Analysis of Jamming-Vulnerabilities of Modern Multi-carrier Communication Systems

Jasmin A. Mahal

Dissertation submitted to the Faculty of the
Virginia Polytechnic Institute and State University
in partial fulfillment of the requirements for the degree of

Doctor of Philosophy
in
Electrical Engineering

T. Charles Clancy, Chair
Robert W. McGwier
Luiz A. DaSilva
Michael J. Roan
Walid Saad

May 09, 2018
Arlington, Virginia

Keywords: Jamming, Anti-jamming, OFDM, OFDMA, SC-FDMA, MISO, Pilot-spoofing, Channel estimation, Multi-carrier Systems, Physical Layer Security

Analysis of Jamming-Vulnerabilities of Modern Multi-carrier Communication Systems

Jasmin A. Mahal

(ABSTRACT)

The ever-increasing demand for private and sensitive data transmission over wireless networks has made security a crucial concern in the current and future large-scale, dynamic, and heterogeneous wireless communication systems. To address this challenge, wireless researchers have tried hard to continuously analyze the jamming threats and come up with improved countermeausres. In this research, we have analyzed the jamming-vulnerabilities of the leading multi-carrier communication systems, Orthogonal Frequency Division Multiplexing (OFDM) and Single-Carrier Frequency Division Multiple Access (SC-FDMA).

In order to lay the necessary theoretical groundwork, first we derived the analytical BER expressions for BPSK/QPSK and analytical upper and lower bounds for 16-QAM for OFDMA and SC-FDMA using Pilot Symbol Assisted Channel Estimation (PSACE) techniques in Rayleigh slow-fading channel that takes into account channel estimation error as well as pilot-jamming effect. From there we advanced to propose more novel attacks on the Cyclic Prefix (CP) of SC-FDMA. The associated countermeasures developed prove to be very effective to restore the system. We are first to consider the effect of frequency-selectivity and fading correlation of channel on the achievable rates of the legitimate system under pilot-spoofing attack. With respect to jamming mitigation techniques, our approaches are more focused on Anti-Jamming (AJ) techniques rather than Low Probability of Intercept (LPI) methods.

The Channel State Information (CSI) of the two transceivers and the CSI between the jammer and the target play critical roles in ensuring the effectiveness of jamming and nulling attacks. Although current literature is rich with different channel estimation techniques between two legitimate transceivers, it does not have much to offer in the area of channel estimation from jammer's perspective. In this dissertation, we have proposed novel, computationally simple, deterministic, and optimal blind channel estimation techniques for PSK-OFDM as well as QAM-OFDM that estimate the jammer channel to the target precisely in high Signal-to-Noise (SNR) environment from a single OFDM symbol and thus perform well in mobile radio channel. We have also presented the feasibility analysis of estimating transceiver channel from jammer's perspective at the transmitter as well as receiver side of the underlying OFDM system.

Analysis of Jamming-Vulnerabilities of Modern Multi-carrier Communication Systems

Jasmin A. Mahal

(GENERAL AUDIENCE ABSTRACT)

Susceptibility to interferences is one of the major inherent vulnerabilities of open and pervasive wireless communications systems. The recent trends to more and more decentralized and ad-hoc communication systems that allow various types of network mobile terminals to join and leave simply add to this susceptibility. As these networks continue to flourish worldwide, the issues of privacy and security in wireless communication networks have become a major research problem. The increasingly severe hostile environments with advanced jamming threats has prompted the corresponding advancement in jamming detection and mitigation techniques. This dissertation has analyzed the jamming-vulnerabilities of the leading multi-carrier communication systems of the modern world. We have designed some novel jamming attacks and the corresponding countermeasures. The performance of these novel more-effective techniques are compared with their less-effective conventional counterparts.

The information of the channel between the legitimate transmitter-receiver pair and between the jammer and the target play critical roles in ensuring the effectiveness of these smart jamming attacks. Although current literature is rich with different channel estimation techniques between the legitimate pair, it does not have much to offer in the area of channel estimation from jammer's perspective. In this dissertation, we have proposed novel channel estimation techniques from jammer's perspective.

Dedication

To the most precious gifts of my life,
my three children,
Nuha, Nadhif, and Numa

Acknowledgments

First and foremost, I would like to thank Allah, the most Gracious, the most Merciful Who has power over everything, to bless me with the ability to complete this dissertation. Then, I would like to thank Dr. T. Charles Clancy, my adviser, who I feel privileged to have had the opportunity to work with for the last six years. Thank you for taking me as a PhD student, for giving me complete freedom to explore my ideas while exposing me to great new ideas, giving directions, and for providing crucial feedback on my works. Dr. Clancy's great enthusiasm for research simply nurtured my own passion for research. Furthermore, the research programs at Hume Center under his direction, has facilitated the whole process of PhD in an organized and targeted manner, and has turned it into a great learning experience.

I am also indebted to my Ph.D. committee members Dr. Robert W. McGwier, Dr. Luiz A. DaSilva, Dr. Michael J. Roan, and Dr. Walid Saad for their valuable feedback. Very special thanks go to my husband who is always there for me with unconditional loving support. I am also thankful to my sister-in-laws' (Dr. Fatima Mirza, Dr. Rehenuma Asmi and Sofiya Saiyed) writing group for their insightful comments on my papers. Finally, I express my deepest gratitude to my parents, my family and my in-laws for their unwavering support and continuous encouragement. Without all of you, it would not have been possible. I feel blessed to have all of you as part of this great accomplishment of my academic career.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Motivation

The two inherent characteristics of the wireless medium, *broadcast* and *superposition*, pose different challenges in ensuring reliable and secure communications in the presence of adversaries. The broadcast nature of wireless communications makes it difficult to prevent transmitted signals from unintended recipients, while superposition leads to the overlapping of multiple signals at the receiver. The adversaries can exploit these vulnerabilities of wireless communications either by intercepting the information from an ongoing transmission without being detected, or by maliciously jamming the intended receiver where the transmitted signal is weakest and thus most vulnerable [1, 2]. The unwanted energy from the jammer, if strong enough, causes the receiver to demodulate the signal from the jammer as opposed to the legitimate transmitter. As the jammer signal is not a replica of what is transmitted, communication is denied on the Radio Frequency (RF) link [3]. Undoubtedly, the openness and easy accessibility of the wireless medium - the major two advantages of wireless networks are at the same time its *Achilles heel*.

Due to the unprecedented ubiquity and proliferation of wireless technologies in Today's

World, jamming in wireless networks has become a major research problem because of the ease in blocking communication in wireless networks. Jamming attacks are a subset of Denial of Service (DoS) attacks which may result in several other higher-layer security problems too.

Radio jamming is an old practice whose origin could be traced back theoretically to the dawn of RF communications [2]. During the Civil War, Confederate soldiers rerouted telegraph wires so that Union units could be deceived by giving false commands - today we would call that spoofing. There was widespread use of communications jamming in World war I and there was a great deal of activity in furthering its development until World War II. Communications Electronic Warfare has been around for over 100 years as an effective tool used primarily for gathering information shaping the battlespace [4]. In the zeitgeist of the Cold War and various conflicts around the world, it has become more recognized worldwide.

Although jamming and anti-jamming physical layer strategies have been of long-standing interest especially in military sector, the technical literature about communication jamming techniques began to appear in unclassified form about 1980. Prior to that, the extensive investment of U.S. Department of Defense in this sector was mostly classified and unavailable to the general public [5]. Due to the proliferation of wireless technologies, jamming-antijamming in wireless communications has emerged as a challenging research problem because of the ease in disrupting communication in wireless networks. The possibility of a malicious shut down of communications is a major concern today, as expressed by the US President's Commission on Critical Infrastructure Protection [6].

In this work, we have focused on the jamming-vulnerabilities of the leading multi-carrier communication systems like Orthogonal Frequency Division Multiplexing (OFDM) and Single-Carrier Frequency Division Multiple Access (SC-FDMA). Instead of simply raising noise floor or causing unacceptable audio or data performance, we have designed smart attack which is aimed at network-specific vulnerabilities. Consequently, the corresponding antijam technique is also customized to a particular network. A smart jammer designed to disrupt GSM

will have less or even no effect against other networks that might be present. So it is important to be able to identify the exact type of network in order for a smart jammer to be effective [2]. The proposed countermeasures are more focused on Anti-Jamming (AJ) techniques rather than Low Probability of Intercept (LPI) methods in order to enable the affected systems sustain through jamming. Multi-carrier communication systems are chosen due to their widespread use in fourth and fifth generation (4G/5G) cellular communications.

We have also explored an untapped area of research: channel estimation from jammer's perspective. The Channel State Information (CSI) of the two transceivers and the CSI between the jammer and the target play critical roles in ensuring the effectiveness of jamming and nulling attacks. Although current literature is rich with different channel estimation techniques between two legitimate transceivers, it does not have much to offer in the area of channel estimation from jammer's perspective. The fundamental difference between CSI estimation from jammer's perspective and that between two legitimate transceivers is one of cooperation. The target system is not cooperative with the EW system when the latter is trying to obtain CSI. This issue alone significantly complicates the situation.

1.2 Summary of Contributions

The novel contributions of this research are as follows

- The detailed derivations of the exact BER expressions for BPSK/QPSK and analytical upper and lower bounds for 16-QAM for OFDMA and SC-FDMA using Pilot Symbol Assisted Channel Estimation (PSACE) techniques in Rayleigh slow-fading channel that takes into account channel estimation error as well as pilot-jamming effect. Instead of widely-used two-dimensional Wiener interpolation between the pilots, we used piecewise-linear interpolation to take advantage of its simplicity in terms of computational complexity.

- Design of the emulated time-domain jamming and nulling attacks on Cyclic Prefix (CP) of SC-FDMA in frequency-selective static channel and the corresponding two novel anti-jamming techniques.

- Analysis of the effect of spatial fading correlation on pilot-spoofing attack in a TDD MISO-OFDM system from information-theoretic perspective. Capacity bounds are derived.

- Design of novel, computationally simple and deterministic blind channel estimation schemes for PSK-OFDM and QAM-OFDM from legitimate transceivers as well as pilot-jammer's perspective. Their effectiveness in formulating the pilot-nulling attacks against OFDM is investigated.

- Feasibility analysis of transceiver channel estimation from jammer's perspective.

1.3 Organization of the Dissertation

The rest of this dissertation is organized as follows. Chapter 2 describes the foundational materials of jamming, anti-jamming techniques and channel estimation from jammer's perspective . Chapter 3 presents the detailed derivations of the analytical BER expressions for BPSK/QPSK and analytical upper and lower bounds for 16-QAM for OFDMA and SC-FDMA using PSACE techniques in Rayleigh slow-fading channel that takes into account channel estimation error as well as pilot-jamming effect. Chapter 4 discusses the design of the emulated time-domain jamming and nulling attacks on CP of SC-FDMA in frequency-selective static channel and the corresponding two novel anti-jamming techniques. Chapter 5 details the effect of spatial fading correlation on pilot-spoofing attack in a TDD MISO-OFDM system from information-theoretic perspective. Chapter 6 presents novel, computationally simple and deterministic blind channel estimation schemes for PSK-OFDM and

QAM-OFDM from legitimate transceivers as well as pilot-jammer's perspective. Chapter 7 analyzes the feasibility of transceiver channel estimation from jammer's perspective. Chapter 8 concludes with the discussion on potential research directions in this area.

Chapter 2

Background

Susceptibility to interference is one of the major inherent vulnerabilities of open and pervasive wireless communications. The current trends to more and more decentralized and ad-hoc communication systems that allow various types of network mobile terminals to join and leave simply add to this susceptibility. As these networks continue to flourish worldwide, the issues of privacy and security in wireless communication networks have taken on an increasingly important role. The increasingly severe hostile environments with advanced jamming threats has prompted the corresponding advancement in jamming detection and mitigation techniques. This chapter presents the background materials on existing and emerging jamming and anti-jamming techniques. It also discusses the issue of channel estimation from jammer's perspective and multi-carrier techniques.

2.1 Jamming Techniques

Jamming techniques are a subset of denial of service (DoS) attacks in which malicious nodes block legitimate communication by causing intentional interference in networks. It is all about getting sufficient energy into the target receiver to overwhelm it. But however

powerful the jammer, unless the power received from the jammer at the target is at or above its maximum receiver power, a suitably strong link can easily burn through the attack [2]. Although jamming attacks are mostly targeted at the physical layer, cross-layer attacks are possible too. In this section, we describe briefly various types of communication jammers.

2.1.1 Noise Jamming

For *noise jamming*, the jamming signal is modulated with a random noise. The bandwidth of the jamming signal can be as wide as the entire spectrum of the target or much narrower occupying a single channel. The noise is generally assumed to be Gaussian. *Broadband Noise* (BBN) jamming places noise energy across the entire frequency spectrum of the target. It is also called *full band* jamming and is sometimes called *barrage jamming*. This type of jamming raises the background thermal noise level at the target and is useful against all sorts of communications. BBN jamming is a direct assault on the channel capacity of a communication system [5]. *Partial-Band Noise* (PBN) jamming places noise energy across multiple but not all channels in the spectrum of the target. These channels may or may not be contiguous. *Narrowband Noise* (NBN) jamming places all of the jammer energy into a single channel. The bandwidth of this energy injection could be the whole width of the channel or it could be only that part of channel carrying data.

2.1.2 Tone Jamming

In tone jamming, one or more tones are strategically placed in the spectrum. Their placement and number affect the performance of jamming. The phase of the jammer relative to the target signal is an important parameter [7]. Assuming the jammer signal is sufficiently larger than the target signal, the symbol is jammed independent of the phase relationship with the jammer placed in non-data frequency. If the jammer is located at data frequency,

then the phase can present a problem. *Single-tone* jamming, also called *spot jamming*, is effective against Direct Sequence Spread Spectrum (DSSS) targets as it overcomes the processing gains at the target and causes deleterious effects at despreading. With the tones in consecutive channel, also known as *comb jamming*, jammer has higher flexibility than its single-tone counterpart.

2.1.3 Swept Jamming

Swept jammer is associated with a relatively narrowband signal which could be as narrow as a tone but more often a PBN signal that sweeps in time across the frequency band of interest. The net effect of such jamming is similar to barrage jamming except its full power is concentrated in each dwell bandwidth. Time is very critical for a swept jammer. The sweeping must be fast enough to ensure the whole band is covered in a sufficiently short period.

2.1.4 Pulse Jamming

A *Pulse jammer* transmits broadband noise for a particular fraction of time and is off for the rest of the time. The receiver characteristics are important to evaluate the effectiveness of the pulse jamming. Pulse jamming is more effective than PBN jamming for DSSS [4].

2.1.5 Follower Jamming

A *follower jammer* has an RF detection capability by which it attempts to scan for a signal, identify the signal as a threat and tune the jammer to that frequency. This jamming is also referred to as *responsive jamming, repeater jamming,* and *repeat-back jamming.* The timing of a follower jammer must conform to certain constraints due to the finite propagation

and processing time of the signals.

2.1.6 Adaptive Jamming

Adaptive jamming is an extension of responsive jamming but with the potential to jam several targets at the same time. It provides an improved method to achieve the same effects as barrage jamming but in a far more focused manner.

2.1.7 Smart Jamming

Smart jammers attempt to disrupt portions of digital signals necessary to deny communications. This jammer targets at network vulnerabilities which may include:

- pilot channels
- synchronization channels
- paging channels
- error correction checksum etc.

Due to its targeted approach, smart jamming is always more effective than its unintelligent counterparts. Although this type of jamming is relatively new compared to the others but much research efforts is expended in the literature at present. This research work is also focused on this type of jamming attacks.

2.2 Jamming Mitigation Techniques

Jamming mitigation techniques can be broadly categorized into two groups:

- low probability of intercept (LPI) techniques, and
- Anti-jamming (AJ) techniques.

The former one is associated with the goal of avoiding interception or detection at all while the later one attempts to be able to communicate even in the presence of jamming. The general approaches for jamming mitigation are as follows:

- power management to minimize the probability of detection or interception
- use of terrain and clutter shielding to limit the ability of the jammer to detect and jam signals
- frequent changes of frequency
- intermittent use of systems and minimizing transmissions
- use of antennas with nulls or low energy output in the direction of jammers
- attempt to make important links parallel to the threat axis by using highly directional antennas
- using spoofing etc.

Spoofing is a method of using an RF system to mimic the parameters of another system. The aim is to deceive the jammer into misidentifying the target until it is too late. This is the modern day version of a traditional method of *ruse de guerre* in which warships used to fly false colors to mislead the other warships [2].

2.3 Channel estimation from jammer's perspective

Knowledge of the Channel State Information (CSI) between the two transceivers and between the jammer and the target play critical role in formulating smart jamming attacks.

The fundamental difference between CSI estimation from jammer's perspective and that between two legitimate transceivers is one of cooperation. The target system is not cooperative with the jammer that is trying to obtain CSI. This issue alone significantly complicates the situation. One significant contribution of this research work is in this untapped area.

2.3.1 Channel Estimation Between Jammer and Target

In this area, the possible approaches are as follows:

- ***reciprocal TDD channel:*** the jammer uses pilot information to estimate reverse channel assuming negligible propagation delay.
- ***blind channel estimation techniques:*** exploits the available received signals and require a large amount of data.
- ***active adversary:*** the jammer can join the network as a valid user and gain CSI information via network interaction.
- ***battle damage assessment:*** exploits available observables to approach the goal in a targeted manner through some kind of optimization of the relevant utility function.

2.3.1.1 Reciprocal TDD Channel

Assuming reciprocal TDD channel, we can adopt the channel estimation technique as described in [8]. The channel training phase is necessary for the base station (BS) to gain the CSI in order to apply beamforming for data transmission. This is achieved by having mobile send the pilot signals to BS. Since the pilot signals are repeatedly used and publicly known, it allows the jammer to estimate the channel between itself and the target taking advantage of these pilots.

2.3.1.2 Blind Channel Estimation Techniques

In a wireless tactical scenario where a jammer attempts to estimate its own channel to the target, the only information available is the target signal intercepted by the jammer and some general knowledge about the standardization of the system adopted by the target. Consequently, the only option available to the jammer is to estimate the channel blindly based on the available channel output. Blind identification of linear systems is a rich area of research. The blind channel estimation methods typically exploit the statistical behavior of the received signals and require a large amount of data. Hence, they suffer severe performance degradation in fast fading channels.

2.3.2 Channel Estimation Between Two Transceivers

Possible approaches in this area are as follows:

- ***feedback channel:*** in certain MIMO scenarios, the target often sends CSI feedback to the transmitter. The jammer can overhear this CSI feedback channel and extrapolate CSI.
- ***active adversary:*** the jammer can join the network as a valid user and gain CSI information via network interaction.
- ***battle damage assessment:*** exploits available observables to approach the goal in a targeted manner through some kind of optimization of the relevant utility function.

2.3.2.1 Feedback Channel

In communication systems, knowledge of the channel condition at the transmitter can provide improved system performance. Channel knowledge enables the transmitter to suitably

adapt its transmission strategy to ensure increased data throughput and/or coverage. This could involve link adaptation, i.e. adaptation of the modulation and coding rate, adaptation of the beamforming/spatial multiplexing parameters in MIMO systems, and adaptive scheduling of different users. Depending on the extent to which the channel knowledge is available at the transmitter, different levels of gains can be achieved [9].

In cellular systems, channel knowledge at the transmitter can be obtained in a variety of ways. In time division duplexed (TDD) systems, pilot transmission on the uplink channel can provide the base station with channel information for downlink transmission assuming that the reciprocal channel is varying slowly over time, i.e., the channel is time correlated. In frequency division duplexed (FDD) systems, exploiting such channel reciprocity to obtain downlink channel information at the base station is typically not an option as the downlink and uplink channels are well separated in frequency, and thus are highly uncorrelated. One possible approach to obtain transmitter side channel information in such systems is to employ feedback, wherein, using downlink pilot symbols, the mobile user can estimate the downlink channel, and feed it back to the base station on the uplink. Depending on the available resources, the feedback could be perfect, i.e. the actual channel coefficients are fed back, or limited i.e. quantized channel coefficients, or some function of the channel coefficients that assists the transmitter decide the transmit configuration to be employed, are fed back [10,11].

A jammer can intercept this feedback channel by passive eavesdropping, in which the malicious nodes detect the information by listening to the message transmission in the broadcasting wireless medium. If the jammer knows the channel between itself and the receiver (the target) which could be carried out by the approaches described above, the jammer can estimate the channel between the two transceivers.

2.3.2.2 Active Adversary

Channel estimation is not a problem for an active adversary. For example, a masquerader who has stolen a legitimate user's credentials attempts to impersonate it to carry out malicious actions. Consequently, it can take advantage of all the channel estimation techniques available in literature between two legitimate transceivers. But as these techniques are based on the cooperation between the transceivers, the adversary has to make sure it does not give away its true identity in process of doing so.

2.3.2.3 battle damage assessment

Battle damage assessment is a process whereby a jammer estimates the performance of a target communication system to assess whether it is being effective. The jammer can assume some bounded range of CSI ambiguity. The jammer performs a hill climbing across the range and observes the target performance by measuring parameters like duty cycle, retransmissions, and adaptive coding/modulation changes. Thus the jammer can estimate unknown CSI. This approach only works if the ambiguity can be resolved within the coherence time of the CSI, so it may not work for mobile targets.

2.4 Multi-carrier Communication Systems

Multi-carrier techniques are widely used in wireless LANs and fourth generation cellular systems. Orthogonal frequency division multiplexing (OFDM) is widely used modulation technique in high-rate wireless systems such as IEEE 802.11a/g wireless local area network (WLAN) standard due to its robustness to frequency selective fading. Multiple access with OFDM can be achieved using TDMA or random access approaches. Orthogonal frequency division multiple-access (OFDMA) is an extension of OFDM to accommodate multiple si-

multaneous users. OFDMA has been adopted for the forward channel in 3GPP long term evolution (LTE) and in both the forward and reverse channels for IEEE 802.16e Worldwide Interoperabilityfor Microwave Access (WiMAX) standard.

OFDMA achieves multiple access by dividing the available sub-carriers into mutually exclusive sets that are assigned to distinct users for simultaneous transmission. The orthogonality of the sub-carriers ensures protection against multiple-access interference. OFDMA has essentially the same advantages and disadvantages as OFDM when compared to single-carrier modulation schemes. It achieves robustness to frequency-selective fading using closely spaced orthogonal sub-carriers, such that frequency-domain equalization (FDE) can be used. However, it also suffers from a high peak-to-average power ratio (PAPR) that requires the use of either PAPR reduction techniques or a highly linear power amplier. OFDMA is attractive for use on the forward link of a cellular system, since all forward link transmissions can use the same RF local oscillator and sample clock reference in their digital-to-analog converters (DACs). However,the use of OFDMA on the cellular reverse link is complicated considerably by the fact that waveform received at the BS from each MS will have a different carrier frequency offset, timing offset, and sampling clock offset.

To overcome the difculties of using OFDMA on the cellular reverse link, a modied form of OFDMA, called single-carrier frequency division multiple access (SC-FDMA) was introduced. SC-FDMA can be viewed as DFT-spread OFDMA, where a block of time-domain data symbols are rst transformed to the frequency-domain using a discrete Fourier transform (DFT) before being applied to an OFDMA modulator. Similar to OFDMA, multiple access is achieved by assigning the users disjoint sets of sub-carriers. The resulting SC-FDMA waveform is a single-carrier modulated waveform having a characteristically much lower PAPR than the corresponding multi-carrier OFDMA waveform. This lower PAPR benets the MS in terms of transmit power efciency, thereby making SC-FDMA very attractive for the cellular reverse link. For this reason SC-FDMA has been adopted as the reverse channel multiple

access scheme for 3GPP LTE.

2.5 Conclusion

Overall, this chapter gives the average reader some background in the topics addressed in this dissertation. Individual chapters have more complete treatment of the topics presented.

Chapter 3

The BER Analysis of OFDMA and SC-FDMA under PSACE and Pilot-Jamming in Rayleigh Slow-Fading Channel

In this chapter, we derived the analytical Bit Error Rate (BER) expressions for OFDMA and SC-FDMA in Rayleigh slow-fading channel for BPSK, QPSK, and 16-QAM modulations under pilot-jamming and pilot symbol assisted channel estimation (PSACE). We addressed the issue by first approaching the BER analysis from general case of PSACE technique in Rayleigh slow-fading channel. The expressions thus derived are then modified for BPSK/QPSK/16-QAM modulations. The equations are further customized to account for the frequency domain Zero-Forcing (ZF) equalization in frequency direction or time direction with application respectively to OFDMA or SC-FDMA without and with pilot-jamming attack. Instead of conventional Wiener interpolation, piecewise-linear interpolation is used for its low computational complexity. Analysis is verified with simulation in MATLAB. The

simulation results match perfectly with the theoretical predictions except for some discrepancies with SC-FDMA. Thorough investigation into the matter reveals the fact that the generalized equations developed in this chapter have to be further modified to account for system-specific features like DFT-precoding for SC-FDMA.

3.1 Introduction

Long Term Evolution (LTE) is the latest advancement in cellular broadband technologies. Adopting a multicarrier approach for multiple access, LTE has opened up the frequency domain as a new dimension of flexibility [12]. On the downlink, LTE utilizes Orthogonal Frequency Division Multiple Access (OFDMA) and the uplink takes advantage of Single-Carrier Frequency-Division Multiple Access (SC-FDMA). These multiple-access solutions come with their characteristic benefits like orthogonality between the carriers, reduced interference and improved network capacity.

Although OFDM is robust to time-dispersive radio channels by confining inter-symbol interference (ISI) within a guard interval at the beginning (Cyclic Prefix) or end (Cyclic Suffix) of each symbol, it suffers from a high peak-to-average power ratio (PAPR) which results in a need for a highly linear power amplifier [13]. This limitation has been handled ingeniously by the introduction of the modified form of OFDMA called SC-FDMA. As transmitter expands the signal bandwidth to cover the bandwidth of the channel in SC-FDMA by adding an extra DFT precoder in front of OFDMA modulator, it can be viewed as DFT-spread OFDMA. Its inherent single-carrier characteristic results in much lower PAPR which in turn allows efficient terminal power amplifier design with a long battery life [14]. Owing to its high signaling rate, the frequency domain equalizer of SC-FDMA is much more complicated than its OFDMA counterpart. Adopting OFDMA for downlink and SC-FDMA for uplink, 3GPP LTE places both the main transmitter burden of highly linear power amplifier and the

main receiver burden of complex equalization at base stations instead of the mobiles [15]. This renders mobiles in LTE power efficient and compact.

OFDMA and SC-FDMA both use PSACE techniques in order to compensate for linear distortion introduced by the multipath fading channel. In these schemes, channel estimation is performed by inserting pilots at selected positions in the time-frequency (symbol-subcarrier) grid. For a given pilot pattern, the Wiener filter estimates channel by minimizing mean-squared estimation error [16]. It carries out an optimal two-dimensional (2-D) Wiener interpolation given the channel statistics and the operating signal-to-noise ratio (SNR). However, it is associated with comprehensive mathematical calculations and also vulnerable to mismatches between the designed and actual channel statistics. Assuming a Gauss-Markov model of fading, the Kalman filter channel estimator minimizes mean-squared variance of the estimation error [17]. This estimation is also computationally intensive. In terms of computational complexity, piecewise-linear interpolation in either time (symbol) or frequency (subcarrier) domain is the simplest technique. However, the simplicity is achieved at the cost of losing bandwidth to pilots.

PSACE techniques are inherently prone to estimation error [18]. These schemes interpolate between pilot tones or symbols to estimate the channel transfer factors for the subcarriers or symbols between the pilots. Thus interference and noise present on the pilots naturally spread across the whole data-spectrum or data-symbols with consequent degradation in effective detection of information. Same is the case with tactical scenarios where adversaries intentionally try to disrupt communications by causing hostile interferences to the desired signals. The pilots of OFDMA and SC-FDMA are lucrative targets for effective and power-efficient smart jammers that attack portions of the signal rather than the entire signal [5]. By jamming the pilots, the smart jammers attempt to deny communications by disrupting the equalization of the system. BER analysis neglecting these practical aspects provides over-optimistic results.

Sanchez-Sanchez, Aguayo-Torres, and Fernandez-Plazaola performed BER analysis of SC-FDMA over Rayleigh and Nakagami-m fading channels assuming perfect channel estimation (CE) [19, 20]. Luo, Andrian, and Zhou carried out BER analysis of OFDM systems under jamming but with perfect CE [21]. In attempt to account for the CE errors, Hoeher explored the performance of OFDM with CE error [22]. Tufvesson and Maseng analyzed BER of OFDM system under channel estimation error using Kalman filter for channel information interpolation [23]. Patel, Stuber, and Pratt studied the OFDM/MC-CDMA systems under imperfect CE and jamming using 2-D Wiener filter for interpolation [18]. Cavers presented closed form expressions for the BER in BPSK, QPSK and a tight upper bound on Symbol Error Rate (SER) in 16-QAM for Pilot Symbol Assisted Modulation using Wiener interpolation but without jamming for Rayleigh faded channel [24], [25]. Athaudage and Jayalath investigated channel estimation error for OFDM system using piecewise-linear interpolation in time and frequency domain [26]. Building upon the works of Cavers and Athaudage-Jayalath, this chapter derives closed-form BER expressions for OFDMA as well as SC-FDMA under PSACE error and pilot-jamming using piecewise-linear interpolation and ZF equalization in a Rayleigh slow-fading AWGN channel using PSK and QAM modulations. Although we have focused on the expressions for BPSK, QPSK, and 16-QAM, the theories can be extended to any modulation schemes.

Despite the availability of comprehensive literature on PSACE and OFDM/OFDMA, our major contributions are as follows.

- The detailed derivations of the exact BER expressions for BPSK/QPSK and analytical upper and lower bounds for 16-QAM for OFDMA and SC-FDMA using PSACE techniques in Rayleigh slow-fading channel that takes into account channel estimation error as well as pilot-jamming effect. Instead of widely-used two-dimensional Wiener interpolation between the pilots, we used piecewise-linear interpolation to take advantage of its simplicity in terms of computational complexity. These expressions depend

on a single parameter, the cross-correlation coefficient μ.

- The rigorous simulation has been performed to verify the analysis. The simulations match perfectly with the theoretical predictions except for slight deviations with SC-FDMA. Exploration of these discrepancies leads to the fact that the BER expressions developed in this paper need to be further modified to include the effect of system-specific features, e.g. DFT-precoding for SC-FDMA.

The remainder of this chapter is organized as follows. Section 3.2 describes the stochastic channel model for Rayleigh fading. Section 3.3 details the derivations of BER in Rayleigh slow-fading Channel using PSACE for BPSK/QPSK/16-QAM modulations. Section 3.4 has the derivations of BER for piecewise-linear interpolation in time/frequency domain with application to OFDMA and SC-FDMA with and without pilot-jamming attack. This section also includes the simplified expressions of BPSK/QPSK with optimum Wiener interpolation. Section 3.5 presents the executive summary of the derivations of BER. Section 3.6 provides the details of the simulations and the simulation results. Section 3.7 ends the chapter with concluding remarks.

Notation

The superscript $(\cdot)^*$ denotes complex conjugate of the variable. $\Re(\cdot)$ denotes the real part and $\Im(\cdot)$ denotes the imaginary part of a variable.

3.2 Stochastic Channel Model for Rayleigh Fading

The cellular wideband channel can be modeled by a tapped delay line as shown in Figure 3.1 to represent a set of discrete resolvable multipath components originated by scattering and reflections from smaller structures [27], [28]. Each channel tap is the superposition of a

large number of scattered plane waves that arrive with approximately the same delay and cause the channel taps to undergo fading. In this chapter, the overall wireless channel is assumed to be discrete multipath fading channel and modeled by a linear time-variant FIR filter having the complex low-pass impulse response

$$h(t,\tau) = \sum_{i=0}^{M-1} C_i e^{j\phi_i(t)} \delta(\tau - \tau_i(t)) \tag{3.1}$$

where C_i, $\phi_i(t)$, $\tau_i(t)$ are respectively the amplitude, time-variant phase, and time-variant delay associated with the i^{th} propagation path with M denoting the total number of propagation paths. Time-variant phase $\phi_i(t)$ is given by

$$\phi_i(t) = \phi_i - 2\pi c\tau_i(t)/\lambda_c + 2\pi f_{D,i} t \tag{3.2}$$

where ϕ_i and $f_{D,i}$ are the phase and Doppler shift, respectively, associated with multipath i. C_i is dependent on the cross-sectional area of the i^{th} reflecting surface or the length of the i^{th} diffraction edge. The phase ϕ_i is randomly introduced by the i^{th} scatterer and can be assumed to be uniformly distributed on $[-\pi, \pi)$. Assuming that the delay values vary very slowly, the above two equations reduce to the following

$$\begin{aligned}
\phi_i(t) &= \phi_i - 2\pi c\tau_i/\lambda_c + 2\pi f_{D,i} t && (3.3)\\
h(t,\tau) &= \sum_{i=0}^{M-1} C_i e^{j\phi_i(t)} \delta(\tau - \tau_i) && (3.4)\\
&= \sum_{i=0}^{M-1} c_i(t)\delta(\tau - \tau_i) \\
&= h_I(t,\tau) + j h_Q(t,\tau). && (3.5)
\end{aligned}$$

For sufficiently large M, by Central Limit Theorem, $h(t,\tau)$ is a complex Gaussian random process in the t variable. For some types of scattering, e.g. 2-D isotropic scattering with the absence of specular components, $h_I(t,\tau)$ and $h_Q(t,\tau)$ at any time t_1 are independent

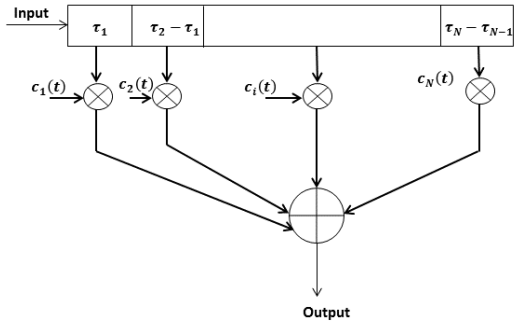


Figure 3.1: Tapped-delay-line channel model with variable tap spacings that emulates a set of discrete resolvable multipath components with variable gains and delays. This model applies to rapidly changing environments.

and identically distributed (i.i.d.) Gaussian random variables with zero mean and variance $= E[{h_I}^2(t_1, \tau)] = E[{h_Q}^2(t_1, \tau)]$. Under these conditions, the envelope of the channel response at any time instant t_1, as given by

$$\alpha = |h(t_1, \tau)| = \sqrt{{h_I}^2(t_1, \tau) + {h_Q}^2(t_1, \tau)} \tag{3.6}$$

is Rayleigh distributed. The time-varying frequency response of the channel is thus given by

$$H(t, f) = \int_{-\infty}^{\infty} h(t, \tau) e^{-j2\pi f \tau} d\tau \tag{3.7}$$

$$= \sum_{i=0}^{M-1} C_i e^{j\phi_i(t)} e^{-j2\pi f \tau_i}. \tag{3.8}$$

In the time-frequency (symbol-subcarrier) grid of a system, the channel frequency response at the n^{th} tone of the m^{th} symbol becomes as follows

$$H[m, n] = H[m\Delta t, n\Delta f] \tag{3.9}$$

$$= \sum_{i=0}^{M-1} C_i e^{j\phi_i(m\Delta t)} e^{-j2\pi n \Delta f \tau_i} \tag{3.10}$$

where Δt and Δf are the symbol duration and subcarrier spacing of the system respectively. In most radio transmission media, the attenuation and phase shift associated with path delay τ_1 are uncorrelated with those associated with path delay τ_2. Under this assumption of uncorrelated scattering and further assuming that the channel is wide-sense-stationary, the channel's spaced-time spaced-frequency correlation function is separable into the product of the spaced-time (spaced-symbol) correlation function and the spaced-frequency (spaced-subcarrier) correlation function as follows

$$\begin{aligned} R[k,l] &= E[H[m+k,n+l]H^*[m,n]] && (3.11)\\ &= {\sigma_H}^2 R_t[k]R_f[l] && (3.12) \end{aligned}$$

where the channel transfer factor's variance, ${\sigma_H}^2$ is given by

$${\sigma_H}^2 = R[0,0] = \sum_{i=0}^{M-1} {\sigma_{h,i}}^2 \qquad (3.13)$$

and ${\sigma_{h,i}}^2$ is the i^{th} Channel Impulse Response (CIR) tap's variance. The spaced-time correlation function depends on the maximum Doppler frequency f_d of the channel as given by widely used Jakes' model [29]

$$\begin{aligned} R_t[k] &= J_0(2\pi k f_d T_{sym}) && (3.14)\\ &= J_0(2\pi k F_d) \\ \text{where, } f_d &= v f_c/c \\ F_d &= f_d T_{sym}. \end{aligned}$$

Here T_{sym}, v, f_c, c, F_d are the symbol duration, relative speed between the transmitter and the receiver, the carrier frequency, the speed of light, and symbol normalized maximum Doppler frequency respectively. $J_0[.]$ is the zeroth-order Bessel function of the first kind.

Corresponding Doppler Power Spectrum (DPS) is given by [29]

$$DPS = \begin{cases} \frac{1}{\pi f_d} \frac{1}{\sqrt{1-(f/f_d)^2}}, (|f| \leq f_d) \\ 0, (|f| > f_d)\,. \end{cases} \tag{3.15}$$

The Jakes' Doppler spectrum follows from the assumptions of horizontal propagation of radio waves, uniform distribution of the angles of arrival at the receiver over $[-\pi, \pi]$, and the omnidirectional antenna pattern. For sampling interval T_s, a total of M tones, and Root Mean Square (RMS) delay-spread $\tilde{\tau}_{rms}$, an exponentially decaying normalized multipath Power Delay Profile (PDP) can be written as

$$PDP = e^{-\frac{\tau M}{\tau_{rms}}} \tag{3.16}$$

$$\text{where, } \tau_{rms} = \tilde{\tau}_{rms}/T_s$$

and for this PDP the normalized spaced-frequency correlation function is as follows [26]

$$R_f[l] = \frac{1}{1 + j2\pi\tau_{rms}l/M}. \tag{3.17}$$

Equations (3.14) and (3.15) as well as (3.16) and (3.17) are Fourier transform pairs under very specific circumstances which is known as wide-sense-stationary uncorrelated scattering (WSSUS) channel conditions [30], [31]. Although, we used these specific PDP, DPS and their associated correlation functions here, the analysis is not limited to them. Rather the analysis applies to any PDP, any DPS and their corresponding Fourier transform correlation functions under WSSUS assumptions.

3.3 BER in Rayleigh Slow-Fading Channel for PSACE with BPSK/QPSK/16-QAM

In multicarrier communication systems that transmit binary information over the Additive White Gaussian Noise (AWGN) channel, the decision statistic for a specific decision boundary at the detector for a particular carrier can be expressed in a general quadratic form [29]

$$D = A|Y_1|^2 + B|Y_2|^2 + CY_1Y_2^* + C^*Y_1^*Y_2 \tag{3.18}$$

where Y_1 and Y_2 are a pair of correlated complex-valued Gaussian random variables. A, B, and C are constants. Such pairs of random variables for different carriers are mutually statistically independent and identically distributed. The probability of error is the probability that $D < 0$ and is given by [29]

$$P_s = Q_1(a,b) - \frac{v_2/v_1}{1+v_2/v_1} I_0(ab)\exp\left[-\frac{1}{2}\left(a^2+b^2\right)\right] \tag{3.19}$$

where $Q_1(a,b)$ is Marcum's Q-function and $I_0(.)$ is zeroth-order modified Bessel function of the first kind. a, b are given by [29]

$$a = \sqrt{\frac{2v_1^2v_2(\alpha_1v_2-\alpha_2)}{(v_1+v_2)^2}} \tag{3.20}$$

$$b = \sqrt{\frac{2v_2^2v_1(\alpha_1v_1+\alpha_2)}{(v_1+v_2)^2}}. \tag{3.21}$$

The parameters v_1, v_2, α_1, and α_2 are related to the means $m_1 = \overline{Y_1}$, $m_2 = \overline{Y_2}$ and the second central moments μ_{12}, μ_{11}, μ_{22} of the complex-valued Gaussian variables Y_1, Y_2 in the

following way assuming $\left(|C|^2 - AB\right) = F > 0$ [29]

$$\begin{aligned}
v_1 &= \sqrt{w^2 + \frac{1}{4\left(\mu_{11}\mu_{22} - |\mu_{12}|^2\right)F}} - w \\
v_2 &= \sqrt{w^2 + \frac{1}{4\left(\mu_{11}\mu_{22} - |\mu_{12}|^2\right)F}} + w \\
w &= \frac{A\mu_{11} + B\mu_{22} + C\mu_{12}^* + C^*\mu_{12}}{4\left(\mu_{11}\mu_{22} - |\mu_{12}|^2\right)F} \\
\alpha_1 &= 2F\left(|m_1|^2\mu_{22} + |m_2|^2\mu_{11} - m_1^* m_2 \mu_{12}\right) \\
&- 2F\left(m_1 m_2^* \mu_{12}^*\right) \\
\alpha_2 &= A|m_1|^2 + B|m_2|^2 + Cm_1 m_2^* + C^* m_1^* m_2 \\
\mu_{12} &= \frac{1}{2}E\left[\left(Y_1 - m_1\right)\left(Y_2 - m_2\right)^*\right].
\end{aligned} \tag{3.22}$$

In a Rayleigh process the averages vanish

$$m_1 = m_2 = 0$$

$$\alpha_1 = \alpha_2 = 0$$

$$a = b = 0.$$

With these values Marcum's Q-function and modified Bessel function become as follows

$$\begin{aligned}
Q_1(a,b) &= \int_b^\infty (x)\, exp\left[-\frac{1}{2}\left(x^2 + b^2\right)\right] I_0(ax)\, dx \\
\Rightarrow Q_1(0,0) &= 1 \\
I_0(0) &= 1.
\end{aligned}$$

Finally the probability of error becomes

$$P_s = \frac{1}{1 + v_2/v_1}. \tag{3.23}$$

Rayleigh fading additive Gaussian noise channel corrupts the signaling waveforms by adding AWGN and multiplying the transmitted signal by a random gain and phase shift. From the perspective of the signal constellation, the multiplicative factor introduced by fading basically scales and rotates the signal constellation as shown in Figure 3.2. The receiver attempts to compensate by scaling and rotating the decision boundaries by multiplying the matched filter output with the complex conjugate of channel estimate. For a particular tone n of the m^{th} symbol, this is accomplished by multiplying the demodulator output $Z_{m,n}$ by the complex conjugate of an estimate of the channel $\widehat{H}^*_{m,n}$ and the decision statistic is given by

$$D_{m,n} = \Re\left\{Z_{m,n}\widehat{H}^*_{m,n}\right\}. \tag{3.24}$$

With multicarrier PSACE, a subset of the available subcarriers or symbols is dedicated to the transmission of specific pilots known to the receiver, which are used for sampling the channel transfer function. Based on these samples, the well-known process of interpolation is used to generate channel transfer factors estimate for each subcarrier or symbol between the pilots. For a noise sample $N_{m,n}$ normalized by pilot, the channel estimate of a particular tone n of the m^{th} symbol can be represented as

$$\widehat{H}_{m,n} = H_{m,n} + N_{m,n}. \tag{3.25}$$

For Rayleigh slow-fading channel, the complex numbers $\{H_{m,n}\}$ are mutually statistically independent and identically distributed zero-mean Gaussian random variables. Consequently, although $\widehat{H}_{m,n}$, $Z_{m,n}$ are correlated, complex-valued, zero-mean, Gaussian random variables, the pairs $\left\{\widehat{H}_{m,n},\, Z_{m,n}\right\}$ are statistically independent but identically distributed with each other. The decision statistic from (3.24) can be written as

$$D_{m,n} = \underbrace{\left|\frac{Z_{m,n} + \widehat{H}_{m,n}}{2}\right|^2}_{|Y_1|^2} - \underbrace{\left|\frac{Z_{m,n} - \widehat{H}_{m,n}}{2}\right|^2}_{|Y_2|^2}. \tag{3.26}$$

Since $\left(\widehat{H}_{m,n},\, Z_{m,n}\right)$ are correlated, complex-valued, zero-mean, Gaussian, Y variables are also correlated, complex-valued, zero-mean, Gaussian random variables. Comparing this decision statistic with (3.18), we get the following values for A, B, and C:

$$A = 1, B = -1, C = 0.$$

Substituting these values into (22) and using the values of v_1, v_2 thus obtained in (3.23), we get

$$P_s = \frac{1}{2}\left\{1 - \sqrt{\frac{\left(\mu_{11} - \mu_{22}\right)^2}{\left(\mu_{11} + \mu_{22}\right)^2 - 4\left(\left|\mu_{12}\right|^2\right)}}\right\}. \tag{3.27}$$

If we express the Y variables in terms of $H_{m,n}$, $Z_{m,n}$, for the n^{th} tone of the m^{th} symbol, (3.27) can be rewritten as

$$P_s\left(m,n\right) = \frac{1}{2}\left(1 - \sqrt{\frac{\left[\Re\left\{\mu\left(m,n\right)\right\}\right]^2}{1 - \left[\Im\left\{\mu\left(m,n\right)\right\}\right]^2}}\right) \tag{3.28}$$

where the cross-correlation coefficient $\mu\left(m,n\right)$ is given by [29]

$$\mu\left(m,n\right) = \frac{E[Z_{m,n}\widehat{H}^*_{m,n}]}{\sqrt{E[|Z_{m,n}|^2]E[|\widehat{H}_{m,n}|^2]}}. \tag{3.29}$$

The expression for the probability of error for a specific decision criterion corresponding to the specific decision boundary depends on a single parameter: the cross-correlation coefficient $\mu\left(m,n\right)$. As this is the probability of decision error, it is actually the SER not BER. Assuming Gray coding where the nearest neighboring symbols differ in only one bit position, symbol errors correspond to single bit errors. In that case,

$$P_b \approx \frac{P_s}{\log_2 s}$$

where $s =$ number of bits in a symbol.

3.3.1 BER for BPSK

For BPSK there is only one decision boundary in the signal constellation. The probability of error is thus the probability that

$$\Re\left\{Z_{m,n}\widehat{H}^{*}_{m,n}\right\} < 0. \tag{3.30}$$

Let us assume that the fading distortion has unity power, i.e. $E[|H_{m,n}|^2] = 1$ and ϵ is the energy per signal waveform. Further assuming without loss of generality that the transmitted signal phase is zero, the symbol-spaced samples at the output of the filter matched to the transmitted pulse $g(t)$ are given by

$$\begin{aligned} Z_{m,n} &= 2\epsilon H_{m,n}X_{m,n} + V_{m,n} \\ &= \epsilon_g H_{m,n}X_{m,n} + V_{m,n} \end{aligned} \tag{3.31}$$

where $X_{m,n}$ is the transmitted symbol for BPSK which is ± 1, i.e. $|X_{m,n}|^2 = 1$, $H_{m,n}$ is the current transfer function of channel at the n^{th} tone of the m^{th} symbol, $V_{m,n}$ is the i.i.d. zero-mean Gaussian random variable with variance σ^2, and ϵ_g is the energy in the transmitted pulse. At the output of matched filter, the variance σ^2 is equal to the Power Spectral Density (PSD) N_o. Exploiting the above assumptions, the fact that AWGN is uncorrelated to the channel transfer factor, and further assuming that $2\epsilon = \epsilon_g = 1$, the numerator and the factors of the denominator of the cross-correlation coefficient are given by

$$E[Z_{m,n}\widehat{H}^{*}_{m,n}] = 2\epsilon X_{m,n}\left\{1 - E[H_{m,n}\Delta H^{*}_{m,n}]\right\} \tag{3.32}$$

$$= X_{m,n}E[H_{m,n}\widehat{H}^{*}_{m,n}] \tag{3.33}$$

$$\widehat{H}_{m,n} = H_{m,n} - \Delta H_{m,n} \tag{3.34}$$

$$E[|Z_{m,n}|^2] = 4\epsilon^2|X_{m,n}|^2 + N_o \tag{3.35}$$

$$= 1 + N_o \tag{3.36}$$

$$E[|\widehat{H}_{m,n}|^2] = 1 - 2\Re\left\{E[H_{m,n}\Delta H^*_{m,n}]\right\} + \sigma^2_{m,n} \tag{3.37}$$

where channel estimation error variance is as follows

$$\sigma^2_{m,n} = E[|\Delta H_{m,n}|^2]. \tag{3.38}$$

Substituting these values into (3.29), we get the expression of the cross-correlation coefficient for BPSK, $\mu_{s2}(m,n)$ as follows

$$\begin{aligned} \mu_{s2}(m,n) &= \frac{X_{m,n}T}{\sqrt{(1+N_o)}} \\ &= \frac{X_{m,n}T}{\sqrt{\left(1+\frac{1}{SNR}\right)}} \\ \text{where, } T &= \frac{\left(1 - E\left[H_{m,n}\Delta H^*_{m,n}\right]\right)}{\sqrt{\left(1 - 2\Re\left\{E\left[H_{m,n}\Delta H^*_{m,n}\right]\right\} + \sigma^2_{m,n}\right)}} \\ \text{and } SNR &= \frac{E_s}{N_o} = \frac{1}{N_o}. \end{aligned} \tag{3.39}$$

As there is only one bit per symbol in BPSK, replacing the above value of the coefficient into (3.28) gives the BER expression for BPSK in Rayleigh slow-fading channel with channel estimation error.

3.3.2 BER for QPSK

For $\pi/4$-QPSK, symbols are, $X_{m,n} = \pm\frac{1}{\sqrt{2}} \pm j\frac{1}{\sqrt{2}}$. So, $|X_{m,n}|^2 = 1$ and $SNR = \frac{E_s}{N_o} = \frac{1}{N_o}$. Here each symbol cell has two decision boundaries. For $X_{m,n} = \frac{1}{\sqrt{2}} + j\frac{1}{\sqrt{2}}$ the decision criteria are

$$\Re\left[Z_{m,n}\widehat{H}^*_{m,n}\right] < 0 \tag{3.40}$$

$$\Im\left[Z_{m,n}\widehat{H}^{*}_{m,n}\right] < 0 \tag{3.41}$$

$$\Re\left[-jZ_{m,n}\widehat{H}^{*}_{m,n}\right] < 0 \tag{3.42}$$

where $\Im[.]$ is replaced with $\Re[-j]$ for simplicity. For (40) the coefficient is given by

$$\mu^{1}_{s4}(m,n) = \frac{X_{m,n}T}{\sqrt{\left(1+\frac{1}{snr}\right)}}. \tag{3.43}$$

For (3.42) the coefficient is given by

$$\mu^{2}_{s4}(m,n) = -j\mu^{1}_{s4}(m,n). \tag{3.44}$$

There are four quadrants in a QPSK signal constellation which are equally likely. Consequently, the symbol error probability and the corresponding bit error probability (assuming Gray coding) are respectively given by

$$P_{s4} = P_s\left(\mu^{1}_{s4}(m,n)\right) + P_s\left(\mu^{2}_{s4}(m,n)\right) \tag{3.45}$$

$$P_{b4} \approx \frac{P_{s4}}{2}. \tag{3.46}$$

3.3.3 BER for QAM

Rectangular QAM signal constellations are considered in this paper due to its distinct advantage of being easily generated as two PAM signals in phase-quadrature. For QAM we have found an upper and lower bounds of BER following Cavers' [24] approach. In 16-QAM, the real and imaginary parts of the symbols take on the values $-3, -1, 1, 3$ and the expected value $E\left[|X_{m,n}|^2\right] = 10$. Before fading the six decision boundaries are

$$\Re[Z_{m,n}] \;=\; 0$$

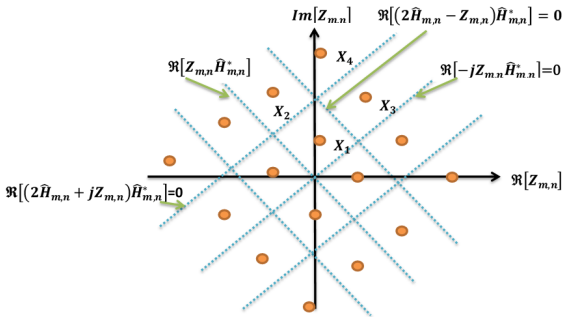


Figure 3.2: 16-QAM decision boundaries after channel fading has scaled and rotated the signal constellation. This distortion is compensated at the receiver by multiplying the demodulator output by the complex conjugate of the channel estimate.

$$\begin{aligned} \Im\left[Z_{m,n}\right] &= 0 \\ \Re\left[Z_{m,n} \pm 2\right] &= 0 \\ \Im\left[Z_{m,n} \pm 2j\right] &= 0. \end{aligned} \tag{3.47}$$

Fading scales and rotates the signal constellation and the six decision boundaries become as follows

$$\begin{aligned} \Re\left[Z_{m,n}\widehat{H}^*_{m,n}\right] &= 0 \\ \Re\left[-jZ_{m,n}\widehat{H}^*_{m,n}\right] &= 0 \\ \Re\left[\left(Z_{m,n} \pm 2\widehat{H}_{m,n}\right)\widehat{H}^*_{m,n}\right] &= 0 \\ \Re\left[\left(-jZ_{m,n} \pm 2\widehat{H}_{m,n}\right)\widehat{H}^*_{m,n}\right] &= 0. \end{aligned} \tag{3.48}$$

From Figure 3.2, there are four different types of cell: $X_1 = 1 + j1$ (interior cell), $X_2 = 1 + j3$ (edge cell type 1), $X_3 = 3 + j1$ (edge cell type 2), $X_4 = 3 + j3$ (corner cell). For interior cells, an error occurs if any of the following is true

$$\Re\left[Z_{m,n}\widehat{H}^*_{m,n}\right] < 0 \tag{3.49}$$

$$\Re\left[-jZ_{m,n}\widehat{H}^*_{m,n}\right] < 0 \tag{3.50}$$

$$\Re\left[\left(2\widehat{H}_{m,n} - Z_{m,n}\right)\widehat{H}^{*}_{m,n}\right] < 0 \tag{3.51}$$

$$\Re\left[\left(jZ_{m,n} + 2\widehat{H}_{m,n}\right)\widehat{H}^{*}_{m,n}\right] < 0. \tag{3.52}$$

The cross-correlation coefficients for (3.49)-(3.52) are respectively given by

$$\mu_{Q11}(m,n) = \frac{Q}{\sqrt{RP}} \tag{3.53}$$

$$\mu_{Q12}(m,n) = -j\mu_{Q1}(m,n) \tag{3.54}$$

$$\begin{aligned}\mu_{Q13}(m,n) &= \frac{E\left[\left(2\widehat{H}_{m,n} - Z_{m,n}\right)\widehat{H}^{*}_{m,n}\right]}{\sqrt{E\left[\left|2\widehat{H}_{m,n} - Z_{m,n}\right|^2\right]E\left[\left|\widehat{H}_{m,n}\right|^2\right]}} \\ &= \frac{2P - Q}{\sqrt{\left[4P - 4\Re\{Q\} + R\right]P}}\end{aligned} \tag{3.55}$$

$$\begin{aligned}\mu_{Q14}(m,n) &= \frac{E\left[\left(2\widehat{H}_{m,n} + jZ_{m,n}\right)\widehat{H}^{*}_{m,n}\right]}{\sqrt{E\left[\left|2\widehat{H}_{m,n} + jZ_{m,n}\right|^2\right]E\left[\left|\widehat{H}_{m,n}\right|^2\right]}} \\ &= \frac{2P + jQ}{\sqrt{\left[4P - 4\Im\{Q\} + R\right]P}}\end{aligned} \tag{3.56}$$

assuming $P = E\left[\left|\widehat{H}_{m,n}\right|^2\right]$, $Q = E\left[Z_{m,n}\widehat{H}^{*}_{m,n}\right]$, and $R = E\left[|Z_{m,n}|^2\right]$. A notable point is $|X_{m,n}|^2 \neq 1$, i.e. $SNR = \frac{E_s}{N_o} \neq \frac{1}{N_o}$ for QAM as was true for PSK modulations considered in subsections (3.3.1) and (3.3.2). Rather for 16-QAM, SNR is as follows

$$SNR = \frac{E_s}{N_o} = \frac{\text{average symbol energy}}{N_o} = \frac{10}{N_o}. \tag{3.57}$$

A close approximation to the error rate for symbol X_1 is obtained using the union bound

$$P_{X_1} \leq \sum_{u=1}^{4} P_{sQ}\left(\mu_{Q1u}\right).$$

Similar calculation could be carried out for the other three types of cell. Assuming,

$$\begin{aligned} P &= E\left[\left|\widehat{H}_{m,n}\right|^2\right] \\ &= 1 - 2\Re\left\{E[H_{m,n}\Delta H^*_{m,n}]\right\} + \sigma^2_{m,n} \\ Q_i &= E\left[Z_{m,n}\widehat{H}^*_{m,n}\right] \\ &= X_i\left\{1 - E[H_{m,n}\Delta H^*_{m,n}]\right\} \\ R_i &= E\left[|Z_{m,n}|^2\right] \\ &= |X_i|^2 + N_o \end{aligned} \tag{3.58}$$

where $i = 1, 2, \cdots, 4$ is the index of different types of cell, the cross-correlation coefficients are listed below

$X_1 = 1 + j1$ **(interior cell)**

$$\begin{aligned} \mu_{Q11} &= \frac{Q_1}{\sqrt{R_1 P}} \\ \mu_{Q12} &= \frac{-jQ_1}{\sqrt{R_1 P}} \\ \mu_{Q13} &= \frac{2P - Q_1}{\sqrt{\left[4P - 4\Re\left\{Q_1\right\} + R_1\right]P}} \\ \mu_{Q14} &= \frac{2P + jQ_1}{\sqrt{\left[4P - 4\Im\left\{Q_1\right\} + R_1\right]P}} \end{aligned} \tag{3.59}$$

$X_2 = 1 + j3$ **(edge cell type 1)**

$$\begin{aligned}
\mu_{Q21} &= \frac{Q_2}{\sqrt{R_2 P}} \\
\mu_{Q22} &= \frac{2P - Q_2}{\sqrt{\left[4P - 4\Re\left\{Q_2\right\} + R_2\right] P}} \\
\mu_{Q23} &= \frac{-2P - jQ_2}{\sqrt{\left[4P - 4\Im\left\{Q_2\right\} + R_2\right] P}}
\end{aligned} \tag{3.60}$$

$X_3 = 3 + j1$ **(edge cell type 2)**

$$\begin{aligned}
\mu_{Q31} &= \frac{-jQ_3}{\sqrt{R_3 P}} \\
\mu_{Q32} &= \frac{-2P + Q_3}{\sqrt{\left[4P - 4\Re\left\{Q_3\right\} + R_3\right] P}} \\
\mu_{Q33} &= \frac{2P + jQ_3}{\sqrt{\left[4P - 4\Im\left\{Q_3\right\} + R_3\right] P}}
\end{aligned} \tag{3.61}$$

$X_4 = 3 + j3$ **(corner cell)**

$$\begin{aligned}
\mu_{Q41} &= \frac{-2P + Q_4}{\sqrt{\left[4P - 4\Re\left\{Q_4\right\} + R_4\right] P}} \\
\mu_{Q42} &= \frac{-2P - jQ_4}{\sqrt{\left[4P - 4\Im\left\{Q_4\right\} + R_4\right] P}}
\end{aligned} \tag{3.62}$$

All the variables are for a particular tone in a specific symbol. As the four types of the cells are equally likely, the final calculation for the SER is as follows

$$P_{sQ}^{16} \leq \frac{1}{4}\sum_{i=1}^{4} P_{X_i}. \tag{3.63}$$

As for corresponding BER, we know that bit error probability is bounded as follows [32]

$$\frac{P_s}{\log_2 s} \leq P_b \leq P_s. \tag{3.64}$$

So for 16-QAM BER is given by

$$\frac{P_{sQ}^{16}}{\log_2 s} \leq P_{bQ}^{16} \leq P_{sQ}^{16}. \tag{3.65}$$

For Gray coding $P_{bQ}^{16} \approx \frac{P_{sQ}^{16}}{\log_2 s}$. Consequently, simulated BER would be much closer to the lower bound. For larger constellations like 64-QAM, the approach adopted above become tedious. In that case, upper bounding the overall BER by the BER of the worst cell - is an attractive alternative. The cell should be the one with the highest error rate which is the interior corner cell farthest from the origin [24].

3.4 BER for Piecewise-linear Interpolation in Time or Frequency Domains with and without Pilot-jamming attacks

This section details the derivations of cross-correlation coefficients in terms of correlation functions of the Rayleigh-faded channel for piecewise-linear interpolation either in time or frequency domain for ZF equalization with and without pilot-jamming attacks. Although

both the frequency and time domain linear interpolations apply to either OFDMA or SC-FDMA, we have explained frequency and time domain interpolations with application to OFDMA and SC-FDMA respectively. This choice is based on two motivations. First of all, we wanted to investigate the applicability of the developed theorems to as many diverse contemporary systems as possible. Second reason is founded on the differences in signal structure of OFDMA and SC-FDMA. As obvious from Figure 3.5 [33], in an OFDMA signal each subcarrier carries one modulated symbol for the entire duration of the OFDMA symbol whereas, in a SC-FDMA signal each modulated symbol occupies the entire bandwidth for its allocated part of the duration of a SC-FDMA symbol. Consequently, if we assume that an OFDMA symbol is passed through a frequency-selective static channel where the subcarrier bandwidth is less than the channel coherence bandwidth and channel is time-invariant over the duration of an OFDMA symbol, it would be an ideal case for the application of piecewise-linear interpolation with ZF equalization in frequency direction. On the other hand, if we assume that a SC-FDMA symbol is transmitted through a time-selective frequency-flat channel where the channel is time-variant within a SC-FDMA symbol, it would be a suitable case for the application of piecewise-linear interpolation with ZF equalization in time direction.

After incorporating the effects of ZF equalization into the BER expressions, the equations have been further modified to take into consideration the adverse effects of pilot-jamming attacks [34]. Pilot-jamming is one of the sophisticated correlated jamming attacks where adversaries exploit *a priori* knowledge about the targets to tailor jamming [35]. They are efficient as well as effective to the extent that they can cause complete denial of communications. Among the different kinds of correlated jamming attacks available in literature, e.g., synchronization attacks [36–38], equalization attacks [39,40] and control channel attacks [35], we have considered one of the equalization attacks in this paper, the pilot-jamming attack. In pilot-jamming attack as shown in Figure 3.3, the jammer with malicious intent attempts to raise the noise floor of the target's pilot tones or symbols by transmitting AWGN signal

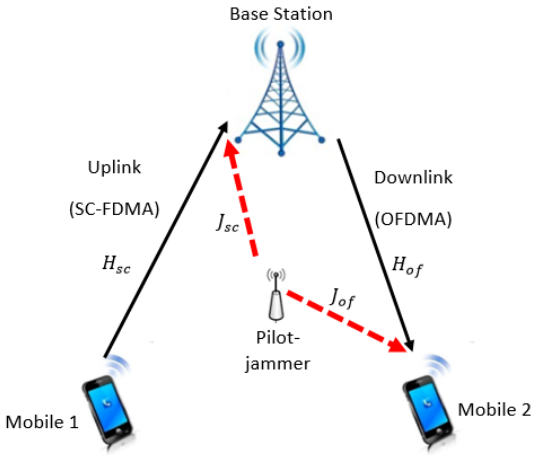


Figure 3.3: Pilot-jamming attacks on SC-FDMA (uplink) and OFDMA (downlink) of LTE cellular system. H_{sc} and H_{of} denote the channels between the transceivers of SC-FDMA and OFDMA respectively. J_{sc} and J_{of} represent the channels between the jammer and the target for SC-FDMA and OFDMA respectively.

on the pilot subcarriers or symbols respectively. It has been assumed that the jammer has *a priori* knowledge about the pilot subcarriers or symbols and is in synchronization with the target. The jammer also knows the associated channel state information (CSI). In Figure 3.3, H_{sc}, J_{sc}, H_{of}, and J_{of} are respectively the channel between SC-FDMA transceiver, channel between jammer and SC-FDMA receiver (the base station), the channel between OFDMA transceiver, channel between jammer and OFDMA receiver (the mobile 2).

3.4.1 BER for OFDMA without and with Pilot-Jamming Attack

For OFDMA, it is assumed that the bandwidth of the equally-spaced subcarriers is less than the channel coherence bandwidth. As a result, although the overall channel is frequency-selective, channel for each subcarrier is frequency-flat. We have also assumed that the channel remains static over an OFDMA symbol. Consequently, the multiplicative factor introduced by each of the M frequency-flat slowly faded Rayleigh sub-channel is given by

$$h = \alpha e^{j\phi} \tag{3.66}$$

where α is Rayleigh distributed and ϕ is uniformly distributed over $-\pi$ to π.

The channel estimation is carried out by piecewise-linear interpolation in frequency, i.e. subcarrier domain as shown in Figure 3.4. The demodulated data symbol for the n^{th} tone of any OFDMA symbol can be written as

$$Z_n = H_n X_n + V_n. \tag{3.67}$$

At pilot location n_j, where $1 \leq j \leq J$ with J as the total number of pilots in an OFDMA symbol, channel estimation is performed using 1-tap equalization

$$\widehat{H}_{n_j} = \frac{Z_{n_j}}{X_{n_j}} = H_{n_j} + \widetilde{V}_{n_j} \tag{3.68}$$

where X_{n_j} is a known symbol at the pilot location and $\widetilde{V}_{n_j}$ is the AWGN normalized by the pilot symbol. In a uniformly-spaced pilot arrangement, for two adjacent pilot tone locations n_1, n_2, the channel estimates are

$$\widehat{H}_{n_1} = H_{n_1} + \widetilde{V}_{n_1} \tag{3.69}$$

$$\widehat{H}_{n_2} = H_{n_2} + \widetilde{V}_{n_2}. \tag{3.70}$$

By interpolation, for any tone n where $n_1 \leq n \leq n_2$

$$\begin{aligned} \widehat{H}_n &= a_n \widehat{H}_{n_1} + b_n \widehat{H}_{n_2} \\ a_n &= \frac{n_2 - n}{n_2 - n_1} \\ b_n &= 1 - a_n. \end{aligned} \tag{3.71}$$

Channel estimation error is as follows

$$\Delta H_n = H_n - \widehat{H}_n \tag{3.72}$$

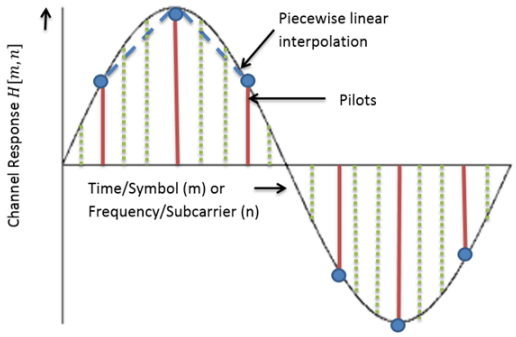


Figure 3.4: Piecewise-linear interpolation in time/symbol or frequency/subcarrier domains. Channel frequency response is sampled by uniformly-spaced pilots and the channel transfer factors between the pilots are estimated by piecewise-linear interpolation between the adjacent pilots.

$$= \quad H_n - a_n H_{n_1} - b_n H_{n_2} - a_n \widetilde{V}_{n_1} - b_n \widetilde{V}_{n_2} \tag{3.73}$$

As the channel impulse response $h(t, \tau)$ is modeled as a complex-valued zero-mean Gaussian random process in the t variable, $H(t, f)$, i.e. H_n for the OFDMA case, has the same statistics. Mean and variance of the error are given by

$$E[\Delta H_n] = 0 \tag{3.74}$$

$$\sigma_n^2 = E[|\Delta H_n|^2] - \{E[\Delta H_n]\}^2 \tag{3.75}$$

$$= E[|\Delta H_n|^2]$$

$$= E[\Delta H_n \Delta H_n^*]. \tag{3.76}$$

Substituting the value from (3.73) into (3.76) and exploiting the facts that AWGN is uncorrelated to the channel transfer factor and AWGN components themselves are uncorrelated, the expression of variance [26] becomes as shown in (3.77), where $R_f(l) = E[H_{n+l} H_n^*]$ and it is symmetric with $R_f(-l) = R_f(l)^*$. Moreover, $L = (n_2 - n_1) =$ pilot tone spacing, and $l = (n - n_1)$. To satisfy Nyquist theorem, $L \leq \lfloor M/M_o \rfloor$ where M_o is the multipath spread as a multiple of the sampling interval T_s. For BPSK or $\pi/4$-QPSK, $|X_{n_1}|^2 = |X_{n_2}|^2 = 1$ but

$$\begin{aligned}\sigma_n^2 &= R_f(0)(1+a_n^2+b_n^2)+\frac{a_n^2 N_o}{|X_{n_1}|^2}+\frac{b_n^2 N_o}{|X_{n_2}|^2}-2a_n\Re\{R_f(l)\}-2b_n\Re\{R_f(L-l)\} \\ &+ 2a_n b_n\Re\{R_f(L)\} \qquad (3.77)\\ \sigma_{n,j}^2 &= R_f(0)(1+a_n^2+b_n^2)-2a_n\Re\{R_f(l)\}+\left(\frac{a_n^2}{|X_{n_1}|^2}+\frac{b_n^2}{|X_{n_2}|^2}\right)(N_o+N_j\rho) \\ &- 2b_n\Re\{R_f(L-l)\}+2a_n b_n\Re\{R_f(L)\} \qquad (3.78)\end{aligned}$$

for QAM they might be different. Using the value from (3.73) we get

$$E[H_n\Delta H_n^*]=R_f(0)-a_n\{R_f(l)\}-b_n\left\{R_f^*(L-l)\right\}. \qquad (3.79)$$

Substituting the value from (3.79) into (3.39), and (3.43), and further assuming that $a_n\{R_f(l)\}+b_n\left\{R_f^*(L-l)\right\}=z_n$, we get the correlation coefficients for the n^{th} tone without jamming for BPSK and $\pi/4$-QPSK respectively

$$\begin{aligned}\mu_{s2}(n) &= \frac{X_n}{\sqrt{\frac{(1+\frac{1}{SNR})(2\Re\{z_n\}+\sigma_n^2-1)}{(z_n)^2}}} \qquad (3.80)\\ &= \frac{\pm 1}{\sqrt{\frac{(1+\frac{1}{SNR})(2\Re\{z_n\}+\sigma_n^2-1)}{(z_n)^2}}} \\ \mu_{s4}^1(n) &= \frac{X_n}{\sqrt{\frac{\left(1+\frac{1}{SNR}\right)(2\Re\{z_n\}+\sigma_n^2-1)}{(z_n)^2}}} \qquad (3.81)\\ &= \frac{\pm\frac{1}{\sqrt{2}}\pm j\frac{1}{\sqrt{2}}}{\sqrt{\frac{\left(1+\frac{1}{SNR}\right)(2\Re\{z_n\}+\sigma_n^2-1)}{(z_n)^2}}}.\end{aligned}$$

For 16-QAM the different parameters for a particular tone n of an OFDMA symbol without jamming are as follows

$$\begin{aligned}P_n &= E\left[\left|\widehat{H}_n\right|^2\right] \\ &= 1-2\Re\{E[H_n\Delta H_n^*]\}+\sigma_n^2\end{aligned}$$

$$= 2\Re\{z_n\} + \sigma_n^2 - 1 \tag{3.82}$$

$$\begin{aligned} Q_{in} &= E\left[Z_n \widehat{H}_n^*\right] \\ &= X_i\{1 - E[H_n \Delta H_n^*]\} \\ &= X_i z_n \end{aligned} \tag{3.83}$$

$$\begin{aligned} R_{in} &= E\left[|Z_n|^2\right] \\ &= |X_i|^2 + N_o. \end{aligned} \tag{3.84}$$

With jamming the expressions would be a little bit different. Jamming attacks are launched by pilot-jammers, one of the widely-used smart jammers. Pilot-jammer attempts to disrupt communications by attacking the pilots only. We assume that the jammer is synchronized with the target signal. The jammer sends out an i.i.d. AWGN jamming signal with Power Spectral Density (PSD) N_j. It transmits only on the pilot tones and it is zero for the non-pilot tones. If we further assume that jammer is uncorrelated with both the channel transfer factor and the channel AWGN, it would produce exactly the same effect on BER as the channel AWGN but not with PSD N_j but rather with effective PSD $N_j\rho$, where, $\rho = \frac{W_p}{W_s}$. W_p and W_s are the bandwidth of the pilot signal and the OFDMA signal respectively. With pilot jamming, the coefficients for the n^{th} tone are given by (3.80), (3.81) with SNR replaced with $SNJR$ = signal to noise-plus-jammer ratio = $\frac{E_s}{N_o + N_j\rho}$ and error variances are replaced with error variance with jammer $\sigma_{n,j}^2$ as given by (3.78)

$$\mu_{s2}(n,j) = \frac{\pm 1}{\sqrt{\frac{(1+\frac{1}{SNJR})(2\Re\{z_n\}+\sigma_{n,j}^2-1)}{(z_n)^2}}} \tag{3.85}$$

$$\mu_{s4}^1(n,j) = \frac{\pm\frac{1}{\sqrt{2}} \pm j\frac{1}{\sqrt{2}}}{\sqrt{\frac{\left(1+\frac{1}{SNJR}\right)(2\Re\{z_n\}+\sigma_{n,j}^2-1)}{(z_n)^2}}}. \tag{3.86}$$

For 16-QAM the different parameters for a particular tone n of an OFDMA symbol with

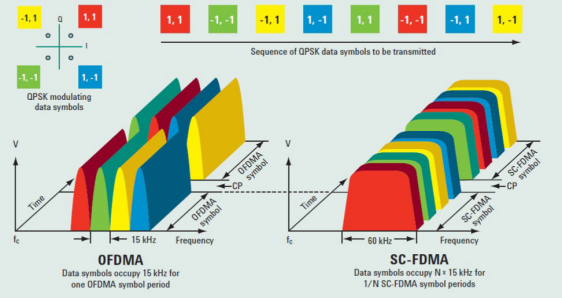


Figure 3.5: Signal structure of OFDMA and SC-FDMA. In OFDMA, each subcarrier is modulated by one data symbol for the entire duration of an OFDMA symbol. For SC-FDMA, each modulated symbol occupies the entire bandwidth for its allocated part of a SC-FDMA symbol duration.

jamming are as follows

$$P_n = 2\Re\{z_n\} + \sigma^2_{n,j} - 1 \tag{3.87}$$

$$Q_{in} = X_i z_n \tag{3.88}$$

$$R_{in} = |X_i|^2 + N_o + N_j\rho. \tag{3.89}$$

3.4.2 BER for SC-FDMA without and with Pilot-Jamming Attack

Due to the differences in signal structure and the assumption of time-selective frequency-flat channel, whatever we have done in the frequency or subcarrier domain for OFDMA has to be translated into the time or symbol domain for SC-FDMA. Similar to pilot tones in OFDMA, we have pilot symbols in SC-FDMA radio frames for channel estimation. These pilot symbols are user specific. In the overall radio frame the pilot symbols of the users are separated by the data symbols of the users. The channel estimation is carried out by piecewise-linear interpolation in time, i.e. symbol domain as shown in Fig. 3.4. For SC-FDMA, the channel estimation error variance [26] for a paritcular symbol m is given by (3.90), where $R_t(k) = E[H_{m+k}H^*_m]$ and it is symmetric with $R_t(-k) = R_t(k)^*$. Moreover $K =$ pilot symbol spacing $= (m_2 - m_1)$, and $k = (m - m_1)$. To satisfy Nyquist theorem,

$$\begin{aligned}\sigma_m^2 &= R_t(0)(1+a_m^2+b_m^2)+\frac{a_m^2 N_o}{|X_{m_1}|^2}+\frac{b_m^2 N_o}{|X_{m_2}|^2}-2a_m\Re\{R_t(k)\}-2b_m\Re\{R_t(K-k)\}\\ &+ 2a_m b_m\Re\{R_t(K)\} \qquad (3.90)\\ \sigma_{m,j}^2 &= R_t(0)(1+a_m^2+b_m^2)-2a_m\Re\{R_t(k)\}+\left(\frac{a_m^2}{|X_{m_1}|^2}+\frac{b_m^2}{|X_{m_2}|^2}\right)(N_o+N_j\rho)\\ &- 2b_m\Re\{R_t(K-k)\}+2a_m b_m\Re\{R_t(K)\} \qquad (3.91)\end{aligned}$$

$K \leq \lfloor 1/2F_d \rfloor$. Changing the subscripts n into m in (3.80), (3.81), we have the SC-FDMA cross-correlation coefficients for m^{th} symbol without jamming

$$\mu_{s2}(m) = \frac{\pm 1}{\sqrt{\frac{(1+\frac{1}{SNR})(2\Re\{z_m\}+\sigma_m^2-1)}{(z_m)^2}}} \qquad (3.92)$$

$$\mu_{s4}^1(m) = \frac{\pm\frac{1}{\sqrt{2}} \pm j\frac{1}{\sqrt{2}}}{\sqrt{\frac{\left(1+\frac{1}{SNR}\right)(2\Re\{z_m\}+\sigma_m^2-1)}{(z_m)^2}}} \qquad (3.93)$$

where, $(a_m\{R_t(k)\}+b_m\{R_t^*(K-k)\})=z_m$. For 16-QAM, the different parameters for a particular symbol m of SC-FDMA frame without jamming are as follows

$$\begin{aligned}P_m &= E\left[\left|\widehat{H}_m\right|^2\right]\\ &= 1-2\Re\{E[H_m\Delta H_m^*]\}+\sigma_m^2\\ &= 2\Re\{z_m\}+\sigma_m^2-1 \qquad (3.94)\\ Q_{im} &= E\left[Z_m\widehat{H}_m^*\right]\\ &= X_i\{1-E[H_m\Delta H_m^*]\}\\ &= X_i z_m \qquad (3.95)\\ R_{im} &= E\left[|Z_m|^2\right]\\ &= |X_i|^2+N_o. \qquad (3.96)\end{aligned}$$

For jamming, considering the same assumptions as with OFDMA, the expressions for coefficients and error variance (as given by (3.91)) would be same as the ones for OFDMA with n replaced with m, f with t, L with K, and l with k.

$$\mu_{s2}(m,j) = \frac{\pm 1}{\sqrt{\frac{(1+\frac{1}{SNJR})(2\Re\{z_m\}+\sigma^2_{m,j}-1)}{(z_m)^2}}} \tag{3.97}$$

$$\mu^1_{s4}(m,j) = \frac{\pm\frac{1}{\sqrt{2}} \pm j\frac{1}{\sqrt{2}}}{\sqrt{\frac{(1+\frac{1}{SNJR})(2\Re\{z_m\}+\sigma^2_{m,j}-1)}{(z_m)^2}}}. \tag{3.98}$$

For 16-QAM the different parameters for a particular symbol m of SC-FDMA frame with jamming are as follows

$$\begin{aligned} P_m &= 2\Re\{z_m\} + \sigma^2_{m,j} - 1 \\ Q_{im} &= X_i z_m \\ R_{im} &= |X_i|^2 + N_o + N_j\rho. \end{aligned} \tag{3.99}$$

3.4.3 BER with Optimum Interpolation

In this paper, we have used linear interpolation due to its low computational complexity. Optimum interpolation like Wiener filtering or Gauss-Markov model-based Kalman Filtering could have been used to estimate the channel transfer factors for the subcarriers/symbols between the pilots. Although these optimum interpolations are computationally intense, the general equations derived above could be reduced to much simplified versions for optimal filters. Wiener filter optimizes mean-squared error of estimation whereas Kalman filter minimizes mean-squared variance of the estimation. At the optimal point, the estimation error produced by the Wiener filter is orthogonal to the estimation [16]. In that case,

$E\left[\widehat{H}_{m,n}\Delta H^*_{m,n}\right] = 0$ results in the following simplifications

$$\begin{aligned} E[H_{m,n}\Delta H^*_{m,n}] &= E\left[\widehat{H}_{m,n}\Delta H^*_{m,n}\right] + E\left[|\Delta H_{m,n}|^2\right] \\ &= \sigma^2_{m,n}. \end{aligned}$$

As a consequence, the cross-correlation coefficient for BPSK becomes real and the BER simplifies to the following [17]

$$P_{s2}(m,n) = \frac{1}{2}\left(1 - \mu_{s2}(m,n)\right) \tag{3.100}$$

$$\begin{aligned} P_{s2}(m,n) &= \frac{1}{2}\left(1 - \frac{1}{\sqrt{1 + \frac{\sigma^2_{m,n} + \frac{1}{SNR}}{1-\sigma^2_{m,n}}}}\right) \\ &= P_{b2}(m,n). \end{aligned} \tag{3.101}$$

For QPSK, the optimality results in the following relationships [17]

$$\begin{aligned} \left|\Re\left[\mu^1_{s4}(m,n)\right]\right| &= \left|\Im\left[\mu^1_{s4}(m,n)\right]\right| \\ = \left|\Re\left[\mu^2_{s4}(m,n)\right]\right| &= \left|\Im\left[\mu^2_{s4}(m,n)\right]\right| \end{aligned} \tag{3.102}$$

$$P_{s4}(m,n) = 2P_s\left(\mu^1_{s4}(m,n)\right) = 2P_s\left(\mu^2_{s4}(m,n)\right) \tag{3.103}$$

$$P_{s4}(m,n) = \left(1 - \frac{1}{\sqrt{1 + \frac{2\sigma^2_{m,n} + \frac{2}{SNR}}{1-\sigma^2_{m,n}}}}\right) \tag{3.104}$$

$$P_{b4}(m,n) = \frac{1}{2}\left(1 - \frac{1}{\sqrt{1 + \frac{2\sigma^2_{m,n} + \frac{1}{SNR_b}}{1-\sigma^2_{m,n}}}}\right) \tag{3.105}$$

where $SNR_b = \frac{E_b}{N_o}$.

3.5 Executive Summary of the Derivations

There are so many derivations so far, it is easy to get lost in myriads of equations and thus fail to grasp the essence of analysis. This section summarizes the major points of derivations to provide connections among different parts of mathematical analysis. Equations (3.28) and (3.29) are the general BER expressions for any PSACE in Rayleigh slow-fading AWGN channel. These foundational expressions are customized in subsections (3.3.1), (3.3.2), and (3.3.3) for BPSK, QPSK, and 16-QAM modulation schemes respectively. Equations in (3.3.1), (3.3.2), and (3.3.3) are further modified into the equations in subsection (3.4.1) to account for frequency-domain piecewise-linear interpolation with ZF equalization in frequency-selective static channel in general with specific application to OFDMA without and with pilot-jamming. On the other hand, subsection (3.4.2) details the modified versions of the same set of equations in (3.3.1), (3.3.2), and (3.3.3) incorporating the effect of time-domain piecewise-linear interpolation with ZF equalization in time-selective frequency-flat channel in general with specific application to SC-FDMA without and with pilot-jamming.

It is noteworthy that for frequency domain interpolation, the foundational equations as well as their modified versions assume slow-fading channel. On the contrary, for time domain interpolation, although the foundational equations are based on slow-fading conditions, their modified versions assume time-selective channel which could be slow-fading as well as fast-fading depending on the values of Doppler spread. These facts lead to the prediction of perfect matching between analytical and simulated BER plots for OFDMA. On the other hand, for SC-FDMA, we expect perfect matching between theories and simulation at low Doppler spread but deviation between the two at high Doppler spread.

3.6 Simulation and Results

Intensive simulations have been carried out to verify the analytical results. The perfectly matched simulation results with slight discrepancies for SC-FDMA have confirmed the theoretical soundness of the derived BER expressions.

3.6.1 Performance of OFDMA

For the OFDMA link-level simulation, we have considered the ITU Pedestrian A channel [12] to simulate multipath. The power delay profile is described in Table I. Table II summarizes the other parameters for simulation. The CP length has been chosen to be longer than the channel delay spread to avoid Inter-block Interference (IBI) between consecutive OFDMA symbols.

Although the channel is estimated perfectly at the pilots, the detection at pilots is still liable to errors due to the presence of AWGN at these points. Consequently, the BER expressions for BPSK, QPSK and QAM at the pilots would be those for frequency-flat, Rayleigh slow-fading AWGN channel with perfect channel estimation as given by

$$P_{b2} = \frac{1}{2}\left(1 - \frac{1}{\sqrt{1+\frac{1}{SNR}}}\right) \tag{3.106}$$

$$P_{b4} = \frac{1}{2}\left(1 - \frac{1}{\sqrt{1+\frac{2}{SNR}}}\right) \tag{3.107}$$

$$\begin{aligned} P_{bQ}^{16} = {} & \frac{1}{SNR}\int_0^\infty \left\{3Q\left(\sqrt{\frac{x}{5}}\right)\right\} \exp^{\frac{-x}{SNR}} dx \\ & - \frac{1}{SNR}\int_0^\infty \left\{\frac{9}{4}\left[Q\left(\sqrt{\frac{x}{5}}\right)\right]^2\right\} \exp^{\frac{-x}{SNR}} dx \end{aligned} \tag{3.108}$$

where $x \geq 0$ and $SNR = \frac{E_s E\left[|H_{m,n}|^2\right]}{N_o} = \frac{E_s}{N_o}$ because for derivations we have assumed that

Table 3.1: Propagation conditions for ITU Pedestrian A channel

Relative delay (ns)	Relative mean power (dB)
0	0
110	-9.7
190	-19.2
410	-22.8

Table 3.2: Simulation assumptions and parameters

Parameters	Values
System bandwidth	5 MHz
Sampling rate	5 Msps
CP length, M_{cp}	20 samples
Transmitter IFFT size (OFDMA/SC-FDMA), M	512
SC-FDMA input block size, U_t	Variable
SC-FDMA DFT precoding size	Variable
SC-FDMA subcarrier mapping	LFDMA
Pulse shaping	None
Equalization	Zero forcing
Channel coding	None
Detection	Hard decision
Pilot Density	1/7

$E\left[|H_{m,n}|^2\right] = 1$. As obvious from (3.108), there is no closed-form expression of BER for 16-QAM with perfect channel estimation. We have performed numerical integration for 16-QAM to calculate BER with perfect CE.

Figure 3.6(a) through Figure 3.6(c) show the BER plots for OFDMA without jamming. The simulated BPSK and QPSK plots match with their analytical counterparts perfectly. As predicted, the simulated QAM plot lies between the upper and lower bounds but closer to the lower bound.

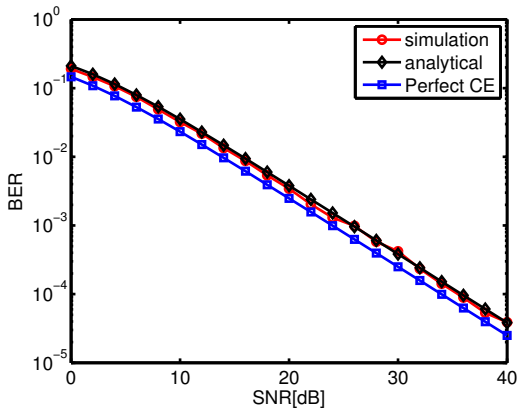
Figure 3.7(a) through Figure 3.7(c) show the BER plots for OFDMA with pilot-tone jamming. They are also in agreement with their analytical counterparts. As obvious from the plots, the curves with jamming and those without jamming are identical. This occurred

because in simulation, assuming the background AWGN negligible, we have used the same range of values for SNR and SJR. But there are distinct differences in simulation. While for jamming, a noise voltage of $\sqrt{\frac{1}{\rho(SJR)}}$ is added to the pilot tones only, for jamming-free scenario a noise voltage of $\sqrt{\frac{1}{SNR}}$ is added to all the tones in an OFDMA symbol. The resemblance among the plots represent the fact that pilot-tone jamming with noise variance $\frac{1}{\rho(SJR)}$ is equivalent to the barrage noise jamming with noise variance $\frac{1}{SNR}$, where, $SJR = SNR$ and $\rho = \frac{W_p}{W_s}$.

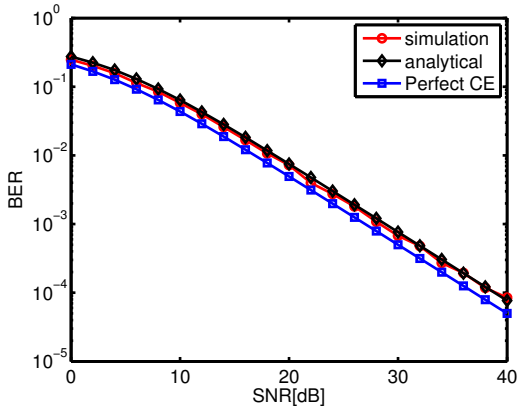
Figure 3.11(a) shows the degradation in BER performance of OFDMA due to pilot-jamming attacks. Simulations are in perfect agreement with the theories. Although, the serial-to-parallel conversion of data symbols and CP insertion at the OFDMA transmitter are still there to reduce ISI to some extent and eliminate IBI, pilot-jamming results in degradation in equalization at the receiver. Consequently, ZF equalization at the detector fails to eliminate ISI within a block and produces irreducible error floor. The plot also reflects that error floor decreases as SJR increases. The higher the SJR, the less powerful the jammers are with consequent less effectiveness in attacks.

3.6.2 Performance of SC-FDMA

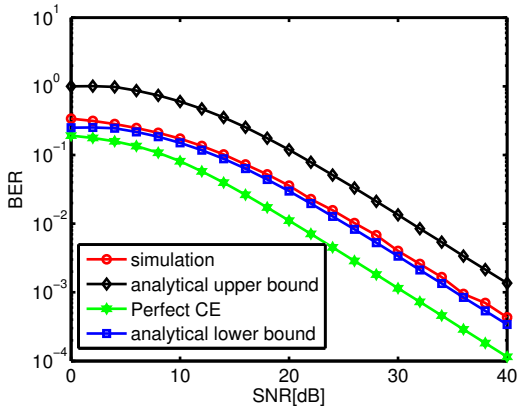
For SC-FDMA, the channel is assumed to be frequency-flat but time-selective during the transmission of a SC-FDMA symbol. This leads to the loss of orthogonality between the symbol's sinc-shaped subcarrier spectra causing subcarrier leakage. The amount of inter-carrier interference (ICI) imposed by this phenomenon depends on the maximum Doppler frequency. Table II shows the parameters for link level simulation of SC-FDMA. We consider localized FDMA, a subcarrier mapping in which modulation symbols are assigned to adjacent subcarriers [15]. The pilot SC-FDMA symbols are not passed through DFT precoding block and are directly applied to IFFT block as is the case with LTE [12].



(a)



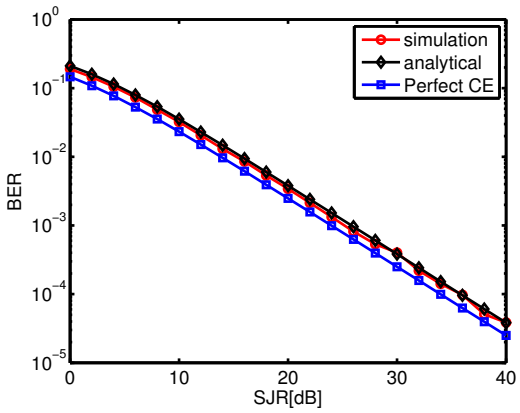
(b)



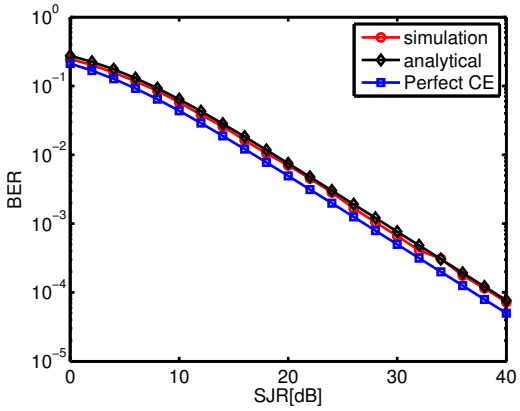
(c)

Figure 3.6: Bit error rate without jamming as a function of SNR for OFDMA: (a) with BPSK, (b) with QPSK, and (c) with 16-QAM

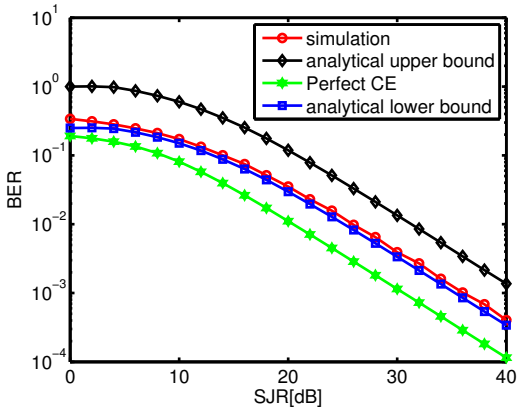
Figure 3.8(a) through Figure 3.9(c) present the plots for BER expressions of SC-FDMA



(a)

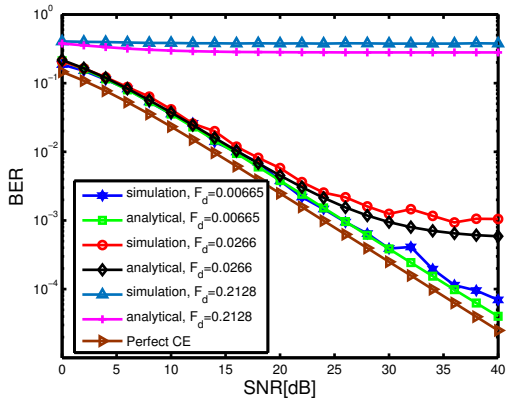


(b)

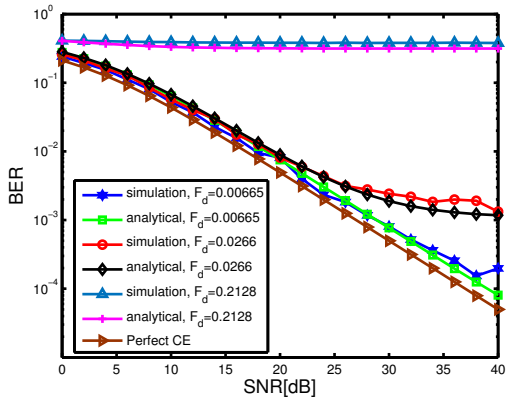


(c)

Figure 3.7: Bit error rate as a function of SJR with pilot-tone jamming assuming negligible AWGN for OFDMA: (a) with BPSK, (b) with QPSK, and (c) with 16-QAM. Figure 3.6 and Figure 3.7 are identical due to the equivalence between pilot-tone jammers with variance $\frac{1}{\rho(SJR)}$ and AWGN with variance $\frac{1}{SNR}$ with $SJR = SNR$.



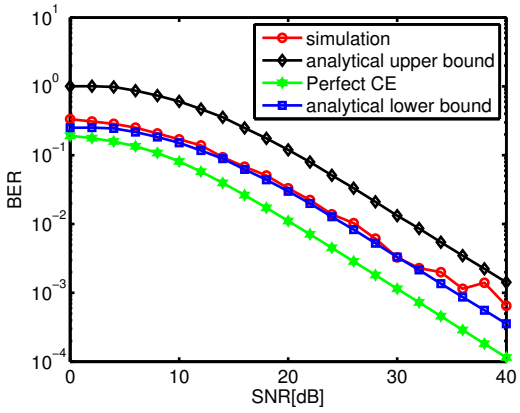
(a)



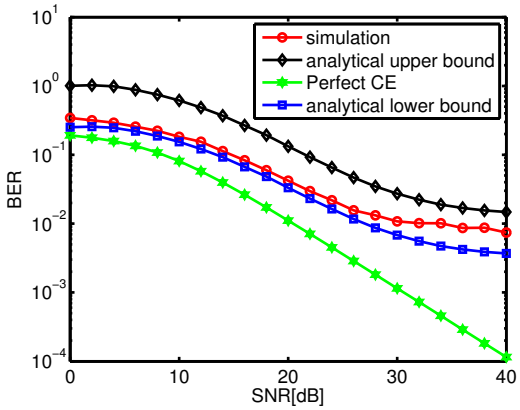
(b)

Figure 3.8: Bit error rate without jamming for SC-FDMA with $F_d = 0.00665$, $F_d = 0.0266$, and $F_d = 0.2128$: (a) for BPSK, and (b) for QPSK. Here $F_d = f_d T_{sym}$ and U_t is kept constant at 24.

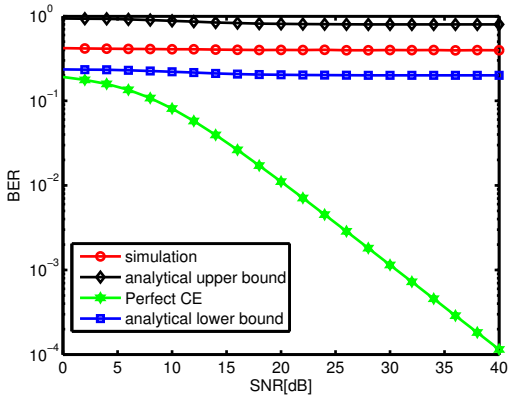
without jamming and Figure 3.10(a) through Figure 3.10(c) present the plots with pilot-tone jamming as functions of SJR assuming zero AWGN. For clarity, the QAM plots are presented in different figures. In these figures, SC-FDMA symbol normalized Doppler frequency is $F_d = f_d T_{sym} = f_d \left(M + M_{cp}\right) T_s$ [41]. As predicted analytically, the simulation agrees very well with the theories at low Doppler but starts to deviate from each other at higher Doppler at high SNR or SJR. It concludes from Figure 3.8(a) through Figure 3.9(c) that time-variant channel imposes a major influence on the BER performance of SC-FDMA. As the F_d increases keeping U_t constant, the deviation of the simulation from the theoretical curve sets in at increasingly lower SNR regimes. For BPSK modulation, deviation starts after 30



(a)



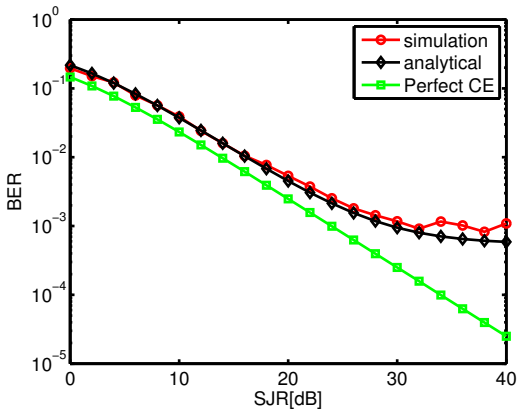
(b)



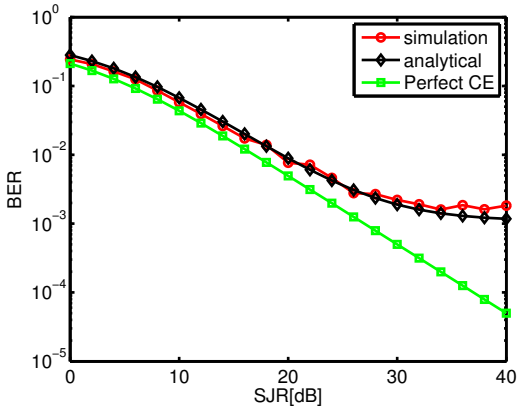
(c)

Figure 3.9: 16-QAM error probability without jamming for SC-FDMA: (a) with $F_d = 0.00665$, (b) with $F_d = 0.0266$, and (c) with $F_d = 0.2128$. U_t is kept constant at 24.

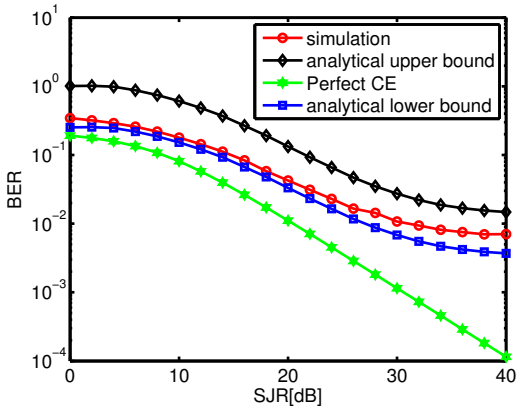
dB, 14 dB, and 2 dB of SNR with $F_d = 0.00665$, $F_d = 0.0266$, and $F_d = 0.2128$ respectively.



(a)

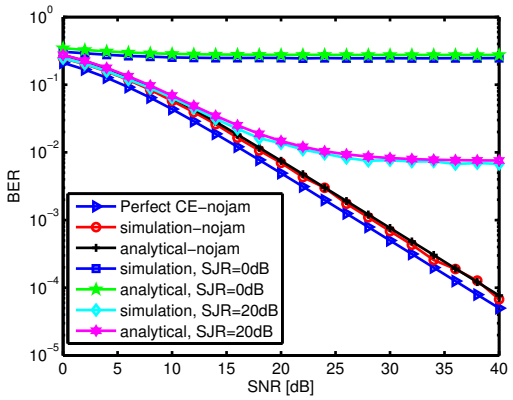


(b)

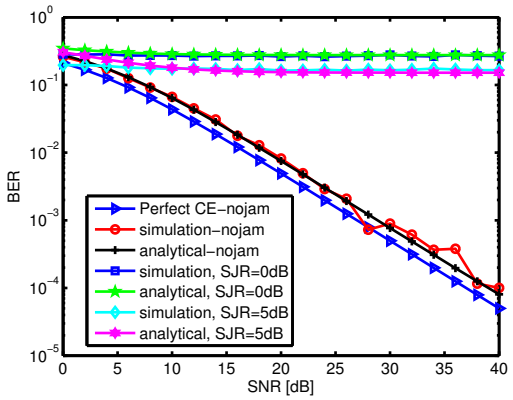


(c)

Figure 3.10: Bit error rate with pilot-tone jamming for SC-FDMA as a function of SJR assuming negligible AWGN with $F_d = 0.0266$: (a) for BPSK, (b) for QPSK, and (c) for 16-QAM. U_t is kept constant at 10.



(a)



(b)

Figure 3.11: Degradation in QPSK BER performance due to pilot-tone jamming attack (a) for OFDMA with SJR at 0 dB and 20 dB, and (b) for SC-FDMA with $F_d = 0.00665$, and with SJR at 0 dB and 5 dB

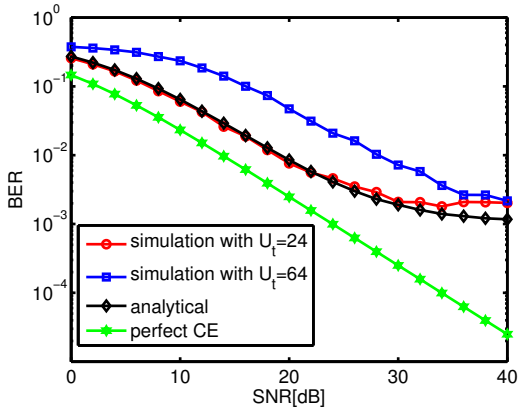


Figure 3.12: Effect of the size of DFT-precoding on BER. DFT-precoder size defines the shape of BER plot before the initiation of the error floor.

Figure 3.8(b) also reflects the fact that higher order modulation is more tolerant to the time-selectivity of the channel. For QPSK modulation, deviation starts after 36 dB, 26 dB, and 6 dB of SNR with $F_d = 0.00665$, $F_d = 0.0266$, and $F_d = 0.2128$ respectively. Before these deviations the simulations are in perfect agreement with the analysis. Figure 3.11(b) shows the degradation in BER performance of SC-FDMA due to pilot-jamming attacks. Simulations are in perfect agreement with the theories except for a little part at low SNR regime for $SJR = 5$ dB.

While doing simulations with SC-FDMA, we have encountered one issue unlike OFDMA. Naturally investigation into the problem has provided us with further insights into the matter. In order to get the plots as matched as possible with the analysis, we had to use different values of U_t for different cases. U_t is the SC-FDMA input block size which also affects the DFT-precoder size. We found the optimum values of U_t for a particular set of the other parameters using heuristic, i.e. trial and error approach. For the simulation, we have used $U_t = 10$ for jamming cases and $U_t = 24$ for cases without jamming to achieve the best possible matched results. Figure 3.12 represents the effect of DFT precoder size on the BER expressions. Obviously, the value of U_t defines the shape of the BER curve till the initiation of the error floor. With higher U_t, the curve is convex in the beginning before the error floor sets in towards the end whereas with lower U_t, the curve is concave in the outset before the introduction of the irreducible residual BER. The concavity and the convexity of the BER plots vanish as they approach the error floor. Although, U_t does not initiate ICI, once ICI is there due to Doppler, the increase in U_t simply makes the situation worse. The more the subcarriers, the more severe is the effect of loss of orthogonality due to ICI, i.e. smearing of information among the subcarriers.

Obviously, the BER expressions in subsection (3.4.2) are missing the effect of U_t. Although, OFDMA in frequency-selective static channel is straightforward implementation of pilot-assisted frequency-domain piecewise-linear interpolation with ZF equalization, SC-FDMA in

time-selective frequency-flat channel is not the direct implementation of pilot-assisted time-domain piecewise-linear interpolation with ZF equalization. Rather SC-FDMA is associated with some extra processing, i.e. DFT-precoding. Consequently, BER expressions derived in subsection (3.4.1) are exact for OFDMA but those in subsection (3.4.2) have to be further modified to incorporate the effect of the DFT-precoding. Finally, it concludes that the BER expressions developed in this paper have to be further modified to incorporate the effects of system-specific features.

3.7 Conclusion

In this chapter, we have derived the analytical expressions of BER for BPSK/QPSK/16-QAM modulation in Rayleigh slow-fading channel for OFDMA and SC-FDMA under pilot-jamming attacks and pilot assisted channel estimation. The theoretical results have been verified with simulations in MATLAB. Simulation results agree perfectly with the theoretical predictions except for some inconsistencies in case of SC-FDMA. Investigation into these discrepancies reveals the fact that the BER expressions derived in this paper have to be further modified to incorporate the effect of system-specific features, e.g. DFT-precoding for SC-FDMA. The future scope of this paper would be to deduce the exact BER expressions for SC-FDMA with the DFT-precoding taken into account.

Although this chapter has dealt with one-dimensional pilot assisted channel estimation either in time or frequency domain, these two piecewise-linear interpolating filters can be easily cascaded to provide 2D-filtering. Interpolation could be performed first in the frequency domain followed by interpolation in the time domain. Alternatively, the interpolation could first be performed in the time direction and then in the frequency direction. Our future extension of this paper would be to study the performance of this cascaded filter as compared to the conventional 2D-Wiener filter.

Chapter 4

Emulated CP Jamming and Nulling Attacks on SC-FDMA and Two Novel Countermeasures

Single-Carrier Frequency Division Multiple Access (SC-FDMA) uses Cyclic Prefix (CP) to mitigate inter-symbol interference (ISI) and inter-channel interference (ICI). CP ensures that the convolution of the channel impulse response with the modulated symbols has the form of a circular convolution. This results in simple one-tap equalization in the receiver by removing ICI. These crucial roles played by the CP make SC-FDMA particularly vulnerable to jamming or nulling attacks through CP. These attacks are effective if the CP is disrupted before passing through the channel. The attacks that happen to jam the signal after it is already through the channel, reduce to no-jamming scenarios in their effectiveness. But signal disruption ensuring signal is not already distorted by channel is practically infeasible. Consequently, in this chapter, we have designed the jammers so that they emulate the effect of CP jamming and nulling in frequency-selective time-invariant channel. We have also proposed two novel countermeasures. Simulations are performed to validate the analytical

predictions about the attacks and the associated countermeasures. The results reflect the fact that CP attacks are particularly suitable for power-constrained jammers in high SNR regime. The newly proposed anti-jamming techniques prove to be very effective in thwarting the attacks.

4.1 Introduction

Third Generation Partnership Project (3GPP) uses SC-FDMA for multiple access in the uplink direction. Like Orthogonal Frequency Division Multiple Access (OFDMA), the multiple access technology for 3GPP downlink, SC-FDMA divides the transmission bandwidth into multiple parallel subcarriers. The use of CP, the guard period, maintains the orthogonality between the subcarriers in frequency-selective channels by transforming the linear convolution of the multipath channel into a circular convolution. The circular convolution removes the ICI which in turn enables the receiver to equalize the channel simply by scaling each subcarrier by a complex gain factor. The CP also prevents ISI a.k.a. inter-block interference (IBI) between consecutive SC-FDMA blocks. However, unlike OFDMA, where the data symbols directly modulate each subcarrier, in SC-FDMA the signal modulated onto a given subcarrier is a linear combination of all the data symbols transmitted at the same instant. Thus all the transmitted subcarriers of an SC-FDMA signal carry a component of each modulated data symbol [12]. This endows SC-FDMA with its critical single-carrier property. As a consequence, the Peak-to-Average Power Ratio (PAPR) of SC-FDMA is sufficiently lower than pure multicarrier transmission schemes like OFDMA.

While the use of CP renders the SC-FDMA with the capability of simple effective detection, the same CP also makes it prone to jamming attacks in tactical scenarios where adversaries intentionally try to jam communications. Although communication electronic warfare (EW) literature is rich with publications on pilot jamming attacks, there are relatively few publi-

cations that have addressed CP jamming attacks. To the authors' knowledge, literature [42] is the only material available online to date. In this Masters thesis, the author studied the effect of CP jamming and barrage jamming on OFDM signal under three environments: no channel, multipath channel, and fading multipath channel. The author found out that with the growing complexity of the channel model, the difference in the effectiveness of each jamming technique becomes less.

In this chapter, building on the mathematical analysis of the operation of CP of SC-FDMA, the authors have designed emulated time-domain jamming and nulling attacks on CP in frequency-selective static AWGN channel. These attacks disrupt the target so that the system will suffer from the same malicious effects if the signal were jammed before being distorted by the channel. They also devised two novel anti-jamming techniques. The analysis is verified with simulations in MATLAB. The proposed countermeasures restore the system perfectly to no-jamming scenario.

The remainder of this chapter is organized as follows. Section 4.2 describes the system model. Section 4.3 details the mathematical analysis of CP. Section 4.4 analyzes the CP attacks. Two novel countermeasures are proposed in section 4.5. Section 6.5 details the simulation and explains the simulation results. Section 6.6 concludes the chapter with final remarks.

4.2 SC-FDMA System Model

Figure 5.2 shows the SC-FDMA uplink system model adopted for analysis in this paper [15]. Each terminal sends a data block consisting of M complex modulation symbols $\left(\mathbf{s}\left[k\right]^{M\times 1}\right)$ at a rate R_s sps, where k is the time-index of a symbol. The M-point discrete Fourier transform (DFT) produces M frequency domain symbols, $\mathbf{S}\left[k\right]^{M\times 1} = \mathbf{F}^{M\times M}\mathbf{s}\left[k\right]^{M\times 1}$, where $\mathbf{F}^{M\times M}$ denotes M-point DFT matrix. These symbols modulate M out of N orthogonal

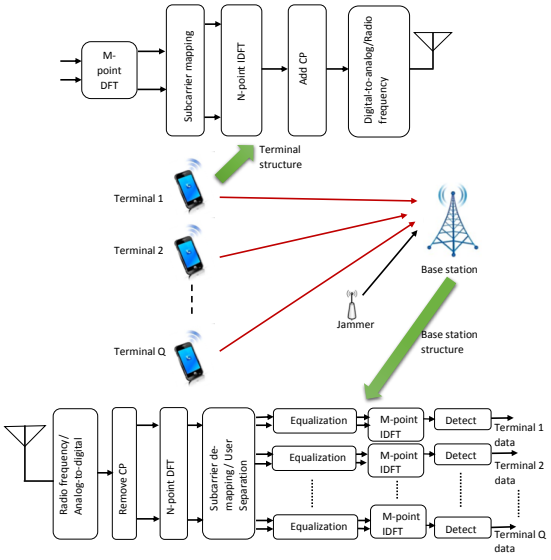


Figure 4.1: SC-FDMA uplink model from a multiple user access perspective with Q terminals, $M < N$

subcarriers spread over a channel bandwidth, $W_{ch} = N \cdot \Delta f\,[\text{Hz}]$, where Δf Hz is the subcarrier spacing. The bandwidth spreading factor, $Q = W_{ch}/R_s = N/M$. Q also tells you how many orthogonal source signals, i.e. terminals the SC-FDMA system can accommodate at a given time.

The subcarrier mapping block assigns frequency domain modulation symbols to subcarriers. We have considered localized FDMA (LFDMA) where the modulation symbols are assigned to M adjacent subcarriers. IDFT in the terminal assigns zeros to the $(N - M)$ unoccupied subcarriers. With $\mathbf{D}^{N\times M}$ denoting subcarrier mapping matrix that starts subcarrier allocation from the 1$^{\text{st}}$ subcarrier, we get the following vector at the output of the subcarrier mapping block

$$\mathbf{X}\left[k\right]_{LFDMA}^{N\times 1} = \mathbf{D}_{LFDMA}^{N\times M}\mathbf{S}\left[k\right]^{M\times 1} \tag{4.1}$$

where $\mathbf{D}_{LFDMA}^{N\times M} = \left[\mathbf{I}^{M\times M}; \mathbf{O}^{(N-M)\times M}\right]$. $\mathbf{I}$ and $\mathbf{O}$ are the identity and zero matrices respectively.

The inverse discrete Fourier transform (IDFT) generates a time domain representation of the N subcarrier symbols, $\mathbf{x}\left[k\right]_{nocp}^{N\times 1} = \mathbf{F^{-1}}^{N\times N}\mathbf{X}\left[k\right]^{N\times 1}$. The parallel-to-serial converter places time domain subcarrier symbols in a time sequence suitable for modulating a radio frequency carrier and transmission to the receiver. Then a set of symbols referred to as cyclic prefix (CP) which is a copy of the last part of the block as shown in fig. 4.2, is inserted, $\mathbf{x}\left[k\right]^{(N+G)\times 1} = \mathbf{T}_{cp}^{(N+G)\times N}\mathbf{x}\left[k\right]_{nocp}^{N\times 1}$. Matrix $\mathbf{T}_{cp}^{(N+G)\times N}$ appends a CP of length G and is of the form $\left[\mathbf{O}^{G\times(N-G)}\ \mathbf{I}^{G\times G};\mathbf{I}^{N\times N}\right]$.

After CP removal, the DFT in the base station (BS) receiver transforms the received signal to the frequency domain to recover the N subcarriers. Assuming the channel impulse response (CIR) has a length, $L \leq G$

$$\begin{aligned}\mathbf{R}\left[k\right] = \mathbf{F}^{N\times N}\mathbf{T}_{cpr}^{N\times(N+G)}\mathbf{H_a}\left[k\right]^{(N+G)\times(N+G)}\mathbf{x}\left[k\right]^{(N+G)\times 1}\\ +\mathbf{F}^{N\times N}\mathbf{T}_{cpr}^{N\times(N+G)}\mathbf{H_b}\left[k\right]^{(N+G)\times(N+G)}\mathbf{x}\left[k-1\right]^{(N+G)\times 1}\\ +\mathbf{F}^{N\times N}\mathbf{T}_{cpr}^{N\times(N+G)}\mathbf{n}\left[k\right]^{(N+G)\times 1}\end{aligned} \tag{4.2}$$

where, matrix $\mathbf{T}_{cpr}^{N\times(N+G)} = \left[\mathbf{O}^{N\times G}\ \mathbf{I}^{N\times N}\right]$ removes CP. With CIR vector between the terminal and the BS, $\mathbf{h}\left[k\right] = \left[h_0\left[k\right]\ \ h_1\left[k\right]\ \ h_2\left[k\right]\cdots h_{L-1}\left[k\right]\right]^T$, $\mathbf{H_a}\left[k\right]^{(N+G)\times(N+G)}$ is defined to be a Toeplitz channel matrix with $\left[h_0\left[k\right]\cdots h_{L-1}\left[k\right]\ \ 0\cdots 0\right]^T$ as the first column and $\left[h_0\left[k\right]\ \ 0\cdots 0\right]$ as the first row. Here, $\left[\cdot\right]^T$ denotes transpose. $\mathbf{H_b}\left[k\right]^{(N+G)\times(N+G)}$ is defined as another Toeplitz channel matrix with $\left[0\cdots 0\right]^T$ for the first column and $\left[0\cdots 0\ h_{L-1}\left[k\right]\cdots h_1\left[k\right]\right]$ for the first row. $\mathbf{n}\left[k\right]$ is the Additive White Gaussian Noise (AWGN) vector. With $G \geq L$, the second term in (4.2) vanishes [43]. During the subcarrier de-mapping process, the base station separates the terminals in the frequency domain by isolating the M frequency domain samples of each source signal

$$\mathbf{Y}\left[k\right]_{LFDMA}^{M\times 1} = \left[\mathbf{D}_{LFDMA}^{N\times M}\right]^T\mathbf{R}\left[k\right]^{N\times 1}. \tag{4.3}$$

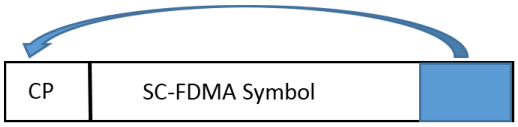


Figure 4.2: SC-FDMA Cyclic Prefix (CP) insertion

As SC-FDMA uses single-carrier modulation, it incurs substantial ISI within a SC-FDMA block which is mitigated by the frequency domain equalizer for each terminal. The IDFT then transforms equalized symbols back to the time domain where the detector produces the received sequence of M modulation symbols for each terminal.

4.3 Mathematical Analysis of CP

The analysis in this section is more focused on the operation of CP. Assuming $G \geq L$, the received discrete-time k^{th} SC-FDMA symbol block from a specific terminal is given by

$$\begin{aligned} \mathbf{r}^{cp}[k]^{(N+G)\times 1} &= \mathbf{H_a}[k]\,\mathbf{x}[k] + \mathbf{H_b}[k]\,\mathbf{x}[k-1] + \mathbf{n}[k] \\ &= \mathbf{I}_{\text{intra}}[k]\,\mathbf{h}[k] + \mathbf{I}_{\text{inter}}[k]\,\mathbf{h}[k] + \mathbf{n}[k] \qquad (4.4) \\ &= \mathbf{I}_{\text{in}}[k]\,\mathbf{h}[k] + \mathbf{n}[k]\,. \qquad (4.5) \end{aligned}$$

As shown in (4.6), in $\mathbf{I}_{\text{in}}[k]$ matrix, purple samples are from the last part of the previous $(k-1)^{\text{th}}$ SC-FDMA symbol block, the red samples are from the CP of the current k^{th} SC-FDMA symbol block, and the black samples are from the non-CP part of the current k^{th} SC-FDMA symbol block [12]. $\mathbf{I}_{\text{intra}}[k]$ which is associated with the interference within the SC-FDMA symbol due to the multipath behavior of the channel is $\mathbf{I}_{\text{in}}[k]$ with the purple samples replaced with zeros. $\mathbf{I}_{\text{inter}}[k]$ which corresponds to IBI, is $\mathbf{I}_{\text{in}}[k]$ with the red and black samples replaced with zeros. To mitigate IBI, the CP, i.e., the first G samples are discarded at the receiver. This eliminates the contribution of matrix $\mathbf{I}_{\text{inter}}[k]$ and the first G

$$\mathbf{I}_{\text{in}}[k] = \mathbf{I}_{\text{intra}}[k] + \mathbf{I}_{\text{inter}}[k]$$

$$= \begin{bmatrix} x_{N-G}[k] & x_{N-1}[k-1] & x_{N-2}[k-1] & \cdots & \cdots & x_{N-L+1}[k-1] \\ x_{N-G+1}[k] & x_{N-G}[k] & x_{N-1}[k-1] & x_{N-2}[k-1] & \cdots & x_{N-L+2}[k-1] \\ \vdots & \vdots & \ddots & \ddots & \ddots & \vdots \\ x_{N-G+L-2}[k] & \cdots & \cdots & \cdots & \cdots & x_{N-1}[k-1] \\ x_{N-G+L-1}[k] & \cdots & \cdots & \cdots & \cdots & x_{N-G}[k] \\ \vdots & \vdots & \ddots & \ddots & \ddots & \vdots \\ x_{N-1}[k] & \cdots & \cdots & \cdots & \cdots & x_{N-L}[k] \\ x_0[k] & x_{N-1}[k] & x_{N-2}[k] & \cdots & \cdots & x_{N-L+1}[k] \\ x_1[k] & x_0[k] & x_{N-1}[k] & \cdots & \cdots & x_{N-L+2}[k] \\ \vdots & \vdots & \ddots & \ddots & \ddots & \vdots \\ x_{L-2}[k] & \cdots & \cdots & \cdots & \cdots & x_{N-1}[k] \\ x_{L-1}[k] & \cdots & \cdots & \cdots & \cdots & x_0[k] \\ \vdots & \vdots & \ddots & \ddots & \ddots & \vdots \\ x_{N-G+L-1}[k] & \cdots & \cdots & \cdots & \cdots & x_{N-G}[k] \\ \vdots & \vdots & \ddots & \ddots & \ddots & \vdots \\ x_{N-1}[k] & x_{N-2}[k] & \cdots & \cdots & \cdots & x_{N-L}[k] \end{bmatrix} \tag{4.6}$$

$$\begin{bmatrix} R_0[k] \\ R_1[k] \\ \vdots \\ R_{N-1}[k] \end{bmatrix} = \underbrace{\begin{bmatrix} X_0[k] & 0 & \cdots & 0 \\ 0 & X_1[k] & \cdots & 0 \\ \vdots & \cdots & \cdots & \vdots \\ 0 & 0 & \cdots & X_{N-1}[k] \end{bmatrix}}_{\mathbf{X}[k]} \begin{bmatrix} H_0[k] \\ H_1[k] \\ \vdots \\ H_{N-1}[k] \end{bmatrix} + \begin{bmatrix} \mathcal{N}_0[k] \\ \mathcal{N}_1[k] \\ \vdots \\ \mathcal{N}_{N-1}[k] \end{bmatrix} \tag{4.7}$$

---

rows of $\mathbf{I}_{\text{intra}}[k]$. 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

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

where noise $\tilde{\mathbf{n}}[k] = [n_G[k], n_{G+1}[k], \cdots, n_{N+G-1}[k]]^T$. The above equation shows that part of the CP would still remain in the received symbol vector even after the removal of CP.

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

$$\mathbf{r}[k] = \mathbf{C}[k]\tilde{\mathbf{h}}[k] + \tilde{\mathbf{n}}[k] \tag{4.8}$$

where $\tilde{\mathbf{h}}[k]^{N\times 1} = [h_0[k], h_1[k], \cdots, h_{L-1}[k], 0, \cdots, 0]^T$. As shown in (4.12), matrix $\mathbf{C}[k]$ is circulant and its Fourier transform is diagonal with eigenvalues given by the DFT of its first column. So, $\mathbf{C}[k] = \mathbf{F}^{-1}\mathbf{X}[k]\mathbf{F}$ with $\mathbf{X}[k]$ diagonal. Replacing this decomposition of $\mathbf{C}$ into (4.8), we have

$$\mathbf{r}[k] = \mathbf{F}^{-1}\mathbf{X}[k]\mathbf{F}\tilde{\mathbf{h}}[k] + \tilde{\mathbf{n}}[k]. \tag{4.9}$$

By applying Fourier transform to (4.9), the received signal in the frequency domain is as shown in (5.26). Summarizing, the CP translates the linear convolution into a circular one. By means of DFT, the circular convolution is transformed into a multiplicative operation in the frequency domain. Thus the transmitted SC-FDMA symbol over a multipath channel is converted into a transmission over N parallel flat-fading channels in the frequency domain at the output of the DFT block in the base station receiver as follows

$$R_m(k) = X_m(k) H_m(k) + \mathcal{N}_m(k) \tag{4.10}$$

where $0 \leq m \leq (N-1)$. This is how CP removes ICI and this also makes equalization much simpler by reducing it to one complex division per subcarrier. In this chapter, we have studied Zero-Forcing (ZF) equalization. For zero-forcing equalization, the channel in the frequency domain is inverted using the estimates of the channel frequency transfer factors in the following way [32], [29]

$$\hat{X}_m(k) = \frac{R_m(k)}{H_m(k)} = X_m(k) + \frac{\mathcal{N}_m(k)}{H_m(k)}. \tag{4.11}$$

4.4 Jamming Attacks

This section describes different types of jamming attacks as launched on CP. As CP is in time domain, all the jammers are generated in time domain.

4.4.1 Different Attacks

We have considered barrage jamming, CP jamming and CP nulling attacks. Jammer is assumed to be synchronized with the target signal and the attack energy is assumed to be evenly distributed among the target discrete-time samples. Barrage jamming is the simplest attack and we have used this as a baseline when evaluating the CP jamming and nulling attacks. In this jamming, the jammer transmits an AWGN scaled to produce the desired SJR, on the entire SC-FDMA symbol. For CP jamming, the jammer sends AWGN to only the CP of each SC-FDMA symbol. In CP nulling attack, we seek to null the CP [34]. This will produce unmodulated subcarriers for the duration of CP. The effectiveness of CP nulling attack relies absolutely on the accurate estimation of channels between the two transceivers, and the jammer's own channel to the target. CP nulling also requires significant a priori knowledge of the target signal structure. As CP jammers attempt to disrupt only parts of digital signal, focusing only on the portions necessary to disrupt or deny communications,

they are also called smart jammers [5].

4.4.2 Channel Estimation

Assuming reciprocal time division duplex (TDD) channel with negligible propagation delay, the jammer can use pilot information to estimate reverse channel between the jammer and the target. In certain Multiple Input Multiple Output (MIMO) scenarios where full spatial multiplexing is used, the target often sends feedback to the third party transmitter which is used to do waterfilling of eigenmodes. The jammer can overhear this Channel State Information (CSI) feedback channel and extrapolate CSI to estimate the channel between the two transceivers. Moreover, the jammer can join the network as a valid user and gain CSI information through interactions with the network.

4.4.3 CP Attacks

With the mathematical analysis and detailed operations of CP described above, it is obvious that CP plays a critical role for effective detection of SC-FDMA symbols at the base station receiver. The two major purposes served by the CP are

1. elimination of IBI, and
2. translation of linear convolution into circular convolution and thus making equalization simpler by removing ICI.

From (4.6), under CP jamming or nulling attack, all the red samples in $\mathbf{I}_{\text{in}}[k]$ matrix would either be contaminated by AWGN or become zero respectively. The removal of CP will discard all the G samples from the top of the $\mathbf{I}_{\text{in}}[k]$ matrix upto the second horizontal line but part of CP would still be left in the received symbol vector. Circulant matrix $\mathbf{C}[k]$ as shown in (4.12) would become $\mathbf{C}_{\text{jam}}[k]$ as shown in (4.13) or $\mathbf{C}_{\text{null}}[k]$ as shown in

$$\mathbf{C}[k] = \begin{bmatrix} x_0[k] & x_{N-1}[k] & \cdots & x_{N-L+1}[k] & x_{N-L}[k] & \cdots & x_1[k] \\ x_1[k] & x_0[k] & \cdots & x_{N-L+2}[k] & x_{N-L+1}[k] & \cdots & x_2[k] \\ \vdots & \ddots & \ddots & \ddots & \ddots & \vdots & \\ x_{N-1}[k] & x_{N-2}[k] & \cdots & x_{N-L}[k] & x_{N-L+1}[k] & \cdots & x_0[k] \end{bmatrix} \tag{4.12}$$

$$\mathbf{C}_{\text{jam}}[k] = \begin{bmatrix} x_0[k] & x_{N-1}[k]+j_{N-1}[k] & \cdots & x_{N-L+1}[k]+j_{N-L+1}[k] & x_{N-L}[k] & \cdots & x_1[k] \\ x_1[k] & x_0[k] & \cdots & x_{N-L+2}[k]+j_{N-L+2}[k] & x_{N-L+1}[k] & \cdots & x_2[k] \\ \vdots & \vdots & \ddots & \ddots & \ddots & \vdots & \\ x_{L-2}[k] & \cdots & \cdots & x_{N-1}[k]+j_{N-1}[k] & x_{N-2}[k] & \cdots & x_{L-1}[k] \\ x_{L-1}[k] & \cdots & \cdots & x_0[k] & x_{N-1}[k] & \cdots & x_L[k] \\ \vdots & \vdots & \ddots & \ddots & \ddots & \vdots & \\ x_{N-1}[k] & x_{N-2}[k] & \cdots & x_{N-L}[k] & x_{N-L+1}[k] & \cdots & x_0[k] \end{bmatrix} \tag{4.13}$$

$$\mathbf{C}_{\text{null}}[k] = \begin{bmatrix} x_0[k] & 0 & \cdots & 0 & x_{N-L}[k] & \cdots & x_1[k] \\ x_1[k] & x_0[k] & \cdots & 0 & x_{N-L+1}[k] & \cdots & x_2[k] \\ \vdots & \vdots & \ddots & \ddots & \ddots & \vdots & \\ x_{L-2}[k] & \cdots & \cdots & 0 & x_{N-2}[k] & \cdots & x_{L-1}[k] \\ x_{L-1}[k] & \cdots & \cdots & x_0[k] & x_{N-1}[k] & \cdots & x_L[k] \\ \vdots & \vdots & \ddots & \ddots & \ddots & \vdots & \\ x_{N-1}[k] & x_{N-2}[k] & \cdots & x_{N-L}[k] & x_{N-L+1}[k] & \cdots & x_0[k] \end{bmatrix} \tag{4.14}$$

(4.14) under CP jamming and nulling attack respectively. These matrices are not circulant anymore. Guard period is still there to absorb IBI but circular convolution is no longer accomplished in the channel with consequent presence of ICI [44]. 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.

It is also noteworthy that the effectiveness of CP attacks is absolutely reliant upon the occurrence of circular convolution in the channel. If CP is attacked at the transmitter before circular convolution with the channel, only then these attacks would be effective. In that case, the SC-FDMA symbol with distorted CP will fail to circularly convolve with the channel. So, one-tap equalization will lose its impact in the receiver. But if it is attacked

at the receiver after passing through the channel, circular convolution is already performed in the channel to remove ICI and make one-tap equalization in the receiver possible. In this case, even if the CP becomes distorted or zero, it will be discarded at the receiver and the rest of the SC-FDMA symbol will still be in its proper form as it is supposed to be after circular convolution in the channel. Consequently, jamming CP after it is transmitted through the channel is equivalent to no-jamming scenario.

4.4.4 Emulated CP Attacks

In the light of the above discussion, CP attacks are effective only when the target signals are jammed before they pass through the channel which is practically infeasible. This real-life limitation is overcome by designing the jammer so that it disrupts the target signal at the receiver in the same way as it would have if the CP of the target signal actually were physically jammed before passing through the channel. Consequently, these jammers are not jamming the CP of the target signal physically, rather they are emulating the effects of CP jammers. Thus they are appropriately called CP attack emulators and corresponding attacks are called emulated CP attacks. According to (4.12), (4.13), and (4.14), the jammer signals should be generated as follows

$$\mathbf{Z}_{\text{jam}}[k] = \mathbf{f}[k]^{-1} * \mathbf{x}_{\text{jam}}[k] * \mathbf{h}[k] \tag{4.15}$$

$$\mathbf{Z}_{\text{null}}[k] = \mathbf{f}[k]^{-1} * \mathbf{x}_{\text{null}}[k] * \mathbf{h}[k] \tag{4.16}$$

where $\mathbf{Z}_{\text{jm}}[k]^{(N+G)\times 1}$ and $\mathbf{Z}_{\text{nl}}[k]^{(N+G)\times 1}$ are respectively the CP jamming and CP nulling jammer vectors with $\mathbf{f}[k]$ as the CIR vector between the jammer and the BS,

$$\mathbf{f}[k] = [f_0[k] \;\; f_1[k] \;\; f_2[k] \cdots f_{V-1}[k]]^T \tag{4.17}$$

$$\mathbf{x}_{\text{jam}}[k]^{(N+G)\times 1} = [j_{N-G}[k], \cdots, j_{N-1}[k], 0, \cdots 0]^T \tag{4.18}$$

$$\mathbf{x}_{\text{null}}\left[k\right]^{(N+G)\times 1} = \left[-x_{N-G}\left[k\right], \cdots, -x_{N-1}\left[k\right], 0, \cdots 0\right]^{T}. \tag{4.19}$$

Here, $*$ denotes convolution. For full realization of the attacks, $G \geq V \geq L$.

4.5 Countermeasures

In this section, we have developed two novel countermeasures for the attacks. The countermeasure for jamming takes advantage of CP at the receiver rather than discarding it. We have assumed that the channel AWGN is negligible.

4.5.1 Countermeasure for Nulling Attack

Under nulling attack, after removal of CP, the received symbol vector is given by

$$\mathbf{r}_{\text{null}}\left[k\right] = \bar{\mathbf{C}}_{\text{null}}\left[k\right]\mathbf{h}\left[k\right]$$

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

with $\bar{\mathbf{C}}$ denoting the corresponding signal matrix $\mathbf{C}$ without extension. In the above equation, $\mathbf{H}_{\text{null}}\left[k\right]$ which can be easily built from the channel estimates, is a lower triangular Toeplitz matrix. This kind of matrix is invertible as long as $h_0\left[k\right] \neq 0$ [45]. For multipath channel, $h_0\left[k\right] = 1$. $\mathbf{x}\left[k\right]_{nocp}$ can be recovered as follows

$$\mathbf{x}\left[k\right]_{nocp} = \mathbf{H}_{\text{null}}\left[k\right]^{-1}\mathbf{r}_{\text{null}}\left[k\right] \tag{4.20}$$

4.5.2 Countermeasure for Jamming Attack

In this case, our goal is to convert $\bar{\mathbf{C}}_{\text{jam}}\left[k\right]$ into $\bar{\mathbf{C}}_{\text{null}}\left[k\right]$ so that we can use the same approach as used for nulling attack to restore the system. This can be done as follows

$$\bar{\mathbf{C}}_{\text{null}}\left[k\right]\mathbf{h}\left[k\right] = \bar{\mathbf{C}}_{\text{jam}}\left[k\right]\mathbf{h}\left[k\right] - \bar{\mathbf{C}}_{noise}\left[k\right]\mathbf{h}\left[k\right] \tag{4.21}$$

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

As obvious from (4.6), under jamming attack, among the G samples of CP, i.e. the first two blocks of matrix $\mathbf{I}_{\text{in}}$, only the red samples would be contaminated by the jammer AWGN but the blue samples which are the last samples of the previous SC-FDMA symbol would remain intact. These uncontaminated samples are known to the receiver as they have already been detected by the receiver in the last epoch. Subtracting these samples from the CP, we have the following

$$\mathbf{r}_{jam}^{cp}\left[k\right]^{G\times 1} - \acute{\mathbf{I}}_{\text{inter}}\mathbf{h}\left[k\right] = \acute{\mathbf{H}}_{\text{null}}\left[k\right]^{G\times G}\mathbf{x}_{jam}^{cp}\left[k\right]^{G\times 1} \tag{4.22}$$

where $\acute{\mathbf{I}}_{\text{inter}}$ is $\mathbf{I}_{\text{inter}}^{(N+G)\times L}$ but of lower dimension $(G\times L)$ with the same non-zero values, $\acute{\mathbf{H}}_{\text{null}}\left[k\right]$ is $\mathbf{H}_{\text{null}}\left[k\right]$ but of lower dimension with the same non-zero values, and $\mathbf{x}_{jam}^{cp}\left[k\right]^{G\times 1} = \left[x_{N-G}\left[k\right]+j_{N-G}\left[k\right],\cdots,x_{N-1}\left[k\right]+j_{N-1}\left[k\right]\right]^{T}$. $\acute{\mathbf{H}}_{\text{null}}\left[k\right]$ is also a lower triangular Toeplitz matrix. Assuming $\mathbf{r}_{jam}^{cp}\left[k\right]^{G\times 1} - \acute{\mathbf{I}}_{\text{inter}}\mathbf{h}\left[k\right] = \check{\mathbf{r}}_{\text{jam}}^{cp}\left[k\right]$, $\mathbf{x}_{jam}^{cp}\left[k\right]$ can be recovered as follows

$$\mathbf{x}_{jam}^{cp}\left[k\right] = \acute{\mathbf{H}}_{\text{null}}\left[k\right]^{-1}\check{\mathbf{r}}_{\text{jam}}^{cp}\left[k\right] \tag{4.23}$$

Table 4.1: Simulation assumptions and parameters for SC-FDMA

Parameters	Values
System bandwidth	5 MHz
Sampling rate	5 Msps
Cyclic prefix, CP	20 samples
Transmitter IFFT size, N	512
SC-FDMA input block size, M	256
Subcarrier mapping	LFDMA
Equalization	ZF
Data modulation	QPSK
Channel estimation	Perfect

$\bar{\mathbf{C}}_{noise}[k]$ can then be constructed from the last $(L-1)$ samples of $\mathbf{x}_{jam}^{cp}[k]$.

When the system is under attack, the equalization is carried out in time-domain. The recovered time-samples are then fed into the N-point DFT block, subcarrier-demapper separates the terminals and feed the frequency-domain samples into the M-point IDFT block.

4.6 Simulation and Results

SC-FDMA 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 [12] 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 4.3 shows the equivalence between the theoretical CP attacks as launched before the signal passes through the channel and their practically realizable emulated counterparts in terms of the degradation they cause the affected system undergo. Obviously, they match

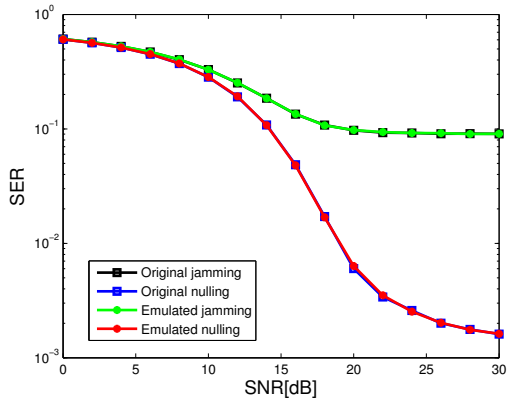


Figure 4.3: Equivalence between the original CP attacks and their emulated counterparts at SJR=0 dB. They match perfectly with each other.

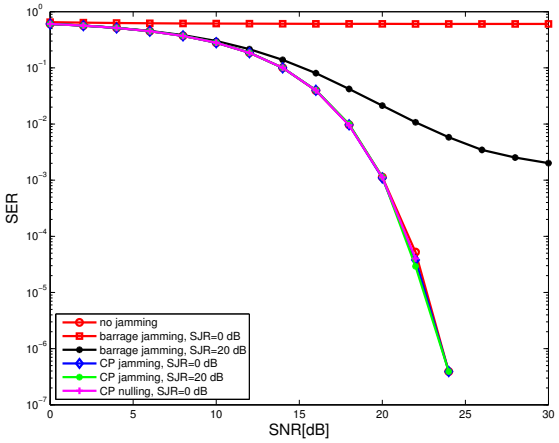


Figure 4.4: Performance of the three jamming techniques in terms of Symbol Error Rate (SER) versus SNR curves. The LFDMA signal is jammed at the receiver after passing through the multipath channel. ZF equalization is used with SJR=0, 20 dB

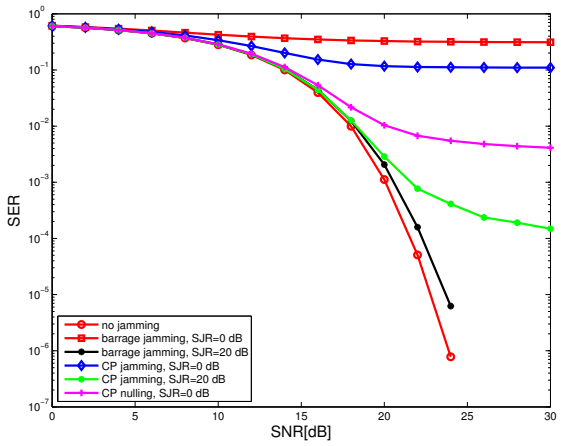
perfectly. Then we have explored the critical role played by the circular convolution of the SC-FDMA symbol with the CIR in determination of the effectiveness of the CP attacks. The SC-FDMA symbol is already convolved with the channel when it is being jammed. As predicted analytically, Figure 4.4 shows the fact that both kind of CP attacks loses all its effectiveness when the SC-FDMA signal is jammed after passing through the multipath channel. In this case, barrage jamming is still effective.

Figure 4.5(a) presents the performance of the three jamming techniques in terms of Symbol Error Rate (SER) analysis and compare them with no-jamming case. ZF equalization is

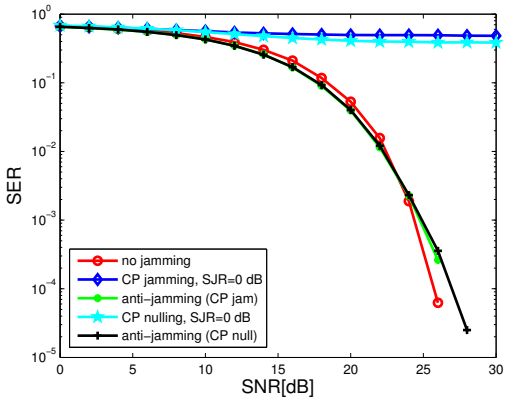
employed at the target and the Signal-to-Jammer-Ratio (SJR) is 0 and 20 dB. We observe that the barrage jamming is outperforming both CP jamming and CP nulling at lower SJR, but CP nulling outperforms the other two at high SJR. With constant signal power, higher SJR implies less jammer power. As the 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. For optimal CP nulling, jammer power is matched with the signal power with consequent zero value for SJR. 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.

Figure 4.5(b) depicts the performance of the two proposed countermeasures. As obvious, they successfully restore the affected system to no-jamming scenario. Figure 4.6 represents the SER performance of the jamming techniques in terms of SJR. They reflect the same fact as already observed in Figure 4.5(a) that the emulated CP attacks are more suitable for power-limited jammers in high SNR regime. In Figure 4.6, the CP nulling has been simulated differently from that in Figure 4.5(a). Figure 4.5(a) depicts the results for optimal CP nulling where the jammer has the perfect knowledge of CSI and the target signal and $SJR = 0dB$. On the other hand, Figure 4.6 presents the results for sub-optimal CP nulling where the jammer has the perfect knowledge of CSI and the target signal but the jammer power is not matched with the signal power.

Figure 4.7 shows the need to accurately model the channel when launching the CP nulling attack. With full channel information, attacks are more efficient.



(a)



(b)

Figure 4.5: Performance of the emulated CP jamming and anti-jamming techniques in terms of Symbol Error Rate (SER) versus SNR curves. ZF equalization is used. (a) Performance of the three jamming techniques with SJR = 0, 20 dB, and (b) performance of the two anti-jamming techniques with SJR = 0 dB.

4.7 Conclusion

In this paper, the authors have investigated the effects of barrage jamming, emulated CP jamming and CP nulling attacks on the SER performance of an SC-FDMA uplink system in frequency-selective time-invariant channel. Due to their higher power efficiency, at high SJR, CP jamming and nulling outperform the barrage jamming in high SNR regime. Consequently, emulated CP jamming and nulling attacks are particularly suitable for power-constrained jammer in high SNR environment. We have also proposed two novel counter-

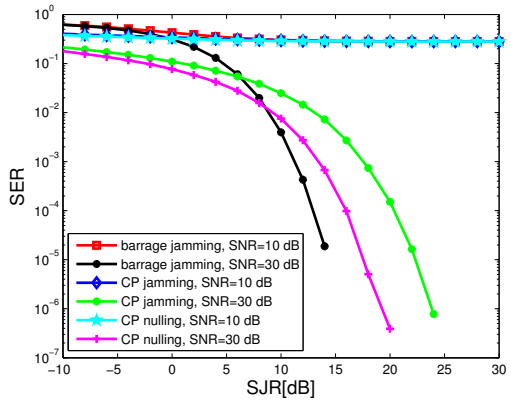


Figure 4.6: Performance of the three jamming techniques in terms of Symbol Error Rate (SER) versus SJR curves. ZF equalization is used with SNR = 10, 30 dB.

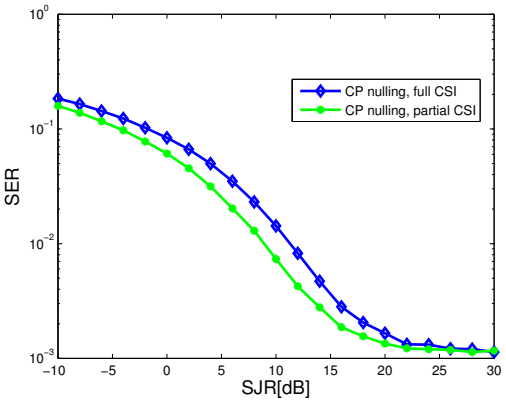


Figure 4.7: Effect of availability of CSI on the performance of the CP nulling technique in terms of Symbol Error Rate (SER) versus SJR curves

measures which prove to be very effective in restoring the system.

Chapter 5

Information-Theoretic Analysis of Pilot-Spoofing Attack in TDD MISO-OFDM System over Correlated Fading Channel

In this chapter we investigate the effect of fading correlation on pilot-spoofing attack in a TDD MISO-OFDM system from information-theoretic perspective. So far all the analysis, whether it is from information-theoretic perspective or signal processing perspective, are carried out under the assumption that MISO channels are independent and identically distributed (i.i.d.) flat fading. This paper is the first one to consider the effect of frequency-selective spatially correlated fading channel on the efficacy of pilot-spoofing attack. By its inherent characteristic, OFDM naturally takes care of the frequency-selectivity of the channel. Capacity bounds are derived. The simulation results show that spatial correlation facilitates the pilot-spoofing attack. The achievable legitimate rate is lower than its i.i.d. counterpart. Although the achievable legitimate rate decreases at a slower rate than its i.i.d.

counterpart.

5.1 Introduction

Recently a tremendous effort has been made on physical layer security to prevent eavesdropping by a malicious user. While various secure transmission schemes are under rapid development, increasingly powerful adversaries also bring in new security attacks. One such example is an active eavesdropper deploying pilot-spoofing attack during reverse training. Reverse training phase of the communication system when it estimates the CSI, provides an exciting opportunity for the eavesdropper to develop smart attacks. Pilot-spoofing attack is based on the pilot contamination phenomenon, first discussed in [46] in multi-cell systems but without security considerations. The security threats of pilot contamination attack are first analyzed in [47]. Pilot-spoofing detection and countermeasures are detailed in [48] and [49].

All the above-mentioned papers assume that MISO channels are independent and identically distributed (i.i.d.). However, in reality, the channels are correlated especially in indoor environments. In this case, channel estimation can achieve better performance by making use of the spatial fading correlation. Since statistics of MISO channels vary very slowly with time, we assume that the correlation matrices are known. With the knowledge of correlation matrix, minimum mean-square-error (MMSE) channel estimation is developed. To authors' knowledge, this is the first work to analyze pilot-spoofing attack on TDD MISO-OFDM taking spatial correlation and frequency selectivity into account. The rest of the paper is organized as follows.

In section 5.2, we introduce a TDD MISO-OFDM system and detail on the legitimate transmission and the passive eavesdropping. Pilot-spoofing attack is analyzed with the incorporation of fading correlation in Section 5.3. In Section 5.4, capacity bounds are derived.

Numerical results are presented in Section 5.5. The paper concludes with Section 6.6.

Notations

In this paper, matrices and vectors are denoted by uppercase and lowercase boldface letters, respectively. $(\cdot)^H$ stands for conjugate transpose. $\text{vec}(\mathbf{X}) = \left[\mathbf{X}^T(0) \cdots \mathbf{X}^T(m) \cdots \mathbf{X}^T(M-1)\right]^T$ where $\mathbf{X}(m)$ is the $(m+1)^{\text{th}}$ column of $\mathbf{X}$. Kronecker product is denoted by $\otimes$ and given by, $\mathbf{X}_{m\times n} \otimes \mathbf{Y}_{p\times q} = [x(1,1)\mathbf{Y} \cdots x(1,n)\mathbf{Y}; \cdots; x(m,1)\mathbf{Y} \cdots x(m,n)\mathbf{Y}]$. $\|\cdot\|$ denotes the Euclidean norm of a vector and $|\cdot|$ represents the absolute value of a scalar.

5.2 System Model

As illustrated in Figure 5.1, the TDD-based MISO-OFDM system consists of a transmitter Alice with $N_t \geq 2$ antennas, a legitimate receiver Bob with single-antenna and an active eavesdropper Eve with single-antenna. All the antennas are assumed to be operating in half-duplex mode. The wireless channels between the three terminals experience large-scale path loss as well as small-scale fading. In order to apply beamforming for the data transmission phase, Alice estimates the CSI using reverse training. The reverse training scheme requires channel reciprocity which holds in time-division duplex (TDD) systems. Channel training is achieved by having Bob send the pilot signals to Alice. Since the pilot signals are repeatedly used and publicly known, it allows the smart eavesdropper Eve to transmit synchronously the same pilot signals during the training phase and thereby biasing the CSI estimation with consequent spoofing of Alice.

Let us assume that the OFDM symbol comprises of M subcarriers. It is further assumed that all the channels between the terminals are block-faded and frequency-selective. The channel varies over the subcarriers but the channel for a given carrier is constant over some blocklength T, i.e., the coherence interval after which it changes to a new independent value

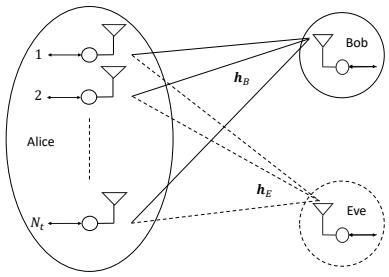


Figure 5.1: System model with three communicating terminals: a transmitter called Alice, a legal receiver known as Bob, and an eavesdropper called Eve. The transmitter is equipped with $N_t \geq 2$ antennas. The legitimate receiver and the eavesdropper, each of them has a single antenna.

based on the channel distribution, that it holds for another interval T, and so on. The channel from Bob to Alice is modeled as $\mathbf{H}_B = \sqrt{\beta_B}\acute{\mathbf{H}}_B$, where β_B denotes the large-scale path loss attenuation and $\acute{\mathbf{H}}_B$ is the small-scale fading gain. Similarly, we denote the channel from Eve to Alice as $\mathbf{H}_E = \sqrt{\beta_E}\acute{\mathbf{H}}_E$. The channel gains $\mathbf{H}_B \in \mathbb{C}^{N_t \times M}$ and $\mathbf{H}_E \in \mathbb{C}^{N_t \times M}$ are matrices with $(m+1)^{\text{th}}$ column $\mathbf{H}_B(m)/\mathbf{H}_E(m)$ denoting the channel gains for m^{th} subcarrier where $m = 0, 1, \cdots, (M-1)$. The channel gains are assumed to be zero-mean. The path loss attenuations are assumed to be constant and known to all terminals.

5.2.1 Legitimate Transmission and Passive Eavesdropping

Let $\mathbf{x}_p = \left[x_{p0}\ x_{p2} \cdots x_{pm} \cdots x_{p(M-1)}\right]^T$ be the normalized OFDM training symbol with block type pilot arrangement where pilot tones are assigned to all subcarriers of a particular OFDM symbol. This type of pilot arrangement is usually considered for slow channel variation and for burst type data transmission schemes, where the channel is assumed to be constant over the burst. At the beginning of every coherence interval which is assumed to span at least several OFDM symbols, Bob transmits its training OFDM symbol $\mathbf{x}_p^B = \sqrt{P_B}\mathbf{x}_p$, where $\sqrt{P_B}$ is the power utilized to send the pilot signal by Bob. We assume that Bob distributes power evenly among pilot subcarriers to ensure optimality [35]. It is

also assumed that cyclic prefix is longer than the expected maximum excess delay of the channel to minimize the effects of inter-symbol and inter-channel interferences.

After removal of the cyclic prefix and DFT, the signal vector received by Alice, $\mathbf{r}^{N_t M\times 1} = \text{vec}\left(\mathbf{R}^{N_t\times M}\right)$, which is formed by stacking the received signal vectors across N_t antennas and M subcarriers can be written as

$$\mathbf{r} = \mathbf{X}_p^B \mathbf{h}_B + \mathbf{n}_A \tag{5.1}$$

where vector, $\mathbf{n}_A^{N_t M\times 1} = \text{vec}\left(\mathbf{N}^{N_t\times M}\right)$, represents the additive noises at the N_t receiving antennas over all M subcarriers. The entries in $\mathbf{N}$ are independent and identically distributed (i.i.d) circularly symmetric complex Gaussian (CSCG) random variable with zero-mean and unit-variance, i.e., $\mathbf{N} \sim \mathcal{CN}(\mathbf{0}, \mathbf{I}_{N_t M})$. The channel vector from Bob to Alice is given by, $\mathbf{h}_B^{N_t M\times 1} = \text{vec}\left(\mathbf{H}_B\right)$, and the pilot symbol matrix $\mathbf{X}_p^B = \text{diag}\left\{\sqrt{P_B} x_{pm} \mathbf{I}_{N_t}\right\}_{m=0}^{M-1}$ is of dimension $N_t M \times N_t M$.

Assuming Alice knows Bob's training power and has accurately obtained the variance of the received signal $\mathbf{r}$, Alice utilizes the Linear MMSE (LMMSE) method to estimate $\mathbf{h}_B$ as given by [50]

$$\hat{\mathbf{h}}_B = \mathbf{C}_{hh}^B \left\{\mathbf{X}_p^B\right\}^H \left(\mathbf{X}_p^B \mathbf{C}_{hh}^B \left\{\mathbf{X}_p^B\right\}^H + \mathbf{C}_{nn}^A\right)^{-1} \mathbf{r} \tag{5.2}$$

where $\mathbf{C}_{hh}^B = E\left(\mathbf{h}_B \mathbf{h}_B^H\right)$ and $\mathbf{C}_{nn}^A = E\left(\mathbf{n}_A \mathbf{n}_A^H\right) = \mathbf{I}_{N_t M}$ are the auto-covariances of $\mathbf{h}_B$ and $\mathbf{n}_A$, respectively. $\mathbf{n}_A$ is also assumed to be independent of $\mathbf{h}_B$, i.e., $\mathbf{C}_{h_B n_A} = \mathbf{0}$. Substituting the value of $\mathbf{C}_{nn}^A$ into (5.2), it further simplifies to

$$\hat{\mathbf{h}}_B = \left(\left\{\mathbf{C}_{hh}^B\right\}^{-1} + \left\{\mathbf{X}_p^B\right\}^H \mathbf{X}_p^B\right)^{-1} \left\{\mathbf{X}_p^B\right\}^H \mathbf{r}. \tag{5.3}$$

Utilizing Maximum Ratio Transmission (MRT) which can be viewed as the spatial version of the well-known matched filter, Alice forms the beamforming vector $\mathbf{w}(m)$ for the m^{th}

subcarrier as follows from the channel estimate $\hat{\mathbf{H}}_B$ for data transmission phase

$$\mathbf{w}(m) = \hat{\mathbf{H}}_B(m) / \left\| \hat{\mathbf{H}}_B(m) \right\| \tag{5.4}$$

where $\hat{\mathbf{H}}_B(m) = \frac{\beta_B \sqrt{P_B}}{(1+P_B \beta_B)} x_{pm}^* \mathbf{r}(m) = \hat{\mathbf{h}}_B(a_m : b_m)$ with $a_m = mN_t + 1$, $b_m = (m+1)N_t$ and $\mathbf{r}(m) = \mathbf{r}(a_m : b_m)$. The received signals at Bob and Eve for the m^{th} subcarrier are

$$y_B(m) = \sqrt{P_A} [\mathbf{H}_B(m)]^H \mathbf{w}(m) x_{dm} + n_B \tag{5.5}$$

$$y_E(m) = \sqrt{P_A} [\mathbf{H}_E(m)]^H \mathbf{w}(m) x_{dm} + n_E \tag{5.6}$$

where $\mathbf{x}_d = \left[x_{d0}\ x_{d2} \cdots x_{dm} \cdots x_{d(M-1)}\right]^T$ is the normalized OFDM data symbol with unit variance sent by Alice, $\sqrt{P_A}$ denotes the power of the message symbol, n_B and n_E are the zero-mean unit-variance complex Gaussian receiver noise at Bob and Eve, respectively. The legitimate system's goal is to provide reliable communication between Alice and Bob while preventing message eavesdropping by Eve.

Eve is acting as a passive eavesdropper here, extracting information by listening. From (5.6), the effective channel fading gain for Eve is $g_E(m) = [\mathbf{H}_E(m)]^H \mathbf{w}(m)$, which is unknown to Eve. However, utilizing the blind channel estimation technique proposed in [51], Eve can extract $\mathbf{g}_E$ as well as $\mathbf{x}_d$ even from a single OFDM symbol in high SNR environment. In this role of passive eavesdropping, Eve does not afflict any damage on the legitimate transmission.

5.3 Pilot-Spoofing Attack

Pilot-spoofing is an active eavesdropping attack. For deterministic training scheme, $\mathbf{x}_p$ is both publicly known and typically specified in the standard. Under pilot-spoofing attack, Eve synchronously broadcasts its training symbol $\mathbf{x}_p^E = \sqrt{P_E}\mathbf{x}_p$ during training phase. $\sqrt{P_E}$

is the power utilized to send the pilot signal by Eve. Eve also distributes power evenly among pilot subchannels for optimality. The signal $\mathbf{r}_{ps} \in \mathbb{C}^{N_t M \times 1}$ received by Alice under pilot-spoofing attack can be conveniently written as

$$\mathbf{r}_{ps} = \mathbf{X}_{ps}^{p} \mathbf{h}_{ps} + \mathbf{n}_{ps} \tag{5.7}$$

where $(\cdot)_{ps}$ denotes the corresponding vector/matrix under pilot-spoofing attack, $\mathbf{h}_{ps}^{2MN_t \times 1} = \left[\mathbf{h}_{BE}^{T}(0) \cdots \mathbf{h}_{BE}^{T}(m) \cdots \mathbf{h}_{BE}^{T}(M-1)\right]^{T}$ and $\mathbf{h}_{BE}(m)$ is as follows, $\mathbf{h}_{BE}(m) = [\mathbf{H}_B(1,m)\ \ \mathbf{H}_E(1,m) \cdots \mathbf{H}_B(N_t,m)\ \ \mathbf{H}_E(N_t,m)]^{T}$. $\mathbf{X}_{ps}^{p}$ is of dimension $MN_t \times 2MN_t$ and given by, $\mathbf{X}_{ps}^{p} = \operatorname{diag}\left\{\mathbf{X}_{BE}(m)\right\}_{m=0}^{M-1}$ where $\mathbf{X}_{BE}^{N_t \times 2N_t}(m)$ is formed by repeating the vector $\left(x_{pm}\left[\sqrt{P_B}\ \sqrt{P_E}\right]\right)$ diagonally N_t times.

Alice applies the LMMSE method to estimate $\mathbf{h}_B$ as given by

$$\begin{aligned} \hat{\mathbf{h}}_{ps} &= \hat{\mathbf{h}}_B(ps) && (5.8) \\ &= \underbrace{\left(\left\{\mathbf{C}_{hh}^{ps}\right\}^{-1} + \left\{\mathbf{X}_{ps}^{p}\right\}^{H} \mathbf{X}_{ps}^{p}\right)^{-1}}_{\mathbf{C}_{hx}^{ps}} \left\{\mathbf{X}_{ps}^{p}\right\}^{H} \mathbf{r}_{ps} && (5.9) \end{aligned}$$

where $\mathbf{C}_{hh}^{ps} = E\left(\mathbf{h}_{ps}\mathbf{h}_{ps}^{H}\right)$ is the auto-covariances of $\mathbf{h}_{ps}$ and $\mathbf{n}_{ps} \sim \mathcal{CN}(\mathbf{0}, \mathbf{I}_{N_t M})$. $\mathbf{n}_{ps}$ is also assumed to be independent of $\mathbf{h}_{ps}$, i.e., $\mathbf{C}_{h_{ps}n_{ps}} = \mathbf{0}$.

Assuming that the elements of $\acute{\mathbf{H}}_B/\acute{\mathbf{H}}_E$ are i.i.d. zero-mean circularly-symmetric complex Gaussian $\mathcal{CN}(0,1)$ random variables, $\left\{\mathbf{C}_{hh}^{ps}\right\}^{-1}$ of dimension $2MN_t \times 2MN_t$ is given by, $\left\{\mathbf{C}_{hh}^{ps}\right\}^{-1} = \operatorname{diag}\left\{\mathbf{C}_{hh}(m)\right\}_{m=0}^{M-1}$ where $\mathbf{C}_{hh}^{2N_t \times 2N_t}(m)$ is formed by repeating the matrix $\operatorname{diag}\left([1/\beta_B\ \ 1/\beta_E]\right)$ diagonally $2N_t$ times. Also $\left(\left\{\mathbf{X}_{ps}^{p}\right\}^{H} \mathbf{X}_{ps}^{p}\right)^{2MN_t \times 2MN_t} = \operatorname{diag}\left\{\mathbf{X}(m)\right\}_{m=0}^{M-1}$ where $\mathbf{X}^{2N_t \times 2N_t}(m)$ is constructed by repeating the matrix $\begin{bmatrix} P_B & \sqrt{P_B}\sqrt{P_E} \\ \sqrt{P_B}\sqrt{P_E} & P_E \end{bmatrix}$ diagonally N_t times. Thus $\mathbf{C}_{hx}^{ps}$ is simply a block diagonal matrix of dimension $2MN_t \times 2MN_t$ with

the block $\frac{\beta_B\beta_E}{1+P_B\beta_B+P_E\beta_E}\begin{bmatrix} \frac{1}{\beta_E}+P_E & -\sqrt{P_B}\sqrt{P_E} \\ -\sqrt{P_B}\sqrt{P_E} & \frac{1}{\beta_B}+P_B \end{bmatrix}$ repeated diagonally MN_t times. For the m^{th} subcarrier, Alice's LMMSE estimation of channels are as follows

$$\hat{\mathbf{H}}_B^{ps}(m) = \frac{\beta_B\sqrt{P_B}}{(1+P_B\beta_B+P_E\beta_E)} x_{pm}^* \mathbf{r}_{ps}(m) \tag{5.10}$$

$$\hat{\mathbf{H}}_E^{ps}(m) = \frac{\beta_E\sqrt{P_E}}{(1+P_B\beta_B+P_E\beta_E)} x_{pm}^* \mathbf{r}_{ps}(m) \tag{5.11}$$

where $\mathbf{r}_{ps}(m) = \mathbf{r}_{ps}(a_m : b_m)$. Obviously, $\hat{\mathbf{H}}_E^{ps}(m) = \frac{\beta_E\sqrt{P_E}}{\beta_B\sqrt{P_B}}\hat{\mathbf{H}}_B^{ps}(m)$.

Remark 1: The above LMMSE channel estimation reflects the fact that Alice's estimation of every channel for a particular subcarrier is simply a scaled version of the same vector $x_{pm}^*\mathbf{r}_{ps}(m)$. *Thus Alice cannot distinguish her channel to Bob from her channel to Eve. Consequently, Alice gets spoofed by Eve.*

Under pilot-spoofing, Alice forms the beamforming vector $\mathbf{w}^{ps}(m)$ for the m^{th} subcarrier as follows

$$\mathbf{w}^{ps}(m) = \hat{\mathbf{H}}_B^{ps}(m) \,/\, \left\| \hat{\mathbf{H}}_B^{ps}(m) \right\|. \tag{5.12}$$

The received signals at Bob and Eve for the m^{th} subcarrier under pilot-spoofing are

$$y_B^{ps}(m) = \sqrt{P_A}\left[\mathbf{H}_B(m)\right]^H \mathbf{w}^{ps}(m)\, x_{dm} + n_B \tag{5.13}$$

$$y_E^{ps}(m) = \sqrt{P_A}\left[\mathbf{H}_E(m)\right]^H \mathbf{w}^{ps}(m)\, x_{dm} + n_E. \tag{5.14}$$

5.3.1 Fading Correlation Model

The channel frequency response at m^{th} subcarrier is given by

$$\mathbf{H}_f(m) = \sum_{l=0}^{L-1} \mathbf{H}_l e^{-j2\pi lm/M} \tag{5.15}$$

where $\mathbf{H}_l$ is the gain matrix of the l^{th} multipath. Let us denote the elements of $\mathbf{H}_f$ and $\mathbf{H}_l$ by h and $\dot{h}$, respectively. Then the channel impulse response vector $\dot{\mathbf{h}}$ and channel frequency response vector $\mathbf{h}$ are given by

$$\dot{\mathbf{h}} = \left[\text{vec}\left(\mathbf{H}_0^T\right) \cdots \text{vec}\left(\mathbf{H}_{L-1}^T\right)\right]^T \tag{5.16}$$

$$\mathbf{h} = \left[\text{vec}\left(\mathbf{H}_f^T\left(0\right)\right) \cdots \text{vec}\left(\mathbf{H}_f^T\left(M-1\right)\right)\right]^T. \tag{5.17}$$

Let $\mathbf{F}$ be the $M \times M$ unitary DFT matrix defined as

$$\mathbf{F} = \frac{1}{\sqrt{M}} \left\{ e^{-j\frac{2\pi(i-1)(j-1)}{M}} \right\}_{i,j=0}^{M-1}. \tag{5.18}$$

The relationship between the impulse and frequency responses under pilot-spoofing attack can be expressed as

$$\mathbf{h}_{ps} = \sqrt{M}\left(\mathbf{F} \otimes \mathbf{I}_{2N_t}\right)\left[\dot{\mathbf{h}}_{ps}^T \; 0 \cdots 0\right]^T. \tag{5.19}$$

Correspondingly,

$$\mathbf{C}_{hh}^{ps} = E\left(\mathbf{h}_{ps}\mathbf{h}_{ps}^H\right). \tag{5.20}$$

With uncorrelated channel impulse response (CIR) taps, the spatial correlation between the subcarriers having the same indices is just the spatial correlation between the antenna elements [52]. Accordingly, $\mathbf{C}_{hh}^{ps}$ is a block diagonal matrix of the following format

$$\mathbf{C}_{hh}^{ps} = \text{diag}\left\{\mathbf{C}_m\right\}_{m=0}^{M-1} \tag{5.21}$$

where $\mathbf{C}_m^{2N_t \times 2N_t}$ is the Hermitian spatial fading correlation matrix of the channel for the m^{th} subcarrier. The main diagonal consist of β_B and β_E repeated alternately N_t times. The off-diagonal elements depend on Alice's antenna parameters.

The eigen-decomposition of the correlation matrix is given by

$$\begin{aligned} \mathbf{C}_{hh}^{ps} &= \mathbf{U}_{hh}\mathbf{\Lambda}_{hh}\mathbf{U}_{hh}^{H} && (5.22)\\ \text{where, } \mathbf{C}_{m} &= \mathbf{U}_{m}\mathbf{\Lambda}_{m}\mathbf{U}_{m}^{H} && (5.23)\\ \mathbf{U}_{hh} &= \operatorname{diag}\left\{\mathbf{U}_{m}\right\}_{m=0}^{M-1} && (5.24)\\ \mathbf{\Lambda}_{hh} &= \operatorname{diag}\left\{\mathbf{\Lambda}_{m}\right\}_{m=0}^{M-1}. && (5.25) \end{aligned}$$

It should be noted that the number of significant eigen values is related to the number of long-term significant taps. Substituting these values into (5.9), we have

$$\hat{\mathbf{h}}_{ps} = \mathbf{U}_{hh}\left(\mathbf{\Lambda}_{hh}^{-1} + \mathbf{U}_{hh}^{H}\left\{\mathbf{X}_{ps}^{p}\right\}^{H}\mathbf{X}_{ps}^{p}\mathbf{U}_{hh}\right)^{-1}\mathbf{U}_{hh}^{H}\left\{\mathbf{X}_{ps}^{p}\right\}^{H}\mathbf{r}_{ps}. \tag{5.26}$$

By the theory of majorization [53], the matrix $\mathbf{U}_{hh}^{H}\left\{\mathbf{X}_{ps}^{p}\right\}^{H}\mathbf{X}_{ps}^{p}\mathbf{U}_{hh}$ must be diagonal for LMMSE, i.e.,

$$\mathbf{U}_{hh}^{H}\left\{\mathbf{X}_{ps}^{p}\right\}^{H}\mathbf{X}_{ps}^{p}\mathbf{U}_{hh} = \mathbf{\Lambda}_{xh}. \tag{5.27}$$

Accordingly, $\hat{\mathbf{h}}_{ps}$ reduces to the following

$$\begin{aligned} \hat{\mathbf{h}}_{ps} &= \mathbf{U}_{hh}\underbrace{\left(\mathbf{\Lambda}_{hh}^{-1} + \mathbf{\Lambda}_{xh}\right)^{-1}}_{\mathbf{\Lambda}}\mathbf{U}_{hh}^{H}\left\{\mathbf{X}_{ps}^{p}\right\}^{H}\mathbf{r}_{ps} && (5.28)\\ &= \mathbf{U}_{hh}\mathbf{\Lambda}\mathbf{U}_{hh}^{H}\left\{\mathbf{X}_{ps}^{p}\right\}^{H}\mathbf{r}_{ps} && (5.29)\\ &= \mathbf{\Delta}_{xh}\left\{\mathbf{X}_{ps}^{p}\right\}^{H}\mathbf{r}_{ps}. && (5.30) \end{aligned}$$

As $\mathbf{U}_{hh}$ is a block diagonal matrix, so is $\mathbf{\Delta}_{xh}$. Let $\mathbf{\Delta}_{xh} = \operatorname{diag}\left\{\mathbf{\Delta}_{xh}(m)\right\}_{m=0}^{M-1}$. For the m^{th}

subcarrier, Alice's LMMSE estimation of channels are as follows

$$\hat{\mathbf{H}}_B^{ps}(m) = \boldsymbol{\Delta}_{xh}^B(m)\,\mathbf{P}_{BE}(m)\,x_{pm}^*\mathbf{r}_{ps}(m) \tag{5.31}$$

$$\hat{\mathbf{H}}_E^{ps}(m) = \boldsymbol{\Delta}_{xh}^E(m)\,\mathbf{P}_{BE}(m)\,x_{pm}^*\mathbf{r}_{ps}(m) \tag{5.32}$$

where $\mathbf{P}_{BE}^{2N_t\times N_t}(m)$ is formed by repeating the vector $\left(\left[\sqrt{P_B}\ \sqrt{P_E}\right]^T\right)$ diagonally N_t times. $\boldsymbol{\Delta}_{xh}^B(m)$ and $\boldsymbol{\Delta}_{xh}^E(m)$ are $N_t\times 2N_t$ matrices comprising of rows from $\boldsymbol{\Delta}_{xh}(m)$ corresponding to B and E, respectively.

Remark 2: Due to the inclusion of spatial correlation, Alice's estimation of every channel for a particular subcarrier is now a vector multiple of the same vector $\mathbf{P}_{BE}x_{pm}^*\mathbf{r}_{ps}(m)$. *Consequently, spatial correlation introduces different weights for different elements of the common vector in contrast with the same weight as for the i.i.d. case. However, Alice still is spoofed by Eve in just a different way.*

5.3.2 Antenna Specification

We assume that Alice has uniform circular antenna with radius D, the scattering angle α, and the central angle of arrival (AOA) Θ which is uniformly distributed. The spatial correlation between antenna element p and q is given by [54]

$$C_{p,q} = e^{j\frac{4\pi D\gamma}{\lambda}}\,\mathrm{sinc}\left(\frac{4D\eta\alpha}{\lambda}\right) \tag{5.33}$$

$$\text{with, } \gamma = \sin\left(\frac{\phi_q-\phi_p}{2}\right)\sin\left(\Theta-\frac{\phi_q+\phi_p}{2}\right) \tag{5.34}$$

$$\eta = \sin\left(\frac{\phi_q-\phi_p}{2}\right)\cos\left(\Theta-\frac{\phi_q+\phi_p}{2}\right) \tag{5.35}$$

where $C_{p,q}$ are the off-diagonal elements of $\mathbf{C}_m$, λ is the wavelength, ϕ is the angle of the element in azimuth plane.

5.4 Capacity Bound

With the above communication system model, channel estimates are available at Alice but neither at Bob nor at Eve. Although Bob and Eve do not know the channel side information (CSI), they have the channel distribution information (CDI). According to Shannon, channel capacity equals the mutual information between the known received signal and the unknown transmitted signal maximized over all possible transmitted signal distributions. Consequently, for Bob the capacity is given by

$$\mathcal{C}_B = \frac{1}{M} \sum_{m=0}^{M-1} \max_{p(x_{dm})} I\left(x_{dm}; y_B^{ps}(m)\right). \tag{5.36}$$

From (5.13), assuming $g_B(m) = [\mathbf{H}_B(m)]^H \mathbf{w}^{ps}(m)$, we have

$$y_B^{ps}(m) = \sqrt{P_A} g_B(m) x_{dm} + n_B \tag{5.37}$$

$$= \sqrt{P_A}\left(\mathbb{E}\left[g_B(m)\right] + \left(g_B(m) - \mathbb{E}\left[g_B(m)\right]\right) x_{dm} + n_B\right.$$

$$= \sqrt{P_A}\mathbb{E}\left[g_B(m)\right] x_{dm} + n_B^{eff}(m). \tag{5.38}$$

where $n_B^{eff}(m) = \sqrt{P_A}\left(g_B(m) - \mathbb{E}\left[g_B(m)\right]\right) x_{dm} + n_B$ is the effective noise which is possibly neither Gaussian nor independent of the data in contrast with the typical received signal expression as in (5.37) where n_B is Gaussian and independent of x_{dm}.

The effective point-to-point channel between Alice and Bob for the m^{th} subcarrier is as shown in (5.38). $\mathbb{E}\left[g_B(m)\right]$ is known to Bob. According to the property of MMSE estimate which is the conditional mean of the measured parameter, the estimate and the zero-mean estimation error are uncorrelated. Consequently, assuming Bob has MMSE estimation of $g_B(m)$ where $\hat{g}_B(m) = \mathbb{E}\left[g_B(m)\right]$, the estimation $\mathbb{E}\left[g_B(m)\right]$ and the estimation error, $\left(g_B(m) - \mathbb{E}\left[g_B(m)\right]\right) = \left(g_B(m) - \hat{g}_B(m)\right) = \tilde{g}_B(m)$ are uncorrelated. Therefore, $\mathbb{E}\left[g_B(m)\right]$ and $n_B^{eff}(m)$ are uncorrelated.

With the above assumptions, we get

$$\mathbb{E}\left[n_B^{eff}(m)\, x_{dm}^*\right] =$$

$$\mathbb{E}\left[\sqrt{P_A}\tilde{g}_B(m)\, x_{dm}x_{dm}^* + n_B x_{dm}^*\right] \tag{5.39}$$

$$= \mathbb{E}\left[\sqrt{P_A}\tilde{g}_B(m)\,|x_{dm}|^2\right] + \mathbb{E}\left[n_B x_{dm}^*\right] \tag{5.40}$$

$$= \sqrt{P_A}\mathbb{E}\left[\tilde{g}_B(m)\right]|x_{dm}|^2 + 0 = 0. \tag{5.41}$$

Therefore, $n_B^{eff}(m)$ is uncorrelated with x_{dm} but not necessarily Gaussian. The variance of the effective noise is given by

$$\mathrm{var}\left\{n_B^{eff}(m)\right\} = 1 + P_A \,\mathrm{var}\left\{\tilde{g}_B(m)\right\} \tag{5.42}$$

$$= 1 + P_A\mathbb{E}\left[\|g_B(m)\|^2\right] + P_A\left(\mathbb{E}\left[g_B(m)\right]\right)^2. \tag{5.43}$$

Applying the *Worst Case Uncorrelated Additive Noise* Theorem from [55], a lower bound on the capacity can be obtained by replacing $n_B^{eff}(m)$ by an independent zero-mean additive Gaussian noise with the same variance. The notion that Gaussian additive noise is the worst for mutual information is not new [56–58]. Let the modified received signal at Bob for the m^{th} subcarrier, $\bar{y}_B^{ps}(m)$ corrupted by the independent zero-mean additive Gaussian noise $\bar{n}_B^{eff}(m)$ with the same variance as $n_B^{eff}(m)$ be given by

$$\bar{y}_B^{ps}(m) = \sqrt{P_A}\mathbb{E}\left[g_B(m)\right]x_{dm} + \bar{n}_B^{eff}(m). \tag{5.44}$$

Correspondingly,

$$I\left(x_{dm}; y_B^{ps}(m)\right) \geq I\left(x_{dm}; \bar{y}_B^{ps}(m)\right). \tag{5.45}$$

For additive Gaussian noise channel, the maximizing input distribution is Gaussian. Consequently, assuming $x_{dm} \sim \mathcal{CN}(0,1)$, the capacity bounds are given by

$$\mathcal{C}_B \geq \frac{1}{M}\sum_{m=0}^{M-1}\log_2\left(1+\frac{P_A\left|\mathbb{E}\left[g_B\left(m\right)\right]\right|^2}{1+P_A\,\mathrm{var}\left\{\tilde{g}_B\left(m\right)\right\}}\right) \tag{5.46}$$

$$= \frac{1}{M}\sum_{m=0}^{M-1}\log_2\left(1+SNR_B\left(m\right)\right) \tag{5.47}$$

$$\mathcal{C}_E \geq \frac{1}{M}\sum_{m=0}^{M-1}\log_2\left(1+\frac{P_A\left|\mathbb{E}\left[g_E\left(m\right)\right]\right|^2}{1+P_A\,\mathrm{var}\left\{\tilde{g}_E\left(m\right)\right\}}\right) \tag{5.48}$$

$$= \frac{1}{M}\sum_{m=0}^{M-1}\log_2\left(1+SNR_E\left(m\right)\right) \tag{5.49}$$

where $g_E\left(m\right)=\left[\mathbf{H}_E\left(m\right)\right]^H\mathbf{w}^{ps}\left(m\right)$.

From the properties of MMSE, $\tilde{\mathbf{H}}_B^{ps}\left(m\right)$ and $\hat{\mathbf{H}}_B^{ps}\left(m\right)$ are uncorrelated and $\tilde{\mathbf{H}}_B^{ps}\left(m\right)$ is zero-mean. As a result, $\mathbb{E}\left[g_B\left(m\right)\right]$ is given by

$$\mathbb{E}\left[g_B\left(m\right)\right] = \mathbb{E}\left[\left[\hat{\mathbf{H}}_B^{ps}\left(m\right)+\tilde{\mathbf{H}}_B^{ps}\left(m\right)\right]^H\frac{\hat{\mathbf{H}}_B^{ps}\left(m\right)}{\left\|\hat{\mathbf{H}}_B^{ps}\left(m\right)\right\|}\right] \tag{5.50}$$

$$= \mathbb{E}\left[\left\|\hat{\mathbf{H}}_B^{ps}\left(m\right)\right\|+\left\{\tilde{\mathbf{H}}_B^{ps}\left(m\right)\right\}^H\frac{\hat{\mathbf{H}}_B^{ps}\left(m\right)}{\left\|\hat{\mathbf{H}}_B^{ps}\left(m\right)\right\|}\right] \tag{5.51}$$

$$= \mathbb{E}\left[\left\|\hat{\mathbf{H}}_B^{ps}\left(m\right)\right\|\right]. \tag{5.52}$$

We also have,

$$\mathbb{E}\left[\left\|g_B\left(m\right)\right\|^2\right] = \mathbb{E}\left[\left\|\hat{\mathbf{H}}_B^{ps}\left(m\right)\right\|^2\right]+$$

$$\mathbb{E}\left[\frac{\left\{\hat{\mathbf{H}}_B^{ps}\left(m\right)\right\}^H}{\left\|\hat{\mathbf{H}}_B^{ps}\left(m\right)\right\|}\left\{\tilde{\mathbf{H}}_B^{ps}\left(m\right)\right\}^H\left\{\tilde{\mathbf{H}}_B^{ps}\left(m\right)\right\}\frac{\hat{\mathbf{H}}_B^{ps}\left(m\right)}{\left\|\hat{\mathbf{H}}_B^{ps}\left(m\right)\right\|}\right]$$

$$= \mathbb{E}\left[\left\|\hat{\mathbf{H}}_B^{ps}\left(m\right)\right\|^2\right]+\mathbb{E}\left[\left\|\tilde{\mathbf{H}}_B^{ps}\left(m\right)\right\|^2\right].$$

So, now $\mathrm{var}\{\tilde{g}_B(m)\}$ can be calculated. As obvious, if we take the spatial correlation into account, the above capacity expressions are too involved to be expressed into closed-form. So the effects of spatial correlation on the capacity are explored in this paper numerically. But the simpler expressions obtained assuming that the elements of $\acute{\mathbf{H}}_B/\acute{\mathbf{H}}_E$ are i.i.d. zero-mean circularly-symmetric complex Gaussian $\mathcal{CN}(0,1)$ random variables and N_t is large, are sufficient enough to present the essence of pilot-spoofing attack. The $SNR_B(m)$ and $SNR_E(m)$ thus derived are given by

$$SNR_B(m) \propto \frac{P_A P_B \beta_B^2 N_t}{P_A \beta_B (P_E \beta_E + 1) + (P_B \beta_B + P_E \beta_E + 1)} \tag{5.53}$$

$$SNR_E(m) \propto \frac{P_A P_E \beta_E^2 N_t}{P_A \beta_E (P_B \beta_B + 1) + (P_B \beta_B + P_E \beta_E + 1)}. \tag{5.54}$$

Remark 3: As P_E increases, $SNR_B(m)$ decreases but $SNR_E(m)$ increases. Consequently, the pilot-spoofing attack can inflict serious damages even when the system adopts a particular encoding-decoding process to achieve the perfect secrecy. The perfect secrecy rate which is defined as the difference of information rates between legitimate and illegitimate channel, may become non-positive under the pilot-spoofing attack.

5.5 Numerical Results

This section explores the effect of spatial correlation on the pilot-spoofing attack. For the multipath channel, we consider ITU Pedestrian A. So the power delay profile (PDP) is as shown in Table 6.1. The system sampling rate is set to 5mega-samples per second (Msps), the channel delay is quantized to the nearest multiples of 200 nsec, and $M = 32$. We assume that the PDP of all sub-channels are the same. The other antenna parameters are as follows: $N_t = 4$, $\Theta = 3\pi/2$, $\alpha = \pi/3$, and $D = 2.5\lambda$.

Fig. 5.2 presents the effect of fading correlation on the damage pilot-spoofing inflicts upon

Table 5.1: Channel delay profile of ITU Pedestrian A

Channel model	Path 1	Path 2	Path 3	Path 4
Delay(nsec)	0	110	190	410
Power(dB)	0	−9.7	−19.2	−22.8

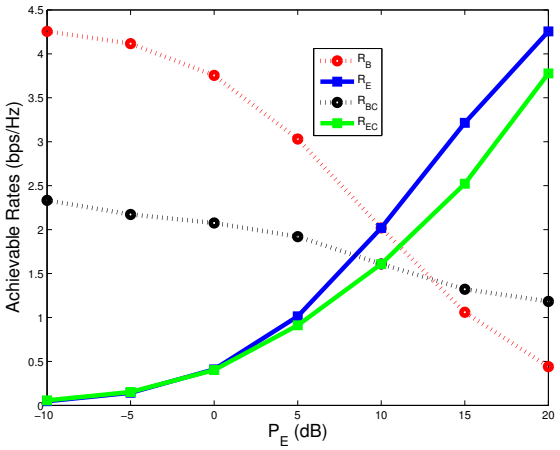


Figure 5.2: Effect of fading correlation on achievable rates under pilot-spoofing attack. $P_A = P_B = 10dB$, $N_t = 4$, $\Theta = 3\pi/2$, $\alpha = \pi/3$, and $D = 2.5\lambda$. R_B, R_E represent the achievable rates of Bob and Eve, respectively for i.i.d. assumption and R_{BC}, R_{EC} are their correlation counterparts.

legitimate transmission. As obvious, fading correlation facilitates pilot-spoofing attack in terms of overall achievable legitimate rate but the rate at which the R_B decreases is lower. The achievable rate of Bob is lower than its i.i.d. counterpart although the damaging effect is not that drastic. But this is the more realistic scenario. This occurs due to the fact that the fading correlation adds more terms in the numerator of (5.53) which are functions of P_E as well as P_B. Consequently, the effect of variation in P_E is not that drastic on SNR_B. The effects of N_t and D/λ on the achievable rates with fading correlation taken into account under pilot-spoofing attack are presented in Fig. 5.3 and Fig. 5.4. Bob's achievable rate gets saturated with large N_t and D/λ. Moreover, the higher number of antenna elements and higher antenna radius endow the legitimate system with anti-spoofing capability till $P_E = P_B$. After that Eve takes over with consequent negative perfect secrecy rate.

Fig. 5.5 shows the effect of scattering angle on the achievable rates of Bob and Eve with

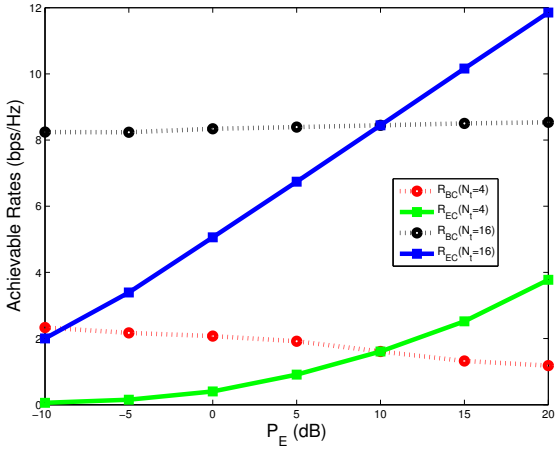


Figure 5.3: Effect of N_t on achievable rates with fading correlation under pilot-spoofing attack. $P_A = P_B = 10dB$, $\Theta = 3\pi/2$, $\alpha = \pi/3$, and $D = 2.5\lambda$.

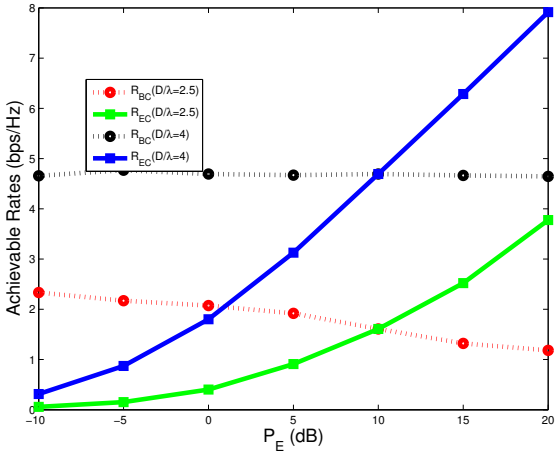


Figure 5.4: Effect of antenna radius on achievable rates with fading correlation under pilot-spoofing attack. $P_A = P_B = 10dB$, $N_t = 4$, $\Theta = 3\pi/2$, and $\alpha = \pi/3$.

fading correlation under pilot-spoofing attack. The higher the scattering angle, lower is the correlation with consequent higher achievable rate.

5.6 Conclusion

In this chapter we explore the effect of fading correlation on pilot-spoofing attack in a TDD MISO-OFDM system from information-theoretic perspective. We are the first one to

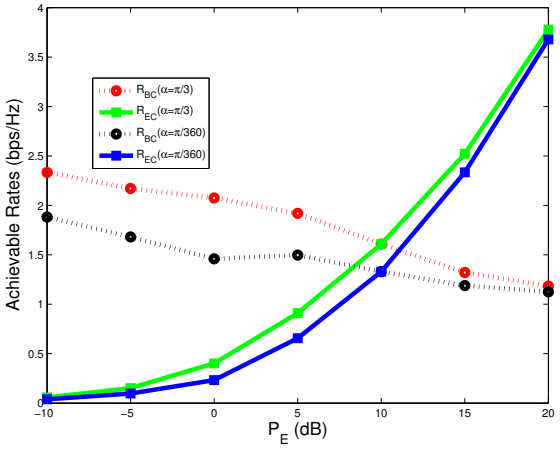


Figure 5.5: Effect of scattering angle on achievable rates with fading correlation under pilot-spoofing attack. $P_A = P_B = 10dB$, $N_t = 4$, $\Theta = 3\pi/2$, and $D = 2.5\lambda$.

consider the effect of frequency-selective spatially correlated fading channel on the efficacy of pilot-spoofing attack. Frequency-selectivity of the channel is handled by OFDM. Capacity bounds are derived. The numerical results show that spatial correlation enhances the effect of pilot-spoofing attack by lowering the achievable legitimate rate than its i.i.d. counterpart. But the achievable legitimate rate declines at a slower rate than that for i.i.d. channel.

Chapter 6

Jammer Blind Estimation of a Third-Party OFDM Channel

Novel, computationally simple and deterministic blind channel estimation schemes for PSK-OFDM and QAM-OFDM are proposed from legitimate transceivers as well as pilot-jammer's perspective. Their effectiveness in formulating the pilot-nulling attacks against OFDM is investigated. The estimators are based on the Least Squares (LS) principle and capitalize on the finite alphabet property of the information symbols. Phase ambiguity resolution requires no reference symbols while scalar ambiguity is resolved at the expense of a single pilot tone. The multipath characteristics of the channel between the target and the jammer are assumed to be Time Division Duplex (TDD) reciprocal. Simulation results are provided to demonstrate the performance of the proposed methods in channel estimation at the pilot locations as well as designing effective pilot-nulling attacks. The proposed methods estimate the jammer channel to the target perfectly to launch precise pilot-nulling attacks on OFDM in very low noise environment. The performance degrades with increasing noise.

6.1 Introduction

Knowledge of the Channel State Information (CSI) between the two transceivers and between the jammer and the target play critical role in formulating the pilot-nulling attacks that seek to null the pilot tones at the OFDM receiver [59]. The fundamental difference between CSI estimation from jammer's perspective and that between two legitimate transceivers is one of cooperation. The target system is not cooperative with the jammer that is trying to obtain CSI. This issue alone significantly complicates the situation.

In a wireless tactical scenario where a jammer attempts to estimate its own channel to the target, the only information available is the target signal intercepted by the jammer and some general knowledge about the standardization of the system adopted by the target, e.g., LTE, WiMAX etc. Consequently, the only option available to the jammer is to estimate the channel blindly based on the available channel output. Blind identification of linear systems is a rich area of research.

Since the seminal paper of Long et. al. [60] on blind estimation of multipath channel, a number of statistical estimation techniques are proposed addressing blind identification of time-invariant (TI) channels [61–63] as well as time-varying (TV) mobile radio channels [64, 65]. But due to their slow convergence rate that often requires a period of hundreds or even thousands of symbols for TI case and at least tens of symbols for TV case, statistical approaches are unsuitable for jammer which has to launch attack on the OFDM target before the estimated CSI expires in a couple of symbols in a highly mobile environment. In contrast to the statistical methods, Chotikakamthron and Suzuki [66] developed a deterministic approach based on the maximum likelihood (ML) principle and finite alphabet property of information symbols. This produces a channel estimate from a single received OFDM symbol but at the cost of huge computational complexity. Another finite alphabet-based method proposed in [67] estimates channel from a single OFDM symbol for PSK but

requires statistical averaging over hundreds of symbols for QAM.

Despite their great success, all these algorithms are plagued with the inherent phase-blindness. Usually, a few pilots or differential modulation schemes are required to remove the ambiguity. To the best of authors' knowledge, only a few papers consider the totally blind channel estimation (TBCE) problem requiring no pilots. Building upon [66], the authors in [68–70] propose a less-complex TBCE assuming slowly-varying channel transfer function coefficients in the frequency domain. They resolve the phase ambiguity by employing two different PSK-modulation schemes, for example QPSK/3-PSK or 8-PSK/7-PSK to adjacent subcarriers within the same OFDM-symbol such that the angles between a signal point of one modulation scheme and any signal point of the other modulation scheme are unique. A more general TBCE technique for PSK and QAM is developed in [71]. This method resolves the phase ambiguity when the greatest common divisor (gcd) of phase ambiguity sets of the adopted modulation schemes is 1. A new frequency-domain TBCE technique is proposed for QAM-OFDM systems in [72] that applies to Line of Sight (LoS) transmission under the conditions that the absolute value of phase rotation is less than $\pi/2$ at all subcarriers, and it is less than $\pi/4$ for at least one subcarrier. Both approaches in [71] and [72] require statistical averaging over hundreds of OFDM symbols.

Unfortunately, dictating the modulation schemes at the target by no means is at the disposal of the jammer. Furthermore, the modulation schemes usually used for OFDM (LTE, WiMAX etc.) are BPSK, QPSK, 16-QAM and 64-QAM that are associated with gcd 2, not 1. Building on the sufficient condition of channel identification in [66], the authors in this paper propose novel, deterministic blind channel estimation schemes that produce channel estimates from a single received OFDM symbol with much less computational complexity not only for PSK-OFDM but also for QAM-OFDM that inherently resolves the phase ambiguity without any pilots, imposing no restrictions on the types of modulation schemes adopted in the adjacent subcarriers. Scalar ambiguity resolution calls for only one pilot. TDD

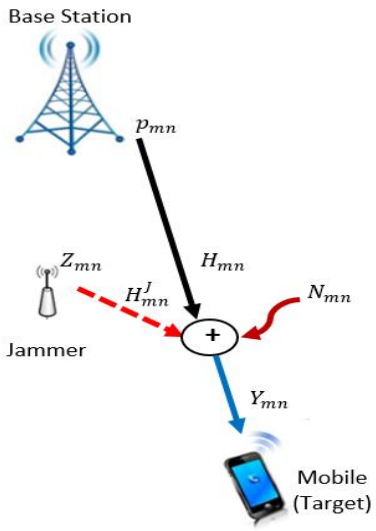


Figure 6.1: Pilot-tone nulling attack on OFDM mobile. H_{mn} is the channel between the legitimate transceivers (Base Station and Mobile) and H^J_{mn} is the channel between the jammer and the target.

reciprocity is assumed for the multipath characteristics of the third-party OFDM channel between the target and the jammer.

The remainder of this paper is organized as follows. Section 6.2 describes the pilot-nulling attack on OFDM mobile. Section 6.3 details the channel identification condition and formulates the LS estimators for PSK as well as QAM-OFDM. The proposed blind channel estimation (BCE) algorithms are detailed in section 6.4. Section 6.5 provides simulation results representing the performance of the proposed BCE algorithms. Section 6.6 concludes the paper with final remarks.

6.2 Pilot Tone Nulling Attack on OFDM

OFDM is a unique modulation in that it builds signals in the frequency domain, converts them to the time domain, transmits them, and then moves them back to the frequency domain for demodulation. This allows many narrowband signals to be easily multiplexed in

the frequency domain. By embedding pilot tones, we can compensate for channel effects and equalize the transmission. After the discrete Fourier transform (DFT) at the receiver, the received sample of the m^{th} subcarrier at the n^{th} symbol interval is given by

$$Y_{mn} = H_{mn}X_{mn} + N_{mn} \tag{6.1}$$

where Y_{mn} and X_{mn} are, respectively, the received and the transmitted symbols, H_{mn} is the channel frequency response and N_{mn} is independent and identically distributed AWGN with distribution $\mathcal{CN}(0, 1)$. Assuming a long enough Cyclic Prefix (CP), we ignore the effects of inter-symbol and inter-channel interference.

In pilot tone nulling attack, we seek to null the pilot tones. The goal is for channel estimate $\hat{H}_{mn}$ to be asymptotically close to zero, such that when $\hat{X}_{mn}$ is computed as $\hat{X}_{mn} = Y_{mn}/\hat{H}_{mn}$, we cause a division by zero that makes $\hat{X}_{mn}$ arbitrarily large. Assuming a jammer can estimate the channel between the two transceivers $\tilde{H}_{mn}$, and its own channel to the target $\hat{H}^J_{mn}$, the jamming signal as shown in Fig. 6.1 is given by

$$Z_{mn} = \frac{\tilde{H}_{mn}}{\hat{H}^J_{mn}} e^{j\pi} p_{mn} \tag{6.2}$$

which is the channel-compensated, π-radian phase shifted version of the pilot tone p_{mn}. The received pilot tone signal under nulling attack is then

$$Y^{\text{null}}_{mn} = H_{mn}p_{mn} + H^J_{mn}\frac{\tilde{H}_{mn}}{\hat{H}^J_{mn}} e^{j\pi} p_{mn} + N_{mn}. \tag{6.3}$$

If the channel estimates are close, i.e., $\tilde{H}_{mn} \approx H_{mn}$ and $\hat{H}^J_{mn} \approx H^J_{mn}$, this term converges to N_{mn}.

6.3 Blind Channel Estimation

6.3.1 Sufficient Condition for OFDM Channel Identification

Assuming M be the number of subcarriers in an OFDM symbol, i.e., $0 \leq m \leq (M-1)$ and L be the channel order, the received signal vector at the n^{th} symbol interval after DFT operation, $\mathbf{y}_n = \left(Y_{0n}\ Y_{1n}\ \cdots\ Y_{(M-1)n}\right)^T$, is given by

$$\begin{aligned} \mathbf{y}_n &= \mathbf{X}_n \mathbf{F} \mathbf{h}_n + \mathbf{n}_n \\ \mathbf{X}_n &= diag\left(X_{0n}, X_{1n}, \cdots, X_{(M-1)n}\right) \\ \mathbf{h}_n &= \left(h_{0n}\ h_{1n}\ \cdots\ h_{(L-1)n}\right)^T \\ \mathbf{F}_{p,q} &= \left(1/\sqrt{M}\right) e^{-j\frac{2\pi}{M}(pq)} \\ \mathbf{n}_n &= \left(N_{0n}\ N_{1n}\ \cdots\ N_{(M-1)n}\right)^T \end{aligned} \tag{6.4}$$

with $0 \leq p \leq (M-1)$, $0 \leq q \leq (L-1)$, $(\cdot)^T$ denoting the transpose of the corresponding vector, and $diag\,(\mathbf{v})$ returning a square diagonal matrix with the elements of vector $\mathbf{v}$ on the main diagonal. Chotikakamthron and Suzuki [66] show that the channel can be estimated from a single received OFDM symbol. Theorem 1 below states a sufficient condition for joint estimation of channel parameters and the transmitted symbols.

Theorem 1 [66]: The channel coefficients $\mathbf{h}$ *and the transmitted symbols as given by* $\mathbf{x}_n = \left(X_{0n}\ X_{1n}\ \cdots\ X_{(M-1)n}\right)^T$ *are uniquely identifiable up to a scaling factor, from a single received OFDM symbol* $\mathbf{y}_n$*, if*

$$M > Q\,(L-1) \tag{6.5}$$

with Q *being the number of distinct ratio* (X_{in}/X_{jn}) *for all possible permutations of symbols* X_{in} *and* X_{jn} *drawn from the symbol alphabet* $\mathcal{S}$*.*

Theorem 1 implies that there is only one vector $\mathbf{x}_n$ and one vector $\mathbf{h}_n$ that yield the received

vector $\mathbf{y}_n$ in the noiseless scenario within an ambiguous complex scalar.

6.3.2 Least-Squares (LS) Estimator

With the noise present, a Least-Squares estimator for both $\mathbf{x}_n$ and $\mathbf{h}_n$ can be constructed. Blind equalization of an OFDM symbol needs to solve

$$\min_{\mathbf{x}_n} \min_{\mathbf{h}_n} \|\mathbf{y}_n - \mathbf{X}_n \mathbf{F} \mathbf{h}_n\|_2^2 .$$

For a given data set $\mathbf{x}_n$, the LS estimate of the channel is

$$\hat{\mathbf{h}}_n = \left(\mathbf{A}_n^H \mathbf{A}_n\right)^{-1} \mathbf{A}_n^H \mathbf{y}_n \tag{6.6}$$

where $\mathbf{A}_n = \mathbf{X}_n \mathbf{F}$ and it is assumed that the columns of $\mathbf{A}_n$ are linearly independent. Here the superscript $(\cdot)^H$ denotes conjugate transpose. Let us define the matrix,

$$\begin{aligned} \mathbf{C}_n &= \mathbf{A}_n \left(\mathbf{A}_n^H \mathbf{A}_n\right)^{-1} \mathbf{A}_n^H & (6.7) \\ &= \mathbf{X}_n \mathbf{F} \left(\mathbf{F}^H \mathbf{X}_n^* \mathbf{X}_n \mathbf{F}\right)^{-1} \mathbf{F}^H \mathbf{X}_n^* & (6.8) \end{aligned}$$

which is nothing but the projection matrix that projects any vector (here $\mathbf{y}_n$) onto the column space of $\mathbf{A}_n$. Here the superscript asterisk denotes conjugate. Utilizing the idempotence $(\mathbf{C}_n^2 = \mathbf{C}_n)$ and Hermitian $\left(\mathbf{C}_n^H = \mathbf{C}_n\right)$ properties of the complex projection matrix, we have

$$\begin{aligned} \hat{\mathbf{x}}_n &= \arg\left(\min_{\mathbf{C}_n(\mathbf{x}_n)} \|\mathbf{y}_n - \mathbf{C}_n(\mathbf{x}_n)\, \mathbf{y}_n\|_2^2\right) & (6.9) \\ &= \arg\left[\min_{\mathbf{x}_n} \left(\mathbf{y}_n^H \mathbf{y}_n - \mathbf{y}_n^H \mathbf{C}_n \mathbf{y}_n\right)\right] & (6.10) \\ &= \arg\left[\max_{\mathbf{x}_n} \left(\mathbf{y}_n^H \mathbf{C}_n \mathbf{y}_n\right)\right] . & (6.11) \end{aligned}$$

If $\hat{\mathbf{x}}_n$ is known, then $\hat{\mathbf{H}}_n\left(\hat{\mathbf{x}}_n\right) = \hat{\mathbf{X}}_n^* \mathbf{y}_n$ is the corresponding LS estimate of the channel frequency response. As this is a Single Input Single Output (SISO) system, assuming TDD reciprocity, jammer to target channel is given by, $\mathbf{H}_n^J = \left(H_{0n}^J \; H_{1n}^J \; \cdots \; H_{mn}^J \; \cdots \; H_{(M-1)n}^J\right)^T = \hat{\mathbf{H}}_n\left(\hat{\mathbf{x}}_n\right)$.

LS Estimator for PSK-OFDM

Due to the constant modulus (CM) property of the PSK modulation scheme, $\mathbf{X}_n^* \mathbf{X}_n = \mathbf{I}_M$. Furthermore, as the columns of $\mathbf{F}$ are orthonormal, $\mathbf{F}^H \mathbf{F} = \mathbf{I}_L$. As a result, (6.11) simplifies to the following

$$\begin{aligned}
\hat{\mathbf{x}}_n &= \arg\left[\max_{\mathbf{x}_n}\left(\mathbf{y}_n^H \mathbf{X}_n \mathbf{F}\mathbf{F}^H \mathbf{X}_n^* \mathbf{y}_n\right)\right] && (6.12)\\
&= \arg\left[\max_{\mathbf{x}_n} Tr\left(\mathbf{X}_n \mathbf{F}\mathbf{F}^H \mathbf{X}_n^* \mathbf{y}_n \mathbf{y}_n^H\right)\right] \\
&= \arg\left[\max_{\mathbf{x}_n} Tr\left(\mathbf{Y}_n^* \mathbf{F}\mathbf{F}^H \mathbf{Y}_n \mathbf{x}_n^* \mathbf{x}_n^T\right)\right] \\
&= \arg\left[\max_{\mathbf{x}_n}\left(\mathbf{x}_n^T \mathbf{Y}_n^* \mathbf{F}\mathbf{F}^H \mathbf{Y}_n \mathbf{x}_n^*\right)\right] && (6.13)
\end{aligned}$$

where $\mathbf{Y}_n = diag\left(Y_{0n}, Y_{1n}, \cdots, Y_{(M-1)n}\right)$ and Tr is the matrix trace. The LS estimator in (6.13) is same as the ML estimator in [66] because the LS estimator is the ML estimator for normally distributed noise.

LS Estimator for QAM-OFDM

As the columns of $\mathbf{A}_n$ are linearly independent, the Hermitian Gram matrix, $\mathbf{G}_n = \mathbf{A}_n^H \mathbf{A}_n = \mathbf{F}^H \mathbf{X}_n^* \mathbf{X}_n \mathbf{F}$ has positive real eigenvalues. For a given $\mathbf{X}_n^* \mathbf{X}_n = \mathbf{R}_n$, $\mathbf{G}_n$ is fixed. In that case, for QAM-OFDM, (6.11) becomes as follows

$$\begin{aligned}
\hat{\mathbf{x}}_n\left(\mathbf{R}_n\right) &= \arg\left[\max_{\mathbf{x}_n}\left(\mathbf{y}_n^H \mathbf{X}_n \mathbf{F}\left(\mathbf{U}_n \mathbf{\Sigma}_n \mathbf{U}_n^H\right)^{-1} \mathbf{F}^H \mathbf{X}_n^* \mathbf{y}_n\right)\right] \\
&= \arg\left[\max_{\mathbf{x}_n}\left(\mathbf{y}_n^H \mathbf{X}_n \mathbf{F}\mathbf{U}_n \mathbf{\Delta}_n^{\frac{1}{2}} \mathbf{\Delta}_n^{\frac{1}{2}} \mathbf{U}_n^H \mathbf{F}^H \mathbf{X}_n^* \mathbf{y}_n\right)\right]
\end{aligned}$$

$$
\begin{aligned}
&= \arg\left[\max_{\mathbf{x}_n} Tr\left(\mathbf{X}_n\mathbf{F}\mathbf{U}_n\boldsymbol{\Delta}_n^{\frac{1}{2}}\boldsymbol{\Delta}_n^{\frac{1}{2}}\mathbf{U}_n^H\mathbf{F}^H\mathbf{X}_n^*\mathbf{y}_n\mathbf{y}_n^H\right)\right] \\
&= \arg\left[\max_{\mathbf{x}_n} Tr\left(\mathbf{Y}_n^*\mathbf{F}\mathbf{U}_n\boldsymbol{\Delta}_n^{\frac{1}{2}}\boldsymbol{\Delta}_n^{\frac{1}{2}}\mathbf{U}_n^H\mathbf{F}^H\mathbf{Y}_n\mathbf{x}_n^*\mathbf{x}_n^T\right)\right] \\
&= \arg\left[\max_{\mathbf{x}_n}\left(\mathbf{x}_n^T\mathbf{Y}_n^*\mathbf{F}\mathbf{U}_n\boldsymbol{\Delta}_n^{\frac{1}{2}}\boldsymbol{\Delta}_n^{\frac{1}{2}}\mathbf{U}_n^H\mathbf{F}^H\mathbf{Y}_n\mathbf{x}_n^*\right)\right] \qquad (6.14)
\end{aligned}
$$

where $\mathbf{G}_n = \mathbf{U}_n\boldsymbol{\Sigma}_n\mathbf{U}_n^H$ with unitary matrix $\mathbf{U}_n \in \mathbb{C}^{L\times L}$ and diagonal eigenvalue matrix $\boldsymbol{\Sigma}_n \in \mathbb{R}^{L\times L}$. Also, $\Delta_n = \boldsymbol{\Sigma}_n^{-1}$, both containing real positive diagonal elements.

From (6.13) and (6.14), it is obvious that these estimators are associated with huge computational complexity for large M. The values of Q for QPSK, 16-QAM and 64-QAM modulation schemes are respectively given by, $Q_{QPSK} = 4$, $Q_{16-QAM} = 52$ and $Q_{64-QAM} = 956$. To meet the channel identification condition, assuming the lowest channel order of 2, i.e., $L = 2$, the minimum values of M which are usually radix-2 numbers to ensure efficient FFT operation, are as follows

$$M_{QPSK}^{\min} > 4 = 8 \ \text{(nearest radix-2 number)} \qquad (6.15)$$

$$M_{16-QAM}^{\min} > 52 = 64 \ \text{(nearest radix-2 number)} \qquad (6.16)$$

$$M_{64-QAM}^{\min} > 956 = 1024 \ \text{(nearest radix-2 number)}\,. \qquad (6.17)$$

LS Estimator from Pilot-Jammer's Perspective

Fortunately, pilot-jammer is interested only in the channel frequency responses at the pilot locations which is always much lower than M, especially when the jammer intends to jam a mobile rather than a base station. In that case the LS estimators are modified as follows for PSK-OFDM

$$
\begin{aligned}
\hat{\mathbf{x}}_{np} &= \arg\left[\max_{\mathbf{x}_{np}}\left(\mathbf{y}_{np}^H\mathbf{X}_{np}\mathbf{F}_p\left(\mathbf{F}_p^H\mathbf{F}_p\right)^{-1}\mathbf{F}_p^H\mathbf{X}_{np}^*\mathbf{y}_{np}\right)\right] \\
&= \arg\left[\max_{\mathbf{x}_{np}}\left(\mathbf{x}_{np}^T\mathbf{Y}_{np}^*\mathbf{F}_p\boldsymbol{\Omega}_{psk}\mathbf{F}_p^H\mathbf{Y}_{np}\mathbf{x}_{np}^*\right)\right] \qquad (6.18)
\end{aligned}
$$

and for QAM-OFDM,

$$\begin{aligned}\hat{\mathbf{x}}_{np}\left(\mathbf{R}_{np}\right) &= \arg\left[\max_{\mathbf{x}_{np}}\left(\mathbf{y}_{np}^{H}\mathbf{X}_{np}\mathbf{F}_{p}\left(\mathbf{G}_{np}\right)^{-1}\mathbf{F}_{p}^{H}\mathbf{X}_{np}^{*}\mathbf{y}_{np}\right)\right] \\ &= \arg\left[\max_{\mathbf{x}_{np}}\left(\mathbf{x}_{np}^{T}\mathbf{Y}_{np}^{*}\mathbf{F}_{p}\boldsymbol{\Omega}_{qam}\mathbf{F}_{p}^{H}\mathbf{Y}_{np}\mathbf{x}_{np}^{*}\right)\right] \end{aligned} \tag{6.19}$$

where $\{\cdot\}_{np}/\{\cdot\}_{p}$ is constructed from $\{\cdot\}_{n}/\{\cdot\}$ by keeping only the elements corresponding to the pilots. $\boldsymbol{\Omega}_{psk}$ for PSK and $\boldsymbol{\Omega}_{qam}$ for QAM are the inverses of the eigen-decompositions of respectively $\left(\mathbf{F}_{p}^{H}\mathbf{F}_{p}\right)$ and $\left(\mathbf{G}_{np}=\mathbf{F}_{p}^{H}\mathbf{R}_{np}\mathbf{F}_{p}\right)$. As the columns of $\mathbf{F}_{p}$ are not orthonormal anymore, $\left(\mathbf{F}_{p}^{H}\mathbf{F}_{p}\right)\neq\mathbf{I}_{P}$, where P is the number of pilots. To ensure that the inverses exist, we have to satisfy that $P\geq L$.

6.4 Blind Detection Algorithm

Our simple blind detection algorithms capitalize on the finite alphabet property of the input OFDM symbol and the inherent characteristics of the objective function as shown below

$$\begin{aligned} & f\left(X_{0n},X_{1n},\cdots,X_{kn},\cdots,X_{(M-1)n}\right)=f\left(\mathbf{x}_{n}\right) \\ &= \begin{cases} \left(\mathbf{x}_{n}^{T}\underbrace{\mathbf{Y}_{n}^{*}\mathbf{F}\mathbf{F}^{H}\mathbf{Y}_{n}}_{\mathbf{K}_{psk}^{M\times M}(n)}\mathbf{x}_{n}^{*}\right) & \text{PSK} \\ \left(\mathbf{x}_{n}^{T}\underbrace{\mathbf{Y}_{n}^{*}\mathbf{F}\mathbf{U}_{n}\boldsymbol{\Delta}_{n}^{\frac{1}{2}}\boldsymbol{\Delta}_{n}^{\frac{1}{2}}\mathbf{U}_{n}^{H}\mathbf{F}^{H}\mathbf{Y}_{n}}_{\mathbf{K}_{qam}^{M\times M}(\mathbf{R}_{n})}\mathbf{x}_{n}^{*}\right) & \text{QAM.} \end{cases} \end{aligned} \tag{6.20}$$

As obvious from (6.20), both the $\mathbf{K}_{psk}^{M\times M}\left(n\right)$ and $\mathbf{K}_{qam}^{M\times M}\left(\mathbf{R}_{n}\right)$ are Hermitian matrices.

Hence, the general expression of (6.20) is as follows

$$f(\mathbf{x}_n) = \sum_{i=0}^{(M-1)} \sum_{j=0}^{(M-1)} K_{ij}^n X_{in} X_{jn}^* \tag{6.21}$$

$$= \sum_{i=0}^{(M-1)} K_{ii}^n |X_{in}|^2 + 2 \sum_{i=0}^{(M-1)} \sum_{\acute{j}=i+1}^{(M-1)} \Re\left\{K_{i\acute{j}}^n X_{in} X_{\acute{j}n}^*\right\} \tag{6.22}$$

where $K_{ij}^n / K_{i\acute{j}}^n$ is the element of $\mathbf{K}(n)$ in the i^{th} row and $j^{\text{th}}/\acute{j}^{\text{th}}$ column. The first term of (6.22) is absolutely phase-ambiguous but the second term depends on the relative phases of the data symbols. So the second term is only source of phase information here.

The optimization in (6.20) or (6.22) apparently seems an onerous task with no obvious and easy solution. A brute force algorithm must exhaust all possible combinations of $\mathbf{x}_n$ to find out the maximum. With $|S|$ be the constellation size, the number of such possible combinations is $|S|^M$ which is simply prohibitive for large constellation size or large OFDM symbol.

From (6.21), for any scalar ambiguity $\alpha = |\alpha| e^{j\theta_{sa}}$ we get

$$f^{\alpha}(\mathbf{x}_n) = \sum_{i=0}^{(M-1)} \sum_{j=0}^{(M-1)} K_{ij}^n \{X_{in}\alpha\} \{X_{jn}\alpha\}^* \tag{6.23}$$

$$= |\alpha|^2 \sum_{i=0}^{(M-1)} \sum_{j=0}^{(M-1)} K_{ij}^n X_{in} X_{jn}^* = |\alpha|^2 f(\mathbf{x}_n). \tag{6.24}$$

Consequently, the objective function $f(\mathbf{x}_n)$ is associated with a scalar ambiguity with unit amplitude, i.e., $|\alpha| = 1$ and phase belonging to an infinite set, i.e., $\theta_{sa} \in [0, 2\pi]$. For QPSK and 16/64-QAM OFDM, the scalar ambiguity set is discrete and simply given by $\{\pm 1, \pm j\}$, i.e., $\theta_{sa} \in \{0, \pi/2, \pi, 3\pi/2\}$. This implies that there are 4 different solutions to (6.22) yielding the same maximum value of the objective function for QPSK and 16/64-QAM OFDM. But a single pilot suffices to resolve this ambiguity in very high SNR environment.

$$\mathbf{K} = \begin{bmatrix} \mathcal{F}_{00}\left|H_0\right|^2\left|X_0\right|^2 & \mathcal{F}_{01}H_0^*H_1X_0^*X_1 & \cdots & \mathcal{F}_{0(M-1)}H_0^*H_{M-1}X_0^*X_{M-1} \\ \mathcal{F}_{10}H_0H_1^*X_0X_1^* & \mathcal{F}_{11}\left|H_1\right|^2\left|X_1\right|^2 & \cdots & \mathcal{F}_{1(M-1)}H_1^*H_{M-1}X_1^*X_{M-1} \\ \vdots & \vdots & \cdots & \vdots \\ \mathcal{F}_{(M-1)0}H_0H_{M-1}^*X_0X_{M-1}^* & \mathcal{F}_{(M-1)1}H_1H_{M-1}^*X_1X_{M-1}^* & \cdots & \mathcal{F}_{(M-1)(M-1)}\left|H_{M-1}\right|^2\left|X_{M-1}\right|^2 \end{bmatrix} \tag{6.25}$$

6.4.1 Deterministic Algorithm

Our goal is to find the maximum value of a multivariate real-valued objective function $f^{\alpha}\left(\mathbf{x}_n\right)$ where $X_{kn} \in \mathcal{S} = \left\{S_1, S_2, \cdots, S_{|S|}\right\}$ with $|S| < \infty$ be the cardinality of $\mathcal{S}$. Let us define, $\dot{\mathbf{F}}_{psk} = \mathbf{F}\mathbf{F}^H$, $\dot{\mathbf{F}}^n_{qam} = \mathbf{F}\mathbf{U}_n\boldsymbol{\Delta}_n^{\frac{1}{2}}\boldsymbol{\Delta}_n^{\frac{1}{2}}\mathbf{U}_n^H\mathbf{F}^H$, and $\mathcal{F}_{ab}$ be the element of $\dot{\mathbf{F}}$ in the a^{th} row and b^{th} column where $0 \leq a, b \leq (M-1)$. With these notations, $\mathbf{K}\left(n/\mathbf{R}_n\right)$ is as shown in (6.25) assuming negligible noises. For compactness, $n/\mathbf{R}_n$ which indicates association with a particular OFDM symbol, is dropped.

With the optimum input sequence, $\mathbf{x}_n^{opt}$ which is the actual OFDM-symbol sent by the transmitter, the objective function reduces to its optimum value, $f^{opt}\left(n\right) = f\left(\mathbf{x}_n^{opt}\right)$, which is given by

$$f^{opt}\left(n\right) = \sum_{i=0}^{(M-1)} \mathcal{F}_{ii}^n\left|H_{in}\right|^2\left|X_{in}^{opt}\right|^4 + 2\sum_{i=0}^{(M-1)}\sum_{\acute{j}=i+1}^{(M-1)} \Re\left\{\mathcal{F}_{i\acute{j}}^n H_{in}^* H_{\acute{j}n}\left|X_{in}^{opt}\right|^2\left|X_{\acute{j}n}^{opt}\right|^2\right\}. \tag{6.26}$$

This $f^{opt}\left(n\right)$ is also the maximum value of the objective function because only the actual OFDM-symbol reduces the Euclidean distance, $\left\|\mathbf{y}_n - \mathbf{X}_n\mathbf{F}\mathbf{h}_n\right\|_2$ to its minimum.

Let us analyze any off-diagonal term $K_{ab} = \mathcal{F}_{ab}H_a^*H_bX_a^*X_b = \mathcal{F}_{ab}H_a^*H_b\left|X_a\right|\left|X_b\right|e^{j(\angle X_b - \angle X_a)}$.

We assume that

$$\theta_{ab} = \left(\underbrace{\angle \mathcal{F}_{ab}}_{\theta^{\mathcal{F}}_{ab}} + \underbrace{\angle H_b - \angle H_a}_{\theta^{h}_{ab}} \right) = \left(\theta^{\mathcal{F}}_{ab} + \theta^{h}_{ab} \right) \tag{6.27}$$

$$\theta^{x}_{ab} = \left(\angle X_b - \angle X_a \right). \tag{6.28}$$

For PSK, due to CM property, magnitudes of X_a/X_b don't matter. For QAM, as we apply the algorithm to a specific $\mathbf{R}_n$, $|X_a|$ and $|X_b|$ are already known. Due to scalar ambiguity, we can choose X_a arbitrarily from the corresponding part of the constellation. Now we have to search through the part of the constellation set corresponding to $|X_b|$ for optimal X_b so that $K_{ab} X^*_b X_a$ reduces to its optimal value $\Re\left\{ \mathcal{F}_{ab} H^*_a H_b \left|X_a\right|^2 \left|X_b\right|^2 \right\}$.

Let us now multiply K_{ab} by the chosen X_a. Taking scalar ambiguity of X_a into consideration, the modified K_{ab} denoted by $\bar{K}_{ab}$ is given by

$$\bar{K}_{ab} = \mathcal{F}_{ab} H^*_a H_b X^*_a X_b \left(\alpha X_a\right) \tag{6.29}$$

$$= \left|\mathcal{F}_{ab}\right| \left|H_a\right| \left|H_b\right| \left|X_a\right|^2 \alpha X_b e^{j\theta_{ab}}. \tag{6.30}$$

Let us denote the part of the constellation associated with $|X_b|$ by $\mathcal{S}_b$. During the search, we multiply $\bar{K}_{ab}$ with $X_{\acute{b}}$ where, $X_{\acute{b}} \in \{X^*_b\}$. Due to symmetry of the constellation diagram $\{X^*_b\} = \mathcal{S}_b$. This operation modifies $\bar{K}_{ab}$ into $\breve{K}_{ab}$ as follows

$$\breve{K}_{ab} = \bar{K}_{ab} X_{\acute{b}} \tag{6.31}$$

$$= \left|\mathcal{F}_{ab}\right| \left|H_a\right| \left|H_b\right| \left|X_a\right|^2 \left|X_b\right|^2 \alpha e^{j\theta_{ab}} e^{j\theta_{b\acute{b}}} \tag{6.32}$$

where $\theta_{b\acute{b}} = \angle X_b + \angle X_{\acute{b}}$. At the optimal point,

$$\breve{K}^{opt}_{ab} = \bar{K}_{ab} X_{\acute{b}}\left(opt\right) = \bar{K}_{ab}\left(\alpha X_b\right)^* \tag{6.33}$$

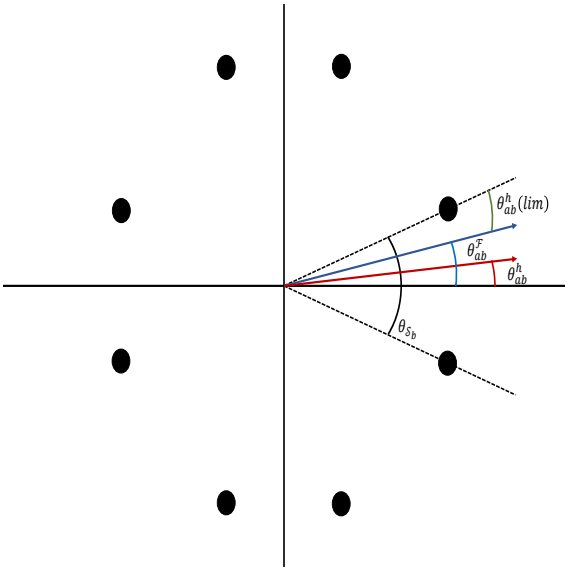


Figure 6.2: $\theta^h_{ab}\,(\text{lim})$ for 16-QAM with $|X_b| = \sqrt{10}$.

$$= |\mathcal{F}_{ab}|\,|H_a|\,|H_b|\,|X_a|^2\,|X_b|^2\,e^{j\theta_{ab}}. \tag{6.34}$$

Obviously, during search, $\breve{K}^{opt}_{ab}$ is basically being rotated by $e^{j\theta_{b\acute{b}}}$ with consequent production of its counterparts, i.e., $\breve{K}_{ab}$s, one in each decision region of $\mathcal{S}_b$. Each decision region is associated with its unique $\Re\left\{\breve{K}_{ab}\right\}$ like positive maximum, positive second maximum, negative maximum, negative second maximum and so on. Value of θ_{ab} tells us which $\Re\left\{\breve{K}_{ab}\right\}$ to look for during search process. From (6.27), θ_{ab} consists of two components. Although $\theta^{\mathcal{F}}_{ab}$ is known to us, we don't know about θ^h_{ab} which depends on channel. For noiseless scenario, $\theta^{\mathcal{F}}_{ab}$ and θ_{ab} will lie in the same decision region if met by the following restriction,

$$\left|\theta^h_{ab}\right| < \left(\frac{1}{2}\theta_{\mathcal{S}_b} - \left|\theta^{\mathcal{F}}_{ab}\right|\right) = \theta^h_{ab}\,(\text{lim}) \tag{6.35}$$

where $\theta_{\mathcal{S}_b}$ is the minimum angular distance between any two signal points on $\mathcal{S}_b$ as shown in Fig. 6.2. Under this circumstance, we can decide on the optimum X_b based on the known value of $\theta^{\mathcal{F}}_{ab}$. The above findings can be summarized into the following theorem.

Theorem 2: The proposed blind detection algorithm can uniquely identify the channel pa-

rameters $\mathbf{H} = [H_a\ H_b]$ *and the corresponding transmitted symbols* $\mathbf{x} = [X_a\ X_b]$ *up to a complex scaling factor by using only the received vector if angular separation between* H_a *and* H_b *is less than* $\theta^h_{ab}\,(lim)$.

Applying the same approach to the elements of matrix $\mathbf{K}$ either along the first row or the upper diagonal, the whole OFDM-symbol and the associated channel parameters can be identified uniquely up to a complex scaling factor. Let us call the former one, row-detection method and the later one, diagonal-detection method. Each one has its own advantages and disadvantages. Row-detection method requires the knowledge of $(M-1)$ $\mathcal{F}_{ab}$s, from $\mathcal{F}_{01}$ to $\mathcal{F}_{0(M-1)}$. Diagonal-detection method needs to know only the value of $\mathcal{F}_{01}$ as $\mathcal{F}_{ab}$ repeats itself diagonally due to the special structure of DFT matrix. Additionally, if $\left|\theta^h_{ab}\right| > \theta^h_{ab}\,(\text{lim})$, in row-detection method, it will affect the evaluation of only the corresponding X_b because evaluation of all X_bs depend on the same X_a, i.e., value of X_0. With diagonal-detection method, the error propagates from its origin to the end of the sequence because in this method, evaluation of X_b depends on the value of previous X_b, i.e., $X_{(b-1)}$.

Remark 1: One major advantage of the proposed method over its counterpart as presented in [68] is that X_a *and* X_b *do not necessarily have to belong to the adjacent subcarriers. As obvious from the formulation of the estimators for pilot-jammer, as long as the matrix* $\mathbf{K}$ *and vector* $\mathbf{x}_n$ *are constructed from their original version by only keeping the elements corresponding to the selected subcarriers, and as long as the number of selected subcarriers is more than the channel length,* X_a *and* X_b *can belong to any subcarrier. But the closer the subcarriers, the higher the probability that* $\left|\theta^h_{ab}\right| < \theta^h_{ab}\,(lim)$.

First we consider the case when signal points in $\mathcal{S}_b$ lie along the $45^0/135^0$ lines on the constellation diagram as is the case with QPSK or 16-QAM with $|X_b| = \sqrt{2}/\sqrt{18}$. The four possible cases with $0^0 \leq |\theta_{01}| < 45^0$ and $\theta_{1\acute{1}} \in \{0, \pi/2, -\pi/2, \pi\}$ are illustrated in Fig. 6.3.

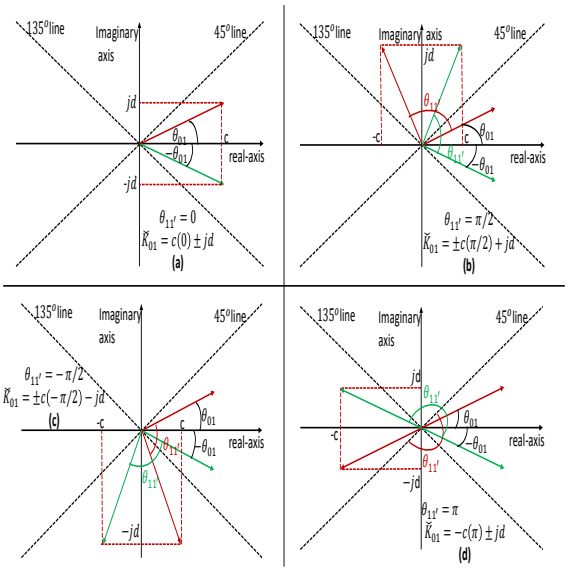


Figure 6.3: The four cases for $0 \leq |\theta_{01}| < 45^o$ and $\theta_{1\acute{1}} \in \{0, \pi/2, -\pi/2, \pi\}$. $2\Re\left\{\breve{K}_{01}^{opt}\right\} = +2c\,(0)$ which is the positive maximum real part of the four choices.

Going from case (a) to (d), $\theta_{1\acute{1}}$ produces the following contributions to the objective function

$$2\Re\left\{\breve{K}_{01}\right\} = \begin{cases} +2c\,(0)\,, & \theta_{1\acute{1}} = 0 \\ \pm 2c\,(\pi/2)\,, & \theta_{1\acute{1}} = \pi/2 \\ \pm 2c\,(-\pi/2)\,, & \theta_{1\acute{1}} = -\pi/2 \\ -2c\,(\pi)\,, & \theta_{1\acute{1}} = \pi \end{cases}$$
$$\text{with } |c\,(0)| \text{ or } |c\,(\pi)| > |c\,(\pi/2)| \text{ or } |c\,(-\pi/2)|\,. \tag{6.36}$$

Obviously, for this phase range of θ_{01}, $2\Re\left\{\breve{K}_{01}^{opt}\right\} = +2c\,(0)$ which is the positive maximum real part of the four choices. Following the same process for other phase-ranges of θ_{01}, we discover that for $45^0 < |\theta_{01}| < 90^0$, $2\Re\left\{\breve{K}_{01}^{opt}\right\} = +2c\,((\pm\pi/2)$ which is the positive minimum real part of the four options, for $90^0 < |\theta_{01}| < 135^0$, $2\Re\left\{\breve{K}_{01}^{opt}\right\} = -2c\,((\pm\pi/2)$ which is the negative maximum real part of the four choices, and for $135^0 < |\theta_{01}| \leq 180^0$, $2\Re\left\{\breve{K}_{01}^{opt}\right\} = -2c\,((\pi)$ which is the negative minimum real part of the four choices.

When the signal points are off the 45^0 or 135^0 lines on the constellation diagram as can be the case with QAM, the scenario is more involved. Based on the value of θ_{01}, there are more values for $2\Re\left\{\breve{K}_{01}^{opt}\right\}$ than just maximum/minimum positive/negative real part. Obviously, the scenarios become phase-ambiguous when θ_{01} is along 45^0 and 135^0 lines with $|c| = |d|$ or along the imaginary axis.

6.4.2 Algorithm for PSK-OFDM

For PSK-OFDM, due to its CM property, $\mathbf{K}_{psk}^{M\times M}(n)$ is always constant for a given OFDM symbol and specific channel order. Let us consider QPSK-OFDM with $\left\{\pm\frac{1}{\sqrt{2}} \pm j\frac{1}{\sqrt{2}}\right\}$ constellation set and assume that $X_{0n} = \frac{1}{\sqrt{2}} + j\frac{1}{\sqrt{2}}$ and $K_{0r}^{n} = \pm c_{0r} \pm j d_{0r}$ with $1 \leq r \leq (M-1)$. Following the algorithm mentioned above, X_{rn} can be easily determined from the table 6.1.

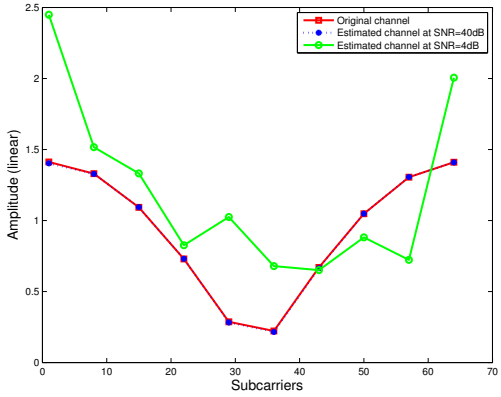
Table 6.1: X_{rn} with $(c_{0r} \neq d_{0r})$.

K_{0r}^{n}	X_{rn} with $(c_{0r} > d_{0r})$	X_{rn} with $(c_{0r} < d_{0r})$
$c_{0r} + jd_{0r}$	$\frac{1}{\sqrt{2}} + j\frac{1}{\sqrt{2}}$	$-\frac{1}{\sqrt{2}} + j\frac{1}{\sqrt{2}}$
$c_{0r} - jd_{0r}$	$\frac{1}{\sqrt{2}} + j\frac{1}{\sqrt{2}}$	$\frac{1}{\sqrt{2}} - j\frac{1}{\sqrt{2}}$
$-c_{0r} + jd_{0r}$	$-\frac{1}{\sqrt{2}} - j\frac{1}{\sqrt{2}}$	$-\frac{1}{\sqrt{2}} + j\frac{1}{\sqrt{2}}$
$-c_{0r} - jd_{0r}$	$-\frac{1}{\sqrt{2}} - j\frac{1}{\sqrt{2}}$	$\frac{1}{\sqrt{2}} - j\frac{1}{\sqrt{2}}$

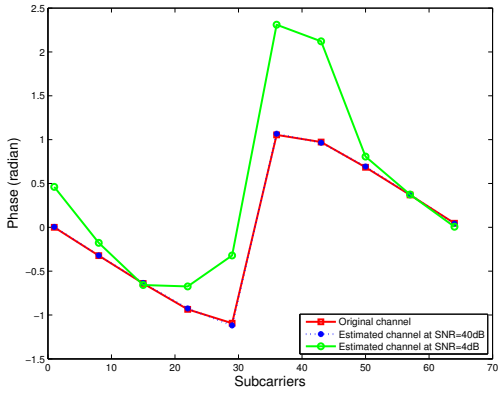
6.4.3 Algorithm for QAM-OFDM

As obvious from (6.20), $\mathbf{K}_{psk}$ is independent of input data sequence due to the CM property of the data symbols but $\mathbf{K}_{qam}$ is absolutely reliant upon the magnitude and the order of the data symbols in the input sequence. Correspondingly, in contrast to $\mathbf{K}_{psk}$ which is constant for a given received OFDM symbol, having a constant $\mathbf{K}_{qam}$ requires not only a given received OFDM symbol but also a given $\mathbf{X}_n^*\mathbf{X}_n$. Consequently, for QAM-OFDM our low-complexity approach is as follows.

First of all we find all possible combinations for $\mathbf{R}_n$. There are 3 different amplitudes



(a)



(b)

Figure 6.4: Performance of the proposed BCE for QPSK-OFDM. The proposed method estimates the channel at the pilot locations perfectly at very high SNR ($SNR \geq 28dB$). It performs poorly at low SNR. FFT size $M = 64$, channel order $L = 2$, and number of pilots $P = 10$ with pilot density 1/7.

for 16-QAM, $\mathcal{A}_{16} = \{\sqrt{2}, \sqrt{10}, \sqrt{18}\}$ and 9 different amplitudes for 64-QAM as given by $\mathcal{A}_{64} = \{\sqrt{2}, \sqrt{10}, \sqrt{18}, \sqrt{26}, \sqrt{34}, \sqrt{50}, \sqrt{58}, \sqrt{74}, \sqrt{98}\}$. Correspondingly, there are 3^M (3^P for pilot-jammer) different $\mathbf{R}_n$s for 16-QAM and 9^M (9^P for pilot-jammer) different $\mathbf{R}_n$s for 64-QAM. Thus the number of $\mathbf{K}_{qam}$ to be calculated for a given OFDM symbol reduces from $16^M/64^M$ to much lower $3^M/9^M$ for legitimate transceivers to even lower $3^P/9^P$ for pilot-jammer.

For a particular $\mathbf{R}_n$, the magnitudes and the order of the data points are fixed but phases are ambiguous. Correspondingly, our next step is to find out the maximum value of the

objective function, $f_{qam}^{opt}(\mathbf{x}_n)_{\mathbf{R}_n}$ for all $\mathbf{R}_n$s, i.e., for all $[\mathbf{K}_{qam}(\mathbf{R}_n)]$s. Finally we choose the maximum among all of the $\left[f_{opt}^{qam}(\mathbf{x}_n)_{\mathbf{R}_n}\right]$s as follows

$$f_{qam}^{opt}(\mathbf{x}_n) = \max_{\mathbf{R}_n} \left[f_{qam}^{opt}(\mathbf{x}_n)_{\mathbf{R}_n}\right]. \tag{6.37}$$

6.4.4 Computational Complexity Analysis

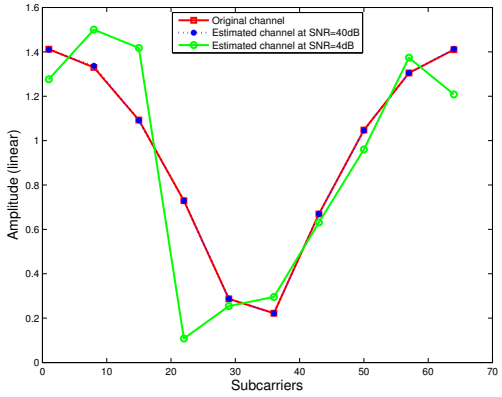
The proposed BCE method provides optimal solution to (6.20) at much lower computational complexity. The exhaustive search which is guaranteed to provide the optimal solution to (6.20) is plagued with huge computational complexity. First of all, for a specific $\mathbf{K}(n/\mathbf{R}_n)$, the exhaustive method has to find out all possible $|S|^M$ combinations of the input OFDM symbol $\mathbf{x}_n$. Then for each possible $\mathbf{x}_n$, $f(\mathbf{x}_n)$ has to be calculated to ultimately get to the optimum. Each calculation of $f(\mathbf{x}_n)$ involves $\{M(M+1)+1\}$ mathematical operations. For the proposed method, one has to look into only $(M-1)$ non-diagonal terms in the first row of $\mathbf{K}(n/\mathbf{R}_n)$ for the row-detection method or $(M-1)$ upper diagonal terms of $\mathbf{K}(n/\mathbf{R}_n)$ for diagonal-detection method. For each term, one has to search through either the whole alphabet set or part of it based on the type of modulation scheme and then compare. So computational complexity reduces from $\mathcal{O}\left(|S|^M\{M(M+1)+1\}+1\right)$ associated with the exhaustive search to $\mathcal{O}\left((M-1)\{|S|+2\}\right)$ corresponding to the proposed method for a given $\mathbf{K}(n/\mathbf{R}_n)$, and to $\mathcal{O}\left(\left|\mathcal{A}_{16/64}\right|^M\{(M-1)\{|S|+2\}\}+1\right)$ for all $\mathbf{R}_n$s of a given symbol. Here $\left|\mathcal{A}_{16/64}\right|$ denotes the cardinality of $\mathcal{A}_{16/64}$. For pilot jammer, the complexity further reduces to $\mathcal{O}\left((P-1)\{|S|+2\}\right)$ for a given $\mathbf{K}(n/\mathbf{R}_n)$, and to $\mathcal{O}\left(\left|\mathcal{A}_{16/64}\right|^P\{(P-1)\{|S|+2\}\}+1\right)$ for all $\mathbf{R}_n$s of a given symbol.

6.5 simulation

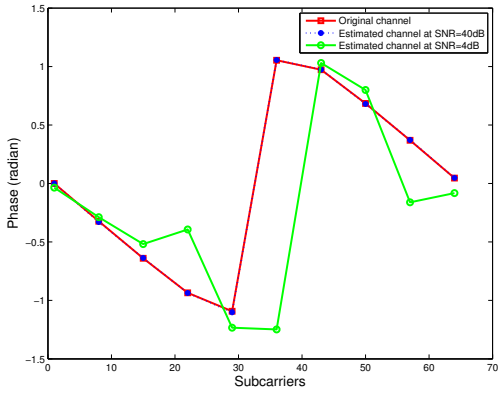
In this section, simulation results are provided to show performance gained by the proposed method. The system operates under multipath channels between the legitimate transceivers and between the jammer and the target with the maximum delay spread equal to the size of the CP. The multipath channel at any instant is described by a main path of amplitude 1.0, plus one or more paths, each having a unique delay, amplitude, and phase with respect to the main path. The third-party OFDM channel is assumed to be TDD reciprocal. For each channel estimation, only data obtained over a single OFDM symbol is used. We simulate the case with $0 < |\theta_{01}| < 45^o$. To ensure this phase range, we keep L to its minimum, i.e., 2 which ensures small phase values for $\mathcal{F}_{ab}$s and use small phase values for the multipaths which results in small phase differences for the Hs. The first subcarrier is used as pilot to resolve the scalar ambiguity.

Fig. 6.4 and Fig. 6.5 present the performance of the proposed blind channel estimation methods. As obvious, the proposed methods estimate the channel perfectly at the pilot locations at very high SNR. The performance becomes increasingly more degraded at lower SNR. With 16-QAM, the estimation is perfect for ($SNR \geq 20dB$) and for QPSK the estimation is perfect for ($SNR \geq 28dB$). The CM property of QPSK makes it more vulnerable to phase ambiguities.

Fig. 6.6 shows the effectiveness of these blind channel estimation methods in formulating pilot-nulling attacks on QPSK and 16-QAM OFDM as compared to pilot-based LS method. We assume that the channel and pilots between the legitimate transceivers are known to the jammer. We further assume that the jammer is synchronized with the target and fast enough to hit the target before the estimated CSI expires in the coherence time of the estimated channel. The attacks are as effective as its pilot-based counterparts at very low noise scenario but while the pilot-based method results in a $(P/M)\,\%$ reduction of useful bandwidth, the



(a)



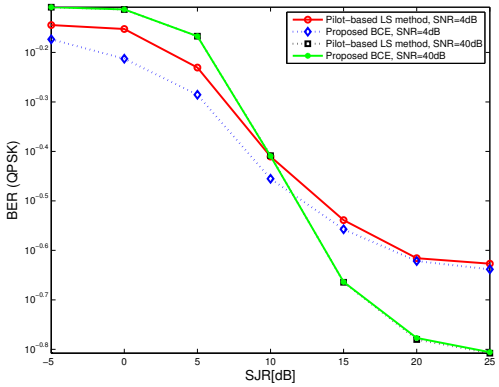
(b)

Figure 6.5: Performance of the proposed BCE for 16-QAM-OFDM. The proposed method estimates the channel at the pilot locations perfectly at very high SNR ($SNR \geq 20dB$). It performs poorly at low SNR. FFT size $M = 64$, channel order $L = 2$, and number of pilots $P = 10$ with pilot density 1/7.

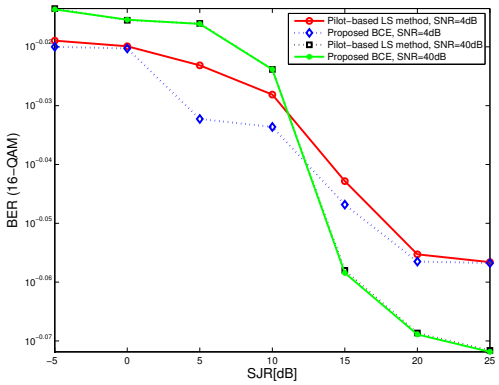
proposed methods reduce the useful bandwidth by only $(1/M)\,\%$.

6.6 Conclusion

In this chapter, we propose novel and less computationally complex blind channel estimation schemes for PSK and QAM-OFDM from legitimate transceivers as well as pilot-jammer's perspective. We explore its effectiveness in formulating the pilot-nulling attacks against OFDM. Simulation results demonstrate the fact that the proposed methods estimate



(a)



(b)

Figure 6.6: Performance of the proposed BCE techniques in formulation of pilot-nulling attacks on QPSK and 16-QAM-OFDM as compared to pilot-based methods. At very high SNR, the proposed methods are as successful as their pilot-based counterparts. The performance degrades at low SNR. SJR stands for Signal-to-Jammer-Ratio.

the third-party jammer channel to the target perfectly to launch precise pilot-nulling attacks on OFDM in very high SNR environment. But the performance degrades with increasing noise. The proposed method inherently resolves the phase-ambiguity and requires only one pilot to resolve the scalar ambiguity. As the jammer or the legitimate receiver requires only one pilot to estimate the channel, the proposed method maximizes the spectral efficiency.

Chapter 7

Jammer Estimation of Transceiver Channel

Pilot-nulling attack requires knowledge of the Channel State Information (CSI) between the two transceivers and between the jammer and the target. In the previous chapter, we propose a blind technique to estimate the channel between the jammer and the target which is highly precise in high SNR. This chapter explores the other half of this major issue, the channel estimation between the transceiver from jammer's perspective.

7.1 Introduction

In closed-loop multiple-input multiple-output (MIMO) communication systems, the target sends quantized CSI to the transmitter over a limited-rate feedback channel [73]. This entails designing a codebook that encapsulates the essential degrees of freedom of the channel and is tailored to the channel model and receiver design. The jammer can overhear this CSI feedback channel. But unless the codebook is known to the jammer, it can not extrapolate the CSI. The jammer can also join the network as a valid user and gain CSI information via

network interaction. Another way to handle the issue is to employ Battle Damage Assessment (BDA). BDA is an adaptive process whereby a jammer estimates the performance of a target communication system to assess whether it is being effective. This is a sequential decision-making problem with state uncertainty which can be modeled as a partially observable Markov decision process (POMDP). In this chapter, we have basically analyzed the feasibility of transceiver channel estimation from jammer's perspective.

7.2 Feasibility Analysis of Jammer Estimation of Transceiver Channel

In modern multi-carrier communication systems, channel estimation can be performed either at the transmitter or at the receiver. An intelligent jammer seeks to disrupt the channel estimation process at either side.

7.2.1 Channel estimation at the transmitter

In multi-carrier precoding-based systems, the transmitter designs its precoder based on the estimates of the legitimate link's CSI and the estimation is done by having the receiver send pilot signals to facilitate the channel estimation at the transmitter, i.e., reverse training. The reverse training scheme requires channel reciprocity which holds in time-division duplex (TDD) systems. During the reverse training phase, if the jammer stays passive rather than launching pilot-spoofing attack as discussed in Chapter Five, the jammer receives signal which is a function of transceiver CSI. For Maximal Ratio Transmission (MRT) precoding or Time Reversal (TR) precoding, the received signal Y_{mn}^{J} at the passive eavesdropper can be written as

$$Y^J_{mn} = H^{TX}_{mn} H^*_{mn} X_{mn} + \acute{N}_{mn} \tag{7.1}$$

where H_{mn} is the transceiver channel, H^{TX}_{mn} is the channel between the base station (BS) and the eavesdropper, $\acute{N}_{mn}$ is the noise at the eavesdropper, and X_{mn} is the symbol transmitted by the BS.

Applying the jammer blind estimation technique as discussed in the previous chapter, the eavesdropper can estimate the effective channel $H^{TX}_{mn} H^*_{mn}$. But to retrieve H^*_{mn} from the estimation of the effective channel, the eavesdropper must know its own channel H^{TX}_{mn} to the BS. But as this is a precoding-based system, eavesdropper is always getting precoded signal from the BS with consequent effective channel between itself and the BS rather than having its own original channel H^{TX}_{mn}. Jammer can send its pilot signal modified by this estimated effective channel. If the jammer is half-duplex, it will be of no use. Because by the time of the next training phase which is the beginning of the next coherence interval, both or either of H^{TX}_{mn}/H_{mn} have already changed. Assuming full-duplex jammer, perceived channel by the BS will be, $H^*_{mn} \pm H^{TX}_{mn} H^*_{mn} \left\{H^{TX}_{mn}\right\}^* = H^*_{mn} \pm H^*_{mn} \left|H^{TX}_{mn}\right|^2$, which is not exactly pilot-nulling scenario.

7.2.2 Channel estimation at the receiver

For ease of reference, we reiterate the pilot-nulling attack on an OFDM receiver again. After the discrete Fourier transform (DFT) at the receiver, the received sample of the m^{th} subcarrier at the n^{th} symbol interval is given by

$$Y_{mn} = H_{mn} X_{mn} + N_{mn} \tag{7.2}$$

where Y_{mn} and X_{mn} are, respectively, the received and the transmitted symbols, H_{mn} is the channel frequency response and N_{mn} is independent and identically distributed AWGN with

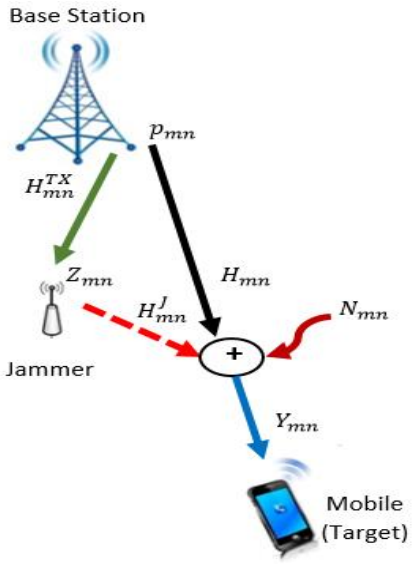


Figure 7.1: Pilot-tone nulling attack on OFDM mobile. H_{mn} is the channel between the legitimate transceivers (Base Station and Mobile) and H_{mn}^{J} is the channel between the jammer and the target.

distribution $\mathcal{CN}(0,1)$. Assuming a long enough Cyclic Prefix (CP), we ignore the effects of inter-symbol and inter-channel interference.

In pilot tone nulling attack, the jammer seeks to null the pilot tones. The goal is for channel estimate $\hat{H}_{mn}$ to be asymptotically close to zero, such that when $\hat{X}_{mn}$ is computed as $\hat{X}_{mn} = Y_{mn}/\hat{H}_{mn}$, we cause a division by zero that makes $\hat{X}_{mn}$ arbitrarily large. Assuming a jammer can estimate the channel between the two transceivers $\tilde{H}_{mn}$, and its own channel to the target $\hat{H}_{mn}^{J}$, the jamming signal as shown in Fig. 7.1 is given by

$$Z_{mn} = \frac{\tilde{H}_{mn}}{\hat{H}_{mn}^{J}} e^{j\pi} p_{mn} \tag{7.3}$$

which is the channel-compensated, π-radian phase shifted version of the pilot tone p_{mn}. The received pilot tone signal under nulling attack is then

$$Y_{mn}^{\text{null}} = H_{mn}p_{mn} + H_{mn}^{J}\frac{\tilde{H}_{mn}}{\hat{H}_{mn}^{J}} e^{j\pi} p_{mn} + N_{mn}. \tag{7.4}$$

If the channel estimates are close, i.e., $\tilde{H}_{mn} \approx H_{mn}$ and $\hat{H}^J_{mn} \approx H^J_{mn}$, this term converges to N_{mn}. Applying the method in previous chapter, we have $\hat{H}^J_{mn}$ available but $\tilde{H}_{mn}$ is not known to the jammer. The jammer employs BDA to deal with this problem.

Battle Damage Assessment

In this case, the jammer is a cognitive learner that is employing BDA to estimate transceiver channel to accomplish its underlying mission of pilot-nulling at the target. At the beginning of each coherence interval, jammer formulates its jamming signal Z_{mn} depending on the estimated channel condition and then transmits it synchronously with the legitimate transmitted signal. The target mobile estimates the channel first from the received signal and then do the equalization. From (7.4), under pilot-nulling attack the perceived channel by the target mobile is $H_{mn} + H^J_{mn}\frac{\tilde{H}_{mn}}{\hat{H}^J_{mn}}e^{j\pi}$ rather than the original channel H_{mn}.

After being demodulated at the target, the decoder first attempts to correct any errors in the received demodulated block, then the decoded block is checked for errors. If no errors are detected, the packets are delivered to the higher layer and an ACK is sent to the legitimate transmitter. Otherwise, the target discards the packets and sends a NAK requesting a retransmission of the same packets. The process is repeated until the packet is successfully received. We assume that the feedback channel is error free and ACK/NAK feedback is intercepted by the jammer without delay. This assumption can be at least approximately satisfied by using a fast feedback link with powerful error control for feedback information. Based on the observation of ACK/NAK, the jammer optimizes its jamming signal accordingly in the next cycle. Due to channel uncertainty, availabilty of ACK/NAK and adaptive nature, this BDA process can be formulated as a POMDP. POMDP replaces the uncertain channel state between the transceiver by belief state which is a distribution over the true channel states.

It is assumed that the legitimate transceiver pair is not aware of the presence of a jammer

in their vicinity. They assume that the packets are lost only due to bad wireless channel conditions.

POMDP Model

Partially Observable Markov Decision Processes provide a rich representation for agents acting in a stochastic domain under partial observability. It models aspects such as the stochastic effects of actions, incomplete information and noisy observations over the environment. POMDP algorithms existing today typically assume discrete models, in which an agent's states, actions, and observations are all discrete, while real-life scenarios are mostly continuous as is the case with our problem. Of course, we can always discretize a problem that is naturally continuous.

Formally, a POMDP is a tuple $(S, A, O, T, Z, R, \gamma)$, where S, A, and O denote the sets of states, actions and observations, respectively. At each time step the agent takes an action $a \in A$ to move from state $s \in S$ to $\acute{s} \in S$. It receives an observation $o \in O$. The model for the system dynamics is specified by a set of conditional probability, $T(s, a, \acute{s}) = p(\acute{s}|s, a)$, which accounts for uncertainty in environment changes. Similarly, the observation model is specified by a set of conditional probability, $Z(\acute{s}, a, o) = p(o|\acute{s}, a)$, which accounts for sensing uncertainty. The function $R(s, a)$ specifies a real-valued reward for the agent if it takes action a in state s. The agent's goal is to choose a sequence of actions that maximizes the expected total reward $\mathbb{E}\left(\sum_{t=0}^{\infty} \gamma^t R(s_t, a_t)\right)$, where s_t and a_t denote the system state and action at time t. The discount factor $\gamma \in [0, 1)$ ensures that the total reward is finite, even when a planning task has an infinite horizon.

Belief

In a POMDP, the state uncertainty is captured in a belief, which is a probability distribution over S. Let $b(s)$ be the current belief on the state. If the agent executes action a and receives observation o, the new belief $\acute{b}(\acute{s})$ is calculated according to the Bayes' rule

$$\acute{b}(\acute{s}) = \eta p(o|\acute{s}, a) \sum_{s \in S} p(\acute{s}|s, a)\, b(s) \tag{7.5}$$

$$\text{with, } \eta = \frac{1}{p(o|b, a)} \tag{7.6}$$

$$= \frac{1}{\sum_{\acute{s} \in S} p(o|\acute{s}, a) \sum_{s \in S} p(\acute{s}|s, a)\, b(s)} \tag{7.7}$$

where η is a normalizing constant. The update uses the system dynamics model and the observation model to integrate information from a and o into the new belief.

Belief-State MDP

For Markovian belief state, a POMDP can be formulated as a Markov decision process where every belief is a state. The resulting *belief-state MDP* is defined on a continuous state space as there are infinite beliefs for any given POMDP. The set of actions in the belief-state MDP is exactly the same as for the POMDP. The state transition function is given by

$$\tau\left(\acute{b}|b, a\right) = p\left(\acute{b}|b, a\right) \tag{7.8}$$

$$= \sum_{o} p\left(\acute{b}|b, a, o\right) \sum_{\acute{s}} p(o|\acute{s}, a) \sum_{s} p(\acute{s}|s, a)\, b(s) \tag{7.9}$$

where $p\left(\acute{b}|b,a,o\right)=\delta_{\acute{b}}$ with δ being the Kronecker delta function. The immediate reward in the belief-state MDP is given by

$$R\left(b,a\right)=\sum_{s}R\left(s,a\right)b\left(s\right). \tag{7.10}$$

Policy and Value Function

The policy in belief-state MDP maps a belief state to an action. The objective is to maximize the expected total discounted reward over an infinite horizon. The expected reward for policy π starting from belief b_0 is defined as

$$V^{\pi}\left(b_0\right)=\sum_{t=0}^{\infty}\gamma^{t}R\left(b_t,a_t\right)=\sum_{t=0}^{\infty}\gamma^{t}\mathbb{E}\left[R\left(s_t,a_t\right)|b_0,\pi\right]. \tag{7.11}$$

The optimal policy π^* is obtained by optimizing the long-term reward and given by

$$\pi^{*}=\arg\max_{\pi}V^{\pi}\left(b_0\right) \tag{7.12}$$

where b_0 is the initial belief. The optimal policy yields the highest expected reward value for each belief state, compactly represented by the optimal value function V^*. This value function is solution to the Bellman optimality equation

$$V^{*}\left(b\right)=\max_{a\in A}\left[R\left(b,a\right)+\gamma\sum_{o\in O}p\left(o|b,a\right)V^{*}\left(\acute{b}\right)\right]. \tag{7.13}$$

7.2.2.1 Formulation of Pilot-nulling Attack as a POMDP

The underlying mission of our BDA is to get our estimation of transceiver channel $\tilde{H}_{mn}$ as close to the original channel H_{mn} as possible. With the transmission of jamming signal synchronous with the legitimate signal, the channel perceived by the target becomes

$H_{mn} - H^J_{mn}\frac{\tilde{H}_{mn}}{\tilde{H}^J_{mn}}$. Our optimization process to get closer to the original H_{mn} requires a constant value for H_{mn} for the optimization interval. So we assume that the coherence interval of the transceiver channel T_c is at least as long as the finite horizon T_p of the POMDP process. Jammer's action set will consist of discrete values of $\tilde{H}_{mn}$. Let us assume that, Jammer's action set for the m^{th} subcarrier of a particular OFDM symbol is given by, $\mathcal{H}^a_m = \left\{\tilde{H}^a_{m1}, \tilde{H}^a_{m2}, \cdots, \tilde{H}^a_{ma}, \cdots, \tilde{H}^a_{mA_m}\right\}$. So the set of channel states of the POMDP which is partially observable to the jammer is: $\mathcal{H}^s_m = \left\{H_{mn} - \tilde{H}^a_{m1}, \cdots, H_{mn} - \tilde{H}^a_{ma}, \cdots, H_{mn} - \tilde{H}^a_{mA_m}\right\} = \left\{H^s_{m1}, \cdots, H^s_{ms}, \cdots, H^s_{mS_m}\right\}$. Obviously the cardinality of the set space S_m and action space A_m are equal.

As H_{mn} is constant, system dynamics depends completely on the dynamics of jammer's action. Correspondingly, $T\left(H^s_{ms}, H^{\acute{s}}_{ms}\right) = p\left(\tilde{H}^{\acute{a}}_{ma}|\tilde{H}^a_{ma}\right)$. The set of observations of the BDA process is given by, $\mathcal{O} = \{ACK, NAK\} = \{\omega_1, \omega_2\}$. Probability of ACK/NAK is reliant on target system's parameters. Assuming that the target system uses (q, r) binary FEC block code which is capable of correcting k bit errors, the ACK probability for a given channel state H^s_{ms} can be written as

$$p\left(ACK|H^s_{ms}\right) = \sum_{u=0}^{k} \begin{pmatrix} q \\ u \end{pmatrix} \left(Pe\left(H^s_{ms}\right)\right)^u \left(1 - Pe\left(H^s_{ms}\right)\right)^{q-u} \tag{7.14}$$

where, $Pe\left(H^s_{ms}\right)$ is the bit-error probability for channel state H^s_{ms}. $Pe\left(H^s_{ms}\right)$ is reliant upon the modulation scheme adopted by the transmitter, here the base station. Obviously Jammer does not know these target system parameters to calculate the probabilities. So jammer obtains the observation probabilities from history of ACK/NAKs which do not define the observation model concretely. Jammer's goal is to make the channel perceived by the target as small as possible. Consequently, the reward function $R\left(H^s_{ms}, H^a_{ma}\right)$ is assumed to be quadratic, $|H^s_{ms}|^2 - |H^a_{ma}|^2$. Quadratic formulation induces a high penalty for large deviations of the state from the origin but a relatively small penalty for small deviations.

So the quadratic reward is equivalent to saying that we want the channel perceived by the target to be close to the origin where the reward is higher.

Remark 1: With linear transition and quadratic rewards, this pilot-nulling attack could have been formulated into a well-defined POMDP where the BDA process could have evolved in a targeted manner and achieved its goal if only there were some concrete observables available other than simply ACK/NAKs. With the availability of only ACK/NAKs, this process will simply reduce to pilot-jamming scenario.

If the observation at the receiver side were a linear function of the transceiver channel H_{mn} as is the case at the transmitter side with precoding-based system, the POMDP problem could have been translated into a Linear-Quadratic Gaussian (LQG) formulation that has nice analytical optimal policies with continuous state and action spaces, and exact belief updates through Kalman filter.

7.3 Conclusion

In this chapter, we have performed the feasibility analysis of pilot-nulling attack at the transmitter as well as the receiver of an OFDM system in a deterministic and adaptive fashion, respectively. At the transmitter side, the precoding-based system provides the jammer with a well-defined observable which has linear relationship with the transceiver channel but unavailability of estimation of jammer channel renders the pilot-nulling attack unachievable. On the other hand, lack of concrete observables at the receiver side, reduces the pilot-nulling attack to mere pilot-jamming attack.

Chapter 8

Conclusion and Future Directions

Wireless communication plays an important role in achieving ubiquitous communication where network devices embedded in environments provide continuous connectivity and services, thus improving human's quality of life. However, due to the exposed nature of wireless links, current wireless communication networks can be easily attacked by jamming technology. Jamming can cause Denial-of-Service (DoS) problem which may result in several other higher-layer security problems. In this dissertation, the jamming vulnerabilities of multi-carrier communication systems in the physical layer are explored.

8.1 Conclusion

In this dissertation, the analytical BER expressions for OFDMA and SC-FDMA in Rayleigh slow-fading channel for BPSK, QPSK, and 16-QAM modulations under pilot-jamming and pilot symbol assisted channel estimation are derived. The issue is addressed by first approaching the BER analysis from general case of PSACE technique in Rayleigh slow-fading channel. The expressions thus derived are then modified for BPSK/QPSK/16-QAM modulations. The equations are further customized to account for the frequency domain ZF equal-

ization in frequency direction or time direction with application respectively to OFDMA or SC-FDMA without and with pilot-jamming attack. Instead of conventional Wiener interpolation, piecewise-linear interpolation is used for its low computational complexity. Analysis is verified with simulation in MATLAB. The simulation results match perfectly with the theoretical predictions except for some discrepancies with SC-FDMA. Thorough investigation into the matter reveals the fact that the generalized equations developed have to be further modified to account for system-specific features like DFT-precoding for SC-FDMA.

Single-Carrier Frequency Division Multiple Access uses Cyclic Prefix to mitigate inter-symbol interference and inter-channel interference. CP ensures that the convolution of the channel impulse response with the modulated symbols has the form of a circular convolution. This results in simple one-tap equalization in the receiver by removing ICI. These crucial roles played by the CP make SC-FDMA particularly vulnerable to jamming or nulling attacks through CP. These attacks are effective if the CP is disrupted before passing through the channel. The attacks that happen to jam the signal after it is already through the channel, reduce to no-jamming scenarios in their effectiveness. But signal disruption ensuring signal is not already distorted by channel is practically infeasible. Consequently, in this dissertation, we have designed the jammers so that they emulate the effect of CP jamming and nulling in frequency-selective time-invariant channel. We have also proposed two novel countermeasures. Simulations are performed to validate the analytical predictions about the attacks and the associated countermeasures. The results reflect the fact that CP attacks are particularly suitable for power-constrained jammers in high SNR regime. The newly proposed anti-jamming techniques prove to be very effective in thwarting the attacks.

This dissertation also explores the effect of fading correlation on pilot-spoofing attack in a TDD MISO-OFDM system from information-theoretic perspective. So far all the analysis, whether it is from information-theoretic perspective or signal processing perspective, are carried out under the assumption that MISO channels are independent and identically

distributed (i.i.d.) flat fading. To the authors' knowledge, we are the first one to consider the effect of frequency-selective spatially correlated fading channel on the efficacy of pilot-spoofing attack. By its inherent characteristic, OFDM naturally takes care of the frequency-selectivity of the channel. Capacity bounds are derived. The simulation results show that spatial correlation facilitates the pilot-spoofing attack. The achievable legitimate rate is lower than its i.i.d. counterpart. Although the achievable legitimate rate decreases at a slower rate than its i.i.d. counterpart.

Novel, computationally simple and deterministic blind channel estimation schemes for PSK-OFDM and QAM-OFDM are proposed in this dissertation from legitimate transceivers as well as pilot-jammer's perspective. Their effectiveness in formulating the pilot-nulling attacks against OFDM is investigated. The estimators are based on the Least Squares (LS) principle and capitalize on the finite alphabet property of the information symbols. Phase ambiguity resolution requires no reference symbols while scalar ambiguity is resolved at the expense of a single pilot tone. The multipath characteristics of the channel between the target and the jammer are assumed to be Time Division Duplex (TDD) reciprocal. Simulation results are provided to demonstrate the performance of the proposed methods in channel estimation at the pilot locations as well as designing effective pilot-nulling attacks. The proposed methods estimate the jammer channel to the target perfectly to launch precise pilot-nulling attacks on OFDM in very low noise environment. The performance degrades with increasing noise. This dissertation also investigates the feasibility of transceiver channel estimation from jammer's perspective.

8.2 Future Scope

Due to the openness of wireless systems, security threats will always be there. Consequently, the scope for future work in this field is always extensive. Only a few select direc-

tions are discussed next. Although this research work has proposed countermeasures for CP attack on SC-FDMA, it is mostly focused on the jamming techniques. There is the other half of the equation too, the anti-jamming capability. So this dissertation can be extended into the analysis of anti-jamming capabilities of multi-carrier communication systems detailing the design of the jamming detection techniques and the corresponding countermeasures.

Although jamming is usually considered a critical threat, Gollakota and Katabi in [74] proved that jamming can be friendly too. They exploited jamming as a defense to counteract eavesdropping attacks. Particularly, a user will be jamming oneself (graciously called *iJam*) on its physical layer so that a snooper cannot detect a legitimate signal. Consequently, another interesting future direction of this research work will be an extension into iJam techniques for modern multi-carrier communication systems.

Additionally, the analytical BER expressions for OFDMA and SC-FDMA under pilot-jamming and pilot symbol assisted channel estimation can be further extended from point-to-point channels to multiple-antenna systems, followed by generalizations to larger multi-user networks with more than two receivers and/or transmitters.

References

[1] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of Physical Layer Security in Multiuser Wireless Networks: A Survey," *IEEE Communications Surveys and Tutorials*, vol. 16, no. 3, pp. 1550–1573, 2014.

[2] A. Graham, *Communications, Radar and Electronic Warfare*. John Wiley & Sons Ltd., 2011.

[3] R. A. Poisel, *Introduction to Communication Electronic Warfare Systems*. Artech House, 2002.

[4] R. A. Poisel, *Foundations of Communications Electronic Warfare*. Artech House, 2008.

[5] R. A. Poisel, *Modern Communications Jamming: Principle and Techniques*. Artech House, 2011.

[6] "President's Commission on Critical Infrastructure Protection." `http://www.pccip.gov`, 1998.

[7] B. K. Levitt, "FH/MFSK Performance in Multitone Jamming," *IEEE Transactions on Selected Areas in Communications*, vol. SAC-3, pp. 627–643, Sep 1985.

[8] A. Babaei, W. H. Tranter, and T. Bose, "A practical precoding approach for radar/communications spectrum sharing," *Cognitive Radio Oriented Wireless Networks (CROWNCOM)*, pp. 13–18, July 2013.

[9] J. Singh, Z. Pi, and H. Nguyen, "Low-Complexity Optimal CSI Feedback in LTE," *IEEE Consumer Communications and Networking Conference (CCNC)*, pp. 472 – 478, Jan. 2013.

[10] D. J. Love, R. W. Heath, , W. Santipach, and M. L. Honig, "What is the Value of Limited Feedback for MIMO Channels?," *IEEE Communications Magazine*, vol. 42, pp. 54–59, Oct. 2003.

[11] D. J. Love, R. W. Heath, V. K. N. Lau, D. Gesbert, B. D. Rao, and M. Andrews, "An Overview of Limited Feedback in Wireless Communication Systems," *IEEE Journal on Sel. Areas in Comm., Special Issue on Exploiting Limited Feedback in Tomorrows Wireless Communication Networks*, vol. 26, pp. 1341–1365, Oct. 2008.

[12] S. Sesia, I. Toufik, and M. Baker, *LTE The UMTS Long Term Evolution From Theory to Practice*. John Wiley & Sons Ltd., 2011.

[13] E. Dahlman, S. Parkvall, and J. Skold, *4G LTE/LTE-Advanced for Mobile Broadband*. Academic Press, 2011.

[14] H. Holma and A. Toskala, *LTE for UMTS Evolution to LTE-Advanced*. John Wiley & Sons Ltd., 2011.

[15] H. G. Myung and D. J. Goodman, *Single Carrier FDMA: A New Air Interface for Long Term Evolution*. Wiley and Sons, Ltd., 2009.

[16] S. Haykin, *Adaptive Filter Theory*. Prentice-Hall, Inc., 2002.

[17] R. Haeb and H. Meyr, "A systematic approach to carrier recovery and detection of digitally phase modulated signals of fading channels," *IEEE Transactions on Communications*, vol. 37, pp. 748 – 754, July 1989.

[18] C. S. Patel, G. Stuber, and T. G. Pratt, "Analysis of OFDM/MC-CDMA under imperfect channel estimation and jamming," *Wireless Communications and Networking Conference*, vol. 2, pp. 954–958, Mar 2004.

[19] J. J. Sanchez-Sanchez, M. C. Aguayo-Torres, and U. Fernandez-Plazaola, "BER Analysis for SC-FDMA Over Rayleigh Fading Channels," in *International Conference on Broadband Communications & Biomedical Applications*, pp. 43–47, Nov 2011.

[20] J. J. Sanchez-Sanchez, M. C. Aguayo-Torres, and U. Fernandez-Plazaola, "BER Analysis for Zero-Forcing SC-FDMA Over Nakagami-m Fading Channels," *IEEE Transaction on Vehicular Technology*, vol. 60, pp. 4077–4081, Oct 2011.

[21] J. Luo, J. H. Andrian, and C. Zhou, "Bit error rate analysis of jamming for OFDM systems," in *Wireless Telecommunications Symposium*, pp. 1–8, Apr 2007.

[22] P. Hoeher, "Pilot symbol aided channel estimation in time and frequency," in *Proc. IEEE Global Telecommun. Conference*, pp. 90–96, 1997.

[23] F. Tufvesson and T. Maseng, "Pilot assisted channel estimation for OFDM in mobile cellular systems," *Vehicular Technology Conference*, vol. 3, pp. 1639 – 1643, May 1997.

[24] J. K. Cavers, "An Analysis of Pilot Symbol Assisted Modulation for Rayleigh Fading Channels," *IEEE Transactions on Vehicular Technology*, vol. 40, pp. 686–693, Nov 1991.

[25] J. K. Cavers, "Pilot Symbol Assisted Modulation in Fading and Delay Spread," in *IEEE Vehicular Technology Conference*, pp. 13–16, 1993.

[26] C. Athaudage and A. Jayalath, "Low-complexity channel estimation for wireless OFDM systems," *14th IEEE Proceedings on Personal, Indoor and Mobile Radio Communications*, vol. 1, pp. 521–525, Sep 2003.

[27] M. M. Jeruchim, P. Balaban, and K. S. Shanmugan, *Simulation of Communication Systems*. Kluwer Academic/Plenum Publishers, 2000.

[28] C. D. Iskander, "A MATLAB-Based Object-Oriented Approach to Multipath Fading Channel Simulation." Unpublished.

[29] J. Proakis, *Digital Communication*. McGraw-Hill, 2000.

[30] R. J. C. Bultitude, "Estimating Frequency Correlation Functions From Propagation Measurements on Fading Radio Channels: A Critical Review," *IEEE Journal on Selected Areas in Communications*, vol. 20, pp. 1133–1143, August 2002.

[31] P. A. Bello and B. D. Nelin, "The Effect of Frequency Selective Fading on the Binary Error Probabilities of Incoherent and Differentially Coherent Matched Filter Receivers," *IEEE Transaction on Communications Systems*, vol. 11, pp. 170–186, Jun. 1963.

[32] G. L. Stuber, *Principles of Mobile Communication*. Springer, 2011.

[33] `http://www.ecee.colorado.edu`.

[34] T. C. Clancy, "Efficient OFDM Denial: Pilot Jamming and Pilot Nulling," in *IEEE International Conference on Communications*, pp. 1–5, Jun 2011.

[35] C. Shahriar, M. LaPan, M. Lichtman, T. C. Clancy, R. McGwier, R. Tandon, S. Sodagari, and J. H. Reed, "PHY-Layer Resiliency in OFDM Communications: A Tutorial," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 1, pp. 292–314, 2015.

[36] M. LaPan, T. C. Clancy, and R. W. McGwier, "Jamming Attacks Against OFDM Timing Synchronization and Signal Acquisition," in *IEEE Military Communications Conference (MILCOM)*, pp. 1–7, Oct 2012.

[37] 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)*, pp. 2886 – 2890, May 2013.

[38] T. Schmidl and D. Cox, "Robust Frequency and Timing Synchronization for OFDM," *IEEE Transactions on Communications*, vol. 45, pp. 1613 – 1621, December 1997.

[39] C. Shahriar and T. C. Clancy, "Performance Impact of Pilot Tone Randomization to Mitigate OFDM Jamming Attacks," in *IEEE Consumer Communications and Networking Conference (CCNC)*, pp. 813–816, Jan 2013.

[40] C. Shahriar, S. Sodagari, and T. C. Clancy, "Performance of Pilot Jamming on MIMO Channels with Imperfect Synchronization," in *IEEE International Conference on Communications (ICC)*, pp. 898 – 902, Jun 2012.

[41] L. Hanzo, M. Munster, B. Choi, and T. Keller, *OFDM and MC-CDMA for Broadband Multi-user Communications, WLANs and Broadcasting*. John Wiley & Sons Ltd., 2003.

[42] A. L. Scott, "Effects of Cyclic Prefix Jamming Versus Noise Jamming in OFDM Signals," Master's thesis, Air Force Institute of Technology, 2011.

[43] P. N. Fletcher, "Iterative Decoding for Reducing Cyclic Prefix Requirement in OFDM Modulation," *Electronics Letters*, vol. 39, pp. 539–541, 2003.

[44] 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.

[45] 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.

[46] J. Jose, A. Ashikhmin, T. L. Marzetta, and S. Vishwanath, "Pilot contamination and precoding in multi-cell TDD systems," *IEEE Trans. Wireless Commun.*, vol. 10, pp. 2640–2651, Aug. 2011.

[47] X. Zhou, B. Maham, and A. Hjorungnes, "Pilot contamination for active eavesdropping," *IEEE Trans. Wireless Commun.*, vol. 11, pp. 903–907, Mar. 2012.

[48] Q. Xiong, Y.-C. Liang, K. H. Li, and Y. Gong, "An Energy-Ratio-Based Approach for Detecting Pilot Spoofing Attack in Multiple-Antenna Systems," *IEEE Transactions on Information Forensics and Security*, vol. 10, pp. 932–940, May 2015.

[49] D. Xu, P. Ren, Y. Wang, Q. Du, and L. Sun, "Ica-sbdc: A channel estimation and identification mechanism for miso-ofdm systems under pilot spoofing attack," in *IEEE ICC*, pp. 1–6, July 2017.

[50] S. M. Kay, *Fundamentals of Statistical Signal Processing: Estimation Theory*. Prentice Hall, 1993.

[51] J. A. Mahal and T. C. Clancy, "Jammer Blind Estimation of a Third-Party OFDM Channel," in *IEEE GLOBECOM*, 2018. under submission.

[52] M. K. Ozdemir, H. Arslan, and E. Arvas, "MIMO-OFDM Channel Estimation for Correlated Fading Channels," in *Proc. IEEE Wireless and Microwave Technol. Conf.*, vol. 1, pp. 1–5, April 2004.

[53] J. H. Kotecha and A. M. Sayeed, "Transmit Signal Design for Optimal Estimation of Correlated MIMO Channels," *IEEE Trans. Signal Processing*, vol. 52, pp. 546–557, Feb. 2004.

[54] J. Wang, S. hua Zhu, and L. Wang, "On the Channel Capacity of MIMO-OFDM Systems," in *Proceedings of ISCIT*, pp. 1325–1328, 2005.

[55] B. Hassibi and B. M. Hochwald, "How much training is needed in multiple-antenna wireless links?," *IEEE Trans. Inf. Theory*, vol. 49, pp. 951–963, Apr. 2003.

[56] M. Pinsker, "Calculation of the rate of information production by means of stationary random processes and the capacity of a stationary channel," *Dokl. Akad. Nauk USSR*, vol. 111, pp. 753–756, Sept. 1956.

[57] S. Ihara, "On the capacity of channels with additive non-Gaussian noise," *Inform. Contr.*, vol. 37, pp. 34–39, Sept. 1978.

[58] R. McEliece and W. Stark, "An information theoretic study of communication in the presence of jamming," *Proc. Int. Conf. Communication*, pp. 45.3.1–45.3.5, 1982.

[59] T. C. Clancy, "Efficient OFDM Denial: Pilot Jamming and Pilot Nulling," in *IEEE International Conference on Communications (ICC)*, pp. 1–5, June 2011.

[60] L. Tong, G. Xu, and T. Kailath, "A New Approach to Blind Identification and Equalization of Multipath Channels," in *Conference Record of the Twenty-Fifth Asilomar Conference on Signals, Systems and Computers*, vol. 2, pp. 856–860, 1991.

[61] E. Moulines, P. Duhamel, J. Cardoso, and S. Mayrargue, "Subspace Methods for the Blind Identification of Multichannel FIR Filters," *IEEE Transactions on Signal Processing*, vol. 43, pp. 516–525, February 1995.

[62] C. Li and S. Roy, "Subspace-Based Blind Channel Estimation for OFDM by Exploiting Virtual Carriers," *IEEE Transactions on Wireless Communications*, vol. 2, pp. 141–150, January 2003.

[63] Q. Shi and Y. Karasawa, "Blind Channel and Frequency Offset Estimation for OFDM via Frequency-Domain Oversampling," in *6th International Conference on Wireless Communications Networking and Mobile Computing (WiCOM)*, pp. 1–5, September 2010.

[64] M. K. Tsatsanis and G. B. Giannakis, "Subspace Methods for Blind Estimation of Time-Varying FIR Channels," *IEEE Transactions on Signal Processing*, vol. 45, pp. 3084–3093, December 1997.

[65] M. Chang and Y. T. Su, "Blind and Semiblind Detections of OFDM Signals in Fading Channels," *IEEE Transactions on Communications*, vol. 52, pp. 744–754, May 2004.

[66] N. Chotikakamthorn and H. Suzuki, "On Identifiability of OFDM Blind Channel Estimation," in *IEEE Vehicular Technology Conference (VTC)*, vol. 4, pp. 2358–2361, September 1999.

[67] S. Zhou and G. B. Giannakis, "Finite-Alphabet Based Channel Estimation for OFDM and Related Multicarrier Systems," *IEEE Transactions on Communications*, vol. 49, pp. 1402–1414, Aug 2001.

[68] M. C. Necker and G. L. Stuber, "Totally Blind Channel Estimation for OFDM over Fast Varying Mobile Channels," in *IEEE International Conference on Communications (ICC)*, vol. 1, pp. 421–425, 2002.

[69] M. C. Necker and G. L. Stuber, "Totally Blind Channel Estimation for OFDM on Fast Varying Mobile Radio Channels," *IEEE Transactions on Wireless Communications*, vol. 3, p. 15141525, Sep. 2004.

[70] M. C. Necker and F. Sanzi, "Generalized 8-PSK for Totally Blind Channel Estimation in OFDM," in *IEEE 59th Vehicular Technology Conference (VTC)*, vol. 2, pp. 924–928, May 2004.

[71] X. Wang, R. Liu, F. He, T. Yang, and B. Hu, "On Scalar Ambiguity in Blind Channel Estimation for OFDM Systems," in *IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, pp. 3725–3728, March 2012.

[72] H. Shiratsuchi and H. Gotanda, "Frequency Domain Blind Channel Estimation without Phase Ambiguity for QAM-OFDM Systems," in *9th International Conference on Signal Processing and Communication Systems (ICSPCS)*, pp. 1–8, Dec. 2015.

[73] D. J. Love, R. W. Heath, W. Santipach, and M. L. Honig, "What is the value of limited feedback for MIMO channels?," *IEEE Communications Magazine*, vol. 42, no. 10, pp. 54–59, 2004.

[74] S. Gollakota and D. Katabi, "ijam: Jamming oneself for secure wireless communication," tech. rep., Massachusetts Institute of Technology, 2010.