern for same radar formulations with NSP algorithm: (1) overlapped-MIMO radar with $K = 1$ plus NSP (single subarray or phased-array), (2) overlapped-MIMO radar with $K = 5$ plus NSP, (3) overlapped-MIMO radar with $K = 10$ plus NSP and (4) MIMO radar with $K = 20$ plus NSP (MIMO). We observe that the projection algorithm has reduced sidelobe suppression as expected. Note that it is still providing encouraging suppression in compared to pure MIMO radar. However, the primary benefits are at the communications side since this NSP algorithm minimizes interference form the radar to the communications system and thus, enables the two to coexist.

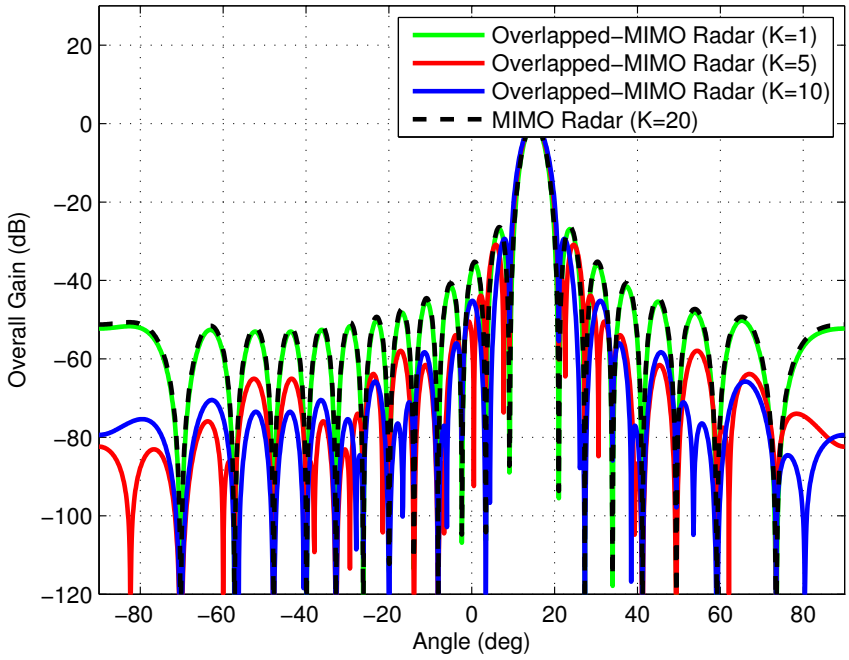

Figure 8.3: Overall beampattern using conventional transmit-receive beamformer where the total number of elements is $M_T = 20$, the number of overlapped subarrays is $K = 5$ and $K = 10$ respectively, the number of elements in each subarray is $(M_T - K + 1) = 16$ and $(M_T - K + 1) = 11$ respectively, and $d_T = 0.5$ wavelength.

The final experiment considers the number of subarrays, K, in the transmitter of the overlapped-MIMO radar that maximizes the benefit for the radar in terms of sidelobe suppression. Note that the radar has most significant impact when the number of virtual arrays, M_ϵ, on transmitter side is maximized (see equation 8.34). Fig. 8.5 shows the impact of varying the number of subarrays K from 1 to M_T on M_ϵ. For $M_T = 20$, $K = 11$ or $K = 12$ results in the highest impact. This knowledge enables determining the structure of overlapping subarrays. The plot of K for $M_T = 10$ and $M_T = 15$ are shown in the same figure to provide a comparative view. This graph enables picking a value for K (the number of subarrays in the overlapped-MIMO structure) that maximizes the virtual antenna array size, thus enhancing the amount of sidelobe suppression in radar beampattern, while retaining the dimension needed for NSP.

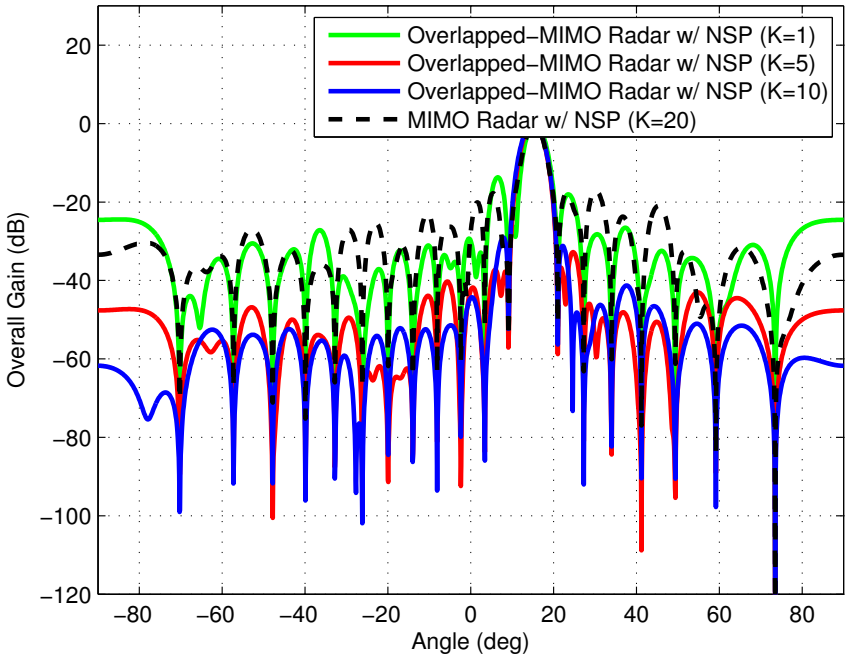

Figure 8.4: Overall beampattern using conventional transmit-receive beamformer and NSP where the total number of elements is $M_T = 20$, the number of overlapped subarrays is $K = 5$ and $K = 10$ respectively, the number of elements in each subarray is $(M_T - K + 1) = 16$ and $(M_T - K + 1) = 11$ respectively, and $d_T = 0.5$ wavelength.

8.10 Summary

In this chapter, we presented a MIMO radar architecture that we named 'overlapped-MIMO' radar and combined a spectrum sharing algorithm called 'null space projection' (NSP) for radar-communications coexistence. In the overlapped-MIMO radar architecture, the transmit array of the radar is partitioned into a number of subarrays that are allowed to overlap. Each antenna subarray transmit waveforms that are orthogonal to other subarrays, but coherent among all the antenna elements of each individual subarrays. The advantage of this architecture is to have a larger *effective* transmit array with increased *diversity gain*. On top of that, we achieved *coherent processing gain* by designing a weight vector for each subarray to form a beam towards certain direction in space [121]. This formulation also improves the overall sidelobe suppression compared to conventional MIMO radar, making it

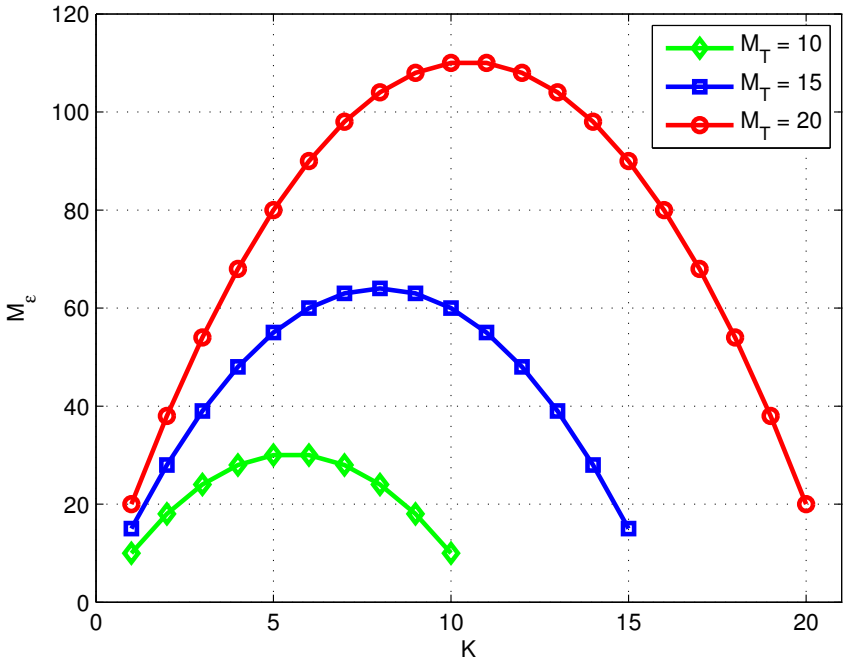

Figure 8.5: The number of subarrays, K, in a overlapped-MIMO radar is varied from 1 to M_T and the resulting effective virtual transmitter array number, M_ϵ is observed for three different transmit antenna sizes, i.e., $M_T = 10$, $M_T = 15$ and $M_T = 20$.This graph enables picking a value for K (the number of subarrays in the overlapped-MIMO structure) that maximizes the virtual antenna array size, thus enhancing the amount of sidelobe suppression in radar beampattern, while retaining the dimension needed for NSP.

suitable for coexisting with communication systems.

Further, we introduced a radar-centric spectrum sharing algorithm that projects the radar signal onto the null space of the communications system's interference channel, which helps to avoid interference from radar. Note that such conventional null space projection is only possible when the physical/virtual number of transmit antennas of the radar is greater than the number of receive antennas of the communications system.

Analytical models for the waveform of the overlapped-MIMO radar and the NSP algorithm are derived in this chapter. Simulations of the coexistence scenario are presented too. Through analytical derivation and as well, simulation results, we showed that the proposed overlapped-MIMO and NSP algorithms outperform conventional schemes and enable radar-

communications system coexistence in the same band. We found that the overlapped-MIMO architecture achieves more than 20 dB sidelobe suppression above conventional MIMO radar when there are 20 physical antenna elements in the radar system. We also observed that, in a similar setup, even though NSP degrades suppression, it still retains more than 10 dB additional sidelobe suppression compared to conventional MIMO radar while reducing interference to the communication systems.

Chapter 9

Conclusions

We conclude this dissertation in this chapter with a summary of our findings that were deduced though the course of our research and a list of possible future work in Section 9.1 and Section 9.2, respectively.

9.1 Findings

The major findings of this research are summarized as follows:

In this dissertation, pilot tone-based jamming attacks against OFDM and OFDMA systems were presented. These attacks seek to manipulate information used by the equalization process to cause errors to a substantial number of symbols. The two attacks detailed were: 1) pilot tone jamming attack where attack values are i.i.d. Gaussian noise and 2) pilot tone nulling attack where pilot values are expected to be known in advance and inverted to synthesize damaging interference. These two equalization attacks were compared from an efficacy viewpoint with conventional wideband jamming (a.k.a. barrage jamming). The goal was to understand how much less total energy was needed to synthesize these attacks as compared to equivalent BER levels caused by barrage jamming of all subcarriers. Through

simulations we demonstrated that pilot tone jamming is 3 dB more efficient and pilot tone nulling is 8 dB more efficient for a target waveform with 1/8 pilot density, QPSK modulation, and target BER of 0.3. The theoretical efficiency improvement of 9 dB for a signal with 1/8 pilot density was not achievable because of the linear interpolation effect. While error introduced in pilot tones spreaded to neighboring subcarriers, this error was averaged and partially mitigated.

In this dissertation, two pilot tone randomization arrangements were proposed in order to mitigate the threat of pilot tone jamming attacks against OFDM systems. The rationale was such that the randomization of the location and the value of pilot tones will be causing the optimal attack to devolve into partial-band data subcarrier jamming. It was found that the conventional 'equal power' and 'equal spaced' pilot tone arrangement performs better than both of these randomization schemes in the absence of pilot tone jamming attacks. The completely random scheme is the worst performer out the three schemes. On the other hand, it was found that both the confined bin scheme and the complete random scheme outperformed the conventional scheme in the presence of pilot tone jamming attack at low SJR. At high SJR, the conventional scheme outperformed rest of the two as the jamming power became too low (compare to transmitted signal) to have an impact on the receiver performance.

In this dissertation, we also discussed cyclic prefix (CP) jamming attacks. In CP jamming attacks, a low duty cycle jammer selectively targets the CP of the signal. The rationale for CP jamming attack was simple – instead of wasting power to jam the entire signal all the time, jam an important portion of the transmission. If CPs could be degraded, the FDE algorithms simply will not work. In addition, destruction of the CP would result in additional ISI. Moreover, as the CP is used for correcting the symbol-time delay and the carrier frequency offset of the signal by correlating the repeated parts of a symbol, injecting a more concentrated jamming signal in just the CP will knock off the correlation, therefore

disrupting the received signal [130]. We proposed countermeasure to CP jamming attacks as well.

In this dissertation, we also presented a power efficient 'asynchronous off-tone' jamming attack against OFDM system. We found that the impact of single-tone and multi-tone partial-band jamming attacks can be stretched out in the spectrum and create greater damage by transmitting jamming signals that have frequency offsets with the received signal. The key advantages of this kind of attack are: 1) power efficient than conventional wideband jamming attacks and 2) it does not require any synchronization with the target signal.

This dissertation introduced two simple antijam techniques (receiver-only and transmitter precoding) that allowed 2×2 MIMO system to operate in the presence of a relatively high-powered malicious jammer with a single antenna. The techniques shaped the signal to be orthogonal to the jammer signal at the receiver. This made the decoder performance independent of the jammer signal power. This means that the jammer, regardless of the power level relative to the intended signal, does not degrade the receiver performance at all!

A new technique for collocated MIMO radar was introduced, which is based on partitioning the transmit array to multiple subarrays that are allowed to overlap. This formulation enables radar to beamform in both transit and receive array. Moreover, both *coherent processing gain* and *diversity gain* can be achieved. This radar waveform has SNR gain improvement and lower sidelobes in beampattern. Radar waveform was modified using a projection matrix to form null in radar beampattern in the direction of communications system. However, we found that the projection algorithm distorts the orthogonality of the radar waveform to some extent, which results in higher sidelobe. Even after that, the new overlapped-MIMO radar waveform retains favorable properties over conventional MIMO radars.

9.2 Future Work

Possible areas to extend and refine the research presented in this dissertation are identified and described in this section. The outline of future research directions is as follows:

- **Pilot Tone Jamming with Modulated Signal**: We observed in Section 4.2 of this dissertation that barrage jamming and pilot tone jamming achieved similar results, but pilot tone jamming required significantly less power, since only pilot tones were needed to be jammed where the channel noise error got distributed across all the subcarriers. Both, barrage jamming and pilot tone jamming, transmit Gaussian noise as jamming signal. Recently in [131], authors have found that modulated jamming has higher efficacy than noise jamming. As future research, we can explore the impact of pilot tone jamming when modulated signal is used instead of Gaussian noise.

- **Explore Mechanisms to Share Randomized Pilot Tones**: To counter the OFDM equalization jamming attacks including the pilot tone jamming attack and the pilot nulling attack, randomization of the locations of the pilot tones was proposed in Section 5.2 of this dissertation. The use of Pseudorandom Keystream for sharing the random pilot tone locations was proposed in Section 5.3. One major drawback of pilot tone randomization was that it makes equally difficult for the legitimate users to rip benefit of this countermeasure. As suggested, Pseudorandom Keystream could be a solution to this problem. However, further knowledge on cryptographic techniques for key management is needed, which can be subject to future research.

- **Developing Jamming Detection Methods**: The detection of jamming signal is an integral part of jamming mitigation strategy. We have briefly introduced the idea of jamming pattern detection in Section 5.1 of this dissertation. However, no further details about the algorithms to detect jamming were presented. It should be an interesting and logical step to further explore various methods for detecting the presence

of jammer and estimating the shape of the jamming waveform. This can enable us to tailor better jam resistant waveform.

- **Refinement of Jamming Taxonomy**: A comprehensive communications jamming taxonomy was developed in Section 3.4 of this dissertation, in an attempt to classify various types of jammers. However, the taxonomy included only communication systems and did not cover radar and radio navigation. Thus, as part of future research, there are rooms for developing radar jamming taxonomy and radio navigation jamming taxonomy. It may be possible to formulate a comprehensive and an all-inclusive taxonomy that applies to all forms of jamming.

- **Extending Spatial Hiding Antijam Schemes**: A practical jam resistant MIMO system that employs the 'receiver-only' and 'transmit precoding' processing techniques is presented in Section 7.3. The analysis presented in this dissertation considered only 2×2 MIMO systems with single antenna jammer, which can be extended to an arbitrary $N \times N$ dimension MIMO systems. In this case, the jammer can comprise multiple antennas as well, making it a true MIMO jamming model. The system model can also be extended further to MIMO-OFDM waveform. The proposed AJ algorithm assumed static or quasi-static channel model. It will be interesting to implement them for time-varying channels. The necessity of feedback CSI to the transmitter does limit the speed of adaptation that the precoding will be able to handle. If the channel conditions vary at such a speed that the feedback required for the precoding cannot keep up with the current set of values for CSI, then the performance of this AJ technique will degrade significantly, which can be a subject to future research.

- **Improvement of Radar-Communications Spectrum Sharing**: An overlapped-MIMO radar waveform was designed in Section 8.4 of this dissertation, which was combined with a radar-centric spectrum sharing algorithm called the null space projection (NSP) algorithm in Section 8.7. The current spectrum sharing model considered a

single MIMO communications node cooperating with the proposed overlapped-MIMO radar. It can be extended to a scenario where overlapped-MIMO radar will be cooperating with multiple communication nodes and projecting to the null space of the communications node that can provide the minimum distortion in radar waveform orthogonality. The homogenous cellular nature of the communications network presented in this work can be extended to multiple heterogeneous networks as well.

References

[1] D. L. Adamy, *EW 102 A Second Course in Electronic Warfare*. Horizon House Publication, Inc, 2004.

[2] D. L. Adamy, *EW 101 A First Course in Electronic Warfare*. Artech House, 2001.

[3] R. A. Poisel, *Modern Communications Jamming: Principle and Techniques*. Artech House, 2011.

[4] S. M. Kay, *Fundamentals of Statistical Signal Processing: Detection Theory*. Prentice Hall PTR, 1998.

[5] "Connecting America: The National Broadband Plan," 2010.

[6] "FCC Band Plan on Public Safety Spectrum at 700 MHz." FCC, August 2007. WT Docket No. 06-150.

[7] T. C. Clancy, "Efficient OFDM Denial: Pilot Jamming and Pilot Nulling," in *Communications, IEEE Int. Conf. on*, Jun. 2011.

[8] M. LaPan, T. C. Clancy, and R. W. McGwier, "Jamming Attacks Against OFDM Timing Synchronization and Signal Acquisition," in *IEEE Military Communications Conference (MILCOM)*, October 2012.

[9] M. LaPan, T. C. Clancy, and R. W. McGwier, "Phase Warping and Differential Scrambling Attacks Against OFDM Frequency Synchronization," in *International Conference on Acoustics Speech and Signal Processing (ICASSP)*, May 2013.

[10] C. Shahriar and T. C. Clancy, "Performance Impact of Pilot Tone Randomization to Mitigate OFDM Jamming Attacks," in *Consumer Communications and Networking Conference (CCNC), IEEE*, Jan 2013.

[11] J. Grimes, "Commercial Wireless Metropolitan Area Network (WMAN) Systems and Technologies," in *Memo 8-39*, Jan. 2009.

[12] T. C. Clancy and T. OShea, "TRANSEC Mitigation Options for Wireless Metropolitan Area Networks," in *Military Communications Conference. IEEE*, Oct. 2009.

[13] L. Sanguinetti, M. Morelli, and H. V. Poor, "Frame Detection and Timing Acquisition for OFDM Transmissions with Unknown Interference," *IEEE Transactions on Wireless Communications*, vol. 9, 2010.

[14] K. Ramiah and M. Zivkovic, "OFDM Synchronization in the Presence of Interference," in *International Conference on Communications, Signal Processing, and their Applications (ICCSPA)*, 2013.

[15] L. Tao, W. H. Mow, V. K. N. Lau, M. Siu, R. S. Cheng, and R. Murch, "Robust Joint Interference Detection and Decoding for OFDM-based Cognitive Radio Systems with Unknown Interference," *IEEE Journals on Selected Areas in Communications*, vol. 25, pp. 566–575, 2007.

[16] P. Sun and L. Zhang, "Narrowband Interference Effect on Timing Synchronization for OFDM-based Spectrum Sharing System," in *International Conference on Wireless and Mobile Communications (ICWMC)*, 2010.

[17] M. Marey and H. Steendam, "Analysis of the Narrowband Interference Effect on OFDM Timing Synchronization," *IEEE Transactions on Signal Processing*, vol. 55, pp. 4558–4566, 2007.

[18] H. Minn, V. Bhargava, and K. Letaief, "A Combined Timing and Frequency Synchronization and Channel Estimation for OFDM," in *IEEE International Conference on Communications (ICC)*, June 2004.

[19] M. Moretti and I. Cosovic, "OFDM Synchronization in an Uncoordinated Spectrum Sharing Scenario," in *IEEE Global Telecommunications Conference (GLOBECOM)*, November 2007.

[20] S. Patil and R. Upadhyay, "A Symbol Timing Synchronization Algorithm for WiMAX OFDM," in *Conference on Computational Intelligence and Communication Networks (CICN)*, October 2011.

[21] J. Kleider, S. Gifford, G. Maalouli, S. Chuprun, and B. Sadler, "Synchronization for RF Carrier Frequency Hopped OFDM: Analysis and Simulation," in *IEEE Military Communications Conference (MILCOM)*, October 2003.

[22] L. Nasraoui, L. Atallah, and M. Siala, "An Efficient Reduced-Complexity Two-Stage Differential Sliding Correlation Approach for OFDM Synchronization in the AWGN Channel," in *IEEE Vehicular Technology Conference (VTC)*, September 2011.

[23] T. Schmidl and D. Cox, "Robust Frequency and Timing Synchronization for OFDM," *IEEE Transactions on Communications*, vol. 45, December 1997.

[24] M. Lichtman, J. Reed, T. Clancy, and M. Norton, "Vulnerability of LTE to Hostile Interference," in *Global Conference on Signal and Information Processing (GlobalSIP), 2013 IEEE*, pp. 285–288, Dec 2013.

[25] G. Philippe, F. Montaigne, J.-C. Schiel, E. Georgeaux, C. Gruet, P.-Y. Roy, P. Force, and P. Mege, "LTE resistance to jamming capability: To which extend a standard LTE system is able to resist to intentional jammers," in *2013 Military Communications and Information Systems Conference (MCC)*, pp. 1–4, Oct 2013.

[26] T. Basar, "The Gaussian test channel with an intelligent jammer," *Information Theory, IEEE Trans. on*, vol. 29, pp. 152–157, Jan 1983.

[27] K. Pietikainen, A. Silvennoinen, M. Hall, and S. G. Haggman, "IEEE 802.11g tolerance to narrowband jamming," in *Military Communications Conference. IEEE*, pp. 1825 – 1830 Vol. 3, Oct. 2005.

[28] J. Park, D. kim, C. Kang, and D. Hong, "Effect of partial band jamming on OFDM-based WLAN in 802.11g," in *Acoustics, Speech, and Signal Processing. IEEE Int. Conf. on*, vol. 4, pp. 560–3, Apr. 2003.

[29] J. Luo, J. Andrian, and C. Zhou, "Bit Error Rate Analysis of jamming for OFDM systems," in *Wireless Telecommunications Symposium, 2007. WTS 2007*, pp. 1 –8, april 2007.

[30] L. Lightfoot, L. Zhang, and T. Li, "Performance of QO-STBC-OFDM in partial-band noise jamming," in *Information Sciences and Systems, 44th Annu. Conf. on*, pp. 1 –6, Mar. 2010.

[31] A. Best and B. Natarajan, "The Effect of Jamming on the Performance of Carrier Interferometry/OFDM," in *Wireless And Mobile Computing, Networking And Communications. IEEE Int. Conf. on*, Aug. 2005.

[32] D. W. Chi and P. Das, "Effects of Nonlinear Amplifier and Partial Band Jammer in OFDM with Application to 802.11n WLAN," in *Military Communications Conference. IEEE*, Oct. 2007.

[33] D. W. Chi and P. Das, "Effects of jammer and nonlinear amplifiers in MIMO-OFDM with application to 802.11n WLAN," in *Military Communications Conference. IEEE*, Nov. 2008.

[34] R. Jha, S. Limkar, and U. Dalal, "Performance Analysis under the Influence of Jamming for WiMAX System," in *Emerging Applications of Information Technology, 2nd Int. Conf. on*, pp. 292 –297, Feb. 2011.

[35] T. Karhima, A. Silvennoinen, M. Hall, and S.-G. Haggman, "IEEE 802.11b/g WLAN tolerance to jamming," in *Military Communications Conference. IEEE*, Oct. 2004.

[36] D. W. Chi and P. Das, "Effect of Jammer on the Performance of OFDM In the Presence of Nonlinearity In Rayleigh Fading Channel with Application to 802.11n WLAN," in *Military Communications Conference. IEEE*, Oct. 2006.

[37] National Telecommunications and Information Administration (NTIA), "An assessment of the near-term viability of accommodating wireless broadband systems in the 1675-1710 MHz, 1755-1780 MHz, 3500-3650 MHz, 4200-4220 MHz, and 4380-4400 MHz bands," October 2010.

[38] S. Sodagari, A. Khawar, T. C. Clancy, and R. McGwier, "A Projection Based Approach for Radar and Telecommunication Systems Coexistence," in *Global Comm. Conf. (GLOBECOM), IEEE*, 2012.

[39] P. Moose, "A Technique for Orthogonal Frequency Division Multiplexing frequency offset correction," *IEEE Transactions on Communication*, vol. 42, pp. 2908–2914, October 1994.

[40] J. van de Beek, "Low-Complex Frame Synchronization in OFDM Systems," in *International Conference on Universal Personal Communications (ICUPC)*, pp. 982–986, November 1995.

[41] R. Negi and J. Cioffi, "Pilot Tone Selection for Channel Estimation in a Mobile OFDM System," *IEEE Trans. Consum. Electron.*, vol. 44, no. 3, pp. 1122–1128, 1998.

[42] S. Adireddy, L. Tong, and H. Viswanathan, "Optimal placement of training for frequency-selective block-fading channels," *Information Theory, IEEE Transactions on*, vol. 48, no. 8, pp. 2338–2353, 2002.

[43] S. Ohno and G. B. Giannakis, "Optimal Training and Redundant Precoding for Block Transmissions with Application to Wireless OFDM," in *Acoustics, Speech, and Signal Processing, 2001. Proceedings. (ICASSP '01). 2001 IEEE Int. Conf. on*, vol. 4, pp. 2389 –2392, 2001.

[44] S. Ohno and G. Giannakis, "Capacity Maximizing MMSE-Optimal Pilots for Wireless OFDM over Frequency-Selective Block Rayleigh-Fading Channels," *Information Theory, IEEE Trans. on*, vol. 50, pp. 2138 – 2145, Sept. 2004.

[45] C. Eklund, R. Marks, K. Stanwood, and S. Wang, "IEEE Standard 802.16: A Technical Overview of the WirelessMAN/sup TM/ Air Interface for Broadband Wireless access," *Communications Magazine, IEEE*, vol. 40, pp. 98 –107, Jun. 2002.

[46] H. Ekstrom, A. Furuskar, J. Karlsson, M. Meyer, S. Parkvall, J. Torsner, and M. Wahlqvist, "Technical solutions for the 3G Long-Term Evolution," *Communications Magazine, IEEE*, vol. 44, pp. 38 – 45, Mar. 2006.

[47] M. Morelli and U. Mengali, "A comparison of pilot-aided channel estimation methods for OFDM systems," *Signal Processing, IEEE Trans. on*, vol. 49, pp. 3065 –3073, Dec. 2001.

[48] J. Stoer and R. Bulirsch, *Intro. to Numerical Analysis*. Springer, 2002.

[49] P. Massopust, *Interpolation and Approximation with Spline and Fractals*. New York, USA: Oxford University Press, 2010.

[50] R. Prasad, *OFDM for Wireless Communications Systems*. Artech, 2004.

[51] R. P. R. van Nee, *OFDM for Wireless Multimedia Communications*. Boston, MA: Artech House, 2000.

[52] K. Fazel and S. Kaiser, *Multi-Carrier and Spread Spectrum Systems: from OFDM and MC-CDMA to LTE and WiMAX*. Wiley, 2008.

[53] R. Jantti, J. Kerttula, K. Koufos, and K. Ruttik, "Aggregate Interference with FCC and ECC White Space Usage Rules: Case Study in Finland," in *New Frontiers in Dynamic Spectrum Access Networks (DySPAN), 2011 IEEE Symposium on*, pp. 599–602, 2011.

[54] L. Shi, K. W. Sung, and J. Zander, "Secondary Spectrum Access in TV-Bands with Combined Co-Channel and Adjacent Channel Interference Constraints," in *Dynamic Spectrum Access Networks (DYSPAN), 2012 IEEE International Symposium on*, pp. 452–460, 2012.

[55] J. H. Reed and N. Tripathi, "Analysis of the V-COMM Report Estimating the Impact of Channel 51 and E Block Interference on Band 12 and Band 17 User Equipment Receivers." FCC, 2012. WT Docket No. 12-69.

[56] J. H. Reed and N. Tripathi, "The 600 MHz Spectrum Auction: An Analysis of the Band Plan Framework." FCC, 2013.

[57] "FCC: Concerning the 600 MHz Band Plan." FCC, May 2013. GN Docket No. 12-268.

[58] E. Millios, D. Kong, M. Weebb, A. Doufexi, G. S. Hilton, A. R. Nix, and J. P. McGeehan, "Impact of Low-Frequency Radar Interference on Digital Terrestrial Television," in *Broadcasting, IEEE Transaction on*, vol. 59, March 2013.

[59] J. E. Bryson and L. E. Strickling, "An Assessment of the Viability of Accommodating Wireless Broadband in the 1755 – 1850 MHz Band." U.S. Department of Commerce, March 2012.

[60] M. Lichtman, J. D. Poston, S. Amuru, C. Shahriar, T. C. Clancy, R. M. Buehrer, and J. H. Reed, "A Communications Jamming Taxonomy," in *IEEE Security and Privacy*, 2015.

[61] E. Bayraktaroglu, C. King, X. Liu, G. Noubir, R. Rajaraman, and B. Thapa, "On the Performance of IEEE 802.11 under Jamming," in *INFOCOM 2008. The 27th Conference on Computer Communications. IEEE*, 2008.

[62] D. Thuente and M. Acharya, "Intelligent jamming in wireless networks with applications to 802.11 b and other networks," in *IEEE MILCOM*, vol. 6, 2006.

[63] S. Amuru and R. M. Buehrer, "Optimal Jamming Strategies in Digital Communications–Impact of Modulation," in *IEEE Global Communications Conference*, Dec. 2014.

[64] R. Chen, J.-M. Park, and J. H. Reed, "Defense against primary user emulation attacks in cognitive radio networks," *IEEE Journal on Selected Areas in Communications*, vol. 26, no. 1, pp. 25–37, 2008.

[65] J. Mitola and G. Q. Maguire Jr, "Cognitive radio: making software radios more personal," *IEEE Personal Communications*, vol. 6, no. 4, pp. 13–18, 1999.

[66] T. C. Clancy and N. Goergen, "Security in cognitive radio networks: Threats and mitigation," in *Cognitive Radio Oriented Wireless Networks and Communications (CrownCom)*, 2008.

[67] F. Renna, N. Laurenti, and Y.-C. Hu, "The Jamming Game in an OFDM Setting," in *Proceedings of the 5th International ICST Conference on Performance Evaluation Methodologies and Tools*, VALUETOOLS '11, (ICST, Brussels, Belgium, Belgium), pp. 496–505, ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), 2011.

[68] J. Li and S.-G. Haggman, "Performance of IEEE802.16-2004 Based System in Jamming Environment and its Improvement with Link Adaptation," in *Personal, Indoor and Mobile Radio Communications, 2006 IEEE 17th International Symposium on*, pp. 1–5, Sept 2006.

[69] I. Harjula, J. Pinola, and J. Prokkola, "Performance of IEEE 802.11 Based WLAN Devices under Various Jamming Signals," in *MILITARY COMMUNICATIONS CONFERENCE, 2011 - MILCOM 2011*, pp. 2129–2135, Nov 2011.

[70] T. Pollet, M. V. Bladel, and M. Moeneclaey, "BER Sensitivity of OFDM Systems to Carrier Frequency Offset and Wiener Phase Noise," *IEEE Transactions on Communications*, vol. 43, Feb/Mar/Apr 1995.

[71] M. Ozdemir and H. Arslan, "Channel Estimation for Wireless OFDM Systems," *Communications Surveys Tutorials, IEEE*, vol. 9, pp. 18–48, Second 2007.

[72] T. C. Clancy and N. Georgen, "Security in Cognitive Radio Networks: Threats and Mitigations," in *3rd International Conference on Cognitive Radio Oriented Wireless Networks and Communications (CrownCom*, 2008.

[73] S. Sodagari and T. C. Clancy, "Efficient Jamming Attack on MIMO Channels," in *Communications (ICC), IEEE Intl. Conf. on*, Jun. 2012.

[74] C. Shahriar, S. Sodagari, and T. C. Clancy, "Performance of Pilot Jamming on MIMO Channels with Imperfect Synchronization," in *Communications (ICC), IEEE Intl. Conf. on*, Jun. 2012.

[75] C. Mueller-Smith and W. Trappe, "Efficient OFDM Denial in the Absence of Channel Information," in *Military Communications Conference, MILCOM 2013 - 2013 IEEE*, pp. 89–94, Nov 2013.

[76] M. Han, T. Yu, J. Kim, K. Kwak, S. Han, and D. Hong, "An Efficient Channel Estimation Algorithm under Narrow-Band Jamming for OFDM Systems," in *Military Communications Conference. IEEE*, Oct. 2006.

[77] M. Han, T. Yu, J. Kim, K. Kwak, S. Lee, S. Han, and D. Hong, "OFDM Channel Estimation With Jammed Pilot Detector Under Narrow-Band Jamming," *Vehicular Technology, IEEE Trans. on*, vol. 57, pp. 1934 –1939, May 2008.

[78] C. Patel, G. Stuber, and T. Pratt, "Analysis of OFDM/MC-CDMA Under Channel Estimation and Jamming," in *Wireless Communications and Networking Conf. IEEE*, vol. 2, pp. 954–58, Mar. 2004.

[79] M. Lichtman, J. Reed, T. Clancy, and M. Norton, "Vulnerability of LTE to Hostile Interference," in *2013 IEEE Global Conference on Signal and Information Processing (GlobalSIP)*, pp. 285–288, Dec 2013.

[80] R. Jover, "Security attacks against the availability of LTE mobility networks: Overview and research directions," in *2013 16th International Symposium on Wireless Personal Multimedia Communications (WPMC)*, pp. 1–9, June 2013.

[81] M. Barbeau, "WiMax/802.16 Threat Analysis," in *Proceedings of the 1st ACM international workshop on Quality of service & security in wireless and mobile networks*, pp. 8–15, ACM, 2005.

[82] S. Chao, W. Ping, and S. Guozhong, "Performance of OFDM in the presence of multitene jamming," in *Robotics and Applications (ISRA), 2012 IEEE Symposium on*, pp. 118 –121, june 2012.

[83] J. G. Proakis, *Digital Communications*. McGraw Hill, 2007.

[84] Y. Cho, J. Kim, W. Yang, and C. Kang, *MIMO-OFDM Wireless Communications with MATLAB*. John Wiley & Sons, 2010.

[85] D. Tse and P. Viswanath, *Fundamentals of Wireless Communication*. Cambridge University Press, 2005.

[86] R. P. Jover, J. Lackey, and A. Raghavan, "Enhancing the security of LTE networks against jamming attacks," in *EURASIP Journal on Information Security*, vol. 7, 2014.

[87] C. Shahriar, M. La Pan, M. Lichtman, T. Clancy, R. McGwier, R. Tandon, S. Sodagari, and J. Reed, "Phy-layer resiliency in ofdm communications: A tutorial," *Communications Surveys Tutorials, IEEE*, vol. PP, no. 99, pp. 1–1, 2014.

[88] R. Haeb and H. Meyr, "A systematic approach to carrier recovery and detection of digitally phase modulated signals of fading channels," *Communications, IEEE Trans. on*, vol. 37, pp. 748 –754, Jul. 1989.

[89] J. G. Proakis, *Digital Signal Processing*. Prentice Hall, 2006.

[90] B. Muquet, Z. Wang, G. Giannakis, M. de Courville, and P. Duhamel, "Cyclic Prefixing or Zero Padding for Wireless Multicarrier Transmissions?," *Communications, IEEE Transactions on*, vol. 50, pp. 2136–2148, Dec 2002.

[91] M. Nisar, W. Utschick, H. Nottensteiner, and T. Hindelang, "On Channel Estimation and Equalization of OFDM Systems with Insufficient Cyclic Prefix," in *Vehicular Technology Conference, 2007. VTC2007-Spring. IEEE 65th*, pp. 1445–1449, April 2007.

[92] S. Sesia, I. Toufik, and M. Baker, *LTE The UMTS Long Term Evolution From Theory to Practice*. John Wiley & Sons Ltd., 2011.

[93] J. Zhu, W. Ser, and A. Nehorai, "Channel Equalization for DMT with Insufficient Cyclic Prefix," *Thirty-Fourth Asilomar Conference on Signals, Systems and Computers*, vol. 2, pp. 951–955, October 2000.

[94] H. V. Poor, *An Introduction to Signal Detection and Estimation*. Springer, 1994.

[95] A. Papoulis and S. U. Pillai, *Probability, Random Variables and Stochastic Processes*. McGraw Hill, 2002.

[96] L. Lightfoot, L. Zhang, J. Ren, and T. Li, "Jamming-resilient subcarrier assignment for OFDMA based space-time coded systems," in *Electro/Information Technology, IEEE Int. Conf. on*, Jun. 2009.

[97] A. Vecchio, "A Bound for the Inverse of a Lower Triangular Toeplitz Matrix," *SIAM Journal on Matrix Analysis and Applications*, vol. 24, no. 4, pp. 1167–1174, 2003.

[98] J. A. Mahal, C. Shahriar, and T. C. Clancy, "Emulated Cyclic Prefix Jamming and Nulling Attacks on SC-FDMA and Two Novel Countermeasures," in *Military Communications Conference, IEEE*, 2015.

[99] R. Miller and W. Trappe, "Subverting MIMO Wireless Systems by Jamming the Channel Estimation Procedure," in *Proceedings of the third ACM Conference on Wireless Network Security*, pp. 19–24, March 2010.

[100] R. Miller and W. Trappe, "On the Vulnerabilities of CSI in MIMO Wireless Communication Systems," in *IEEE Transactions on Mobile Computing*, pp. 1–14, August 2011.

[101] M. R. and T. W., "Short Paper: ACE - Authenticating the Channel Estimation Process in Wireless Communication Systems," in *Proceedings of the fourth ACM Conference on Wireless Network Security (WiSec)*, pp. 91–96, 2011.

[102] J. Wang and A. Swindlehurst, "Cooperative jamming in mimo ad-hoc networks," in *Signals, Systems and Computers, 2009 Conference Record of the Forty-Third Asilomar Conference on*, pp. 1719–1723, Nov 2009.

[103] D. Wang, G. Zhu, and Z. Hu, "Optimal pilots in frequency domain for channel estimation in MIMO-OFDM systems in mobile wireless channels," in *Vehicular Technology Conference, 2004. VTC 2004-Spring. 2004 IEEE 59th*, vol. 2, pp. 608–612 Vol.2, May 2004.

[104] Z. Wu, J. He, and G. Gu, "Design of optimal pilot-tones for channel estimation in MIMO-OFDM systems," in *Wireless Communications and Networking Conference, 2005 IEEE*, vol. 1, pp. 12–17 Vol. 1, March 2005.

[105] S. Sodagari and T. Clancy, "On Singularity Attacks in MIMO Channels," *Wiley Transactions on Emerging Telecommunications Technologies*, May 2013. doi: 10.1002/ett.2657.

[106] V. R. Cadambe and S. A. Jafar, "Interference alignment and degrees of freedom of the k-user interference channel," *IEEE Trans. Inf. Theory*, vol. 54, pp. 3425–3441, August 2008.

[107] R. Tresch and M. Guillaud, "Cellular interference alignment with imperfect channel knowledge," in *Proc. IEEE Intl. Conf. Commun. (ICC)*, Dresden, Germany, June 2009.

[108] G. Bresler, A. Parekh, and D. Tse, "The approximate capacity of the many-to-one and one-to-many gaussian interference channels," *IEEE Trans. Inf. Theory*, vol. 56, pp. 4566–4592, Sept 2010.

[109] M. A. Maddah-Ali, A. S. Motahari, and A. K. Khandani, "Communication over MIMO X channels: Interference alignment, decomposition, and performance analysis," *IEEE Trans. Inf. Theory*, vol. 54, pp. 3457–3470, August 2008.

[110] A. J. Viterbi, "Spread spectrum communications: Myths and realities," *IEEE Communications Magazine*, vol. 17, May 1979.

[111] W. F. Gabriel, "Adaptive arrays - an introduction," *Proceedings of the IEEE*, vol. 64, pp. 239–272, Feb 1976.

[112] K. C.-J. Lin, S. Gollakota, and D. Katabi, "Random access heterogeneous mimo networks," in *Proc. of SIGCOMM*, Toronto, Canada, Aug 2011.

[113] N. Jindal, J. G. Andrews, and S. Weber, "Rethinking MIMO for wireless networks: Linear throughput increases with multiple receive antennas," *Proc. IEEE Intl. Conf. Commun. (ICC)*, 2009.

[114] W. Liu, M. Z. I. Sarkar, and T. Ratnarajah, "Combined approach of zero forcing precoding and cooperative jamming: A secrecy tradeoff," in *Proc. of IEEE Wireless Communications and Networking Conference (WCNC)*, 2013.

[115] Q. Yan, H. Zeng, T. Jiang, M. Li, W. Lou, and Y. Hou, "Mimo-based jamming resilient communication in wireless networks," in *INFOCOM, 2014 Proceedings IEEE*, pp. 2697–2706, April 2014.

[116] C. Wang, E. Au, R. Murch, W. H. Mow, R. Cheng, and V. Lau, "On the Performance of the MIMO Zero-Forcing Receiver in the Presence of Channel Estimation Error," *Wireless Communications, IEEE Transactions on*, vol. 6, pp. 805–810, March 2007.

[117] C. A. Cole, "A spatial hiding anti-jam communications technique," *IEEE Communications Letters (submitted)*, 2013.

[118] A. Khawar, A. Abdel-Hadi, T. Clancy, and R. McGwier, "Beampattern Analysis for MIMO Radar and Telecommunication System Coexistence," in *Computing, Networking and Communications (ICNC), International Conference on*, pp. 534–539, Feb 2014.

[119] A. Khawar, A. Abdel-Hadi, and C. Clancy, "Spectrum Sharing between S-band Radar and LTE Cellular System: A Spatial Approach," in *IEEE DySPAN*, 2014.

[120] J. Li and P. Stoica, *MIMO Radar Signal Processing*. John Wiley & Sons, Inc, 2009.

[121] A. Hassanien and S. Vorobyov, "Phased-MIMO Radar: A Tradeoff Between Phased-Array and MIMO Radars," *Signal Processing, IEEE Transactions on*, vol. 58, pp. 3137–3151, June 2010.

[122] H. Yi, "Nullspace-Based Secondary Joint Transceiver Scheme for Cognitive Radio MIMO Networks Using Second-Order Statistics," in *Communications (ICC), IEEE Intl. Conf. on*, pp. 1–5, May 2010.

[123] Y. Noam and A. Goldsmith, "Blind Null-Space Learning for Spatial Coexistence in MIMO Cognitive Radios," in *Communications (ICC), IEEE International Conference on*, pp. 1726–1731, June 2012.

[124] A. Khawar, A. Abdel-Hadi, and T. C. Clancy, "A mathematical analysis of LTE interference on the performance of S-band military radar systems," in *13th Annual Wireless Telecommunications Symposium (WTS)*, (Washington, DC, USA), Apr. 2014.

[125] J. Li and P. Stoica, "Mimo radar with colocated antennas," *Signal Processing Magazine, IEEE*, vol. 24, pp. 106–114, Sept 2007.

[126] C.-Y. Chen and P. Vaidyanathan, "MIMO Radar Space-Time Adaptive Processing Using Prolate Spheroidal Wave Functions," *IEEE Trans. Signal Process.*, Feb 2008.

[127] Q. He, R. Blum, H. Godrich, and A. Haimovich, "Target Velocity Estimation and Antenna Placement for MIMO Radar with Widely Separated Antennas," *Selected Topics in Signal Processing, IEEE Journal of*, vol. 4, pp. 79–100, Feb 2010.

[128] Q. He, R. Blum, H. Godrich, and A. Haimovich, "Target Velocity Estimation and Antenna Placement for MIMO Radar With Widely Separated Antennas," *IEEE J. Sel. Topics in Signal Process.*, Feb 2010.

[129] A. Khawar, *Spectrum Sharing between Radar and Communication Systems*. PhD thesis, Virginia Tech, 2015.

[130] A. L. Scott, "Effects of Cyclic Prefix Jamming Versus Noise Jamming in OFDM Signals," Master's thesis, Air Force Inst. Of Tech Wright-Patterson AFB OH Graduate School of Engineering and Management, 2011.

[131] C. A. Cole, "Analysis of a Power Efficient Modulated Jamming Technique," in *IEEE Military Communications Conference*, 2012.