

SIGNAL PROCESSING TECHNIQUES FOR SECURITY ENHANCEMENT OF WIRELESS NETWORKS AT THE PHYSICAL LAYER

A THESIS SUBMITTED TO
THE GRADUATE SCHOOL OF
ENGINEERING AND NATURAL SCIENCES
OF ISTANBUL MEDIPOL UNIVERSITY
IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR
THE DEGREE OF
MASTER OF SCIENCE
IN
ELECTRICAL, ELECTRONICS ENGINEERING AND CYBER SYSTEMS

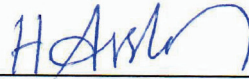
By
Morteza Soltani
March, 2017

Signal Processing Techniques for Security Enhancement of Wireless
Networks at the Physical Layer

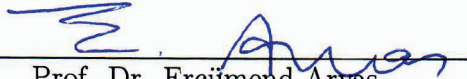
By Morteza Soltani

March, 2017

We certify that we have read this thesis and that in our opinion it is fully adequate,
in scope and in quality, as a thesis for the degree of Master of Science.



Prof. Dr. Hüseyin Arslan(Advisor)



Prof. Dr. Ercüment Arvas



Assist. Prof. Dr. Ali Görçin

Approved by the Graduate School of Engineering and Natural Sciences:

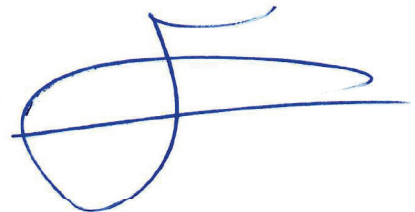


Prof. Dr. Talip Alp
Director of the Graduate School of Engineering and Natural Sciences

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Name, Last Name: MORTEZA SOLTANI

Signature :

A handwritten signature in blue ink, consisting of a large, stylized loop on the left and a horizontal line extending to the right, with a small flourish above the line.

ABSTRACT

SIGNAL PROCESSING TECHNIQUES FOR SECURITY ENHANCEMENT OF WIRELESS NETWORKS AT THE PHYSICAL LAYER

Morteza Soltani

M.S. in Electrical, Electronics Engineering and Cyber Systems

Advisor: Prof. Dr. Hüseyin Arslan

Co-Advisor: Assist. Prof. Dr. Tunçer Baykaş

March, 2017

Broadcast nature of wireless communications enables reaching multiple parties simultaneously. However, due to this property, the security of information transmission is prone to eavesdropping of unauthorized receivers. Efforts to keep information secret from malicious eavesdroppers started long before radio communications. Many methods have been developed such as high-layer encryption of the data using secret keys shared between users and steganography i.e. watermarking, which are used in wireless communications as well. On top of all of these protection schemes, system designers envision to use the properties of the wireless communications, such as, fading, noise and interference to enhance security at the physical layer. Such methods are termed as physical layer security.

Physical layer security has been conventionally addressed from an information-theoretic viewpoint and has been extended by signal processing techniques. In this context, this dissertation presents signal processing algorithms that aim to secure the communications of two of the dominant wireless systems, namely, Orthogonal Frequency Division Multiplexing (OFDM) systems and Multiple-Input Multiple-Output (MIMO) systems.

Motivated by this objective, chapter 2 studies a secure pilot-based channel estimation technique called pilot manipulation in OFDM systems. Particularly, we propose two novel algorithms, which manipulate pilot tones according to legitimate channels' phase and amplitude characteristics. Both algorithms decrease the channel estimation quality of the eavesdropper considerably, while the amplitude based algorithm provides high quality reception at the legitimate receiver. We provide resulting pilot error rates of the proposed algorithms. In addition, we show the effect of threshold selection to channel estimation quality both at the

legitimate receiver and eavesdropper.

Considering multiple antenna systems, chapter 3 examines Multiple-Input Single-Output (MISO) wiretap channels with antenna subset activation. In this protocol, a randomly selected subset of transmit antennas is chosen for location-based secure communications in fading channels. For an active antenna set, the transmitted data signal is precoded at each transmit antenna as a function of the channel response between the corresponding transmit antenna of the transmitter and the receive antenna of the legitimate receiver. Two techniques for channel-based precoding of the data signals are proposed. For both precoders, we derive closed-form expressions for the average minimum guaranteed secrecy rate and the probability of non-zero minimum guaranteed secrecy rate in Rayleigh fading channels. Moreover, a detailed comparison between the secrecy performance of the proposed precoders is given. It is revealed that the ratio between the number of active antennas and the total number of antennas at Alice, i.e., the thinning ratio, plays a vital role in the secrecy performance of the proposed methods.

Finally, in chapter 4, we propose and analyze randomized beamforming with generalized selection transmission (RBF/GST) to enhance physical layer security in MISO wiretap channels. With GST, Q antennas out of N antennas are selected at the transmitter to maximize the output signal to noise ratio at the legitimate receiver. Moreover, RBF is responsible for delivering secure communications in the presence of advanced eavesdroppers. We first examine the secrecy performance of GST by deriving the closed-form expressions for the exact and asymptotic secrecy outage probability. To further boost secrecy performance of GST, we adopt RBF/GST and derive the ergodic secrecy rate in closed-form. We demonstrate that RBF/GST can effectively improve communication secrecy in block fading channels with a reasonable cost in terms of the amount of required signal processing, hardware complexity and power consumption.

Keywords: Physical layer security, channel estimation, pilot manipulation, MISO wiretap channel, antenna subset activation, generalized selection transmission, randomized beamforming.

ÖZET

SİNYAL İŞLEME TEKNİKLERİ İÇİN FİZİKSEL KATMAN KABLOSUZ AĞLARDA GÜVENLİK GELİŞTİRİLMESİ

Morteza Soltani

Elektrik-Elektronik Mühendisliği ve Siber Sistemler, Yüksek Lisans

Tez Danışmanı: Prof. Dr. Hüseyin Arslan

Tez Eş Danışmanı: Assist. Prof. Dr. Tunçer Baykaş

Mart, 2017

Kablosuz haberleşmede yayın doğası gereği aynı anda birden fazla tarafa ulaşmayı sağlar. Bu özelliğ nedeniyle, bilgi aktarımının güvenliği, yetkisiz alıcıların dinlenmesine meyillidir. Kötü amaçlı dinleyicilerden bilginin gizli tutulma çabaları, radyo iletişimi öncesinde başlamıştır. Kullanıcılar arasında paylaşılan gizli anahtarları ve kablosuz iletişimde de kullanılan stenografi yani filigran yöntemini kullanarak verilerin üst katmanlı şifrelenmesi gibi pek çok yöntem geliştirilmiştir. Sistem tasarımcıları, tüm bu koruma şemalarının üzerine, fiziksel katmandaki güvenliği artırmak için sönümlenme, gürültü ve parazit gibi kablosuz iletişim etkilerini kullanmayı düşünüyorlar. Bu yöntemlere fiziksel katman güvenliği denir.

Fiziksel katman güvenliği geleneksel olarak bir bilgi kurma aşısından ele alınmış ve sinyal işleme teknikleri ile genişletilmiştir. Bu bağlamda, bu tez, baskın kablosuz sistemlerin, yani Dikey Frekans Bölmeli Çoğullama (OFDM) sistemlerinin ve Çok Girişli Çoklu ıkış (MIMO) sistemlerinin iletişimini sağlamayı amaçlayan sinyal işleme algoritmalarını sunmaktadır.

Bölüm 2, bu amaçla motive edilen, OFDM sistemlerinde pilot manipülasyon denilen güvenli bir pilot tabanlı kanal tahmini tekniğini inceler. Özellikle, iki yeni algoritma öneriyoruz, bu algoritmalar pilot tonları meşru kanalların faz ve genlik özelliklerine göre manipüle ediyor. Her iki algoritma, dinleyicinin kanal tahmini kalitesini önemli ölçüde düşürürken, genlik tabanlı algoritma, meşru alıcıda yüksek kalitede alım almasını sağlar. Önerilen algoritmaların elde edilen pilot hata oranları sonuç olarak verilmektedir. Buna ek olarak, eşik seçiminin kanal algılama kalitesine olan etkisini hem meşru alıcı hem de dinleyicilerde

göstermektedir.

Birden fazla anten sistemi göz önüne alındığında, bölüm 3, anten alt kümesinin etkinleştirilmesi ile birlikte Çok Girişli Tek Çıkışlı (MISO) telsiz hatlarını inceler. Bu protokolda, rastgele seçilmiş bir iletim antenleri alt kümesi, solma kanallarındaki konuma dayalı güvenli iletişim için seçilmiştir. Aktif bir anten seti için, aktarılan veri sinyali, vericinin ilgili gönderici anteniyle meşru alıcının alıcı anteni arasındaki kanal tepkisinin bir fonksiyonu olarak her bir verici anteninde önceden kodlanır. Veri sinyallerinin kanal tabanlı ön kodlaması için iki teknik önerilmiştir. Her iki ön-kodlayıcı için de, ortalama minimum garanti güvencesi oranı için kapalı form ifadeleri ve Rayleigh sönümleme kanallarında sıfır olmayan asgari garantili gizlilik oranının olasılığı türetilir. Dahası, önerilen ön-kodlayıcıların gizlilik performansı arasında ayrıntılı bir karşılaştırma verilmiştir. Aktif antenlerin sayısı ile Alice'teki toplam anten sayısı arasındaki oranın, yani inceltme oranının, önerilen yöntemlerin gizlilik performansında hayati bir rol oynadığı ortaya çıkmaktadır.

Son olarak, 4. bölüm, MISO telefon dinleme kanallarındaki fiziksel katman güvenliğini arttırmak için raslantısal hüzme oluşturma işlemini genelleştirilmiş seçim iletimiyle (RBF/GST) önererek alaniz etmektedir. GST ile, meşru alıcıdaki çıkış sinyalinin gürültüye oranını en üst düzeye çıkarmak için vericide N antenden Q anten seçilir. Üstelik, RBF, gelişmiş dinlemcilerin varlığında güvenli iletişim sunmaktadır. İlk olarak, gizli ve asimtotik gizlilik kesilmesi ihtimali için kapalı form ifadelerimiz aracılığıyla GST'nin fiziksel katman gizliliğini karakterize etmekteyiz. GST'nin gizlilik performansını daha da artırmak için RBF/GST'yi kabul ederek, ergodik gizlilik oranını kapalı formda türetilir. Gerekli sinyal işleme, donanım karmaşıklığı ve güç tüketimi açısından mantıklı bir maliyetle blok sönümleme kanallarında RBF/GST'nin iletişim gizliliğini etkin bir şekilde artırabileceğini gösterilmektedir.

Anahtar sözcükler: Fiziksel katman güvenliği, kanal tahmini, pilot manipülasyon, MISO kablo TV kanalı, anten alt seti etkinleştirme, genelleştirilmiş seçim iletimi, rastgele ışın Oluşturma.

Acknowledgement

I would like to express my deepest gratitude to my advisor Prof. Hüseyin Arslan for his continuous guidance and for introducing me to the exciting and promising topic of physical layer security. Indeed, with his encouragement, expertise and advice, the goals of the thesis were successfully achieved.

I would also like to sincerely thank my Co-Advisor Dr. Tunçer Baykaş for his excellent advice and his continuous support. His efforts in providing me with constant feedback are greatly appreciated.

Moreover, I want to express my heartfelt appreciation to my family and friends for their continuous encouragement and their moral support.

Finally, I am grateful to the Scientific and Technological Research Council of Turkey (TUBITAK) for the financial supports I have received during my research and studies.

Contents

1	Introduction	1
1.1	Information-theoretic approaches versus signal processing techniques for physical layer security	2
1.2	Thesis outline	3
2	Achieving Secure Communication Through Pilot Manipulation	5
2.1	System Model	6
2.2	Pilot Manipulation Algorithms	8
2.2.1	Phase-Based Pilot Manipulation	9
2.2.2	Amplitude-Based Pilot Manipulation	11
2.3	Simulation Scenarios and Results	12
2.4	Conclusions	16
3	Antenna Subset Activation for Location-Based Secure MISO Wireless Communications in Fading Channels	18
3.1	Protocol Description	21

3.1.1	System Model	21
3.1.2	Precoder Design	23
3.1.3	Antenna Subset Activation in Fading Channels	24
3.2	Secrecy Performance Evaluation of the ASA in Fading Channels .	29
3.2.1	Preliminaries	29
3.2.2	Minimum Guaranteed Secrecy Rate	32
3.2.3	Probability of Non-Zero Minimum Guaranteed Secrecy Rate	34
3.3	Numerical Results	35
3.4	Conclusions and Future Research	39
4	Randomized Beamforming with Generalized Selection Transmis- sion for Security Enhancement in MISO Wiretap Channels	41
4.1	Algorithm Description	43
4.1.1	System Model	43
4.1.2	Generalized Selection Transmission (GST)	43
4.1.3	Randomized Beamforming with Generalized Selection Transmission (RBF/GST)	44
4.2	Secrecy Performance	46
4.2.1	Secrecy Performance of GST	46
4.2.2	Secrecy Performance of RBF/GST	49
4.3	Numerical Results	51

<i>CONTENTS</i>	xi
4.4 Conclusions	53
5 Concluding Remarks	54
5.1 Summary	54
5.2 Future Research	55
Bibliography	56
Appendices	61

List of Figures

2.1	System model consisting of legitimate transmitter (Alice) and receiver (Bob), and eavesdropper (Eve) with multipath fading channels.	7
2.2	Pilot manipulation decision regions.	10
2.3	Bit Error Rate performance of different channel estimation with phase-based pilot manipulation.	12
2.4	Average Mean Square Error of different channel estimation with phase-based pilot manipulation.	13
2.5	Bit Error Rate Performance versus different threshold values at 15 and 25 dB E_b/N_0	14
2.6	Bit error rate performance with amplitude-based pilot manipulation with MMSE channel estimation.	15
2.7	Average Mean Square Error with amplitude-based pilot manipulation and MMSE channel estimation.	16
2.8	Pilot Error Rate performance with MMSE channel estimation for phase-based and amplitude-based pilot manipulation.	17
3.1	MISO wiretap channel with the ASA and Precoding.	22

3.2 Received 16-QAM constellation points at Bob and Eve with the CI precoder 25

3.3 Received 16-QAM constellation points at Bob and Eve with the EBF Precoder. 29

3.4 Average Minimum Guaranteed secrecy rate versus received average SNR at Bob with the utilization of the CI precoder at Alice for different thinning ratio values. 35

3.5 The probability of non-zero secrecy rate versus average received SNR at Bob with the utilization of the CI precoder for different thinning ratio values. 36

3.6 Average Minimum Guaranteed secrecy rate versus received average SNR at Bob with the utilization of the EBF precoder at Alice for different thinning ratio values. 37

3.7 The minimum Guaranteed secrecy rate versus β for different received average SNR at Bob with the EBF precoder. 38

3.8 The thinning ratio values that maximizes average minimum guaranteed secrecy rate versus received average SNR at Bob with the EBF precoder. 39

3.9 The probability of non-zero secrecy rate versus average received SNR at Bob with the utilization of the EBF precoder for different thinning ratio values. 40

4.1 The exact and asymptotic secrecy outage probabilities of GST versus $\bar{\gamma}_M$ for $\bar{\gamma}_W = 5$ dB and $R_S = 1$ 51

4.2 Comparison of the ergodic secrecy rate between RBF/GST and CBF/GST versus $\bar{\gamma}_M$ for $\bar{\gamma}_W = 15$ dB. 52

List of Tables

A.1	Table of corresponding probabilities to each set of $b(k)$ and $b(\ell)$	63
-----	--	----

Chapter 1

Introduction

Confidential data transmission has been always a critical issue for wireless communications due to its open and broadcast nature. Particularly, this property of wireless medium makes information transmission prone to eavesdropping attacks performed by receivers with malicious purposes. Conventionally, secure communications (regardless of the medium of transmission being either wired or wireless) has been addressed by cryptographic schemes [1]. However, traditional cryptographic techniques are applied in the higher layers of the communication stack (such as application) and do not offer any secrecy at the transmission level. Therefore, physical layer security has been recently emerged as a promising solution for delivering secure communications at the transmission level. Physical layer security techniques enable the possibility of perfect secure communications by only exploiting the properties of the wireless communications, e.g., fading, noise, and interferences without relying on high-layer encryption [2].

1.1 Information-theoretic approaches versus signal processing techniques for physical layer security

Physical layer security has been conventionally addressed from an information-theoretic viewpoint and has been extended by signal processing techniques to offer wireless secrecy at the transmission level. Information-theoretic approaches deliver secure information transmission with a justifiable cost in terms of the capacity and quality requirements of the secured network. Particularly, information-theoretic security is based on the combination of cryptographic schemes with channel coding techniques to exploit the randomness offered by wireless channel in order to guarantee some secrecy against eavesdroppers. For example, in his seminal work [3], Shannon considered a secure communication system based on secret-key encryption. He introduced the notion of perfect secrecy and proved its existence under the condition that the entropy of the secret key is equal or larger than that of the confidential message. Apart from the key-based security methods, Wyner in [4] proposed that secure communication can also be possible without sharing any secret keys. He showed that perfect secrecy is achievable if the quality of the main channel is higher than the wiretap channel for discrete memoryless channels. Under such assumption, he concluded that the existence of channel coding not only guarantees robustness to transmission errors but also a desired level of confidentiality. Motivated by Wyner's results, researchers have evaluated the conditions for perfect secrecy in different wiretap channels, such as broadcast channels [5], Gaussian channels [6], MIMO channels [7] and relay channels [8]. On the other hand, signal processing techniques try to secure the communications of the networks that lack the demanding computational capabilities of cryptographic services [9]. This is the case of internet of things networks or heterogeneous ad-hoc networks that require power efficient and low computationally complex security services [10].

1.2 Thesis outline

This thesis aims to provide efficient and practical signal processing algorithms to secure wireless networks at the physical layer against intelligent eavesdroppers. We propose secure transmission strategies in order to enhance the security of the two dominant wireless communication systems, namely, Orthogonal Frequency Division Multiplexing (OFDM) systems and Multiple-Input Multiple-Output (MIMO) systems. Particularly, for both systems, we devise transmission schemes that consider constrained transmission resources in terms of power, bandwidth and antennas.

In chapter 2, we focus on the training phase in OFDM system and propose two discriminatory secure pilot-based channel estimation approaches that severely degrades the eavesdropper's quality of channel estimation. More specifically, by manipulating the pilot symbols based on the channel state information shared between legitimate parties, we propose power efficient algorithms by which intended receiver is able to estimate the channel correctly while eavesdropper estimates its own channel erroneously, thus guaranteeing performance discrimination between the legitimate receiver and the eavesdropper.

Chapter 3 studies secure communications in MIMO wiretap channels. Here, we propose and analyze precoding-enabled antenna subset activation (ASA) for location-based secure communication in Rayleigh fading channels. We devise our secure transmission scheme in a way that prior to the transmission of confidential data, the symbols are first precoded as a function of channel response between transmitter and authorized receivers. After data precoding, a randomly selected subset of transmit antennas are activated for transmission of each symbol. We investigate the secrecy performance of our proposed methods by deriving closed-form expressions for the average minimum guaranteed secrecy rate and the probability of non-zero minimum guaranteed secrecy rate in Rayleigh fading channels.

We develop another effective secure transmission strategy to enhance the physical layer security in MISO wiretap channels in chapter 4. Here, we first show that transmit beamforming (TBF) in MISO wiretap channels is not efficient in terms of hardware complexity, amount of signal processing and cost. Additionally, under block fading assumption, TBF is a susceptible scheme to intelligent

eavesdroppers equipped with advanced channel estimation techniques. We then propose and analyze randomized beamforming with generalized selection transmission (RBF/GST) to jointly address the issues of TBF.

Finally, chapter 5 concludes this thesis, where we highlight our main findings, summarize the main results and give future research directions.

Chapter 2

Achieving Secure Communication Through Pilot Manipulation

The main proposition of physical layer security is enabling secure communication, without exclusively using encryption at higher layers. This can be achieved primarily in two ways: by developing secret keys from the very nature of the wireless communication medium or by designing transmission methods which limits the information at the eavesdropper [11]. For the case of exploiting the random nature of wireless channels for generating secret keys, Koorapaty *et al.* relied on the independence of the channels between transmitter/receiver and transmitter/eavesdropper to use the phase of the fading coefficients as a secret key [12]. In [13] key generation process is performed by benefiting from the unique level crossing rates of the fading processes at the legitimate terminals. Authors in [14] proposed a secret key generation by discretization of wireless multipath coefficients. In [15] and [16], authors use channel state information shared between transmitter and legitimate receivers as a secret key to interleave either the modulated symbols associated with a selected number of subcarriers or to interleave subcarriers themselves. secure communication is also possible without sharing any secret keys but using intelligent transmission schemes. As an example, one

many inject artificial noise to degrade the channel condition of the eavesdropper [17, 18, 19].

The aforementioned techniques aim to guarantee secrecy in the data transmission phase. It is possible to discriminate the channel estimation performances at legitimate receivers and eavesdroppers. Authors in [20] proposed the insertion of artificial noise during transmission of pilot symbols to degrade the channel estimation performance at the eavesdropper.

Our novel contribution in this chapter is to degrade eavesdroppers ability during channel estimation phase without introducing artificial noise. More specifically, by manipulating the pilot symbols based on the channel state information shared between legitimate parties, we propose power efficient algorithms by which intended receiver is able to estimate the channel correctly while eavesdropper estimates its own channel erroneously, thus guaranteeing performance discrimination between the legitimate receiver and the eavesdropper.

The rest of the chapter is organized as follows: Section 2.1 introduces system model. In Section 2.2 we describe the proposed pilot manipulation algorithms. The simulation scenarios and results are presented in Section 2.3. Finally, Section 2.4 concludes the chapter and gives future directions.

2.1 System Model

We consider an OFDM system that consists of a legitimate transmitter (Alice), a legitimate receiver (Bob), and a passive Eavesdropper (Eve) as shown in Fig. 2.1.

The forward and reverse channels between legitimate users are assumed to occupy the same frequency band and remain constant over several time slots. Hence, Alice and Bob would experience and observe identical channels based on the reciprocity property of wireless channels [21]. We assume that Eve does not possess any information about the legitimate channel because the channel response is unique to the location of the transmitter and receiver as well as the environment. More specifically, a rich scattering environment is assumed and the condition of Eve being at least a couple of wavelengths farther from Bob is also

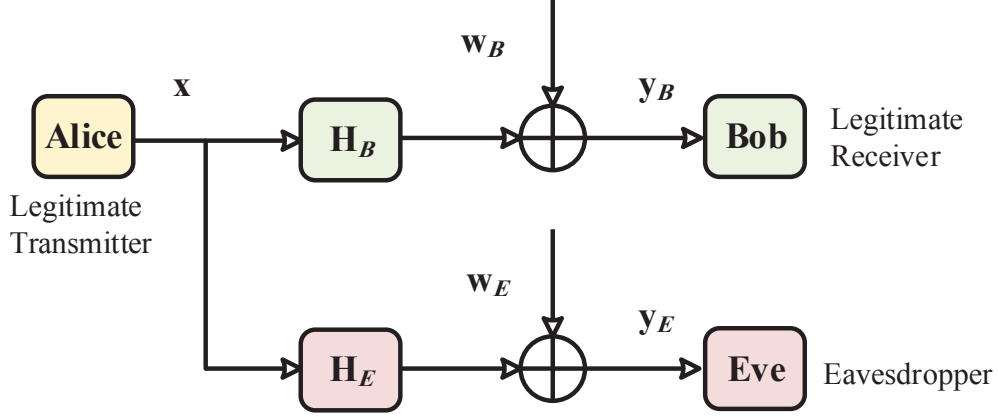


Fig. 2.1: System model consisting of legitimate transmitter (Alice) and receiver (Bob), and eavesdropper (Eve) with multipath fading channels.

fulfilled.

Assuming the frequency domain OFDM symbol $\mathbf{x} \in \mathbb{C}^{N \times 1}$ is transmitted from Alice, the signals received by Bob and Eve are denoted by $\mathbf{y}_B \in \mathbb{C}^{N \times 1}$ and $\mathbf{y}_E \in \mathbb{C}^{N \times 1}$, respectively, where N indicates the number of subcarriers. In the received vectors, the k th element ($k = 0, 1, \dots, N - 1$) corresponds to the k th subcarrier. The received signal vectors are given by

$$\begin{aligned} \mathbf{y}_B &= \mathbf{H}_B \mathbf{x} + \mathbf{w}_B, \\ \mathbf{y}_E &= \mathbf{H}_E \mathbf{x} + \mathbf{w}_E, \end{aligned} \quad (2.1)$$

where $\mathbf{H}_B \in \mathbb{C}^{N \times N}$ and $\mathbf{H}_E \in \mathbb{C}^{N \times N}$ denote corresponding channels, $\mathbf{w}_B \in \mathbb{C}^{N \times 1}$ and $\mathbf{w}_E \in \mathbb{C}^{N \times 1}$ denote circularly symmetric complex Gaussian noise vectors with zero mean and variances σ_B^2 and σ_E^2 at Bob and Eve. Assuming that the cyclic prefix (CP) is longer than the delay spread, channel matrices \mathbf{H}_B and \mathbf{H}_E become diagonal with diagonal entries being $\{H_B(0), H_B(1), \dots, H_B(N - 1)\}$ and $\{H_E(0), H_E(1), \dots, H_E(N - 1)\}$.

We assume that communication starts with an OFDM symbol containing pilot subcarriers followed by data OFDM symbols. The channel estimation results derived from the first OFDM symbol is used to detect data symbols. We assume that both Bob and Eve are relying on pilot symbols for channel estimation. As

such, blind channel estimation or data directed channel estimation are out of the scope of this chapter. Among channel estimation methods which rely on pilot symbols, we consider the performances of Least Squares (LS) and Minimum Mean Square Error (MMSE) channel estimation methods. The estimation of pilot signals based on LS method is given by

$$\begin{aligned}\tilde{H}_B(k, k) &= \frac{Y_B(k)}{X(k)} = H_B(k) + \frac{W_B(k)}{X(k)}, \\ \tilde{H}_E(k, k) &= \frac{Y_E(k)}{X(k)} = H_E(k) + \frac{W_E(k)}{X(k)},\end{aligned}\tag{2.2}$$

where $\tilde{H}_B(k, k)$ and $\tilde{H}_E(k, k)$ are the diagonal entries of channel matrices, $Y_B(k)$ and $Y_E(k)$ are the received pilot symbol at the k th subcarrier, $W_B(k)$ and $W_E(k)$ denote the additive noise in frequency domain and the pilot symbols are assumed to be $X(k) = 1$ for all k .

Let $\tilde{\mathbf{H}}_B$ and $\tilde{\mathbf{H}}_E$ denote the diagonal matrices containing estimated channel coefficients obtained in (2.2). The estimated channel coefficients obtained via MMSE channel estimation at Bob and Eve are

$$\begin{aligned}\hat{\mathbf{H}}_B &= \mathbf{R}_{B\tilde{B}}(\mathbf{R}_{BB} + \frac{\sigma_B^2}{\sigma_x^2}\mathbf{I}_N)^{-1}\tilde{\mathbf{H}}_B, \\ \hat{\mathbf{H}}_E &= \mathbf{R}_{E\tilde{E}}(\mathbf{R}_{EE} + \frac{\sigma_E^2}{\sigma_x^2}\mathbf{I}_N)^{-1}\tilde{\mathbf{H}}_E,\end{aligned}\tag{2.3}$$

where σ_x^2 denotes the variance of the pilot symbols, \mathbf{R}_{BB} , \mathbf{R}_{EE} are auto-covariance matrices and $\mathbf{R}_{B\tilde{B}}$, $\mathbf{R}_{E\tilde{E}}$ are cross-covariance matrices between the estimated and perfect channel state information at Bob and Eve respectively.

2.2 Pilot Manipulation Algorithms

We are proposing two algorithms to enhance communication secrecy. In both algorithms, pilots are manipulated according to the previous subcarrier's instantaneous channel information that are observed at the side of Alice. To enable

these algorithms, first Bob broadcasts a signal which includes OFDM pilot symbol to Alice.

The received pilots inside the OFDM symbol denoted by $X[k]$ are used to estimate the channel. The LS estimation at Alice $\hat{\mathbf{H}}_{\mathbf{A},\text{LS}}$ is

$$\begin{aligned} H_A(k, k) &= \frac{Y_A(k)}{X(k)}, \\ \tilde{\mathbf{H}}_{\mathbf{A},\text{LS}} &= \text{diag}\{H_A(k, k)\}, \end{aligned} \quad (2.4)$$

and MMSE estimation $\hat{\mathbf{H}}_{\mathbf{A},\text{LMMSE}}$ is presented as

$$\hat{\mathbf{H}}_{\mathbf{A},\text{MMSE}} = \mathbf{R}_{\mathbf{A}\tilde{\mathbf{A}}} (\mathbf{R}_{\mathbf{A}\mathbf{A}} + \frac{\sigma_{\mathbf{A}}^2}{\sigma_{\tilde{\mathbf{A}}}^2} \mathbf{I}_{\mathbf{N}})^{-1} \tilde{\mathbf{H}}_{\mathbf{A}} \quad (2.5)$$

First algorithm is based on the phase of the pilot tones whereas the second one is based on the amplitude of the pilot tones. We provide detailed descriptions in following subsections.

2.2.1 Phase-Based Pilot Manipulation

For phase-based pilot manipulation, the instantaneous channel phase of each subcarrier is compared with a properly selected thresholds Λ . In order to maximize the unpredictability during eavesdropping, pilots from Alice should have equal chance of being manipulated or not. As channel estimates $\tilde{\mathbf{H}}_{\mathbf{A},\text{LS}}$ and $\hat{\mathbf{H}}_{\mathbf{A},\text{MMSE}}$ in (2.4), (2.5) follow a zero-mean complex Gaussian distribution, the estimated channel phase vector, $\{\hat{\theta}_A(0), \hat{\theta}_A(1), \dots, \hat{\theta}_A(N-1)\}$, are i.i.d uniformly distributed variables over $[-\pi, \pi]$. Therefore, the threshold can be selected as: $\Lambda = 0$. After estimating the channel, Alice manipulates the pilots according to the following

$$\hat{X}[k] = \begin{cases} X[k] & k = 0 \\ jX[k] & \hat{\theta}_A[k-1] > 0, k \neq 0, \\ X[k] & \hat{\theta}_A[k-1] < 0, k \neq 0 \end{cases} \quad (2.6)$$

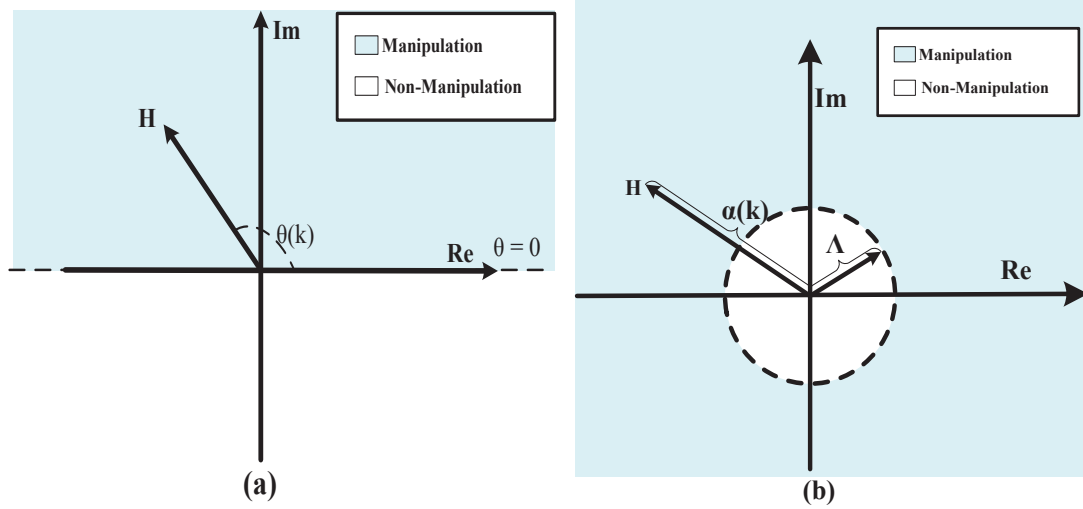


Fig. 2.2: Pilot manipulation decision regions.

where vector $\hat{\mathbf{x}} = [\hat{X}(0), \hat{X}(1), \dots, \hat{X}(N-1)]$ includes manipulated pilots, $\hat{\theta}$ is the channel phase vector of the estimated channel and $k = 0, 1, \dots, N-1$.

Decision regions for phase-based pilot manipulation are shown in Fig. 2.2.(a). The received OFDM signals containing manipulated pilots at Bob and Eve are

$$\begin{aligned}\hat{\mathbf{y}}_{\mathbf{B}} &= \mathbf{H}_{\mathbf{B}}\hat{\mathbf{x}} + \mathbf{w}_{\mathbf{B}} \\ \hat{\mathbf{y}}_{\mathbf{E}} &= \mathbf{H}_{\mathbf{E}}\hat{\mathbf{x}} + \mathbf{w}_{\mathbf{E}}\end{aligned}\quad (2.7)$$

Since the first pilot is not manipulated as indicated in (2.6), Bob estimates the channel coefficient of the first pilot using (2.2) and compares the phase of the estimate with the threshold for demanipulation of the the following pilot. General equation for pilot demanipulation is given as

$$\hat{X}[k] = \begin{cases} \hat{X}[k] & k = 0 \\ -j\hat{X}[k] & \hat{\theta}_B[k-1] > 0, k \neq 0 \\ \hat{X}[k] & \hat{\theta}_B[k-1] < 0, k \neq 0 \end{cases}\quad (2.8)$$

After demanipulation of the pilots, if necessary the MMSE channel estimation

methods shown in (2.5) is used.

The probability that Bob and Alice disagree on whether a pilot is manipulated or not, $p_{Er,\theta}(k)$, can be given as

$$p_{Er,\theta}(k) = \frac{1}{2}P(\hat{\theta}_A(k) > 0, \hat{\theta}_B(k) \leq 0) + \frac{1}{2}P(\hat{\theta}_A(k) \leq 0, \hat{\theta}_B(k) > 0), \quad (2.9)$$

where $k = 1, 2, \dots, N - 1$.

Following subsection explains amplitude-based pilot manipulation.

2.2.2 Amplitude-Based Pilot Manipulation

The algorithm for amplitude-based pilot manipulation is as follows

$$\hat{X}[k] = \begin{cases} X[k] & k = 0 \\ jX[k] & \hat{\alpha}_A[k - 1] > \Lambda, k \neq 0 \\ X[k] & \hat{\alpha}_A[k - 1] < \Lambda, k \neq 0 \end{cases} \quad (2.10)$$

where $\hat{\alpha}_A$ is the estimated channel amplitude vector and Λ is the threshold for manipulation decision as shown in Fig. 2.2.(b).

Similar to the phase-based algorithm the demanipulation algorithm performed by Bob is

$$\hat{\hat{X}}[k] = \begin{cases} \hat{X}[k] & k = 0 \\ -j\hat{X}[k] & \hat{\alpha}_B[k - 1] > \Lambda, k \neq 0 \\ \hat{X}[k] & \hat{\alpha}_B[k - 1] < \Lambda, k \neq 0 \end{cases} \quad (2.11)$$

The pilot error rate for this case can be calculated by the probability of the event

$$p_{Er,\alpha}(k) = \frac{1}{2}P(\hat{\alpha}_A(k) > \Lambda, \hat{\alpha}_B(k) \leq \Lambda) + \frac{1}{2}P(\hat{\alpha}_A(k) \leq \Lambda, \hat{\alpha}_B(k) > \Lambda), \quad (2.12)$$

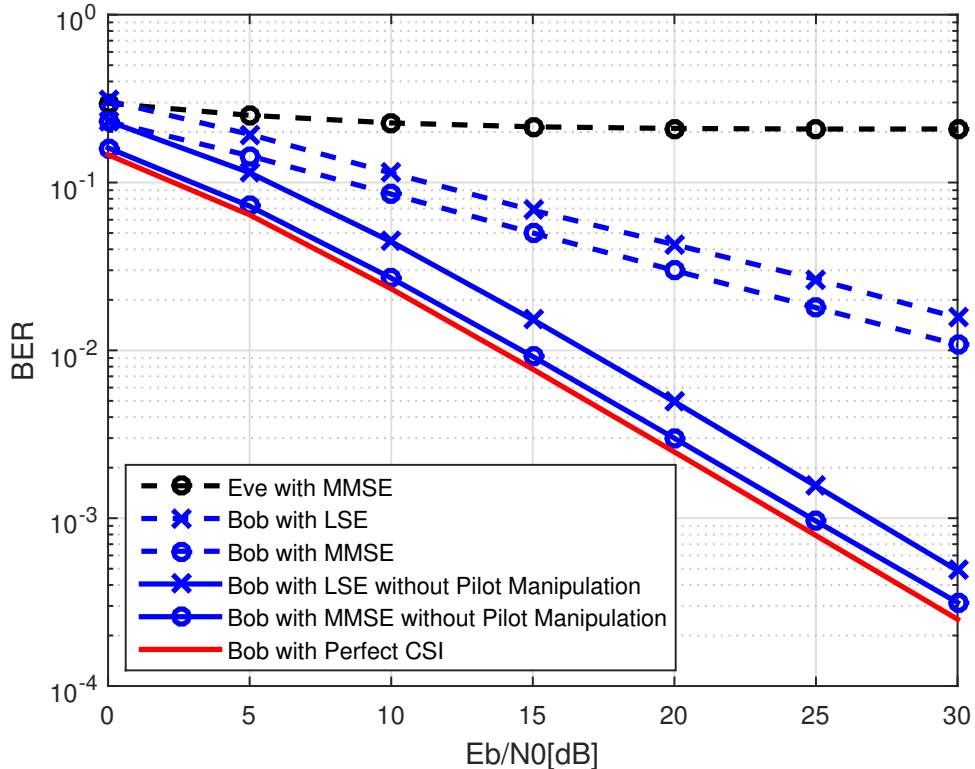


Fig. 2.3: Bit Error Rate performance of different channel estimation with phase-based pilot manipulation.

where $k = 1, 2, \dots, N - 1$.

We investigate effects of different threshold values on Bob and Eve's reception performance in the next section, which includes simulation results.

2.3 Simulation Scenarios and Results

In our simulations, we assume a 10-tap quasistatic Rayleigh fading channel. The modulation scheme is chosen to be QPSK.

The first results are acquired for the phase-based pilot manipulation algorithm and are shown in Fig. 2.3. Both LSE and MMSE channel estimation methods are utilized at Bob and Eve. Although not shown, the performance at Eve is the

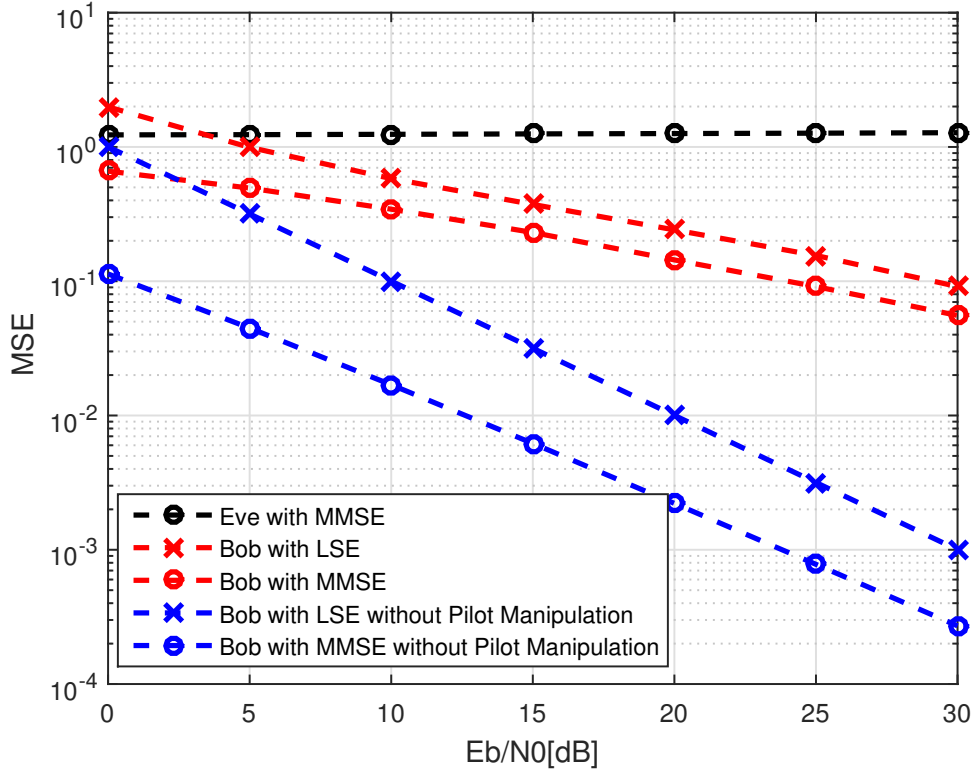


Fig. 2.4: Average Mean Square Error of different channel estimation with phase-based pilot manipulation.

same for both methods and error floor at a BER of 0.2 is observed. The algorithm is successful to decrease the BER performance at Eve. For Bob, MMSE channel estimation performs better than LSE channel estimation, however its performance is still unacceptable, when compared to BER performance without using the pilot manipulation algorithm.

Fig. 2.4 depicts the mean square error at the receivers of Bob and Eve. As expected Eve's performance is the worst. The mean square error performance at Bob's receiver follows the BER performances shown in the Fig. 2.3. The use of the phase-based algorithm increases BER and MSE in such a level that it would be illogical to be used at the legitimate receiver.

The second set of simulations are obtained for amplitude-based pilot manipulation algorithm. Unlike the phase-based, for which selecting the threshold value

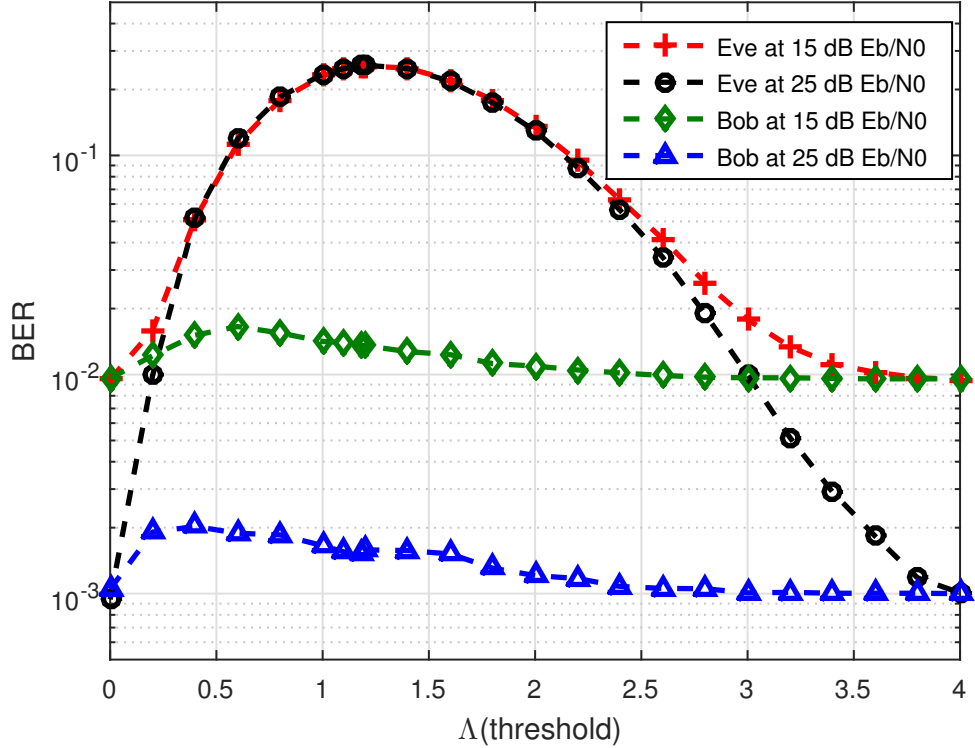


Fig. 2.5: Bit Error Rate Performance versus different threshold values at 15 and 25 dB E_b/N_0 .

was straightforward, for the amplitude-based algorithm determining the right threshold is essential. For this purpose, we obtained BER performance at 15 and 25 dB E_b/N_0 for Bob and Eve with different threshold values for normalized amplitude values. Since Rayleigh Fading channel is simulated, normalization results in Gaussian distributed in-phase and quadrature components with variances equal to 0.5. With the results shown in Fig. 2.5, we have found that when the threshold is chosen to be median value ($\sqrt{\ln(4)} \approx 1.18$) of the Rayleigh distribution, the performance of Eve is minimized for the reason that the ambiguity at the Eve's receiver is maximized. On the other hand there is small amount of performance difference for Bob at different threshold values. As a result system designers may choose the optimum threshold value according to their needs. Next we provide BER and MSE performances of Bob and Eve with the optimum

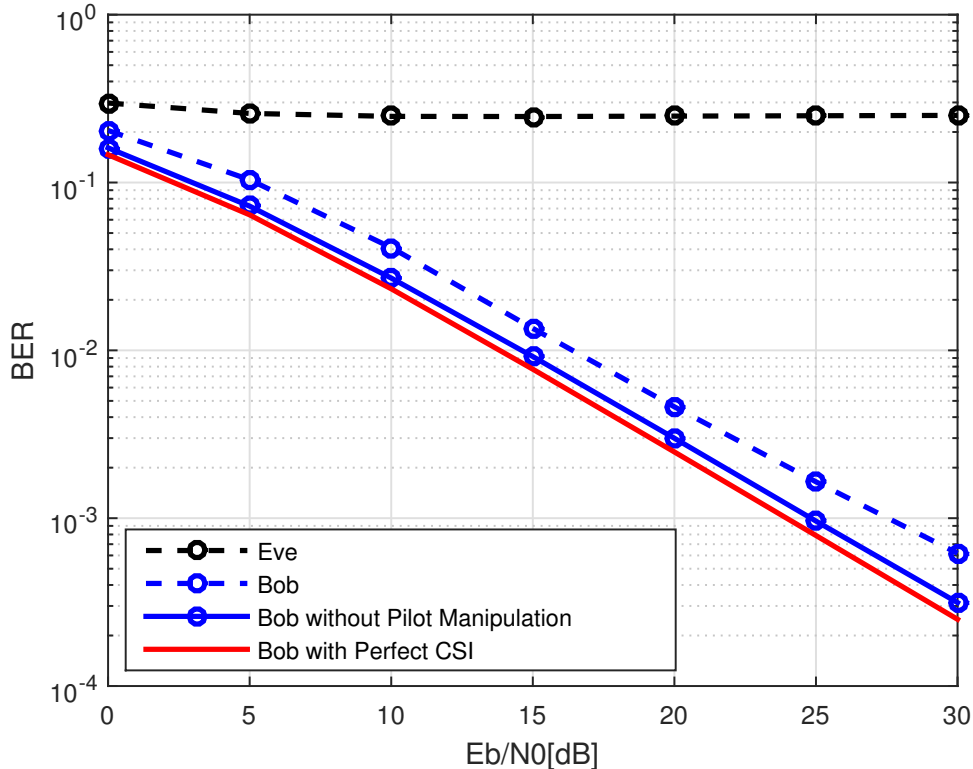


Fig. 2.6: Bit error rate performance with amplitude-based pilot manipulation with MMSE channel estimation.

protection threshold.

Figures 2.6, 2.7 provide the BER and MSE performances with MMSE channel estimation. Since the LSE has poorer performance, we did not provide simulation results. Similar to phase-based pilot manipulation, we observe in Fig. 2.6 the algorithm provides enough protection against eavesdropping. On top of that, the performance at Bob is only 3 dB inferior than a receiver which does not utilize the algorithm. If we examine the MSE results shown in Fig. 2.7, the MSE performance at Eve is similar compared to performance shown in Fig. 2.4 whereas considerable improvement is observed at the performance of Bob.

The last figure of this section compares the pilot error rates of different manipulation schemes. The superiority of the amplitude-based pilot manipulation compared to phase-based one is observed one more time in Fig. 2.8. Due to the

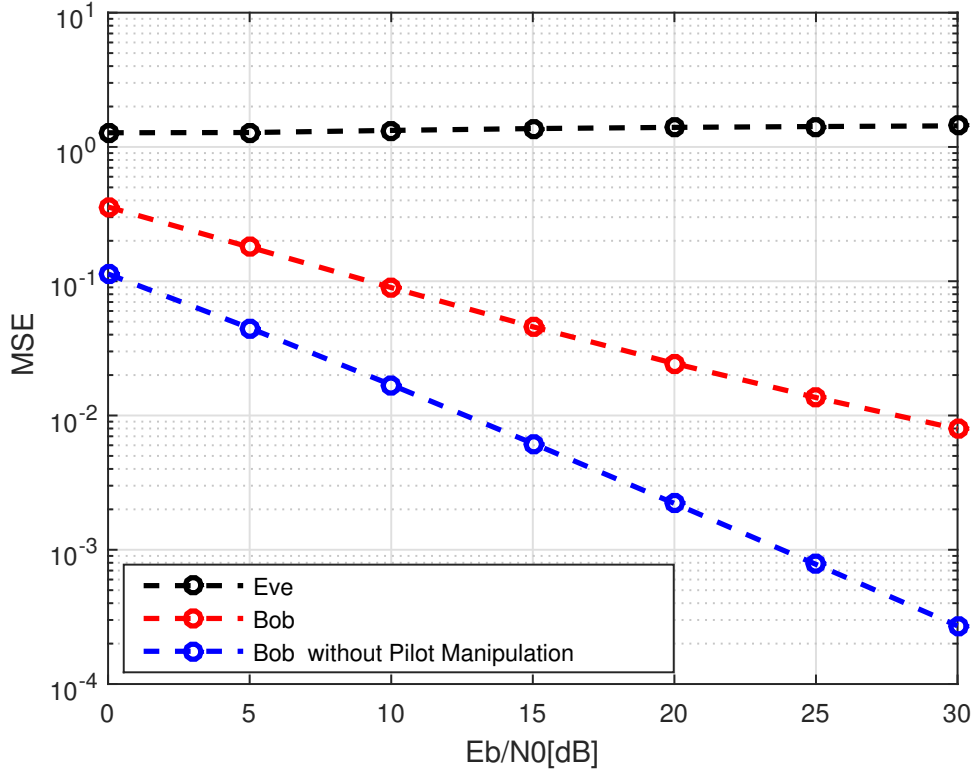


Fig. 2.7: Average Mean Square Error with amplitude-based pilot manipulation and MMSE channel estimation.

nature of the Rayleigh fading channel, phase-based pilot manipulation results in higher pilot error rate since manipulation at Alice and demanipulation at Bob may mismatch at faded subcarriers. For amplitude-based approach, the algorithm does not manipulate the pilots if fading is observed, thus reduces the pilot error rate.

2.4 Conclusions

In this chapter, we introduced two novel algorithms to improve the security of wireless communications via decreasing the ability of the eavesdropper's channel

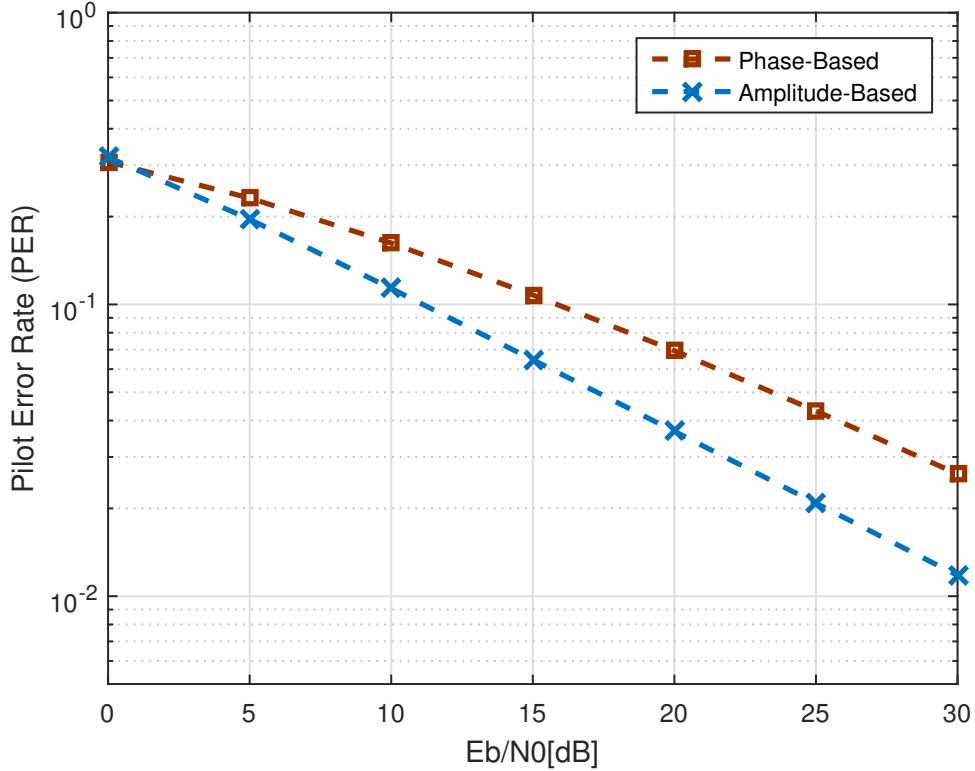


Fig. 2.8: Pilot Error Rate performance with MMSE channel estimation for phase-based and amplitude-based pilot manipulation.

estimation. Both algorithms were based on manipulating the pilot symbols according to the channel observed between the legitimate transmitter and receiver. The first algorithm used the phase of the channel coefficients to decide the manipulation whereas the second one relied on the channel coefficient amplitudes. According to simulation results both algorithms reduced the reception performance at the eavesdropper to a level, in which pilot based channel estimation was useless. We showed that the amplitude based algorithm has a lower pilot error rate and provides satisfactory performance at the legitimate receiver. We investigated the effect of the manipulation threshold and found that there is an optimum threshold for the security of the channel and the performance at the legitimate receiver.

Chapter 3

Antenna Subset Activation for Location-Based Secure MISO Wireless Communications in Fading Channels

From an information-theoretic viewpoint, the essence of physical layer security is to maximize the secrecy rate [22, 23], which is defined as the rate difference of a legitimate channel and an eavesdropper channel. In this context, security techniques are required to improve the rate of the legitimate channel and impair the rate of the wiretap channel, simultaneously.

Apart from the information theoretic perspective, one of the most common signal processing techniques to secure the confidential data transmission is to spread the signal in frequency [24], so that the malicious receivers cannot capture and decode the signal. However, the spread spectrum (DS/SS) approaches have a common assumption that no information is known about the spreading codes by the malicious receivers, which can hardly hold in practice [25] where they can be estimated by the eavesdroppers. On the other hand, wireless channel based precoding approaches [12, 26] are based on the assumption that can be failed by invoking the advanced processing capabilities for blind channel estimation and

decoding of the transmitted signal [27].

Recently, it has been shown that multiple antenna techniques can effectively enhance physical layer security. For example, if the transmitter is equipped with multiple antennas, the information signal may be transmitted in the null space of the eavesdropper channel. In this case, the eavesdropper fails to receive any information regardless of its relative distance with respect to the transmitter. Another possible approach in multiple-input multiple-output (MIMO) scenarios is to degrade the reception performance of possible eavesdroppers by inserting artificial noise (AN) to the useful data without affecting the legitimate receiver performance [17]. This is achieved by selecting the noise vector from the nullspace of the MIMO channel between the transmitter and the legitimate receivers. However, multiple requirements for this to be effective, i.e., waste of transmit power for AN emission and existence of the nullspace reduce the attractiveness of such secrecy method. Another effective multiple-antenna enabled physical layer security technique, is to simultaneously increase the quality of the main channel and decreasing that of the wiretap channel by transmit beamforming (TBF). In directional transmissions for phased-array antenna transmitters, TBF creates symbols with high gain along a particular direction while purposely suppresses the gain in other directions. this approach inherently serves for the communication secrecy. However, when the eavesdropper is closer to the transmitter than the legitimate receiver can, she still have sufficient received power to detect the confidential data. Furthermore, TBF in phased-array transmission does not provide secure communication when the malicious receiver is located along the same direction with the intended receiver. Recently, the first problem is addressed partially for millimeter wave (mm-Wave) channels by considering the angular sidelobes in the directional radiation patterns that might cause the information leakage. With the adaptive advancements on beamforming, intelligent schemes such as Directional Modulation (DM) [28, 29] and Antenna Subset Modulation (ASM) [30] are proposed to randomize the signal received by eavesdroppers positioned at directions other than the direction of the legitimate receivers.

Although the aforementioned techniques promise some degrees of secrecy in the wireless communication scenarios by reducing the area where the transmitted signal is broadcasted, a true location-based information security considering both

the angle and the distance of the intended receiver is away from being provided by the current techniques. This chapter tackles the fundamental issue in wireless communication in terms of communication secrecy, i.e., broadcasting nature of the radio transmission, with the main objective of providing location-specific secure information transmission for MISO scenarios. Here, we study another effective signal processing approach to enhance the physical layer security in MISO wiretap channels. In this approach, a randomly selected subset of transmit antennas is activated for each symbol transmission, or for each set of symbols. For an active antenna set, the transmitted data signal is precoded at each activated transmit antenna as a function of the channel response between the corresponding transmit antenna of Alice and receive antenna of Bob. For an active antenna set, the transmitted data signal is precoded at each transmit antenna as a function of the channel response between this antenna and intended receive antenna. Two different channel-based precoding techniques are considered, namely channel inversion precoding and eigenbeamformer precoding. After selection of an active antenna set, the first precoder pre-compensates the phase and amplitude distortions of the channel response of each active antenna on the transmitted signal. Although this leads in a sharply defined constellation at the legitimate receiver with no effect on the decoding performance, it is not efficient in terms of overall transmission power. In order to overcome this problem, the second precoder solely corrects the phase distortion of the fading gain associated with each active antenna. This, however, introduces amplitude distortion to the received signal at the legitimate receiver. We investigate the secrecy performance of the proposed channel-based precoding schemes in terms of the average minimum guaranteed secrecy rate and the probability of non-zero minimum guaranteed secrecy rate.

The main contributions of the chapter are summarized as follows

- The concept of location specific secure transmission is introduced by applying channel-based precoding-enabled antenna subset activation (ASA) in MISO wiretap channels.
- Two channel-based precoding schemes are considered for delivering secure as well as reliable transmission to the legitimate receiver. The proposed channel-based precoding schemes provide simple receiver architecture since

channel estimation and equalization are no longer required for reliable signal reception at the legitimate receiver.

- The secrecy performance of the proposed precoding-enabled ASA schemes is investigated. More specifically, by considering the notion of minimum guaranteed secrecy rate, we show that, regardless of the position of the eavesdropper with respect to the transmitter, still secure communication can be achievable with a high probability. Furthermore, we derive the closed-form expressions of the minimum guaranteed secrecy rate and probability of non-zero minimum guaranteed secrecy rate for both of the precoding schemes.
- The effect of the thinning ratio, i.e., the ratio between the number of active antennas to the total number of antennas, on the secrecy performance of the proposed schemes is examined. In particular, in the case of the eigenbeamformer precoding, we analyze the trade-off between security and reliability for the legitimate link.
- Finally, a detailed comparison for the secrecy performance of the proposed precoding schemes is provided.

The remainder of this chapter is organized as follows. In Section 3.1, we introduce the channel model, explain the precoding techniques and describe the channel-based precoding with ASA in fading environments. Section 3.2 evaluates the secrecy performance of the ASA in Rayleigh fading channels. In Section 3.3, we provide numerical results and discussions. Finally, section 3.4 concludes the chapter and summarizes the findings.

3.1 Protocol Description

3.1.1 System Model

We assume a MISO wiretap channel where Alice is a multiple antenna transmitter equipped with N antennas, while the legitimate receiver (Bob) and an

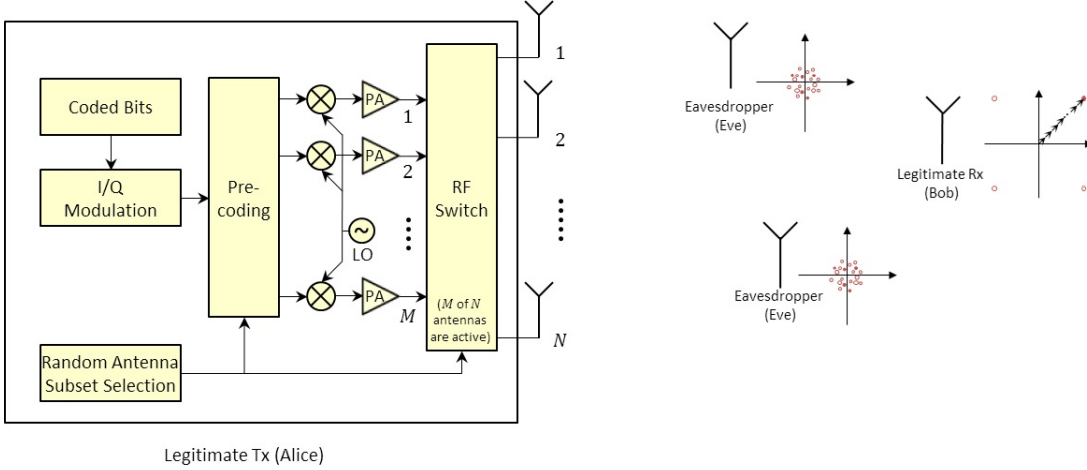


Fig. 3.1: MISO wiretap channel with the ASA and Precoding.

eavesdropper (Eve) are both assumed to be single antenna receivers as illustrated in Fig. 3.1. Furthermore, we consider that the main and wiretap channels are both quasi-static independent identically distributed (i.i.d) block Rayleigh fading channels. In this setup, we focus on a passive eavesdropping scenario, where there is no Channel State Information (CSI) feedback between Alice and Eve. As such, the CSI of the wiretap channel is not known.

For this MISO wiretap channel, we propose an ASA protocol to boost the achievable secrecy rate. In the considered scenario, the received downsampled signals y and z at time index n at Bob and Eve can be presented respectively as

$$y(n) = \mathbf{h}^T \mathbf{x}(n) + w_y(n), \quad (3.1)$$

$$z(n) = \mathbf{g}^T \mathbf{x}(n) + w_z(n), \quad (3.2)$$

where $\mathbf{x}(n)$ is an $N \times 1$ complex vector representing the transmitted signal vector at time index n , while $w_y(n)$ and $w_z(n)$ are independent and identically distributed (i.i.d.) circularly symmetric additive white Gaussian noise samples with zero mean and unit variance at the legitimate receiver and eavesdropper, respectively. In (3.1) and (3.2), \mathbf{h} and \mathbf{g} are both $N \times 1$ complex vectors representing the main and wiretap channels, respectively. Here, the channels are assumed to be flat Rayleigh fading. That is, $\mathbf{h} \sim \mathcal{CN}(\mathbf{0}, \sigma_h^2 \mathbf{I}_N)$ and $\mathbf{g} \sim \mathcal{CN}(\mathbf{0}, \sigma_g^2 \mathbf{I}_N)$, respectively, while \mathbf{h} , \mathbf{g} , $w_y(n)$ and $w_z(n)$ are independent, unless otherwise stated.

With the flat-fading, the channel from each transmit antenna to the receive antennas of Bob and Eve, is a complex multiplicative factor. We assume that Alice knows \mathbf{h} perfectly, while Eve knows \mathbf{h} and \mathbf{g} perfectly. This represents the best possible scenario for the eavesdropper.

3.1.2 Precoder Design

The precoder design plays a crucial role in our secure transmission techniques. Conventionally, precoding techniques have been used for various purposes, such as achieving higher throughput in MIMO systems [31], improving receiver performance in the presence of multiple access interference in multiple access channels [32] and reduction of out of band emission in OFDM systems [33]. On the other hand, in this work, we use precoders for the sake of enhancing physical layer security. In particular, we adopt two precoding schemes, namely channel inversion (CI) and eigenbeamformer (EBF). If a CI precoding is used, the proposed communication can support any type of QAM modulation, since CI forces the received constellation points to be exactly at their desired locations. However, the limitation of this precoder is that for the antennas that are in deep fade, the transmission power to compensate the fading effect might be too high, which may result in inefficient transmission with unbalanced power loading across the antennas. As opposed to CI precoder, the EBF precoder is based on the the phase correction of the channel, thus transmission power can be kept constant. Nevertheless, with the usage of EBF precoder, multilevel QAM modulations may not be supported.

Assuming \mathbf{P}_A as the $N \times N$ precoder matrix being used in the transmission of Alice, the transmitted signal vector \mathbf{x} can be written as

$$\mathbf{x}(n) = \mathbf{P}_A \mathbf{u}(n), \quad (3.3)$$

where $\mathbf{u}(n)$ is an $N \times 1$ transmitted symbol vector with the power constraint as $\frac{1}{J} \sum_{n=1}^J \mathbb{E}[|u(n)|^2] = P$. Since we focus on a single user communication, the entries of the symbol vector are identical, i.e., $\mathbf{u}(n) = [u_1, \dots, u_N]^T = \mathbf{1}u(n)$, where $\mathbf{1}$ is

an $N \times 1$ vector with entries all identical to 1.

The CI precoding matrix is given by

$$\mathbf{P}_{\text{ACI}} = \text{diag}\left\{\frac{1}{h_1}, \dots, \frac{1}{h_N}\right\}, \quad (3.4)$$

where $\text{diag}\{\cdot\}$ is a diagonal matrix with diagonal entries identical to the inverted fading gains of the main channel. Likewise, the diagonal entries of the EBF precoding matrix are

$$\mathbf{P}_{\text{AEBF}} = \text{diag}\left\{\frac{h_1}{|h_1|}, \dots, \frac{h_N}{|h_N|}\right\}^H. \quad (3.5)$$

In contrast to the CI precoder, the entries of \mathbf{P}_{AEBF} are simply the inverted phase of the main channel coefficients.

3.1.3 Antenna Subset Activation in Fading Channels

In this subsection, we propose the ASA with precoding that can be used in fading channels. In this scheme, Alice uses a subset of M ($M < N$) antennas in the array for the transmission of a given symbol, and this subset changes from one symbol duration to another. Under the assumption of Non Line of Sight (NLOS) Rayleigh fading channels, the specific location of Bob defines a complex symbol in the I-Q plane. Thus, the effect of precoding and antenna subset activation on the transmitted signal at time index n are succinctly represented by $\mathbf{x}(n) = \frac{1}{M}\mathbf{P}_A\mathbf{B}(n)\mathbf{u}(n)$, where $\mathbf{B}(n)$ is the subset activation matrix and it is an $N \times N$ diagonal matrix with binary diagonal entries with the constraint of $\text{tr}\{\mathbf{B}(n)\} = M$. The diagonal entries of $\mathbf{B}(n)$ thus encodes the M -antenna subset activated for transmitting n th symbol, i.e., the position with ones indicate active antennas while zeros indicate unused antennas.

Now that we have introduced our signal model along with the precoding as well as the ASA algorithm, we next focus on the analysis of the received signals at Bob and Eve for each of the precoders.

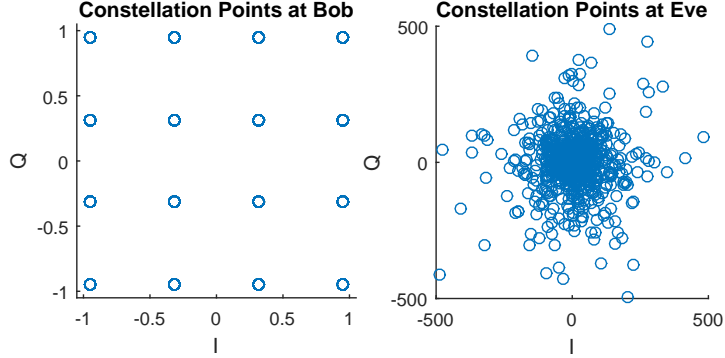


Fig. 3.2: Received 16-QAM constellation points at Bob and Eve with the CI precoder

3.1.3.1 Channel Inversion Precoder

With this Precoder, prior to the transmission, each symbol is first precoded by the inverted fading gain over each transmit antenna. Afterwards a subset of antennas is chosen for transmitting the symbol. Substituting (3.4) into (3.1) and 3.2, the received signals at Bob and Eve at time instant n are given by

$$y(n) = \underbrace{\frac{1}{M}[h_1, \dots, h_N] \left(\text{diag}\left\{\frac{1}{h_1}, \dots, \frac{1}{h_N}\right\} \mathbf{B}(n) \mathbf{1} \right)}_{g_{B,CI}(n)=1} u(n) + w_y(n) \quad (3.6)$$

$$= g_{B,CI}(n)u(n) + w_y(n), \quad (3.7)$$

$$z(n) = \underbrace{\frac{1}{M}[g_1, \dots, g_N] \left(\text{diag}\left\{\frac{1}{h_1}, \dots, \frac{1}{h_N}\right\} \mathbf{B}(n) \mathbf{1} \right)}_{\text{complex scalar dependant on } \mathbf{h}, \mathbf{g} \text{ and } \mathbf{B}(n)} u(n) + w_z(n) \quad (3.8)$$

$$= g_{E,CI}(\mathbf{h}, \mathbf{g}, \mathbf{B}(n))u(n) + w_z(n), \quad (3.9)$$

for some $\mathbf{B}(n) \in \mathcal{B}$, where \mathcal{B} denote the set of all such matrices \mathbf{B} . The Bob's scaling factor $g_{B,CI}(n)$ that appears in (3.7) is in general a function of both main channel (precoding) and the activation matrix. With the CI precoder, the various (scaled and phase shifted) signal replicas add coherently and result in sharp constellation points, i.e., $y(n) = u(n) + w_y(n)$ since $g_{CI,B}(n) = 1, \forall \mathbf{B}(n) \in \mathcal{B}$. However, outside of an area where its relative distance with respect to Bob is greater than half a wavelength (assuming rich scattering environment surrounding Bob and NLOS communications), the signals add up misaligned in phase as well

as amplitude. Depending on the antenna subset chosen and main and wiretap vectors, the desired modulated symbol appears to Eve as scaled and rotated. As shown in Fig. 3.2, this creates a blurred constellation \mathcal{C}_E that is very different from the target constellation \mathcal{C}_B . The constellation points received by Eve appear randomized because of the random choice of an antenna subset for each symbol, i.e., $g_{CI,E}(\mathbf{P}_{\mathbf{A}_{CI}}, \mathbf{g}, \mathbf{B}(n)) \neq 1$ and is in general a complex random value for $\mathbf{g} \neq \mathbf{h}$ that changes as fast as symbol rate.

The additional constellation points created by the ASA with precoding can equivalently be thought of as interference generated by distorting the stationarity of the wiretap channel. While switching the active antenna subset does not alter the constellation points received by Bob, the symbols are distorted in both phase and amplitude for receivers which do not have the same or very similar channel response to Bob. Therefore, the received instantaneous signal to interference plus the noise ratios (SINR) of the main and wiretap channels are desired for evaluating the secrecy performance of the ASA. With the CI precoder, the effective channel between Alice and Bob becomes a complex AWGN channel. Hence, the received instantaneous SNR at Bob is given by

$$\gamma_{BCI} = \frac{P}{\sigma_B^2}. \quad (3.10)$$

On the other hand, the received instantaneous SNR at Eve is not as straightforward as Bob. We rewrite the received signal at Eve as follows

$$z(n) = g_{E,CI}(n)u(n) + w_z(n), \quad (3.11)$$

where $g_{E,CI}$ is the effective channel between Alice and Eve. It has to be stressed that this effective channel is responsible for distorting received constellation at Eve in order to degrade its reception performance. In the following section, we show that the average of this effective channel over a fading block results in a value that only depends on the precoding vector used at Alice and wiretap channel. Since Eve knows the perfect CSI of its own channel as well as the CSI of Bob, she can calculate the mean of the observed effective channel and use this

value for detecting the confidential data. In other words, we consider

$$z(n) = \underbrace{\mathbb{E}_{\mathbf{B}}[g_{E,CI}(n)]u(n)}_{\text{Useful Information}} + \underbrace{\{g_{E,CI}(n) - \mathbb{E}_{\mathbf{B}}[g_{E,CI}(n)]\}}_{\text{Interference}}u(n) + w_z(n). \quad (3.12)$$

Thus, the received SINR at Eve is given by

$$\gamma_{ECI} = \frac{|\mathbb{E}_{\mathbf{B}}[g_{E,CI}(n)]|^2 P}{\mathbb{E}_{\mathbf{B}}[|g_{E,CI}(n) - \mathbb{E}_{\mathbf{B}}[g_{E,CI}(n)]|^2] P + \sigma_E^2}. \quad (3.13)$$

In (3.13), the denominator represents the variance of the effective channel plus noise power. The effective channel is changing as fast as symbol rate and considerably degrades the reception performance of Eve and prevents here from detecting sensitive information.

3.1.3.2 Eigenbeamformer Precoder

One of the major drawback of the CI precoder is that the power distribution over the antennas is not efficient. Depending on the fading coefficient associated with each antenna element, some of the antennas may transmit low power signals while the others may transmit with an enormous amount of power due to the inversion of the fading gains. Thus, considering another type of precoder that solves this issue is a must. With the EBF precoder, the transmitted power from each antenna element is kept constant. However, this results in the amplitude variation on the signal received by Bob and hence degrades the secrecy performance. The received

signals at Bob and Eve at time instant n are

$$y(n) = \underbrace{\frac{1}{M}[h_1, \dots, h_N] \left(\text{diag} \left\{ \frac{h_1^*}{|h_1|}, \dots, \frac{h_N^*}{|h_N|} \right\} \mathbf{B}(n) \mathbf{1} \right)}_{\text{real scalar dependant on } \mathbf{h} \text{ and } \mathbf{B}(n)} u(n) + w_y(n), \quad (3.14)$$

$$= g_{B,EBF}(\mathbf{P}_{\mathbf{A}_{EBF}}, \mathbf{B}(n)) u(n) + w_y(n) \quad (3.15)$$

$$z(n) = \underbrace{\frac{1}{M}[g_1, \dots, g_N] \left(\text{diag} \left\{ \frac{h_1^*}{|h_1|}, \dots, \frac{h_N^*}{|h_N|} \right\} \mathbf{B}(n) \mathbf{1} \right)}_{\text{complex scalar dependant on } \mathbf{h}, \mathbf{g} \text{ and } \mathbf{B}(n)} u(n) + w_z(n), \quad (3.16)$$

$$= g_{E,EBF}(\mathbf{P}_{\mathbf{A}_{EBF}}, \mathbf{g}, \mathbf{B}(n)) u(n) + w_z(n). \quad (3.17)$$

The scaling factors of Bob and Eve under utilization of the EBF precoder are

$$g_{B,EBF}(n) = \frac{1}{M} \sum_{k=1}^N |h_k| b(k, n)$$

$$g_{E,EBF}(n) = \frac{1}{M} \sum_{k=1}^N g_k \frac{h_k^*}{|h_k|} b(k, n)$$

where $b(k, n)$ is the k th diagonal element of $\mathbf{B}(n)$. Similar to the previous case, we assume that the average of the effective channels of Bob and Eve over one fading block, i.e., $\mathbb{E}_{\mathbf{B}}\{g_{B,EBF}\}$ and $\mathbb{E}_{\mathbf{B}}\{g_{E,EBF}\}$ are used for detecting the received signal and the variations around these values are regarded as interference that degrades the reception performance. Similar to the SINR analysis presented for CI precoder, the received SINR at Bob and Eve with the EBF precoding can respectively be written as

$$\gamma_{B,EBF} = \frac{|\mathbb{E}_{\mathbf{B}}[g_{B,EBF}(n)]|^2 P}{\mathbb{E}_{\mathbf{B}}[|g_{B,EBF}(n) - \mathbb{E}_{\mathbf{B}}[g_{B,EBF}(n)]|^2] P + \sigma_B^2}, \quad (3.18)$$

$$\gamma_{E,EBF} = \frac{|\mathbb{E}_{\mathbf{B}}[g_{E,EBF}(n)]|^2 P}{\mathbb{E}_{\mathbf{B}}[|g_{E,EBF}(n) - \mathbb{E}_{\mathbf{B}}[g_{E,EBF}(n)]|^2] P + \sigma_E^2}. \quad (3.19)$$

where $g_{B,EBF}(n)$ and $g_{E,EBF}(n)$ are the effective main and wiretap channels with the usage of the EBF, respectively. The denominator of (3.18) shows that the received signal at Bob, unlike the case with CI precoder, is distorted with the interference due to the effect of the EBF precoding. This interference degrades

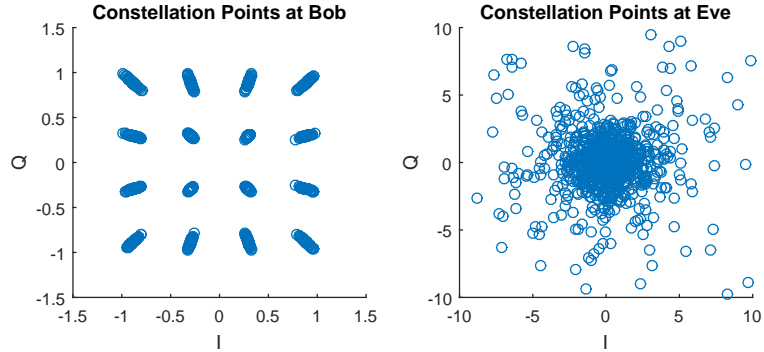


Fig. 3.3: Received 16-QAM constellation points at Bob and Eve with the EBF Precoder.

the reception performance of Bob and thus affects the secrecy rate. However, the induced interference at Eve is still in a level that she receives a completely distorted constellation. Fig. 3.3 shows the received constellation points at Bob and Eve. It is clear that due to the phase correction performed in the transmission of each symbol, the constellation points at Bob are aligned towards a line with the the same phase as the phase of the transmitted symbol. While, the received constellation points at Eve are the superposition of misaligned points.

3.2 Secrecy Performance Evaluation of the ASA in Fading Channels

In this section, we present a comprehensive investigation on the secrecy performance of the ASA technique in fading channels. The derivation of the minimum guaranteed secrecy rate and probability of non-zero minimum guaranteed secrecy rate for CI and EBF precoders are given throughout the section.

3.2.1 Preliminaries

We first present a set of statistical properties of γ_{BCI} , γ_{BEBF} , γ_{ECI} , and γ_{EEBF} which will be frequently involved in the subsequent derivation.

3.2.1.1 CI precoder

The instantaneous received SNR at Bob and Eve are given in (3.10) and (3.13). Since the effective channel of Bob is turned into a complex AWGN channel, the exact PDF of γ_{BCI} is given by

$$f_{\gamma_{BCI}}(x) = \delta(x - \gamma_{BCI}), \quad (3.20)$$

where $\delta(\cdot)$ is the Dirac delta function.

The detection performance of Eve severely suffers from the interference induced by both the ASA and Precoding. Therefore, we assume that the communication observed by Eve is interference limited rather than noise limited and instead of using SNR metric for Eve, we consider SIR for the subsequent derivations. The received SIR at Eve is given by

$$\gamma_{ECI} = \frac{|\mathbb{E}_{\mathbf{B}}[g_{E,CI}(n)]|^2}{\mathbb{E}_{\mathbf{B}}[|g_{E,CI}(n) - \mathbb{E}_{\mathbf{B}}[g_{E,CI}(n)]|^2]}, \quad (3.21)$$

where the numerator is

$$|\mathbb{E}_{\mathbf{B}}[g_{E,CI}(n)]|^2 = \left| \frac{1}{N} \sum_{k=1}^N \frac{g_k}{h_k} \right|^2, \quad (3.22)$$

and the denominator is

$$\frac{N-M}{(N-1)M} \left(\left[\frac{1}{N} \sum_{k=1}^N \left| \frac{g_k}{h_k} \right|^2 \right] - \left| \frac{1}{N} \sum_{k=1}^N \frac{g_k}{h_k} \right|^2 \right). \quad (3.23)$$

Proof. See Appendix A. □

Furthermore, γ_{ECI} is exponentially distributed with parameter $\lambda_E = \frac{1-\beta}{\beta} \frac{N}{N-1}$, where β is the thinning ratio and is defined as $\beta \triangleq \frac{M}{N}$. Thus, the PDF of γ_{ECI} is given by

$$f_{\gamma_{ECI}}(y) = \lambda_E e^{-\lambda_E y} u(y), \quad (3.24)$$

where $u(\cdot)$ is the unit step function.

Proof. See Appendix B. □

3.2.1.2 EBF precoder

With the EBF precoder the received SINR at Bob has a different formulation and PDF. In (3.18), the numerator has the format of

$$|\mathbb{E}_{\mathbf{B}}[g_{B,EBF}(n)]|^2 P = \left[\frac{1}{N} \sum_{k=1}^N |h_k| \right]^2 P \quad (3.25)$$

and the denominator is given by

$$\frac{N-M}{(N-1)M} \left(\left[\frac{1}{N} \sum_{k=1}^N |h_k|^2 \right] - \left[\frac{1}{N} \sum_{k=1}^N |h_k| \right]^2 \right) P + \sigma_B^2 \quad (3.26)$$

Proof. See Appendix C. □

Equations (3.25) and (3.26) can respectively be regarded as the estimators of the mean and variance of the Rayleigh distribution with parameter $\sigma_{\mathbf{h}}$. The estimation performance depends on the sample set size which in our case is identical to the total transmit antennas. As the number of antennas at Alice increases, the estimation becomes more accurate and approaches

$$\gamma_{B_{EBF}} = \frac{\left(\frac{\pi}{2}\sigma_{\mathbf{h}}^2\right)P}{\frac{N-M}{(N-1)M} \left(\frac{4-\pi}{2}\sigma_{\mathbf{h}}^2\right)P + \sigma_B^2}. \quad (3.27)$$

The difference between (3.10) and 3.27 is that with the EBF precoder the received signal at Bob is always interference polluted, even at high SNR regime.

Similar to the previous case with CI precoder, the PDF of $\gamma_{B_{EBF}}$, tends to a delta function as

$$f_{\gamma_{B_{EBF}}}(x) = \delta(x - \gamma_{B_{EBF}}). \quad (3.28)$$

Also the PDF of $\gamma_{E_{EBF}}$ with the EBF precoding is similar to the PDF of that

with CI precoder

$$f_{\gamma_{E_{EBF}}}(y) = \lambda_E e^{-\lambda_E y} u(y). \quad (3.29)$$

Proof. See Appendix D. □

3.2.2 Minimum Guaranteed Secrecy Rate

Now that we have the PDF of γ_B and γ_E for both CI and EBF precoders, we turn our focus to the calculation of the secrecy rate of the proposed schemes. Since in our analysis we consider that the reception of Eve is not affected by AWGN, we stick to the notion of minimum guaranteed secrecy rate which is given by [17]

$$R_{sec,mg} = \max \{ \log(1 + \gamma_B) - \log(1 + \gamma_E) \}^+, \quad (3.30)$$

where $\{x\}^+$ stands for $\max\{x, 0\}$ operator. It is worth noting that in the absence of the ASA ($M = N$), the received SIR of Eve with both of the precoders, will be infinite, leading minimum guaranteed secrecy rate to be zero, i.e., $R_{sec,mg} \doteq 0$. The presence of the ASA technique limits the SIR of Eve, allowing for non-zero minimum guaranteed secrecy rate. Furthermore, $R_{sec,mg}$ is affected by the choice of the number of active antennas. The more is the number of active antennas, the less is the interference affecting the reception of Eve and thus the less is the secrecy rate.

In (3.30), $R_{sec,mg}$ is a random variable as it depends on the random channel gains \mathbf{h} and \mathbf{g} . The average minimum guaranteed secrecy rate is defined by taking the expectation of $R_{sec,mg}$ over different realizations of \mathbf{h} and \mathbf{g} . Formally,

$$\bar{R}_{sec,mg} = \mathbb{E}_{\mathbf{h}, \mathbf{g}} [R_{sec,mg}]. \quad (3.31)$$

In other words, the average minimum guaranteed secrecy rate is given by

$$\bar{R}_{sec,mg} = \int_0^\infty \int_0^\infty [\log_2(1 + x) - \log_2(1 + y)] f_{\gamma_B}(x) f_{\gamma_E}(y) dx dy. \quad (3.32)$$

It has to be noted that since the fading channel coefficients of Bob and Eve, are

assumed to be uncorrelated, the random variables γ_{BCI} , γ_{BEFF} , γ_{ECI} , and γ_{EETF} are also uncorrelated. Incorporating correlated fading channels for Bob and Eve is a topic of future work. After substitution of (3.20) and (3.24) into (3.32), we get

$$\begin{aligned}
\bar{R}_{sec,mg} &= \int_0^\infty \int_0^\infty [\log_2(1+x) - \log_2(1+y)] \delta(x - \gamma_B) \lambda_E \exp(-\lambda_E y) dx dy \\
&= \underbrace{\int_0^\infty \int_0^\infty \log_2(1+x) \delta(x - \gamma_B) \lambda_E \exp(-\lambda_E y) dx dy}_{I_1} \\
&\quad - \underbrace{\int_0^\infty \int_0^\infty \log_2(1+y) \delta(x - \gamma_B) \lambda_E \exp(-\lambda_E y) dx dy}_{I_2}. \tag{3.33}
\end{aligned}$$

The calculation of I_1 is trivial and is equal to $\log_2(1 + \gamma_B)$, while the derivation of I_2 is not straightforward and is given by

$$\begin{aligned}
I_2 &= \int_0^\infty \delta(x - \gamma_B) dx \int_0^\infty \log_2(1+y) \lambda_E \exp(-\lambda_E y) dy \\
&= \int_0^\infty \log_2(1+y) \lambda_E \exp(-\lambda_E y) dy \\
&= \int_0^\infty \log_2 e \ln(1+y) \lambda_E \exp(-\lambda_E y) dy \tag{3.34}
\end{aligned}$$

By changing the variable $1 + y = z$, we have

$$I_2 = \log_2 e \exp(\lambda_E) \int_1^\infty \ln(z) \lambda_E \exp(-\lambda_E z) dz. \tag{3.35}$$

Using the integration by parts technique, I_2 will be

$$I_2 = \log_2 e \exp(\lambda_E) \int_1^\infty \frac{\exp(-\lambda_E z)}{z} dz = \log_2 e \exp(\lambda_E) E_1(\lambda_E). \tag{3.36}$$

where $E_1(\cdot)$ is the exponential integral function.

The average minimum guaranteed secrecy rate is now given by

$$\bar{R}_{sec,mg} = \left\{ \log_2(1 + \gamma_B) - \log_2 e \exp(\lambda_E) E_1(\lambda_E) \right\}^+ \cdot [(bits/s)/Hz]. \tag{3.37}$$

It is worth mentioning that the average minimum guaranteed secrecy rate performance of the CI precoder is given by replacing γ_B in (3.38) by (3.10). Likewise, $\bar{R}_{sec,mg}$ of the EBF precoder is calculated using (3.27) instead of γ_B .

3.2.3 Probability of Non-Zero Minimum Guaranteed Secrecy Rate

In this subsection, we examine the condition for the existence of non-zero minimum guaranteed secrecy rate. According to (3.30), the probability of non-zero minimum guaranteed secrecy rate is formulated as

$$\begin{aligned} \Pr(R_{sec,mg} > 0) &= \Pr(\gamma_B > \gamma_E) \\ &= \int_0^\infty \int_0^x f_{\gamma_B}(x) f_{\gamma_E}(y) dx dy. \end{aligned} \quad (3.38)$$

By substituting (3.20) and (3.24) into (3.38) and solving the integral, we derive the probability of non-zero minimum guaranteed secrecy rate for the CI precoder as

$$\begin{aligned} \Pr(R_{sec,mg} > 0)_{CI} &= \\ &= 1 - \exp\left(-\frac{1-\beta}{\beta} \frac{N}{N-1} \gamma_{BCI}\right), \end{aligned} \quad (3.39)$$

Similar to the derivation of the probability of non-zero minimum guaranteed secrecy rate with the CI precoder, this metric with the EBF precoder has the format of

$$\begin{aligned} \Pr(R_{sec,mg} > 0)_{EBF} &= \\ &= 1 - \exp\left(-\frac{1-\beta}{\beta} \frac{N}{N-1} \gamma_{BEF}\right) \end{aligned} \quad (3.40)$$

Equation (3.39) shows that the thinning ratio (β), the total number of antennas (N) and the average received SNR at Bob affect the probability of non-zero minimum guaranteed secrecy rate. As β approaches to 1, our scheme becomes less

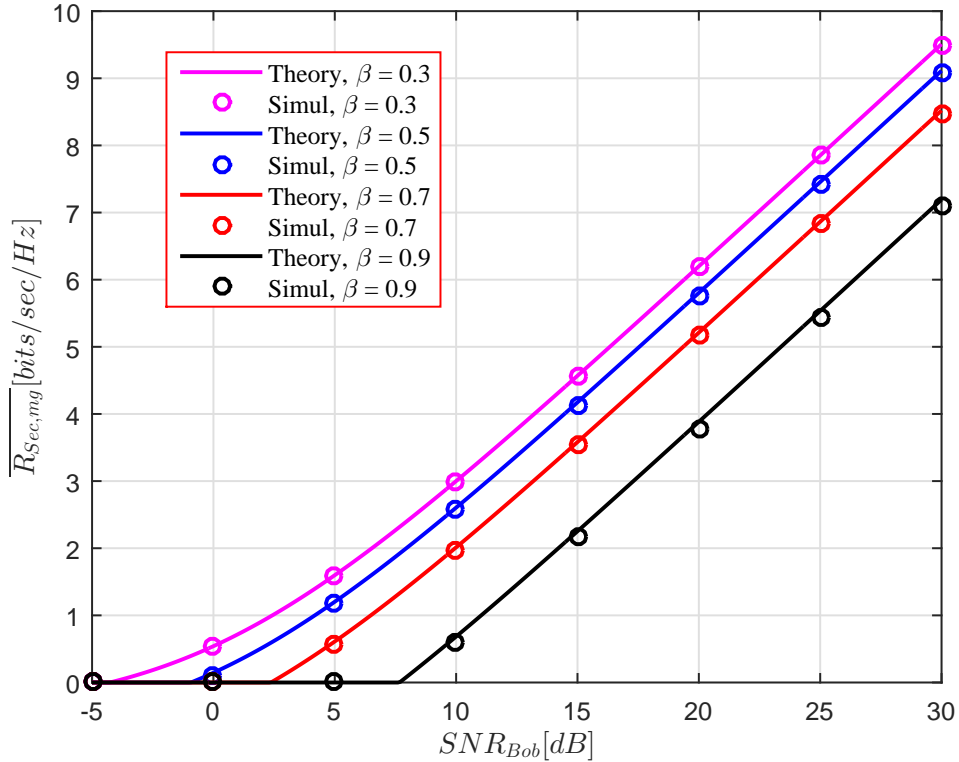


Fig. 3.4: Average Minimum Guaranteed secrecy rate versus received average SNR at Bob with the utilization of the CI precoder at Alice for different thinning ratio values.

secure. On the one hand, as β approaches to 0, this probability approaches to 1 and it guarantees secure transmission. On the other hand, with small values of β , i.e., small number of active antennas, M , the interference part of $\gamma_{B_{E_{BF}}}$ in (3.27) becomes stronger and thus the secrecy rate in contrast to the CI precoder secrecy rate performance, in high SNR regime tends to a finite value.

3.3 Numerical Results

In this section we examine the secrecy performance of the proposed precoding techniques with ASA. For the numerical results, we assume that the variance of the fading coefficients are unity. Finally, the verification of the analytical results is done using Monte Carlo simulations.

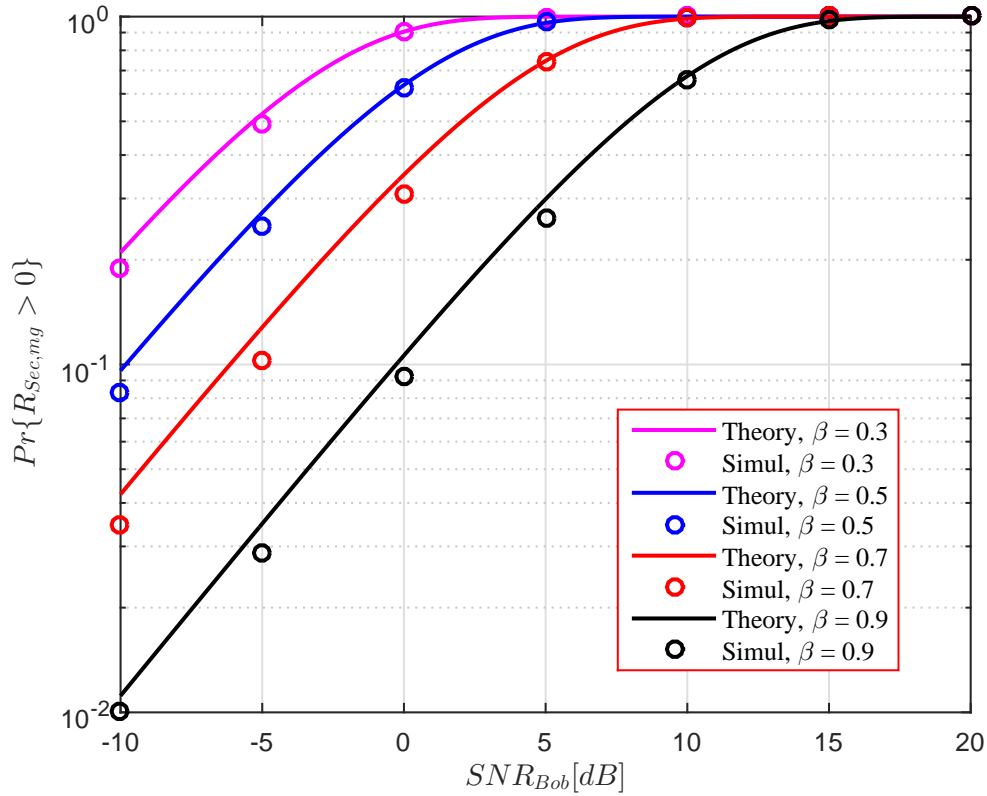


Fig. 3.5: The probability of non-zero secrecy rate versus average received SNR at Bob with the utilization of the CI precoder for different thinning ratio values.

Fig. 3.4 plots the average minimum guaranteed secrecy rate versus received average SNR at Bob when CI precoder is used. It is observed that for a fixed SNR value, with the decrease of β , the average minimum guaranteed secrecy rate increases. Furthermore, it is evident that with a fixed value for β , the minimum guaranteed secrecy rate increases with the average SNR. Moreover, when Bob is located relatively at far distance with respect to Alice, the higher values of β do not provide secure communications.

Fig. 3.5 shows the probability of non-zero minimum guaranteed secrecy rate versus average SNR with the CI precoder. It is shown that with a fixed value for β , $\Pr\{R_{sec,mg} > 0\}$ increases with the average SNR. In addition, for a fixed value of the average SNR, $\Pr\{R_{sec,mg} > 0\}$ increases as β decreases. Interestingly, a non-zero secrecy rate rate exists even for the thinning ratio values close to 1.

Fig. 3.6 illustrates the average minimum guaranteed secrecy rate versus the

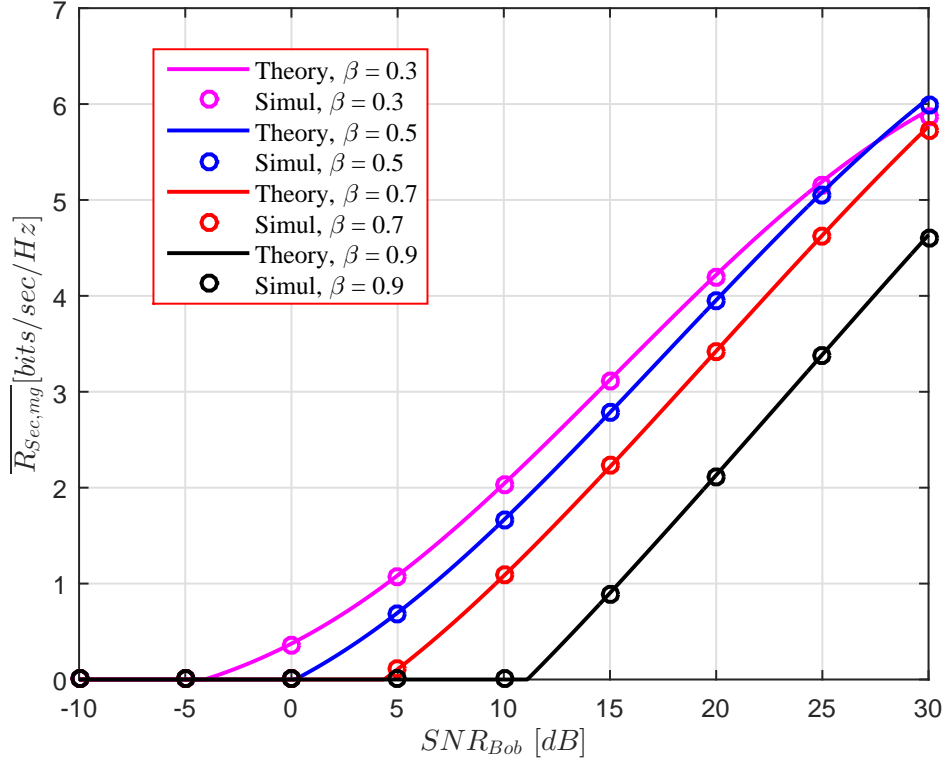


Fig. 3.6: Average Minimum Guaranteed secrecy rate versus received average SNR at Bob with the utilization of the EBF precoder at Alice for different thinning ratio values.

average SNR at Bob when the EBF precoder is used. Similar to the CI precoder case, for a fixed SNR value, the average minimum guaranteed secrecy rate increases as β decreases and with a fixed value for β , the minimum guaranteed secrecy rate increases with the average SNR. Moreover, when Bob is located relatively at far distances with respect to Alice, the higher values of thinning ratio do not provide any secure communications. The difference between the average minimum guaranteed secrecy rate performance with the EBF precoder to that of with the CI precoder is that for each thinning ratio, $R_{sec,mg}$ in high SNR regime, approaches a specified and finite value and thus, a compromise between β and the secrecy rate is observed.

Fig. 3.7 depicts $\bar{R}_{sec,mg}$ versus β . The figure examines the compromise between the choice of β and the minimum guaranteed secrecy rate performance. It is evident that $\bar{R}_{sec,mg}$ is a convex function in β and for a fixed average SNR, there exists a β that maximizes $\bar{R}_{sec,mg}$. Moreover, It is observed that for low average

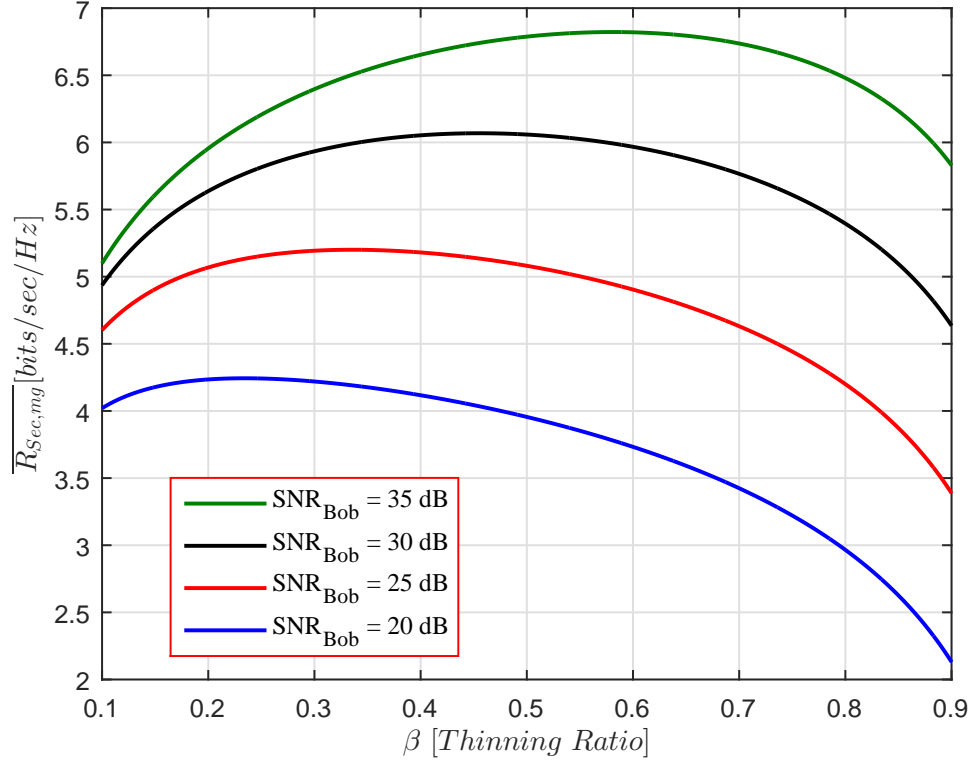


Fig. 3.7: The minimum Guaranteed secrecy rate versus β for different received average SNR at Bob with the EBF precoder.

SNR values, comparatively lower values of β maximizes the secrecy rate. As the average SNR increases, the value of β that maximizes the secrecy rate also increases.

Additionally, in Fig. 3.8, we evaluate the compromise between the selection of thinning ratio and average SNR. From the figure, when Bob is located relatively at far distance with respect to Alice, i.e, low SNR values, $\bar{R}_{sec,mg}$ is maximized with small values of thinning ratio. However, as the SNR increases, the thinning ratio that maximizes $\bar{R}_{sec,mg}$ increases.

Finally, Fig. 3.9 presents the non-zero minimum guaranteed secrecy rate versus the average SNR for different thinning ratio values and with the EBF precoder. Similar to the CI precoder performance, $\Pr\{R_{sec,mg} > 0\}$ is an ascending function in SNR when β is fixed. Furthermore, for a fixed SNR value, as β decreases, $\Pr\{R_{sec,mg} > 0\}$ increases. For the sake of comparison for this performance metric between EBF and CI precoders, we observe that for a fixed SNR and β

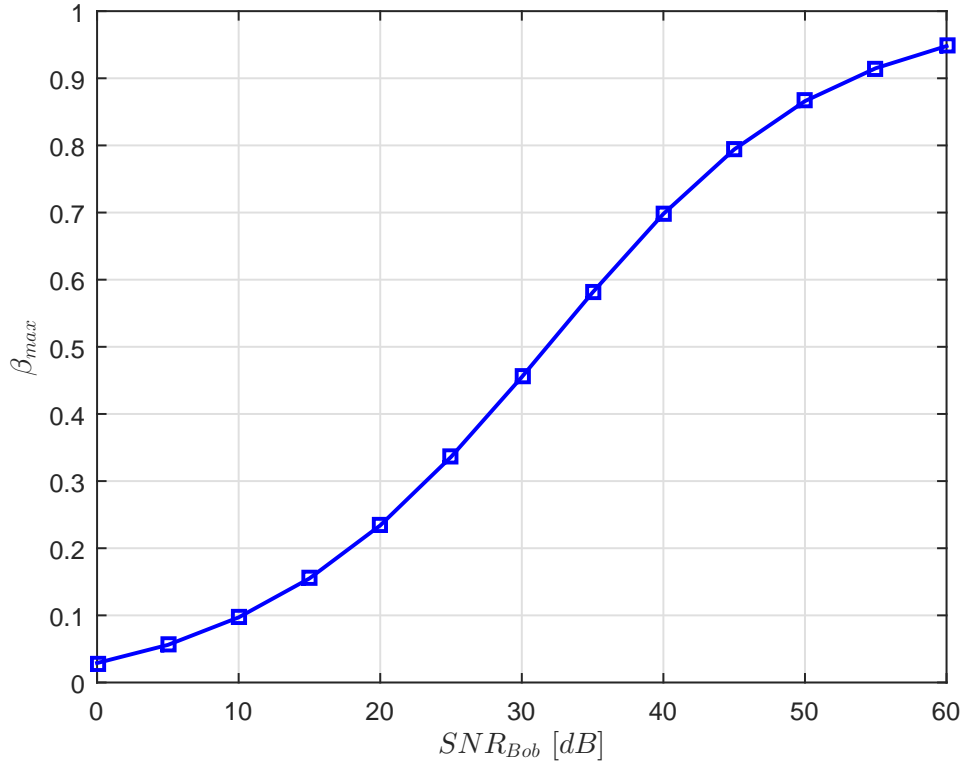


Fig. 3.8: The thinning ratio values that maximizes average minimum guaranteed secrecy rate versus received average SNR at Bob with the EBF precoder.

values, e.g., 0 dB and 0.5, $\Pr\{R_{sec,mg} > 0\}$ with CI precoder is 0.65 while with EBF it is 0.55. Therefore, the CI precoder outperforms the EBF precoder in terms of secrecy performance.

3.4 Conclusions and Future Research

In order to enhance physical layer security in MISO wiretap channels, in this chapter we investigated the achievability of a true location specific secure wireless transmission by exploiting antenna subset activation with channel-based precoding. For delivering secure as well as reliable communication to the legitimate receiver, two channel-based precoding schemes were introduced. The transmitted symbols are first precoded as a function of the wireless channel in a quasi-static

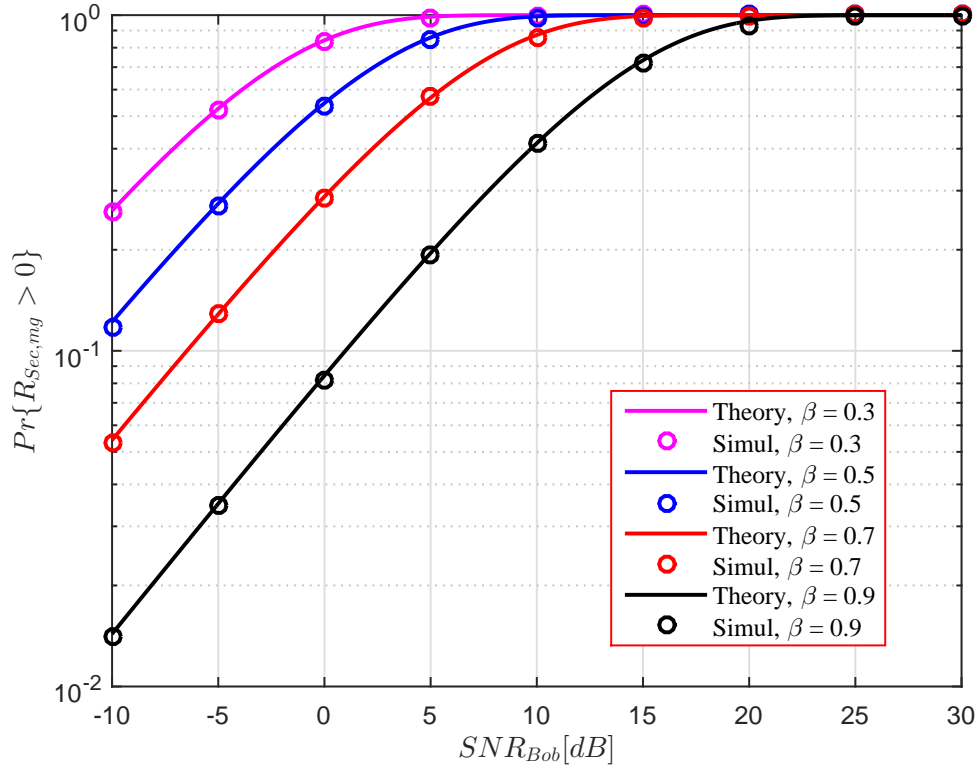


Fig. 3.9: The probability of non-zero secrecy rate versus average received SNR at Bob with the utilization of the EBF precoder for different thinning ratio values.

fading environment, and then a randomly selected subset of antennas becomes active for transmitting them. We evaluated the secrecy performance of our proposed schemes by deriving closed-form expressions of the minimum guaranteed secrecy rate as well as the probability of non-zero minimum guaranteed secrecy rate. Our results demonstrated that the thinning ratio plays a critical role in the secrecy performance of the proposed schemes. In particular, with the case of eigenbeamformer precoding, a trade-off between security and reliability of the legitimate link was observed. In addition, we showed that the channel inversion precoding outperforms eigenbeamformer precoding in terms of secrecy performance at the cost of unstable power loading across transmit antennas.

Chapter 4

Randomized Beamforming with Generalized Selection Transmission for Security Enhancement in MISO Wiretap Channels

Degrees of freedom in achieving secure communication remarkably increase in the presence of multiple antenna techniques [34]. In this context, a promising approach is to design a transmit beamformer (TBF) via direction selection and power allocation [35]. The goal is to enhance the strength of information signal and to impair the eavesdropped signal simultaneously by making use of spatial degrees of freedom. The secrecy performance of multiple antenna beamforming methods is mainly governed by the amount of channel state information (CSI) available at the transmitter. Under the assumption of perfect CSI availability of both main and wiretap channels at transmitter, authors in [36] showed that the secrecy capacity-achieving beamformer has a direction along the generalized eigenvector corresponding to the maximum generalized eigenvalues of the main and wiretap channel. In case that full main CSI and partial or none wiretap CSI

are available at the transmitter, the optimal beamformer is aligned with the main channel direction [37]. However, in this case, a secrecy outage is unavoidable. The secrecy outage probability of the latter case was investigated in [38] for block fading channels.

Although TBF can be seen as an optimal approach, there are two major problems associated with such transmission method. Firstly, the number of RF chains connected to each antennas and the amount of required signal processing is relatively high. Secondly, under the assumption of block fading, an intelligent eavesdropper equipped with multiple antennas as well as blind equalization techniques can detect the confidential data and violates the secure communications. The former problem has been partially addressed by adopting transmit antenna selection (TAS) scheme to reduce the cost and hardware complexity [39]. However, in [40], it is proved that TAS is not an optimal approach in terms of secrecy performance. The latter problem has been investigated by [41]. In this proposal, an approach called artificial fast fading (AFF) is used to randomize the received signal at eavesdroppers and prevent them from capturing any confidential data. However, the first problem of TBF scheme holds for AFF approach due to the transmission from all of the antennas.

Hence, in this chapter we study an effective signal processing technique to strike a balance between secrecy performance and items such as hardware complexity, power consumption, size, etc., in MISO wiretap channels. Particularly, we propose and analyze a generalized selection transmission scheme with randomized beamforming (RBF/GST) to address both of the problems of TBF simultaneously. With GST, instead of choosing all the available antennas for beamforming, we select only a subset of antennas for transmission. Thus, GST reduces the cost, hardware complexity, power consumption and amount of signal processing to a reasonable level. Besides, RBF provides robust secure transmission against intelligent eavesdroppers. Assuming a passive eavesdropping scenario, we first derive closed-form expressions for the exact and asymptotic secrecy outage probabilities with GST over Rayleigh fading channels. Our asymptotic results reveal that GST achieves the same secrecy outage diversity gain as TBF in MISO wiretap channels. We then derive the ergodic secrecy rate of GST and RBF/GST under the assumption of active eavesdropping. These results indicate that RBF/GST

outperforms GST in terms of ergodic secrecy rate performance and RBF/GST can significantly enhance the security of the MISO wiretap channel. Finally, we show that by reducing the number of antennas for transmission to a certain level, the secrecy performance of the proposed methods is not considerably affected.

4.1 Algorithm Description

4.1.1 System Model

We consider a MISO wiretap channel where the transmitter (Alice) is a multiple antenna transmitter equipped with N antennas, while the legitimate receiver (Bob) and an eavesdropper (Eve) are assumed to be single antenna receivers. Moreover, we focus on quasi-static fading channels in which the main and wiretap channels are both i.i.d block Rayleigh fading channels.

4.1.2 Generalized Selection Transmission (GST)

This subsection describes the signal model of the GST scheme. Here, we consider that Bob feedbacks the CSI of the main channel to Alice. With the availability of CSI of the main channel, Alice selects Q ($1 \leq Q \leq N$) transmit antennas among N antennas that maximize the output SNR at Bob. Based on this selection scheme, Alice first ranks the transmit antennas in terms of their instantaneous fading gain in an ascending format. Denote the channel coefficient from Alice k th transmit antenna to the receive antenna of Bob as h_k , where $1 \leq k \leq N$. Let $|h_1|^2 \leq |h_2|^2 \leq \dots \leq |h_N|^2$ be the order statistics from arranging $\{|h_k|^2\}_{k=1}^N$ in ascending order of magnitude. Then Alice selects the last Q variable(s) in the order statistics. We denote \mathcal{A} as a set that contains the indexes of the chosen antennas. Finally, Alice beamforms the confidential data using the vector $\mathbf{w}(i) = \mathbf{h}_Q / \|\mathbf{h}_Q\|$, where $\mathbf{h}_Q = [h_1, h_2, \dots, h_Q]^T$ denotes the main channel vector between Q selected transmit antennas at Alice and the receive antenna at Bob

and $\|\cdot\|$ indicates the Euclidean norm.

In order to transmit confidential message \mathbf{s} , Alice encodes it into a codeword $\mathbf{x} = [x(1), \dots, x(i), \dots, x(m)]$, where m is the length of \mathbf{x} . The transmitted codeword is constrained with an average power of P , i.e., $\frac{1}{m} \sum_{i=1}^m \mathbb{E} \left[|x(i)|^2 \right] \leq P$, where $\mathbb{E}\{\cdot\}$ is the expectation operator. In the main channel, the received signal at Bob at time i is given by

$$y_M(i) = \mathbf{h}_Q^H \mathbf{w}(i) x(i) + n_M(i) = \|\mathbf{h}_Q\| x(i) + n_M(i), \quad (4.1)$$

where $n_M(i)$ denotes the additive white Gaussian noise (AWGN) component with zero mean and variance σ_M^2 . In the wiretap channel, the received signal at Eve at time i can be written as

$$y_W(i) = \mathbf{g}_Q^H \mathbf{w}(i) x(i) + n_W(i), \quad (4.2)$$

where $\mathbf{g}_Q = [g_1, g_2, \dots, g_Q]^T$ is the eavesdropper's channel vector between Q selected transmit antennas at Alice and the receive antenna at Eve, and $n_W(i)$ is the AWGN term at Eve with variance σ_W^2 .

Since the selected antennas at Alice are independent of \mathbf{g}_Q , the Q strongest transmit antennas for Bob corresponds to a random transmit antennas for Eve.

4.1.3 Randomized Beamforming with Generalized Selection Transmission (RBF/GST)

As mentioned, when the main and wiretap channels are block fading, Eve can exploit some advanced blind channel estimation techniques to attain the effective CSI (the product of beamforming vector and the wiretap channel coefficients) and coherently detect the confidential signals. Hence, to enhance the security of GST, we adopt a randomized beamforming transmission technique such as those in [41] to corrupt the received signal of the eavesdropper by a time varying multiplicative noise. The basic idea is to make $\mathbf{h}_Q^H \mathbf{w}(i)$ deterministic but $\mathbf{g}_Q^H \mathbf{w}(i)$ changing randomly in each symbol interval. As such, Eve experiences an equivalent fast

fading channel which prevents the blind channel estimation.

As for designing time varying weighting coefficients, Alice selects the beamforming vector $\mathbf{w}(i) = [w_1(i), w_2(i), \dots, w_Q(i)]^T$, where the first $Q - 1$ elements of vector $\mathbf{w}(i)$ are randomly generated while the last element of the vector is determined using the constraint $\mathbf{h}_Q^H \mathbf{w}(i) = \|\mathbf{h}_Q\|$. We assume that $w_k(i)$, $k = 1, \dots, Q - 1$ are i.i.d complex Gaussian distributed random variables with zero mean and variance σ_0^2 and the last element is given by

$$w_Q(i) = \frac{\|\mathbf{h}_Q\| - \sum_{k \in \mathcal{A}, k=1}^{Q-1} h_k^* w_k(i)}{h_Q^*}. \quad (4.3)$$

With RBF/GST, the received signal at Bob is still (4.1). We note that [41] considers $\mathbf{h}_Q^H \mathbf{w}(i) = 1$ as a constraint for determining the last element in weighting vector. This makes the effective channel between Alice and Bob (effective main channel) to be an AWGN channel. Thus, the received signal does not benefit from the diversity gain offered by the multiple antenna array transmission. However, by assuming (4.1) as the signal model, the received SNR at Bob is maximized and so is the rate of the effective main channel.

The received signal at Eve can be written as

$$y_E^{RBF}(i) = \mathbf{g}_Q^H \mathbf{w}(i)x(i) + n_W(i) = g_E(i)x(i) + n_W(i), \quad (4.4)$$

where $g_E(i) \triangleq \mathbf{g}_Q^H \mathbf{w}(i)$ is the effective channel between Alice and Eve (effective wiretap channel). According to the results presented in [41], the effective wiretap channel $g_E(i)$ is a SISO fast fading channel that can vary as fast as the symbol rate. Thus, $g_E(i)$ is a complex Gaussian random variable satisfying

$$g_E(i) \sim \mathcal{CN}\left(\mu_E, \sigma_E^2\right), \quad (4.5)$$

where $\mu_E = \frac{g_Q^*}{h_Q^*} \|\mathbf{h}_Q\|$ and $\sigma_E^2 = \sum_{k \in \mathcal{A}, k=1}^{Q-1} \left|g_k^* - \frac{g_Q^* h_k^*}{h_Q^*}\right|^2 \sigma_0^2$ are the mean and the variance of $g_E(i)$. Equation (4.5) suggests that over each fading block of the original channels \mathbf{h}_Q and \mathbf{g}_Q , the effective wiretap channel is a Ricean fast fading channel. The introduced fast fading considerably degrades the channel estimation

performance of Eve and prevents her from detecting confidential data coherently.

Finally, since \mathbf{h}_Q is a block fading channel, due to the inversion behavior of the RBF/GST weighting vector as indicated in (4.3), the average transmit power of Alice can be extremely large. To resolve this issue, Alice chooses $|h_Q| = \max\{|h_k|\}_{k=1}^N$, i.e., choose the antenna with the largest fading gain as h_Q in (4.3).

4.2 Secrecy Performance

This section fully characterizes the secrecy performance of RBF/GST. We first quantify the exact and asymptotic secrecy performances achieved by GST by deriving the exact and asymptotic secrecy outage probabilities in closed-forms. Then we delve into the ergodic secrecy rate analysis of RBF/GST.

4.2.1 Secrecy Performance of GST

In this subsection, we consider that the CSI of the wiretap channel is not available to either Alice or Bob. In such a scenario, we adopt the secrecy outage probability as the main performance measure to evaluate the secrecy performance of GST. Therefore, before deriving the secrecy outage probability, we first present the statistics of the instantaneous received signal to noise ratio (SNR) at Bob and Eve.

The instantaneous received SNR at Bob with GST is $\gamma_M = \bar{\gamma}_M \|\mathbf{h}_Q^H \mathbf{w}(i)\|^2 = \bar{\gamma}_M \|\mathbf{h}_Q\|^2$, with $\bar{\gamma}_M = P/\sigma_M^2$. Likewise, the instantaneous received SNR at Eve is $\gamma_W = \bar{\gamma}_W \|\mathbf{g}_Q^H \mathbf{w}(i)\|^2$, where $\bar{\gamma}_W = P/\sigma_W^2$. The cumulative distribution function (CDF) of γ_M can be derived as [42]

$$F_{\gamma_M}(z) = \epsilon_0 + \sum_{k=1}^Q \epsilon_k \frac{z^{(k-1)} e^{-\frac{z}{\bar{\gamma}_M}}}{\Gamma(k)} + \sum_{k=Q+1}^N \epsilon_k e^{-\frac{kz}{\bar{\gamma}_M}}, \quad (4.6)$$

where $\Gamma(\cdot)$ stands for the Gamma function and ϵ_k is

$$\epsilon_k = \begin{cases} 1 & k = 0 \\ \bar{\gamma}_M^{1-k} \left[-1 + \sum_{\ell=Q+1}^N (-1)^{\ell-k} \right. \\ \quad \left. \times \frac{\binom{N}{N-\ell} \binom{\ell-1}{\ell-Q-1}}{\left(\frac{\ell}{Q} - 1\right)^{Q-k+1}} \right] & 1 \leq k < Q \\ -\bar{\gamma}_M^{1-Q} \binom{N}{N-Q} & k = Q \\ \frac{(-1)^k \binom{N}{N-Q} \binom{k-1}{k-Q-1}}{\left(\frac{k}{Q} - 1\right)^Q} & Q < k \leq N. \end{cases} \quad (4.7)$$

It can be proved that γ_W is exponentially distributed due to the fact that the beamforming vector at Alice is independent from eavesdropper's channel [38], yielding

$$F_{\gamma_W}(z) = 1 - e^{-\frac{z}{\bar{\gamma}_W}}. \quad (4.8)$$

The instantaneous secrecy rate of GST is given by $R_{Sec} = [R_M - R_W]^+$, where $[x]^+$ denotes $\max\{0, x\}$, $R_M = \log_2(1 + \gamma_M)$ is the instantaneous rate of the main channel and $R_W = \log_2(1 + \gamma_W)$ stands for the instantaneous rate of the wiretap channel.

The secrecy outage probability of GST is given by

$$\begin{aligned} P_{out}(R_S) &= \Pr\{R_{Sec} < R_S\} \\ &= \int_0^\infty F_{\gamma_M} \left[2^{R_S} (1+z) - 1 \right] f_{\gamma_W}(z) dz, \end{aligned} \quad (4.9)$$

where $R_S > 0$ is a predefined secrecy rate and $f_{\gamma_W}(\cdot)$ denote the probability density function (pdf) of γ_W and it is obtained by taking the first derivative of F_{γ_W} in (4.8). Substituting this pdf and (4.6) into (4.9) and solving the integral, the exact secrecy outage probability of GST is derived in closed-form as

$$P_{out}(R_S) = 1 + \theta_1 + \theta_2, \quad (4.10)$$

where θ_1 and θ_2 are defined as

$$\theta_1 = \sum_{k=1}^Q \frac{\epsilon_k}{\bar{\gamma}_W \Gamma(k)} \sum_{j=0}^{k-1} \frac{\xi \Gamma(j+1)}{\left(\frac{1}{\bar{\gamma}_W} + \frac{2^{R_S}}{\bar{\gamma}_M}\right)^{(j+1)}}, \quad (4.11)$$

$$\theta_2 = \sum_{k=Q+1}^N \epsilon_k \frac{e^{-\frac{(2^{R_S}-1)k}{Q\bar{\gamma}_M}}}{\bar{\gamma}_W} \left(\frac{1}{\bar{\gamma}_W} + \frac{2^{R_S}k}{Q\bar{\gamma}_M}\right)^{-1}. \quad (4.12)$$

In (4.11), we define ξ as

$$\xi = \binom{k-1}{j} \left(2^{R_S} - 1\right)^{k-1} e^{-\frac{(2^{R_S}-1)k}{Q\bar{\gamma}_M}} \left(\frac{2^{R_S}}{2^{R_S}-1}\right)^j. \quad (4.13)$$

Notice that, when $N = Q$, (4.10) reduces to

$$P_{out}(R_S) = 1 - \sum_{k=1}^N \sum_{j=0}^{k-1} \frac{\xi \Gamma(j+1)}{\bar{\gamma}_M^{(k-1)} \bar{\gamma}_W \Gamma(k) \left(\frac{1}{\bar{\gamma}_W} + \frac{2^{R_S}}{\bar{\gamma}_M}\right)^{(j+1)}}, \quad (4.14)$$

which is the same result as that in [40, eq. (12)].

Since in the high SNR regime of the main channel (i.e., $\gamma_B \rightarrow \infty$), the secrecy outage diversity gain and the secrecy outage SNR gain govern the secrecy outage probability, we derive an asymptotic secrecy outage expression. To do so, we proceed by deriving the first order expansion of $F_{\gamma_M}(z)$ in (4.6). This can be derived as $F_{\gamma_M}(z) \approx 1 / \left(Q^{(N-Q)} Q!\right) (z/\bar{\gamma}_M)^N$. Accordingly, we find the asymptotic secrecy outage probability as

$$P_{out}^\infty(R_S) = \left(\Delta \bar{\gamma}_M\right)^{-G_D}, \quad (4.15)$$

where $G_D = N$ is the secrecy outage diversity gain and Δ is the secrecy outage SNR gain. In (4.15), Δ is given by

$$\Delta = \left[\sum_{u=0}^N \binom{N}{u} \frac{2^{uR_S} (2^{R_S}-1)^{N-u} u! \bar{\gamma}_W^u}{Q^{(N-Q)} Q!} \right]^{-\frac{1}{N}} \quad (4.16)$$

According to (4.15), the following points present various advantages of exploiting

GST in the main channel: (I) With the approach of $\bar{\gamma}_M$ to infinity, the secrecy outage probability tends to zero. (II) The maximum secrecy outage diversity gain of N is achieved and thus GST has the same secrecy outage diversity gain as TBF. (III) The secrecy outage diversity gain is not affected by the choice of Q . The impact of Q is only reflected in the secrecy outage SNR gain.

4.2.2 Secrecy Performance of RBF/GST

This subsection focuses on the active eavesdropping scenario, where the CSI of the wiretap channel is also available to Alice. Under such assumption, the ergodic secrecy rate quantifies the secrecy performance of RBF/GST.

Denote \bar{R}_{Sec}^{RBF} as the ergodic secrecy rate of RBF/GST. According to the definition of secrecy rate, we can write \bar{R}_{Sec}^{RBF} as

$$\bar{R}_{Sec}^{RBF} = \left\{ I(y_B; x) - I(y_E; x) \right\}^+. \quad (4.17)$$

where $I(y_B^{RBF}; x)$ and $I(y_E^{RBF}; x)$ represent the average mutual information of the main channel and wiretap channel, respectively. Based on (4.1), $I(y_B^{RBF}; x)$ can be written as

$$\begin{aligned} I(y_B^{RBF}; x) &= \mathbb{E} \left\{ \log_2 (1 + \gamma_M) \right\} \\ &= \frac{1}{\ln 2} \int_0^\infty \ln(1 + \gamma_M) f(\gamma_M) d\gamma_M, \end{aligned} \quad (4.18)$$

where $f(\gamma_M)$ is the pdf of γ_M and is derived by taking the first derivative of (4.6). Substituting this pdf into (4.18) and solving the integral, we calculate the ergodic rate of the main channel as

$$\begin{aligned} I(y_B^{RBF}; x) &= \frac{1}{\ln 2} \left\{ - \sum_{k=1}^Q \epsilon_k \bar{\gamma}_M^{(k-1)} e^{\frac{1}{\bar{\gamma}_M}} E_k \left(\frac{1}{\bar{\gamma}_M} \right) \right. \\ &\quad \left. - \sum_{k=Q+1}^N \epsilon_k e^{\frac{k}{Q\bar{\gamma}_M}} E_1 \left(\frac{k}{Q\bar{\gamma}_M} \right) \right\}, \end{aligned} \quad (4.19)$$

where $E_k(\cdot)$ is the generalized exponential integral function. On the other hand, the average mutual information of the wiretap channel is

$$I(y_E^{RBF}; x) = \mathbb{E}_{\mathbf{h}_Q, \mathbf{g}_Q} \left\{ h(y_E^{RBF}) - h(y_E^{RBF} | x) \right\}, \quad (4.20)$$

where $h(\cdot)$ is the differential entropy. Based on [41, eq. (28,30)], when x is Gaussian distributed ($x \sim \mathcal{CN}(0, P)$), $h(y_E^{RBF})$ and $h(y_E^{RBF} | x)$ are found respectively as

$$h(y_E^{RBF}) = -2\pi \int_0^\infty \log_2 P_y(\alpha_y) P_y(\alpha_y) \alpha_y d\alpha_y, \quad (4.21)$$

$$h(y_E^{RBF} | x) = \log_2(\pi e \sigma_W^2) + \frac{1}{\ln 2} e^{\frac{1}{\beta}} E_1\left(\frac{1}{\beta}\right), \quad (4.22)$$

where $\beta = \sigma_E^2 \bar{\gamma}_W$, $\alpha_y = |y_E^{RBF}|$ and $P_y(y)$ is

$$P_y(y) = \int_0^\infty \frac{2\alpha}{\pi \sigma_W^2 \sigma_E^2 (\alpha^2 \bar{\gamma}_W + 1)} I_0\left(\frac{2\alpha \alpha_\mu}{\sigma_E^2}\right) \times \exp\left(-\frac{|y|^2}{(\alpha^2 \bar{\gamma}_W + 1) \sigma_W^2} - \frac{\alpha^2 + \alpha_\mu^2}{\sigma_E^2}\right) d\alpha, \quad (4.23)$$

where $I_0(\cdot)$ is the zero order modified Bessel function of the first kind, $\alpha = |g_E|$ and $\alpha_\mu = |\mu_E|$. Finally, secrecy rate of RBF/GST is given by subtracting (4.20) from (4.19).

For the sake of secrecy performance comparison between GST and RBF/GST, we also derive the closed-form expression for the ergodic secrecy rate of GST. In doing so, we replace the pdf of γ_M with that of γ_W in (4.18) and by solving the integral, we derive the rate of the wiretap channel as

$$\bar{R}_W = \frac{1}{\ln 2} e^{\frac{1}{\bar{\gamma}_W}} E_1\left(\frac{1}{\bar{\gamma}_W}\right). \quad (4.24)$$

where \bar{R}_W is the ergodic rate of the wiretap channel when GST is used at Alice. The ergodic secrecy rate of GST is given by subtracting (4.24) from (4.19).

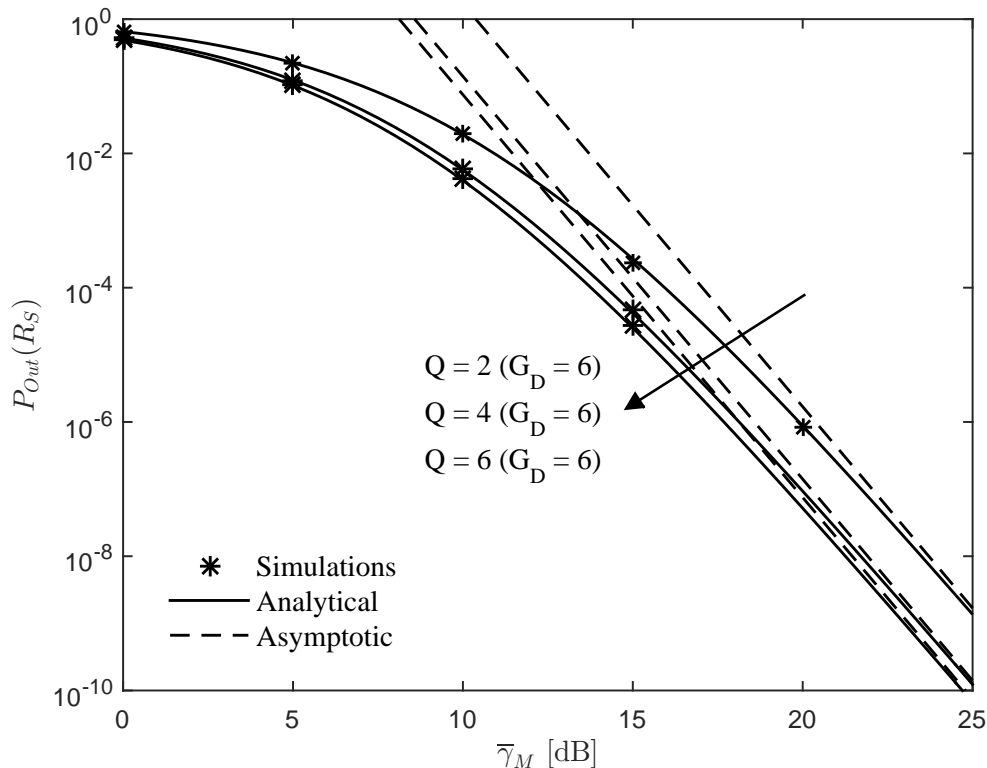


Fig. 4.1: The exact and asymptotic secrecy outage probabilities of GST versus $\bar{\gamma}_M$ for $\bar{\gamma}_W = 5$ dB and $R_S = 1$.

4.3 Numerical Results

In this section, we present the numerical results to evaluate the secrecy performances of both GST and RBF/GST schemes.

Fig. 4.1 plots the exact and asymptotic secrecy outage probabilities of GST versus $\bar{\gamma}_M$ for $\bar{\gamma}_W = 5$ dB and $R_S = 1$. From the figure we can see that the asymptotic secrecy outage probability obtained from (4.15) accurately predicts the secrecy outage diversity and SNR gains. We also observe that the exact secrecy outage probability given in (4.10) are in precise agreement with the Monte Carlo simulations marked with ‘*’. Furthermore, we note that GST achieves full diversity (i.e., $G_D = 6$) regardless of Q . More importantly, we see that the increase of Q implies in a better secrecy outage performance. Nevertheless, the figure shows that when $\bar{\gamma}_M < \bar{\gamma}_W$, the secrecy performance of GST is violated.

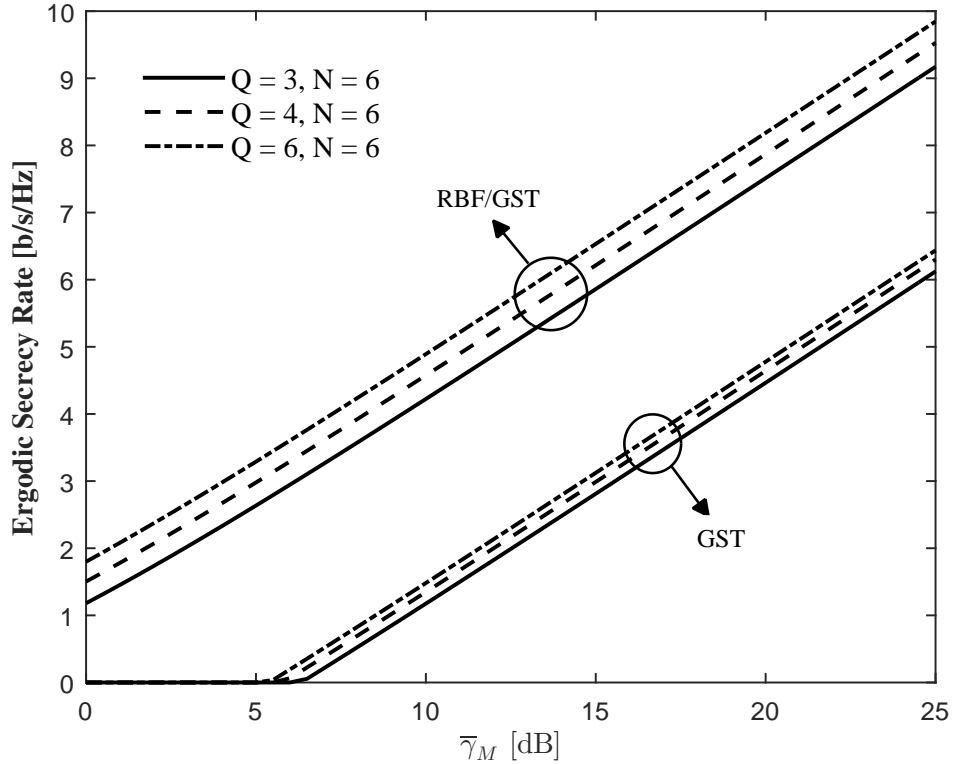


Fig. 4.2: Comparison of the ergodic secrecy rate between RBF/GST and CBF/GST versus $\bar{\gamma}_M$ for $\bar{\gamma}_W = 15$ dB.

Fig. 4.2 compares the ergodic secrecy rate of RBF/GST with that of GST versus $\bar{\gamma}_M$ for different Q . We first observe that RBF/GST outperforms GST in terms of ergodic secrecy rate performance. We also note that ergodic secrecy rate increases with increasing Q . We observe that the difference between the ergodic secrecy rate with $Q = N = 6$ and $Q = 4, N = 6$ is not considerable. Thus, by decreasing Q to a certain number, which in turn reduces the amount of signal processing, hardware complexity and cost, the ergodic secrecy rate is not considerably degraded.

4.4 Conclusions

We proposed RBF/GST to resolve the disadvantages of TBF in block fading channel. We examined the secrecy performance of RBF/GST via our closed-form expressions for the ergodic secrecy rate and the secrecy outage probability. Our results indicated that GST achieves the same maximum secrecy outage diversity gain as TBF. Furthermore, we demonstrated that RBF/GST can significantly enhance the secrecy performance of MISO wiretap channel with a reasonable cost and hardware complexity.

Chapter 5

Concluding Remarks

5.1 Summary

In this dissertation, we investigated the design of practical signal processing schemes to improve the secrecy performances of OFDM and MIMO systems in wireless networks. In particular, the core of this dissertation was based on the analysis of signal-processing enabled physical layer security.

In chapter 2, we proposed pilot manipulation in OFDM systems as a secure pilot-based channel estimation technique to discriminate between channel estimation performances of Bob and Eve. According to the obtained simulation results within the chapter, we concluded that this algorithm reduces the reception performance at the eavesdropper to a level, in which pilot based channel estimation is useless.

In chapter 3, we considered MISO systems and proposed precoding-enabled antenna subset activation as an effective signal processing scheme to enhance physical layer security in fading channels. This algorithm delivered secure as well as reliable communications by enhancing the received signal power at legitimate receiver and impaired the received signal quality at eavesdropper simultaneously. According to the closed-form expressions derived throughout this chapter, we summarized that the type of channel-based precoding and the ratio between the

active and total transmit antennas were the key parameters for designing such secure transmission scheme.

Finally, in chapter 4, we showed that in spite of its effectiveness in transmission performance, TBF was highly vulnerable to advanced eavesdropping attacks in block fading channels. Therefore, the chapter proposed RBF/GST with the objective of robust secure communications in MISO wiretap channels. It was demonstrated that RBF/GST requires less hardware complexity, cost, size and signal processing compared to TBF and it is more effective than TBF from secrecy performance viewpoint.

5.2 Future Research

The work presented in this thesis can be extended in different ways. First, designing more intelligent secure pilot-based channel estimation techniques that are robust to channel estimation errors would be of interest. Second, analyzing ASA under the assumptions such as the availability of imperfect CSI at transmitter, presence of correlation between transmit antennas and advanced multiple antenna eavesdroppers is also of interest. Finally, one could investigate the effects of imperfect CSI and presence of multiple antenna eavesdropper on secrecy performance of RBF/GST.

Bibliography

- [1] W. Stallings, *Cryptography and Network Security: Principles and Practices*. Pearson Education, 3rd ed., 2002.
- [2] X. Chen, D. W. K. Ng, W. Gerstacker, and H. H. Chen, “A Survey on Multiple-Antenna Techniques for Physical Layer Security,” *IEEE Communications Surveys Tutorials*, vol. PP, no. 99, pp. 1–1, Nov. 2016.
- [3] C. E. Shannon, “Communication Theory of Secrecy Systems,” *Bell Systems Technical Journal*, vol. 28, no. 4, pp. 656–715, 1949.
- [4] A. D. Wyner, “The Wire-tap Channel,” *Bell Systems Technical Journal*, vol. 54, no. 8, pp. 1355–1387, Jan. 1975.
- [5] I. Csiszár and J. Körner, “Broadcast Channels with Confidential Messages,” *IEEE Transactions on Information Theory*, vol. 24, no. 3, pp. 339–348, May 1978.
- [6] S. Leung-Yan-Cheong and M. Hellman, “The Gaussian Wire-tap channel,” *IEEE Transactions on Information Theory*, vol. 24, no. 4, pp. 451–456, Jul. 1978.
- [7] A. Khisti and G. W. Wornell, “Secure Transmission With Multiple Antennas Part II: The MIMOME Wiretap Channel,” *IEEE Transactions on Information Theory*, vol. 56, no. 11, pp. 5515–5532, Nov. 2010.
- [8] L. Lai and H. E. Gamal, “The Relay-Eavesdropper Channel: Cooperation for Secrecy,” *IEEE Transactions on Information Theory*, vol. 54, no. 9, pp. 4005–4019, Sept. 2008.

- [9] L. N. R. Zurita, *Optimising Multiple Antenna Techniques for Physical Layer Security*. PhD thesis, University of Leeds, 2014.
- [10] W. Saad, X. Zhou, Z. Han, and H. V. Poor, “On the Physical Layer Security of Backscatter Wireless Systems,” *IEEE Transactions on Wireless Communications*, vol. 13, no. 6, pp. 3442–3451, Jun. 2014.
- [11] A. Mukherjee, S. Fakoorian, J. Huang, and A. Swindlehurst, “Principles of Physical Layer Security in Multiuser Wireless Networks: A Survey,” *Communications Surveys Tutorials, IEEE*, vol. 16, no. 3, pp. 1550–1573, Mar. 2014.
- [12] H. Koorapaty, A. Hassan, and S. Chennakeshu, “Secure Information Transmission for Mobile Radio,” in *IEEE International Symposium on Information Theory (ISIT)*, pp. 381–385, Aug. 1998.
- [13] C. Ye, S. Mathur, A. Reznik, Y. Shah, W. Trappe, and N. B. Mandayam, “Information-Theoretically Secret Key Generation for Fading Wireless Channels,” *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 2, pp. 240–254, Jun. 2010.
- [14] C. Ye, A. Reznik, G. Sternberg, and Y. Shah, “On the Secrecy Capabilities of ITU Channels,” in *IEEE 66th Vehicular Technology Conference, VTC-Fall*, pp. 2030–2034, Sept. 2007.
- [15] H. Li, X. Wang, and Y. Zou, “Dynamic Subcarrier Coordinate Interleaving for Eavesdropping Prevention in OFDM Systems,” *IEEE Communication Letters.*, vol. 18, no. 6, pp. 1059–1062, 2014.
- [16] H. Li, X. Wang, and J. Chouinard, “Eavesdropping-Resilient OFDM System Using Sorted Subcarrier Interleaving,” *IEEE Transactions on Wireless Communications*, vol. 14, no. 2, pp. 1155–1165, 2015.
- [17] S. Goel and R. Negi, “Guaranteeing Secrecy using Artificial Noise,” *IEEE Transactions on Wireless Communications*, vol. 7, no. 6, pp. 2180–2189, 2008.

- [18] X. Zhou and M. McKay, "Secure Transmission With Artificial Noise Over Fading Channels: Achievable Rate and Optimal Power Allocation," *IEEE Transactions on Vehicular Technology*, vol. 59, no. 8, pp. 3831–3842, 2010.
- [19] H. Qin, Y. Sun, T.-H. Chang, X. Chen, C.-Y. Chi, M. Zhao, and J. Wang, "Power Allocation and Time-Domain Artificial Noise Design for Wiretap OFDM with Discrete Inputs," *IEEE Transactions on Wireless Communications*, vol. 12, no. 6, pp. 2717–2729, Jun. 2013.
- [20] C.-W. Huang, T.-H. Chang, X. Zhou, and Y.-W. Hong, "Two-Way Training for Discriminatory Channel Estimation in Wireless MIMO Systems," *IEEE Transactions on Signal Processing*, vol. 61, no. 10, pp. 2724–2738, May 2013.
- [21] J. Ran and L. Li, "An Adaptive Method Utilizing Channel Reciprocity in TDD-LTE System," in *IET International Conference on Communication Technology and Application (ICCTA)*, pp. 896–900, Oct. 2011.
- [22] J. Barros and M. R. D. Rodrigues, "Secrecy Capacity of Wireless Channels," *2006 IEEE International Symposium on Information Theory (ISIT)*, pp. 356–360, July. 2006.
- [23] Y. O. Basciftci, O. Gungor, C. E. Koksal, and F. Ozguner, "On the Secrecy Capacity of Block Fading Channels with a Hybrid Adversary," *IEEE Transactions on Information Theory*, vol. 61, no. 3, pp. 1325–1343, Mar. 2015.
- [24] Y. Hwang and H. Papadopoulos, "Physical-layer secrecy in awgn via a class of chaotic ds/ss systems: Analysis and design," *IEEE Transactions on Signal Processing*, vol. 52, no. 9, pp. 2637–2649, Sept. 2004.
- [25] M. J. Mihaljevic and J. D. Golic, "Convergence of a Bayesian Iterative Error-Correction Procedure on a Noisy Shift register Sequence.," in *EUROCRYPT*, vol. 658, pp. 124–137, Springer, 1992.
- [26] A. Hero, "Secure Space-Time Communication," *IEEE Transactions on Information Theory*, vol. 49, no. 12, pp. 3235–3249, Dec. 2003.

- [27] Y. Inouye, “Criteria for Blind Deconvolution of Multichannel Linear Time-Invariant Systems,” *IEEE Transactions on Signal Processing*, vol. 46, no. 12, pp. 3432–3436, Dec. 1998.
- [28] M. Daly and J. Bernhard, “Directional Modulation Technique for Phased Arrays,” *IEEE Transactions on Antennas and Propagation*, vol. 57, no. 9, pp. 2633–2640, Sept. 2009.
- [29] M. Daly and J. Bernhard, “Beamsteering in pattern reconfigurable arrays using directional modulation,” *IEEE Transactions on Antennas and Propagation*, vol. 58, no. 7, pp. 2259–2265, Jul. 2010.
- [30] N. Valliappan, A. Lozano, and R. Heath, “Antenna subset modulation for secure millimeter-wave wireless communication,” *IEEE Transactions on Communications*, vol. 61, no. 8, pp. 3231–3245, Aug. 2013.
- [31] C. Windpassinger, R. F. H. Fischer, T. Vencel, and J. B. Huber, “Precoding in Multiantenna and Multiuser Communications,” *IEEE Transactions on Wireless Communications*, vol. 3, no. 4, pp. 1305–1316, Jul. 2004.
- [32] R. L.-U. Choi, K. B. Letaief, and R. D. Murch, “MISO CDMA Transmission with Simplified Receiver for Wireless Communication Handsets,” *IEEE Transactions on Communications*, vol. 49, no. 5, pp. 888–898, May 2001.
- [33] X. Huang, J. A. Zhang, and Y. J. Guo, “Out-of-Band Emission Reduction and a Unified Framework for Precoded OFDM,” *IEEE Communications Magazine*, vol. 53, no. 6, pp. 151–159, Jun. 2015.
- [34] T. Liu and S. Shamai, “A Note on the Secrecy Capacity of the Multiple-Antenna Wiretap Channel,” *IEEE Transactions on Information Theory*, vol. 55, no. 6, pp. 2547–2553, Jun. 2009.
- [35] C. Jeong, I. M. Kim, and D. I. Kim, “Joint Secure Beamforming Design at the Source and the Relay for an Amplify-and-Forward MIMO Untrusted Relay System,” *IEEE Transactions on Signal Processing*, vol. 60, no. 1, pp. 310–325, Jan. 2012.

- [36] A. Khisti, G. Wornell, A. Wiesel, and Y. Eldar, “On the Gaussian MIMO Wiretap Channel,” in *2007 IEEE International Symposium on Information Theory*, pp. 2471–2475.
- [37] S. Shafiee and S. Ulukus, “Achievable Rates in Gaussian MISO Channels with Secrecy Constraints,” in *2007 IEEE International Symposium on Information Theory*, pp. 2466–2470.
- [38] S. Gerbracht, C. Scheunert, and E. A. Jorswieck, “Secrecy Outage in MISO Systems With Partial Channel Information,” *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 2, pp. 704–716, 2012.
- [39] H. Alves, R. D. Souza, M. Debbah, and M. Bennis, “Performance of Transmit Antenna Selection Physical Layer Security Schemes,” *IEEE Signal Processing Letters*, vol. 19, no. 6, pp. 372–375, Jun. 2012.
- [40] N. S. Ferdinand, D. B. da Costa, A. L. F. de Almeida, and M. Latva-aho, “Secrecy Outage Performance of MISO Wiretap Channels with Outdated CSI,” in *2014 IEEE International Conference on Communications Workshops (ICC)*, pp. 789–793.
- [41] H. M. Wang, T. Zheng, and X. G. Xia, “Secure MISO Wiretap Channels With Multiantenna Passive Eavesdropper: Artificial Noise vs. Artificial Fast Fading,” *IEEE Transactions on Wireless Communications*, vol. 14, no. 1, pp. 94–106, Jan. 2015.
- [42] X. Cai and G. B. Giannakis, “Performance Analysis of Combined Transmit Selection Diversity and Receive Generalized Selection Combining in Rayleigh Fading Channels,” *IEEE Transactions on Wireless Communications*, vol. 3, no. 6, pp. 1980–1983, Nov. 2004.
- [43] A. Dvoretzky, “Asymptotic Normality for Sums of Dependent Random Variables,” *Proceedings of the Sixth Berkeley Symposium on Mathematical Statistics and Probability*, vol. 2, pp. 513–535, 1972.

Appendices

A SIR Analysis of Eve with CI

According to (3.9), the instantaneous effective channel of Eve with the CI precoder case is

$$g_{E,CI}(n) = \frac{1}{M} \sum_{k=1}^N \frac{g_k}{h_k} b(k, n).$$

Hence, this channel is a function of three independent random vectors, namely, \mathbf{h} , \mathbf{g} and $\mathbf{B}(n)$. The average of this channel with respect to \mathbf{B} is

$$\begin{aligned} \mathbb{E}_{\mathbf{B}}[g_{E,CI}(n)] &= \mathbb{E}_{\mathbf{B}} \left[\frac{1}{M} \sum_{k=1}^N \frac{g_k}{h_k} b(k, n) \right] = \frac{1}{M} \sum_{k=1}^N \frac{g_k}{h_k} \mathbb{E}_{\mathbf{B}}[b(k, n)] \\ &= \frac{1}{M} \sum_{k=1}^N \frac{g_k}{h_k} \frac{M}{N} = \frac{1}{N} \sum_{k=1}^N \frac{g_k}{h_k}. \end{aligned}$$

Now the variation around the mean of Eve's effective channel can be written as

$$g_{E,CI}(n) - \mathbb{E}_{\mathbf{B}}[g_{E,CI}(n)] = \sum_{k=1}^N \frac{g_k}{h_k} \left(\frac{b(k, n)}{M} - \frac{1}{N} \right).$$

Now, we find the numerator and denominator of (3.21). The calculations of the denominator are as follows

$$\begin{aligned}
\mathbb{E}_{\mathbf{B}} \left[\left| g_{E,CI}(n) - \mathbb{E}_{\mathbf{b}}[g_{E,CI}(n)] \right|^2 \right] &= \mathbb{E}_{\mathbf{B}} \left\{ \left(\sum_{k=1}^N z_k \left[\frac{b(k,n)}{M} - \frac{1}{N} \right] \right) \right. \\
&\times \left. \left(\sum_{\ell=1}^N z_{\ell} \left[\frac{b(\ell,n)}{M} - \frac{1}{N} \right] \right)^* \right\} = \mathbb{E}_{\mathbf{B}} \left\{ \sum_{k=1}^N \sum_{\ell=1}^N z_k z_{\ell}^* \left[\frac{b(k,n)}{M} - \frac{1}{N} \right] \left[\frac{b(\ell,n)}{M} - \frac{1}{N} \right] \right\} \\
&= \sum_{k=\ell=1}^N |z_k|^2 \underbrace{\mathbb{E}_{\mathbf{B}} \left\{ \left[\frac{b(k,n)}{M} - \frac{1}{N} \right]^2 \right\}}_{\star} + \\
&\sum_{k,\ell=1, k \neq \ell}^N z_k z_{\ell}^* \underbrace{\mathbb{E}_{\mathbf{B}} \left\{ \left[\frac{b(k,n)}{M} - \frac{1}{N} \right] \left[\frac{b(\ell,n)}{M} - \frac{1}{N} \right] \right\}}_{\star\star},
\end{aligned}$$

where $z_k = \frac{g_k}{h_k}$. In the above equation the derivations of \star and $\star\star$ are required for simplifying the denominator of Eve's SIR. To do so, we need to find the probability of the following events: $b(k,n) = 1$ corresponds to $\binom{N-1}{M-1}$ possible combinations to position a 1 in $M-1$ positions amongst $N-1$ positions. $b(k,n) = 0$ corresponds to $\binom{N-1}{M}$ possibilities to position a 1 in M positions among $N-1$ positions. The total number of possibilities to place M 1s is $\binom{N}{M}$. Therefore, the probability to have $b(k,n) = 1$ is $p_1 = \frac{\binom{N-1}{M-1}}{\binom{N}{M}}$ and the probability to have $b(k,n) = 0$ is $p_0 = \frac{\binom{N-1}{M}}{\binom{N}{M}}$. By simplifying the mentioned probabilities $p_1 = \frac{M}{N}$ and $p_0 = \frac{N-M}{N}$. By deriving p_0 and p_1 we can find the close form of \star .

$$\begin{aligned}
\star &= \left(-\frac{1}{N}\right)^2 p_0 + \left(\frac{1}{M} - \frac{1}{N}\right)^2 p_1 \\
&= \frac{N-M}{N^3} + \frac{M(N-M)^2}{N(MN)^2} = \frac{N-M}{MN^2}.
\end{aligned}$$

For the second term ($\star\star$), we first find the probabilities of $b(k,n) = b(\ell,n) = 1$, $b(k,n) = b(\ell,n) = 0$, $b(k,n) = 1, b(\ell,n) = 0$ and $b(k,n) = 0, b(\ell,n) = 1$. The following table gives these probabilities

Value	Number of Possibilities	Probability
$b(k) = b(\ell) = 1$	$\binom{N-2}{M-2}$	$p_{11} = \frac{\binom{N-2}{M-2}}{\binom{N}{M}}$
$b(k) = 1, b(\ell) = 0$	$\binom{N-2}{M-1}$	$p_{10} = \frac{\binom{N-2}{M-1}}{\binom{N}{M}}$
$b(k) = 0, b(\ell) = 1$	$\binom{N-2}{M-1}$	$p_{01} = \frac{\binom{N-2}{M-1}}{\binom{N}{M}}$
$b(k) = b(\ell) = 0$	$\binom{N-2}{M}$	$p_{00} = \frac{\binom{N-2}{M}}{\binom{N}{M}}$

Table A.1: Table of corresponding probabilities to each set of $b(k)$ and $b(\ell)$.

Now the desired term is

$$\star\star = p_{11}\left(\frac{1}{M} - \frac{1}{N}\right)^2 + 2p_{10}\left(\frac{1}{M} - \frac{1}{N}\right)\left(-\frac{1}{N}\right) + p_{00}\left(\frac{1}{N}\right)^2 = -\frac{N-M}{(N-1)N^2M}.$$

Thus we have

$$\begin{aligned} \mathbb{E}_{\mathbf{B}} \left[\left| g_{E,CI}(n) - \mathbb{E}_{\mathbf{B}}[g_{E,CI}(n)] \right|^2 \right] &= \sum_{k=1}^N \frac{N-M}{MN^2} |z_k|^2 + \sum_{\substack{k,\ell=1 \\ k \neq \ell}}^N \left(-\frac{N-M}{(N-1)MN^2} \right) z_k z_\ell^* \\ &= \sum_{k=1}^N \frac{N-M}{MN^2} |z_k|^2 + \sum_{k,\ell=1}^N \left(-\frac{N-M}{(N-1)MN^2} \right) z_k z_\ell^* - \sum_{k=1}^N \left(-\frac{N-M}{(N-1)MN^2} \right) |z_k|^2 \\ &= \sum_{k=1}^N \left(\frac{N-M}{(N-1)MN} + \frac{N-M}{(N-1)MN^2} \right) + \left(-\frac{N-M}{(N-1)MN^2} \right) \sum_{k=1}^N z_k \left[\sum_{\ell=1}^N z_\ell \right]^* \\ &= \frac{N-M}{(N-1)M} \left\{ \left[\frac{\sum_{k=1}^N |z_k|^2}{N} \right] - \left| \frac{\sum_{k=1}^N z_k}{N} \right|^2 \right\}, \end{aligned}$$

and the SIR of Eve with CI precoder is

$$\gamma_{E_{CI}} = \frac{\left| \frac{1}{N} \sum_{k=1}^N z_k \right|^2}{\frac{N-M}{(N-1)M} \left\{ \left[\frac{\sum_{k=1}^N |z_k|^2}{N} \right] - \left| \frac{\sum_{k=1}^N z_k}{N} \right|^2 \right\}}. \quad (\text{A.1})$$

B SIR PDF of Eve with CI

Having calculated the closed form of received SIR at Eve, now we find the probability density function of this parameter. In (3.24), we replace the $\frac{g_k}{h_k}$ by z_k . After dividing the numerator and denominator of (A.1) by $\frac{1}{N} \sum_{k=1}^N |z_k|^2 = \frac{\|\mathbf{z}\|_2^2}{N}$ we have

$$\gamma_{ECI} = \frac{\left| \sum_{k=1}^N \frac{z_k}{\sqrt{N}\|\mathbf{z}\|_2} \right|^2}{\frac{N-M}{(N-1)M} \left\{ 1 - \left| \sum_{k=1}^N \frac{z_k}{\sqrt{N}\|\mathbf{z}\|_2} \right|^2 \right\}}. \quad (\text{B.2})$$

Now the PDF of $\left| \sum_{k=1}^N \frac{z_k}{\sqrt{N}\|\mathbf{z}\|_2} \right|^2$ is desired. the random variables $\frac{z_k}{\sqrt{N}\|\mathbf{z}\|_2}, k = 1, \dots, N$ are all identically distributed over the complex sphere with $2N$ dimension and thus are dependent. The sum of dependent identically distributed random variables can also be approximated by Gaussian distribution[43]. Therefore, the PDF of $\sum_{k=1}^N \frac{z_k}{\sqrt{N}\|\mathbf{z}\|_2}$ is approximated by $\mathcal{CN}(0, \frac{1}{N})$ which results into an exponential distribution of $\left| \sum_{k=1}^N \frac{z_k}{\sqrt{N}\|\mathbf{z}\|_2} \right|^2$ with the parameter $\lambda_{CI} = \frac{1}{N}$. One of the main reasons that our scheme provides secure communication is the utilization of large antenna arrays at Alice side. Assuming $N(N > 10)$ is large, the probability of the

$$\Pr \left(\left| \sum_{k=1}^N \frac{z_k}{\sqrt{N}\|\mathbf{z}\|_2} \right|^2 \ll 1 \right) \simeq 1.$$

Therefore, in the denominator of γ_{ECI} , this term compared to 1 is negligible and we approximate γ_{ECI} as

$$\gamma_{ECI} = \frac{M(N-1)}{N-M} \left| \sum_{k=1}^N \frac{z_k}{\sqrt{N}\|\mathbf{z}\|_2} \right|^2 \sim \exp \left(\lambda_E = \frac{1-\beta}{\beta} \frac{N}{N-1} \right). \quad (\text{B.3})$$

C SINR Analysis of Bob with EBF

Similar to the derivation done in the Appendix A, in this appendix we calculate the SINR ($\gamma_{B,EBF}$) received at Bob with the EBF precoding. The instantaneous effective channel of Bob with the EBF precoder is

$$g_{B,EBF}(n) = \frac{1}{M} \sum_{k=1}^N |h_k| b(k, n).$$

and the mean of this channel with respect to all the realization of activation vector across one fading block is

$$\mathbb{E}_{\mathbf{B}} [g_{B,EBF}(n)] = \frac{1}{N} \sum_{k=1}^N |h_k|.$$

By following the similar procedure as in Appendix A, the variation of this effective channel around its mean is

$$\mathbb{E}_{\mathbf{B}} \left[\left| g_{B,EBF}(n) - \mathbb{E}_{\mathbf{B}} [g_{B,EBF}(n)] \right|^2 \right] = \frac{N-M}{(N-1)M} \left(\left[\frac{1}{N} \sum_{k=1}^N |h_k|^2 \right] - \left[\frac{1}{N} \sum_{k=1}^N |h_k| \right]^2 \right). \quad (\text{C.4})$$

Therefore, the received SINR at Bob over each fading block is

$$\gamma_{B,EBF} = \frac{\left[\frac{1}{N} \sum_{k=1}^N |h_k| \right]^2 P}{\frac{N-M}{(N-1)M} \left(\left[\frac{1}{N} \sum_{k=1}^N |h_k|^2 \right] - \left[\frac{1}{N} \sum_{k=1}^N |h_k| \right]^2 \right) P + \sigma_B^2}. \quad (\text{C.5})$$

Unlike (B.2) which is varying from one block to another, (C.5) is fixed across all of the fading blocks and only varies with the transmitted power to noise ratio, i.e., $\frac{P}{\sigma_B^2}$. Thus, the PDF of received SINR at Bob over each block similar to that of with CI precoder, is given by a delta function. Furthermore, the numerator of (C.5) is the sample mean of the Rayleigh distributed samples and thus with the assumption of having large amount of antenna arrays at Alice, this can be given as

$$\frac{1}{N} \sum_{k=1}^N |h_k| = \sigma_{\mathbf{h}} \sqrt{\frac{\pi}{2}}, \quad (\text{C.6})$$

where $\sigma_{\mathbf{h}}$ is the Rayleigh distribution parameter related to the Alice to Bob's channel vector. The term inside the parenthesis in (C.4) is the sample variance of the Rayleigh distributed samples and (with the sufficiently large number of antennas at Alice) it is given as

$$\left[\frac{1}{N} \sum_{k=1}^N |h_k|^2 \right] - \left[\frac{1}{N} \sum_{k=1}^N |h_k| \right]^2 = \frac{4 - \pi}{2} \sigma_{\mathbf{h}}^2. \quad (\text{C.7})$$

By substituting (C.6) and (C.7) into (C.5), $\gamma_{B_{EBF}}$ will be

$$\gamma_{B_{EBF}} = \frac{\left(\frac{\pi}{2} \sigma_{\mathbf{h}}^2 \right) P}{\frac{N - M}{(N - 1)M} \left(\frac{4 - \pi}{2} \sigma_{\mathbf{h}}^2 \right) P + \sigma_B^2}.$$

In contrast to the received SNR at Bob with CI precoder, with this precoder even in high SNR regime, i.e., $\frac{P}{\sigma_B^2} \rightarrow \infty$, the SINR is limited and so is the secrecy rate.

D SIR Analysis of Eve with EBF

The instantaneous effective channel of Eve with EBF precoder is

$$g_{E,EBF}(n) = \frac{1}{M} \sum_{k=1}^N g_k \frac{h_k^*}{|h_k|} b(k, n).$$

By denoting $\Theta = [\theta_1, \dots, \theta_N]$ as the corresponding phase vector of the Bob's fading coefficient, we rewrite $g_{E,EBF}(n)$ as

$$g_{E,EBF}(n) = \frac{1}{M} \sum_{k=1}^N g_k \exp(-j\theta_k) b(k, n).$$

Similar to the calculations in Appendix A, the received SIR at Eve's side can be written as

$$\gamma_{E_{EBF}} = \frac{\left| \frac{1}{N} \sum_{k=1}^N g'_k \right|^2}{\frac{N-M}{(N-1)M} \left\{ \left[\frac{\sum_{k=1}^N |g'_k|^2}{N} \right] - \left| \frac{\sum_{k=1}^N g'_k}{N} \right|^2 \right\}}, \quad (\text{D.8})$$

where $g'_k = g_k \exp(-j\theta_k)$. By dividing the numerator and denominator of (D.8) to $\frac{1}{N} \sum_{k=1}^N |g'_k|^2 = \frac{\|\mathbf{g}'\|_2^2}{N}$, $\gamma_{E_{EBF}}$ will be

$$\gamma_{E_{EBF}} = \frac{\left| \sum_{k=1}^N \frac{g'_k}{\sqrt{N}\|\mathbf{g}'\|_2} \right|^2}{\frac{N-M}{(N-1)M} \left\{ 1 - \left| \sum_{k=1}^N \frac{g'_k}{\sqrt{N}\|\mathbf{g}'\|_2} \right|^2 \right\}}, \quad (\text{D.9})$$

where the random variables $\frac{g'_k}{\sqrt{N}\|\mathbf{g}'\|_2}, k = 1, \dots, N$ are approximated to be complex Gaussian distributed, i.e., $\frac{g'_k}{\sqrt{N}\|\mathbf{g}'\|_2} \sim \mathcal{CN}(0, \frac{1}{N})$. With the same approximation we consider in Appendix B for $\left| \sum_{k=1}^N \frac{g'_k}{\sqrt{N}\|\mathbf{g}'\|_2} \right|^2$, $\gamma_{E_{EBF}}$ has an exponential distribution with the same parameter as introduced in Appendix B.