SECURE MULTI-ANTENNA TRANSMISSION WITH FINITE-ALPHABET SIGNALING

A DISSERTATION SUBMITTED TO
THE GRADUATE SCHOOL OF ENGINEERING AND SCIENCE
OF BILKENT UNIVERSITY
IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR
THE DEGREE OF
DOCTOR OF PHILOSOPHY
IN
ELECTRICAL AND ELECTRONICS ENGINEERING

By
Sina Rezaei Aghdam
December 2017

Secure Multi-Antenna Transmission with Finite-Alphabet Signaling
By Sina Rezaei Aghdam
December 2017

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

Tolga Mete Duman (Advisor)

Erdal Arıkan

Ayşe Melda Yüksel Turgut

Sinan Gezici

Ali Özgür Yılmaz

Approved for the Graduate School of Engineering and Science:

Ezhan Karaşan
Director of the Graduate School

ABSTRACT

SECURE MULTI-ANTENNA TRANSMISSION WITH FINITE-ALPHABET SIGNALING

Sina Rezaei Aghdam
Ph.D. in Electrical and Electronics Engineering
Advisor: Tolga Mete Duman
December 2017

With the ever-growing demand for services that rely on transmission over wireless networks, a challenging issue is the security of the transmitted information. Due to its open nature, wireless communications is prone to eavesdropping attacks. Typically, secrecy of the transmitted information is ensured with the aid of cryptographic techniques, which are deployed on upper layers of the network protocol stack. However, due to the need for key distribution and management, cryptographic solutions are difficult to implement in decentralized networks. Moreover, the security provided by key based solutions is not provable from a mathematical point of view. Physical layer security is an alternative or complement to the cryptographic techniques, which can resolve the complexities associated with key distribution and management. The basic principle of physical layer security is to exploit the randomness of the communication channels to allow a transmitter deliver its message to an intended receiver reliably while guaranteeing that a third party cannot infer any information about it. Much of the existing research in physical layer security focuses on investigating the information theoretic limits of secure communications. Among different techniques proposed, multiple-antenna based solutions have been shown to exhibit a high potential for enhancing security. Furthermore, Gaussian inputs are proved to be the optimal input distributions in a variety of scenarios. However, due to the high detection complexity, Gaussian signaling is not used in practice, and the transmission is carried out with the aid of symbols drawn from standard signal constellations.

In this thesis, we develop several secure multi-antenna transmission techniques under the practical finite-alphabet input assumption. We first consider multiple-input multiple-output (MIMO) wiretap channels under finite-alphabet input constraints. We assume that the statistical channel state information (CSI) of the eavesdropper is available at the transmitter, and study two different scenarios regarding the transmitter's knowledge on the main channel CSI (MCSI) including

availability of perfect and statistical MCSI at the transmitter. In each scenario, we introduce iterative algorithms for joint optimization of data precoder and artificial noise. We also propose different strategies to reduce the computational complexity associated with the transmit signal design. Moreover, we consider the setups with simultaneous wireless information and power transfer (SWIPT), and propose transmission schemes for achieving the trade-off between the secrecy rate and the harvested power. We demonstrate the efficacy of the proposed transmit signal design algorithms via extensive numerical examples.

We also introduce several secure transmission schemes with spatial modulation and space shift keying (SSK). We derive an expression for the achievable secrecy rate, and develop precoder optimization algorithms for its maximization using transmitter side CSI. Furthermore, we introduce a group of secure SSK transmission schemes, which rely on dynamic antenna index assignment over reciprocal channels. Our results reveal that the fundamentally different working principle of SSK opens up new avenues for secure multi-antenna transmission.

Keywords: Physical layer security, finite-alphabet inputs, MIMO communications, channel state information, precoding, artificial noise, cut-off rate, simultaneous wireless information and power transfer, spatial modulation, space shift keying.

ÖZET

SONLU GİRDİ SETİNE SAHİP SİNYALLERLE ÇOK ANTENLİ GÜVENLİ İLETİM

Sina Rezaei Aghdam
Elektrik ve Elektronik Mühendisliği, Doktora
Tez Danışmanı: Tolga Mete Duman
Aralık 2017

Kablosuz ağlar üzerinden bilgi aktarmaya dayanan hizmetlere olan talebin gittikçe artmasıyla, iletilen bilgilerin güvenliği zorlayıcı bir konuya dönüşmüştür. Dışa açık olan yapıları ile kablosuz ağlar, gizli dinleme saldırılarına maruz kalmaktadır. Genellikle, iletilen bilgilerin gizliliği, ağ protokol yığınının üst katmanlarına yerleştirilen şifreleme teknikleriyle sağlanmaktadır. Ancak, anahtar dağıtım ve yönetim ihtiyacı nedeniyle, kriptografik çözümlerin merkeziyetçi olmayan şebekelerde uygulanması zordur. Bunun yanında, anahtar tabanlı çözümlerle sağlanan güvenliğin matematiksel bir kanıtı da yoktur. Fiziksel katman güvenliği, anahtar dağıtımı ve yönetimi ile ilgili karmaşıklıkları giderebilen şifreleme tekniklerine bir alternatif veya tamamlayıcıdır. Fiziksel katman güvenliğindeki temel ilke, iletişim kanallarının rastlantısallığını kullanarak, bir vericinin mesajını istenen bir alıcıya güvenilir bir şekilde iletirken üçüncü biri tarafın mesajla ilgili herhangi bir bilgi elde edilemediğini garanti altına almaktır. Fiziksel katman güvenliği ile ilgili araştırmaların çoğunluğunda, güvenli iletişimin teorik sınırlarının araştırılması üzerinde durulmaktadır. Önerilen farklı teknikler arasında, çoklu anten çözümlerinin, güvenliği arttırmak için yüksek bir potansiyel sergilediği gösterilmiştir. Ayrıca, Gauss girdilerinin en uygun girdi dağılımı olduğu çeşitli senaryolar için kanıtlanmıştır. Fakat, tespit karmaşıklığının yüksek olması nedeniyle, uygulamada Gauss sinyallemesi kullanılmamaktadır ve iletim, standart sinyal gruplamalarından alınan sembollerin yardımıyla gerçekleştirilmektedir.

Bu tezde, pratik sonlu-alfabe girdisi varsayımı altında birkaç çok antenli güvenli iletim tekniği geliştiriyoruz. İlk olarak sonlu alfabe girdi kısıtlamaları altında çok girdili çok çıktılı (MIMO) hat dinleme kanallarını inceliyoruz. Gizli dinleyicinin istatistiksel kanal durum bilgisinin vericide mevcut olduğu senaryonun yanında esas dinleyicinin mükemmel veya istatistiksel kanal bilgisinin vericide mevcut olduğuna ilişkin iki farklı senaryoyu inceliyoruz. Her senaryoda,

önkodlayıcı ve yapay gürültünün ortak optimizasyonu için yinelemeli algoritmalar sunuyoruz. Ayrıca, iletim sinyali tasarımındaki hesaplama karmaşıklığını azaltmak için farklı stratejiler öneriyoruz. Dahası, eşzamanlı kablosuz bilgi ve güç aktarımı (SWIPT) yaklaşımının kullanıldığı kurulumları inceliyoruz ve gizlilik oranı ile elde edilen güç arasındaki dengeyi sağlamak için iletim şemaları geliştiriyoruz. Önerilen yayın sinyali tasarım algoritmalarının etkinliğini sayısal örneklerle kanıtlıyoruz.

Ayrıca, uzaysal modülasyon ve uzay kaydırmalı anahtarlama (SSK) ile de birkaç güvenli iletim şeması sunuyoruz. Elde edilebilir gizlilik oranı için bir ifade elde ediyoruz ve verici tarafında kanal durum bilgisini kullanarak gizililik oranının maksimizasyonu için önkodlayıcı optimizasyon algoritmaları geliştiriyoruz. Ek olarak, karşılıklı (reciprocal) kanallar üzerinden dinamik anten indeksi atamasını kullanan bir grup güvenli SSK iletim şeması sunuyoruz. Sonuçlarımız, SSK'nın temelde farklı çalışma prensibinin güvenli çok antenli iletim tasarımı için yeni yollar açtığını ortaya koymaktadır.

Anahtar sözcükler: Fiziksel katmanda güvenlik, sonlu alfabe girdileri, çok girdili çok çıktılı iletişim, kanal durumu bilgisi, önkodlama, yapay gürültü, kesim oranı, eşzamanlı kablosuz bilgi ve güç aktarımı, uzaysal modülasyon, uzay kaydırmalı anahtarlama.

Acknowledgement

First and foremost, I would like to express my deepest gratitude to my supervisor, Prof. Tolga M. Duman for his endless support, encouragement, and patience during the past four years. I greatly appreciate his comments and ideas from which I have learned a lot. He has definitely been the most inspirational person in my life.

I am indebted to my PhD committee (TİK) members, Prof. Sinan Gezici and Prof. Melda Yüksel, who provided me with their precious suggestions during the past two years. I also would like to thank Prof. Erdal Arıkan and Prof. Ali Özgür Yılmaz for accepting to serve as jury members in my PhD thesis defense.

This work was supported by the Scientific and Technical Research Council of Turkey (TÜBİTAK) under the grants 113E223 and 114E601. I gratefully acknowledge this support.

I would like to thank my friend Mehdi Dabirnia for the fruitful discussions and his assistance in the progress of my research. I would also like to express my thanks to my friends Mahdi Shakiba Herfeh, Serdar Hanoğlu, Ersin Yar, Mert Özateş, Alireza Nooraiepour, Umut Demirhan, Nurullah Karakoç, Aras Yurtman, Mehdi Kazempour, Soheil Taraghinia, Akbar Alipour, Parisa Sharif, Burak Şahinbaş, Dilara Oğuz and Caner Odabaş who made my past four years in Bilkent University a memorable episode of my life.

I would like to express my eternal gratitude to my parents for their everlasting love and support. Last, but not least, I would like to thank my love Sepideh who has been my best friend during the past few years, and her love, great companionship and encouragements helped me get through this stage.

Contents

1 Introduction **1**

1.1 Contributions of the Thesis 3

1.2 Thesis Outline 5

1.3 Notation 6

2 Preliminaries on Physical Layer Security **7**

2.1 Fundamentals of Physical Layer Security 7

2.1.1 Different Notions of Secrecy 8

2.1.2 Secrecy Capacity of Single-Antenna Wiretap Channels . . 9

2.1.3 Secrecy Capacity of MIMO Wiretap Channels 12

2.2 Single-Antenna Wiretap Channels with Finite-Alphabet Inputs . . 12

2.3 MIMO Wiretap Channels with Finite-Alphabet Inputs 15

2.3.1 Transmit Signal Design with Full CSI 16

2.3.2 Perfect MCSI and Statistical ECSI 17

2.3.3 Perfect MCSI Only 18

2.3.4 Statistical MCSI and ECSI 19

2.4 Secure Simultaneous Wireless Information and Power Transfer . . 19

2.5 Secure Space Shift Keying Transmission 21

2.6 Chapter Summary 23

3 Transmit Signal Design for MIMO Wiretap Channel with Finite-Alphabet Inputs **24**

3.1 System Model and Preliminaries 24

3.2 Transmit Signal Design with Perfect MCSI 27

3.2.1 Related Works 27

3.2.2 Problem Formulation 27
3.2.3 Precoder and Artificial Noise Design 28
3.2.4 Direct Maximization of $R_{s,l}$ 29
3.2.5 Cut-off Rate Based Approximation for $R_{s,l}$ 32
3.2.6 Generalized Artificial Noise-Aided Precoding 35
3.2.7 Per-Group Precoding for Large MIMO Wiretap Channels . 38
3.2.8 Numerical Examples 42
3.3 Transmit Signal Design with Statistical MCSI 48
3.3.1 Related Works 48
3.3.2 Problem Formulation 49
3.3.3 Precoder Optimization 50
3.3.4 Joint Precoder and Artificial Noise Optimization 51
3.3.5 Numerical Results 52
3.4 Chapter Summary 53

4 Secure Wireless Information and Power Transfer with Constellation-Constrained Inputs 55
4.1 Related Works 56
4.2 MISO SWIPT Wiretap Channels 56
4.2.1 System Model and Problem Formulation 57
4.2.2 Secrecy Rate-Harvested Energy Trade-off Under Perfect CSIT 60
4.2.3 Secrecy Rate-Harvested Energy Trade-off with Statistical ECSIT 63
4.2.4 Low Complexity Two-Stage Precoder Design 64
4.3 Generalization to MIMO Setups 66
4.4 Numerical Examples 68
4.5 Chapter Summary 74

5 Physical Layer Security with Space Shift Keying Transmission 76
5.1 Related Works 78
5.2 Achievable Secrecy Rates 78
5.2.1 System Model and Problem Formulation 78
5.2.2 Mutual Information and Secrecy Rate 80
5.2.3 Space Shift Keying 81

5.2.4 Spatial Modulation 81
5.2.5 Numerical Examples 83
5.3 Secure Precoding Algorithms 87
5.3.1 System Model for Precoded SSK 87
5.3.2 Precoding for Secrecy Rate Maximization 89
5.3.3 Low Complexity Precoding Schemes 91
5.3.4 Numerical Results 95
5.4 Space Shift Keying with Dynamic Antenna Index Assignment . . 97
5.4.1 System Model for SSK with Dynamix Antenna Index Assignment 99
5.4.2 CSI-Based Antenna Index Assignment 100
5.4.3 Asymptotic Ergodic Secrecy Rates with Perfect Reciprocity 101
5.4.4 Reliability under Imperfect Reciprocity 102
5.4.5 Threat of a Nearby Eavesdropper 104
5.4.6 Dynamic Antenna Index Assignment based on Rotated Channels 105
5.4.7 Numerical Examples 107
5.5 Chapter Summary 110

6 Summary and Conclusions **111**

A Proof of Proposition 3.1 **126**

B Derivation of the Cut-off Rate Expression in (3.30) **127**

C Derivation of $\nabla_{\mathbf{P}_D} R'_{s,l}$ **129**

D Convergence Proofs for Algorithms 1 and 2 **130**

E Derivation of $\nabla_{\mathbf{P}_D} R_{s,l}$ and $\nabla_{\mathbf{P}_E} R_{s,l}$ **132**

List of Figures

2.1 Capacity of an AWGN channel with Gaussian and constellation-constrained inputs. 14
2.2 Secrecy rates with PSK and QAM inputs over a degraded Gaussian wiretap channel ($\mathrm{SNR}_e = \mathrm{SNR}_b - 1.5$ dB). 15
2.3 A SWIPT scenario with a single IR and a single ER (potential eavesdropper). 20
2.4 The encoding and decoding processes of spatial modulation with $N_t = 4$ and QPSK inputs. 22

3.1 The MIMOME setup. 25
3.2 Secrecy rates with QPSK inputs for a wiretap channel with $(N_t, N_{r_b}, N_{r_e}) = (2, 1, 1)$ with the main channel given in (3.74) and the eavesdropper channel with $\rho_t = 0.9$ and $\rho_r = 1$. 43
3.3 Convergence of Algorithm 1 for the same setting as Fig. 3.2. . . 44
3.4 Achievable secrecy rates for fading main channel, with different values of M ($N_t = 2$ and $N_{r_e} = N_{r_b} = 1$). 46
3.5 Ergodic Secrecy Rates with different number of antennas at the receiver ends ($N_t = 4$, BPSK inputs). 47
3.6 Ergodic secrecy rates for BPSK inputs using Algorithm 2 with and without per-group precoding. 48
3.7 Ergodic secrecy rates for BPSK input with different transmit signal design approaches ($\rho_{tb} = 0.9$ and $\rho_{rb} = 0.6$). PMCSI and SMCSI stand for perfect and statistical MCSI, respectively. 53

4.1 The system model. 57

4.2 Achievable secrecy rates versus harvested power with QPSK and Gaussian inputs for the channels given in (4.51) and (4.52) and with perfect CSI of both channels at the transmitter. 69
4.3 Achievable ergodic secrecy rates versus average harvested power over $4 \times 1 \times 1$ channels with BPSK inputs and statistical ECSIT. 70
4.4 Achievable ergodic secrecy rates versus average harvested power over $4 \times 2 \times 2$ channels with BPSK inputs and perfect CSIT. . . . 71
4.5 The optimal portions of the total power allocated to information bearing signal (denoted by Data), energy signal (denoted by BF) and artificial noise (denoted by AN) in $4 \times 2 \times 2$ channel with perfect CSIT. 72
4.6 Achievable ergodic secrecy rates versus average harvested power over $4 \times 2 \times 2$ channels with BPSK inputs and statistical ECSIT. 73
4.7 The optimal portions of the total power allocated to information bearing signal (denoted by Data), energy signal (denoted by BF) and artificial noise (denoted by AN) in $4 \times 2 \times 2$ channel with statistical ECSIT. 74

5.1 Tridimensional signal constellation corresponding to spatial modulation with 4 antennas and QPSK symbols. 77
5.2 Secrecy rate for a SSK system with different number of transmit antennas. $N_{r_e} = N_{r_b} = 1$. 83
5.3 Secrecy rate for a SSK system with different number of receiver antennas at the legitimate receiver and the eavesdropper. $N_t = 4, N_{r_e} = N_{r_b} = N_r$. 84
5.4 Secrecy rate for a spatial modulation system with different underlying signal constellations. $N_t = 2$, $N_{r_e} = N_{r_b} = 1$. 85
5.5 Comparison of secrecy rates for spatial modulation and general MIMO and SIMO systems. $N = 4$, $N_{r_e} = N_{r_b} = 2$. 86
5.6 An example demonstrating the working principle of Algorithm 5. 93
5.7 Average secrecy rate for precoded SSK with $N_{r_e} = 1$. 95
5.8 Average secrecy rate for precoded SSK with $N_{r_e} > 1$. 96
5.9 SSK with dynamic antenna index assignment. 98
5.10 CSI-based antenna index assignment (Scheme 1). 100

5.11 Dynamic antenna index assignment to avoid wiretapping by a nearby eavesdropper (Scheme 2). 106
5.12 Achievable secrecy rates at high SNRs for SSK transmissions with the CSI-based antenna index assignment under perfect reciprocity. 107
5.13 BER for SSK with $N_t = 4$, $N_{r_b} = N_{r_e} = 1$ under perfect and imperfect reciprocity, and with and without channel correlation between Bob and Eve. 108
5.14 SSK with dynamic antenna index assignment (DAIA) versus transmit preprocessing scheme, $(N_t, N_{r_b}, N_{r_e}) = (4, 4, 4)$. 109

List of Tables

2.1 Three notions of secrecy. 9

3.1 The number of matrix multiplication steps required for calculation of the secrecy rate and its cut-off rate-based approximation. . . . 34

5.1 CPU times required for obtaining precoder for secure SSK transmission (Intel Core-i7-4770, 3.4 GHz) 97

5.2 Probability of antenna index mismatch for $\tau = 0.05$. 104

Abbreviations

AWGN	additive white Gaussian noise
BER	bit error rate
CSI	channel state information
CSIT	channel state information at the transmitter
DMC	discrete memoryless channel
DMWC	discrete memoryless wiretap channel
ECSI	eavesdropper's channel state information
ECSIT	eavesdropper's channel state information at the transmitter
ER	energy receiver
GSVD	generalized singular value decomposition
i.i.d.	independent identically distributed
IR	information receiver
KKT	Karush-Kuhn-Tucker
MCSI	main channel state information
MIMO	multiple-input multiple-output
MIMOME	multiple-input multiple-output multi-antenna eavesdropper
MISO	multiple-input single-output
MISOME	multiple-input single-output multi-antenna eavesdropper
MISOSE	multiple-input single-output single-antenna eavesdropper

ML	maximum likelihood
MSE	mean squared error
PAM	pulse amplitude modulation
PSK	phase shift keying
QAM	quadrature amplitude modulation
RF	radio frequency
SIMO	single-input multiple-output
SINR	signal to interference and noise ratio
SNR	signal to noise ratio
SSK	space shift keying
SWIPT	simultaneous wireless information and power transfer

Chapter 1

Introduction

Wireless communications has become an indispensable part of our everyday lives. As more and more data is being transmitted over wireless links, along with the reliability of the transmission, ensuring secrecy of the sensitive information has become a challenging issue. Traditionally, this issue is addressed using higher (network) layer solutions and via computation-based mechanisms such as encryption. On the other hand, the security provided by these methods mainly relies on the conjecture that the encryption function is difficult to invert, which is not provable from a mathematical point of view. With the ever-increasing computing power, encryption may no longer prevent information leakage to sophisticated adversaries. Moreover, implementation of key-based secure communications requires complicated protocols for key distribution and management, which is highly challenging to implement over decentralized wireless networks.

Securing transmission at the physical layer is an alternative or a complement to the cryptographic solutions. The basic idea is to exploit the inherent randomness of the channel for achieving secrecy. Dissimilar to encryption based methods, in the schemes employing physical layer security, no constraint is placed on the computational capability of the eavesdropper. Furthermore, no key distribution/management is required in its implementation.

While there were only sporadic efforts on exploring the potential of physical layer security until about a decade ago, with the proliferation of wireless networks, and especially, those with minimal infrastructure, it has recently been given considerable attention. Numerous recent studies have focused on characterization of the fundamental limits of secure communications in a variety of settings ranging from point-to-point to multi-antenna and multi-user communications scenarios [1, 2].

Exploiting the spatial degrees of freedom offered by multi-antenna transmission techniques has proven to offer an effective means for enhancing security at the physical layer. In particular, it is possible to adopt a variety of powerful techniques, e.g., precoding and artificial noise injection, so as to maximize the quality difference between the signals received at the legitimate receiver and the eavesdropper. The secrecy capacity of the multiple-input multiple-output (MIMO) wiretap channel has been established in [3–5].

In addition to the investigation of information-theoretic limits of secure communications, a recent major focus has been on the practical aspects of physical layer security. On the other hand, there are still many important issues, which should be addressed so as to facilitate adoption of physical layer security in real world wireless communication systems. To name a few, the impacts of practical channel models, actual signaling techniques and feasibility of channel state information (CSI) at different nodes should be investigated [6].

Much of the existing research in the literature of physical layer security considers Gaussian signaling, which is proved to be the optimal signaling strategy in a variety of scenarios. However, due to their high detection complexity, Gaussian signaling is not used in practice and the transmission is carried out with the aid of discrete inputs drawn from standard constellations such as phase shift keying (PSK) or quadrature amplitude modulation (QAM). Hence, understanding the impact of the finite-alphabet input constraints and designing secure transmission schemes with constellation-constrained inputs is a mandatory step towards enabling implementation of systems employing physical layer security in practice.

1.1 Contributions of the Thesis

The aim of this thesis is to shed light on the impact of finite-alphabet inputs on the secrecy performance over multi-antenna wiretap channels as well as to develop secure transmission techniques under this practical constraint. Investigating the performance-complexity trade-offs associated with the transmit signal design in different scenarios is another key objective. In particular, we study MIMO wiretap channels under finite-alphabet input constraints with different assumptions on the CSI at the transmitter (CSIT). We also investigate secure simultaneous wireless information and power transfer (SWIPT) with constellation-constrained inputs. Furthermore, we propose different (secure) spatial modulation and space shift keying (SSK) transmission schemes. Our contributions in each of these three main titles are summarized as follows.

MIMO Wiretap Channels with Finite-Alphabet Inputs: We consider a general MIMO multiple-antenna eavesdropper (MIMOME) channel, and under the assumption that the channel inputs are drawn from standard constellations, we propose transmit signal design algorithms with the aid of statistical CSI of the eavesdropper's channel along with the perfect or statistical CSI of the main channel. Our proposed transmission strategies rely on precoding and artificial noise injection. We introduce iterative algorithms for maximization of the instantaneous secrecy rate, which rely on joint optimization of the precoder and artificial noise.

Since directly maximizing the instantaneous secrecy rate possesses a high computational complexity due to the need for several evaluations of the mutual information expression (which lacks closed-form), we formulate a cut-off rate based approximation and utilize it as the precoder design metric. In addition, for MIMO wiretap channels with a large number of transmit antennas, we propose a per-group precoding scheme, as a further reduced complexity solution. We also characterize the impact of different CSIT assumptions on the achievable secrecy rates.

Our results for this line of investigations have been published in [7–9].

Secure SWIPT with Constellation-Constrained Inputs: We consider a scenario where a multi-antenna transmitter aims at transmitting data to an information receiver (IR) while simultaneously transferring power to an energy receiver (ER), which should be kept ignorant about the messages intended for the IR. We first review the optimal solutions for 1) maximizing the secrecy rate without taking into account the energy harvesting process at the ER, and 2) maximizing the harvested power at the ER without considering the secrecy requirement. After demonstrating that maximization of the secrecy rate and maximization of the harvested energy are two conflicting problems, we introduce a transmit signal design algorithm for achieving the trade-off between them. The proposed algorithm relies on precoding and artificial noise injection. Specifically, we introduce a framework for jointly optimizing the data and artificial noise precoders such that an ergodic secrecy rate is maximized under the constraint that the harvested energy exceeds a predefined threshold. As performing a full search for the optimal data precoder and artificial noise covariance matrices possesses a high computational complexity, we propose a two-stage transmit signal design technique, which serves as a low complexity alternative to the joint precoder and artificial noise design approach.

Our results for secure SWIPT with constellation-constrained inputs have been submitted as a conference paper [10].

Secure Spatial Modulation and Space Shift Keying: We study spatial modulation and space shift keying (SSK), which are relatively new transmission schemes for low-complexity implementation of MIMO systems, in the context of physical layer security. SSK transmission relies on encoding information via active antenna indices. We first derive expressions for the mutual information, and formulate an achievable secrecy rate for the scenarios where the channel inputs are drawn from SSK or spatial modulation constellation sets. Then, under the assumption of availability of CSIT, we introduce a framework for precoder optimization. Furthermore, we develop several low-complexity transmit signal design approaches.

Along this line of investigations, we also introduce a secure SSK transmission

scheme over reciprocal channels, which relies on an adaptive antenna index assignment procedure. In the proposed scheme, the transmitter assigns the antenna indices according to a decreasing order of the magnitudes of their instantaneous channel gains. Under the reciprocity assumption, the legitimate receiver can simply acquire the antenna index assignment pattern initiated by the transmitter and can detect the transmitted bits accordingly. In contrast, an eavesdropper, which is sufficiently far from the legitimate receiver observing a statistically independent channel, cannot track the antenna index assignment pattern, and as a result, fails to detect the message. We also propose a dynamic antenna index assignment approach according to a rotated channel, which is robust to imperfect reciprocity and prevents a nearby eavesdropper whose channel is highly correlated with that of the legitimate receiver from decoding the transmitted message.

Our results on secure SSK transmissions have been published in [11–13].

1.2 Thesis Outline

The rest of this thesis is organized as follows. In Chapter 2, we provide the fundamentals of physical layer security and review the existing results in the literature of physical layer security with finite-alphabet inputs. Chapter 3 discusses the problem of secure transmission over MIMO wiretap channels with finite-alphabet inputs where we develop different transmit signal design algorithms. In Chapter 4, we focus on characterization of the trade-off between the security and the harvested power in SWIPT systems. That is, we introduce transmit signal design algorithms over MIMO SWIPT wiretap channels with constellation-constrained inputs. Chapter 5 is dedicated to the study of spatial modulation and SSK in the context of physical layer security, where after deriving expressions for achievable secrecy rates, we introduce different secure SSK transmission schemes. Concluding remarks and some directions for future studies are provided in Chapter 6.

1.3 Notation

Throughout the thesis, vectors and matrices are denoted with lowercase and uppercase bold letters, respectively. Scalars are denoted with either uppercase or lowercase non-bold letters. Our notation makes no distinction between random variables and their realizations as this distinction is made clear from the context. The expectation of a random variable x is represented by $\mathbb{E}_x\{.\}$, and $(.)^H$, $(.)^T$ and $\| \, . \, \|_F$ denote Hermitian, transpose and Frobenius norm operations, respectively. Probability mass (or density) function of a random variable x is denoted $P_x(.)$. The entropy of a discrete random variable w is denoted by $H(w)$, and $I(x; y|w)$ refers to the mutual information between random variables x and y conditioned on the random variable w. a^n stands for a sequence of length n, i.e., $a^n = \{a(1), a(2), \ldots, a(n)\}$. The notation $\mathcal{CN}(\mathbf{m}, \mathbf{R})$ denotes a circularly symmetric complex Gaussian random vector with mean vector $\mathbf{m}$ and covariance matrix $\mathbf{R}$.

Chapter 2

Preliminaries on Physical Layer Security

In this chapter, we provide some necessary preliminaries, which will be helpful for the material covered in the thesis. After a brief review of the fundamental concepts in information theoretic security, we present an overview on the literature of physical layer security with finite-alphabet inputs. Moreover, we briefly review security issues in SWIPT and discuss the potentials of physical layer in providing secrecy. Finally, we explain the fundamental working principle of spatial modulation and SSK and motivate their use in the context of physical layer security.

2.1 Fundamentals of Physical Layer Security

The wiretap channel model, originally introduced by Wyner in [14], is the most basic scenario in the study of physical layer security. In this model, while the sender Alice wishes to transmit a message signal to a legitimate receiver Bob; a third party, Eve, is present with the capability of eavesdropping on Alice's signal. The channel between Alice and Bob, and the channel between Alice

and Eve are referred to as the main channel and the eavesdropper's channel, respectively. In physical layer security, one is interested in transmitting in such a way to maximize the transmission rate over the main channel while keeping the eavesdropper ignorant about the message. This leads to the notion of secrecy capacity, which is defined as the maximum rate at which the transmitter can use the main link so as to deliver its message to the legitimate receiver in a way that the eavesdropper cannot successfully obtain any information about the message. Characterization of the secrecy capacity is one of the most fundamental problems in the literature of physical layer security in that it can provide us with vital implications on how secure transmission techniques can be designed.

2.1.1 Different Notions of Secrecy

Consider a transmitter who wishes to transmit a message m to a legitimate receiver while trying to keep an eavesdropper ignorant about the message. m is mapped to a codeword x^n using a stochastic encoder with n denoting the number of channel uses. Then, x^n is transmitted and y^n and z^n are received at the legitimate receiver and the eavesdropper, respectively. The eavesdropper's level of uncertainty is quantified using the equivocation rate given by

$$R_e = \frac{1}{n} H(m|z^n), \tag{2.1}$$

which is nothing but a measure of how unlikely it is that the eavesdropper can infer source information from its received signal. According to this definition, large equivocation rates are equivalent to higher secrecy levels.

There are different metrics for measuring the secrecy guaranteed by a specific scheme among which the information-theoretic ones are recognized as the strongest. Perfect secrecy is achievable in a system if the message m and its corresponding encoder output x^n are statistically independent [15]. This can be expressed as $I(m; x^n) = 0$, which means that the mutual information between the message and the encoded signal is exactly zero. This is to say, the eavesdropper is not capable of recovering the message via observation of the encoder output in view of the fact that this encoded signal does not provide any information about

the message. For this form of secrecy to be guaranteed, a secret key of the length at least equal to the length of the message should be used. However, weaker requirements can be adopted for evaluation of the secrecy in practical scenarios. A system is called to operate with strong secrecy if $\lim_{n\to\infty} I(m; z^n) = 0$, which means that if we consider codewords of n symbols being transmitted by Alice as x^n, the information leaked by observation of the received vector z^n shall go to zero as n goes to infinity. On the other hand, the condition $\lim_{n\to\infty} \frac{1}{n} I(m; z^n) = 0$ is referred to as weak secrecy. In particular, weak secrecy requires the asymptotic rate of information leakage to be sublinear in n. Different notions of secrecy which are used to measure the secrecy guaranteed by a specific scheme are summarized in Table. 2.1.

Table 2.1: Three notions of secrecy.

Notion	Requirement
Perfect Secrecy [15]	$I(m; x^n) = 0$
Strong Secrecy [16]	$\lim_{n\to\infty} I(m; z^n) = 0$
Weak Secrecy [14]	$\lim_{n\to\infty} \frac{1}{n} I(m; z^n) = 0$

2.1.2 Secrecy Capacity of Single-Antenna Wiretap Channels

The notion of secrecy capacity was originally introduced by Wyner in [14] for degraded wiretap channels. In the scenario studied in [14], the main channel and the eavesdropper's channel are assumed to be discrete memoryless channels (DMCs) where Eve's observation of the transmitted signal is a degraded version of the signal received by Bob. Wyner showed that, the secrecy capacity for this scenario can be expressed as the difference of the mutual information between Alice and Bob with that of Alice and Eve, maximized over all input distributions.

Generalization of the notion of secrecy capacity to the case of additive white Gaussian noise (AWGN) channels has been accomplished in [17]. While it has been assumed in [14] that x and z are conditionally independent given y, a weaker

notion than degradedness has been assumed in [17], that is, it is shown that, for the case of a Gaussian wiretap channel, nonzero secrecy capacity can be attained if Bob receives the signal through a less noisy channel.

While the scenarios considered in [14] and [17] put the eavesdropper at a disadvantage, Csiszár and Körner have studied the problem of secrecy for non-degraded channels in [18]. In this channel model, referred to as broadcast channel with confidential messages, the message transmitted by Alice contains a common message intended to both Bob and Eve as well as a secret message, which is intended for Bob only, and is needed to be kept secret from Eve. It is shown that the secrecy capacity over a discrete memoryless wiretap channel (DMWC) is given by:

$$C_s = \max_{P_{x|u}(x|u), P_u(u)} I(u;y) - I(u;z), \tag{2.2}$$

where u is an auxiliary random variable. With a given $P_{yz|x}(y,z|x)$, the secrecy capacity is achieved by maximizing the difference of the mutual information terms corresponding to the main and eavesdropper's channels over all joint distributions $P_{ux}(u,x)$ where u satisfies the Markov chain relationship $u \to x \to yz$.

In order to study the physical layer security in wireless communication scenarios, we need to extend the wiretap channel model to a model which takes into account the fading phenomenon. Assuming a narrowband transmission, fading is modeled as multiplicative gains over the ma0in and eavesdropper's channels, denoted by h_b and h_e, respectively. The first characterization of the role of fading in providing physical layer security is given in [19] where quasi-static fading channels are considered towards the legitimate receiver and the eavesdropper. It is shown via analyzing the secrecy outage probability that, in presence of fading, secure transmission is possible even in the scenarios where the eavesdropper has a better SNR. The secrecy capacity over block fading channels has been derived in [20] under the assumption that each coherence interval is long enough to allow for invoking proper random coding arguments. Given that the transmitter knows either the main CSI (MCSI) or both the main and the eavesdropper CSI (ECSI)

perfectly, an achievable secrecy rate can be formulated as [20]

$$R_s = \mathbb{E}_{h_b,h_e}\Big\{\big[I(x;y|h_b) - I(x;z|h_e)\big]^+\Big\}, \tag{2.3}$$

where $[a]^+ = \max\{a, 0\}$. It has been shown in [20] that the secrecy capacity that is achieved under the full CSI assumption serves as an upper bound on the secrecy capacity when only MCSI is known at the transmitter. This is due to the fact that with the knowledge on instantaneous ECSI, the transmitter is capable of realizing a more efficient transmission, which provides additional gains in terms of secrecy rates. For instance, when perfect knowledge of both channels are available, the transmitter can optimize the transmit power according to the instantaneous values of the channel gains h_b and h_e, providing a higher secrecy rate with respect to the case where the optimization of the transmit power is carried out according to the main channel only.

Under the assumption that the transmitter does not know the realizations of the channels, and it only has their statistics, assuming that each receiver knows its own channel, the secrecy capacity can be obtained with the aid of the results for the case of DMWC [18] as

$$C_s = \max_{P_{x|u}(x|u),P_u(u)} I(u;y,h_b) - I(u;z,h_e), \tag{2.4}$$

where u satisfies the Markov chain relationship $u \to x \to (y,h_b),(z,h_e)$. This is obtained by treating h_b and h_e as channel outputs at the legitimate receiver and at the eavesdropper, respectively [21], [22]. Using the chain rule of mutual information and noting the fact that h_b and h_e are independent of x and u, the expression in (2.4) can be modified as

$$C_s = \max_{P_{x|u}(x|u),P_u(u)} \mathbb{E}_{h_b} I(u;y|h_b) - \mathbb{E}_{h_e} I(u;z|h_e). \tag{2.5}$$

Determining the optimal joint distribution $P_{ux}(u,x)$ and the resulting exact secrecy capacity is an open problem. However, by ignoring the channel prefixing, secrecy can be quantified using an achievable ergodic secrecy rate in the following form

$$R_s = \Big[\mathbb{E}_{h_b} I(x;y|h_b) - \mathbb{E}_{h_e} I(x;z|h_e)\Big]^+. \tag{2.6}$$

2.1.3 Secrecy Capacity of MIMO Wiretap Channels

Multiple-input multiple-output (MIMO) wiretap channel is an extension of the wiretap channel to a scenario where all the nodes, namely Alice, Bob and Eve, are equipped with multiple antennas. The secrecy capacity for this setup has been determined independently by Khisti and Wornell [3] and Oggier and Hassibi [4]. The results in [18] are employed by Khisti and Wornell so as to develop a genie-aided upper bound on the secrecy capacity in the general case of non-degraded MIMO wiretap channels. While their characterization is through a saddlepoint, Oggier and Hassibi propose an alternative approach through a single optimization process. It has been shown in both [3] and [4] that the achievable secrecy rate is maximized when the channel input is Gaussian, and the secrecy capacity of a MIMO wiretap channel is given by

$$C_s = \max_{\mathbf{K}_x \succeq 0, Tr(\mathbf{K}_x)=P} \log\det(\mathbf{I} + \mathbf{H}_b \mathbf{K}_{\mathbf{x}} \mathbf{H}_b^H) - \log\det(\mathbf{I} + \mathbf{H}_e \mathbf{K}_{\mathbf{x}} \mathbf{H}_e^H), \qquad (2.7)$$

where $\mathbf{K}_{\mathbf{x}} = \mathbb{E}\{\mathbf{x}\mathbf{x}^H\}$, and $\mathbf{H}_b \in \mathbb{C}^{N_{r_e} \times N_t}$ and $\mathbf{H}_e \in \mathbb{C}^{N_{r_e} \times N_t}$ are the channel matrices corresponding to the legitimate receiver and the eavesdropper, respectively.

An alternative characterization of the secrecy capacity of the MIMO wiretap channel is presented by Liu and Shamai in [5] where they consider a more general matrix constraint on the channel input. While [3–5] prove that the optimal input is Gaussian, the optimal input covariance needs to be determined using numerical optimization approaches (see, e.g., [23, 24]).

2.2 Single-Antenna Wiretap Channels with Finite-Alphabet Inputs

As a first step in studying physical layer security under the finite-alphabet input assumption, the impacts of standard constellations on the achievable secrecy rates of Gaussian wiretap channel are studied in [25] and [26]. In [25], the authors evaluate the constellation-constrained secrecy capacity and highlight an

important behavioral difference between finite-alphabet (e.g., PSK and QAM) and Gaussian inputs, that is, for a fixed noise variance at Eve, the secrecy rate curves for PSK or QAM plotted against the SNR have global maxima at finite SNR values. Investigation of the secrecy capacity of the pulse amplitude modulation (PAM) inputs over a degraded Gaussian wiretap channel in [26] leads to a similar conclusion. In addition, the authors in [26] demonstrate that when finite constellations are employed, using all the available power for information bearing signal transmission may not be optimal. The reason behind these observations has its roots in the mutual information expressions. That is, the capacity under an average power constraint over an AWGN channel is given by

$$C = \log_2(1 + SNR), \tag{2.8}$$

in bits per complex dimension, and it is an increasing function of the SNR. On the other hand, the capacity of the constellation-constrained AWGN channel can be calculated as [27]

$$I(x;y) = \log_2 |\mathcal{X}| - \mathbb{E}_{x,y}\left\{ \log_2 \frac{\sum_{x' \in \mathcal{X}} p_{y|x'}(y|x')}{p_{y|x}(y|x)} \right\}, \tag{2.9}$$

where $\mathcal{X}$ is a constellation set and $|\mathcal{X}|$ denotes its cardinality. Dissimilar to the capacity expression in (2.8), the mutual information term in (2.9) converges to $\log_2 |\mathcal{X}|$ at high SNRs (see Fig. 2.1). This means that by increasing the transmit power, the mutual information terms $I(x;y)$ and $I(x;z)$ (calculated using (2.9)) will reach the saturation value, and the secrecy rate drops to zero. This is also verified in Fig. 2.2, where the secrecy rates are obtained by evaluating the difference of the mutual information terms corresponding to the main and eavesdropper's channels, under the assumption that the SNR at the eavesdropper (denoted by SNR_e) is lower than the legitimate reciever's SNR (denoted by SNR_b) by 1.5 dB. This also clarifies that using all the available transmit power for information transmission in the high SNR regime is not optimal [26]. Furthermore, it can be observed from Fig. 2.2 that higher secrecy rates are achieved over Gaussian wiretap channels by increasing the modulation orders.

Fading introduces new potentials for securing communications at the physical layer. Specifically, the randomness due to the channel fluctuations can be

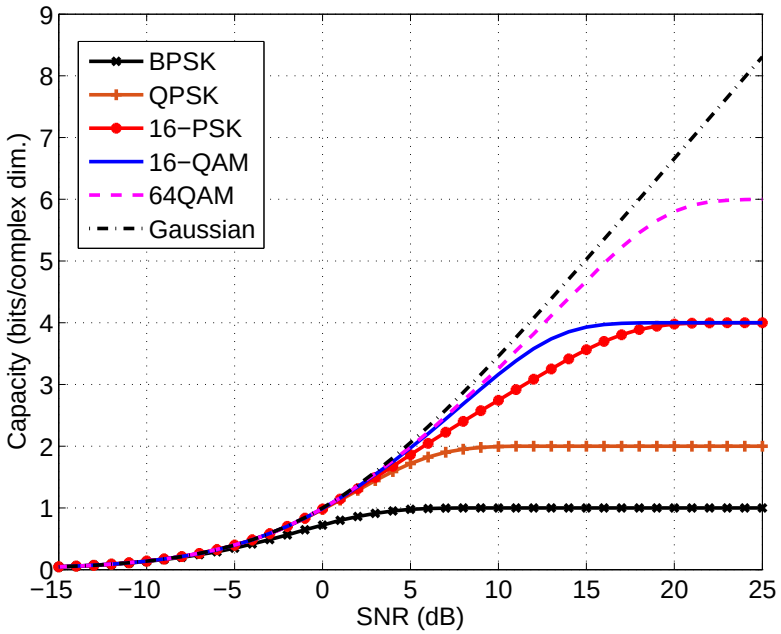

Figure 2.1: Capacity of an AWGN channel with Gaussian and constellation-constrained inputs.

exploited opportunistically by a transmitter to guarantee secrecy even in the scenarios where the eavesdropper possesses a higher SNR (on average) than the legitimate receiver. Dissimilar to the Gaussian wiretap channel where Gaussian input is secrecy capacity achieving, in the presence of fading, discrete signaling may achieve higher secrecy rates. For instance, it has been shown in [28] that, when Bob's channel gain is on average worse than that of Eve's, QAM inputs achieve higher secrecy rates at low and moderate SNR regimes. This is because the discrete nature of QAM inputs limits the leakage at the eavesdropper whose channel is unusually good. At sufficiently high SNRs, however, the secrecy rate with QAM inputs drop to zero similar to what is observed for the case of Gaussian wiretap channels.

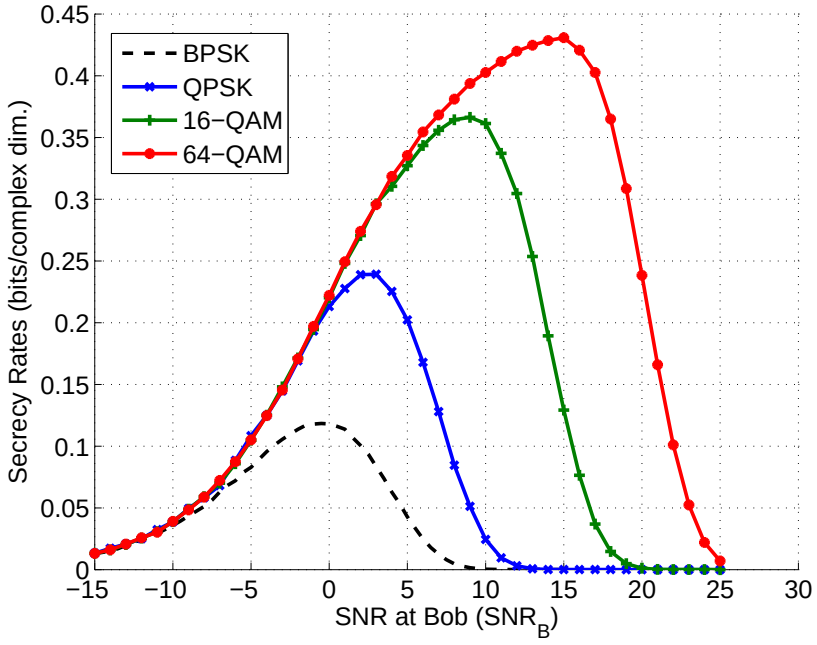

Figure 2.2: Secrecy rates with PSK and QAM inputs over a degraded Gaussian wiretap channel ($\mathrm{SNR}_e = \mathrm{SNR}_b - 1.5$ dB).

2.3 MIMO Wiretap Channels with Finite-Alphabet Inputs

Taking advantage of the spatial degrees of freedom introduced by multi-antenna transmission can serve as an efficient solution to prevent secrecy rate of standard constellations from dropping to zero at high SNRs. Transmit precoding and artificial noise injection serve as important approaches for enhancing secrecy [2]. Via precoding, it is possible to strengthen (or weaken) the transmitted signals in certain directions. Accordingly, it can be used as an effective tool to increase the quality difference between the signals received at the legitimate receiver and the eavesdropper. Beamforming is a special case of precoding where the transmitter is restricted to rank-one transmissions. It has a lower complexity with respect to the transmit precoding solution, achieved at the price of some performance loss. Furthermore, injection of artificial noise [29, 30] can effectively degrade the

reception at the eavesdropper while having no (or minimal) effect on the signal received at the legitimate receiver. To take advantage of the potentials offered by the channel fading, the transmitter needs a level of knowledge on the CSI of both channels. In what follows, we review the existing solutions for secure transmission over MIMO wiretap channels with finite-alphabet inputs under different CSIT assumptions.

2.3.1 Transmit Signal Design with Full CSI

The most optimistic assumption regarding the transmitter's CSI knowledge is availability of perfect instantaneous realizations of the channel matrices $\mathbf{H}_b$ and $\mathbf{H}_e$. This assumption is justifiable in the scenarios where Eve is an authorized user in the network, however, she should be kept ignorant about the confidential messages transmitted from Alice to Bob. In this case, the transmitter can take advantage of the full CSI knowledge to design a precoder which results in the maximal quality difference between the signals received at the legitimate receiver and the eavesdropper.

With the aid of the perfect CSI corresponding to both channels, a generalized singular value decomposition (GSVD) precoding solution has been proposed in [31] using which the MIMO multi-antenna eavesdropper (MIMOME) channel is converted into a bank of parallel channels, and a power allocation strategy is formulated to maximize the achievable secrecy rate.

The necessary conditions for optimum transmit precoding are derived in [32], and it is demonstrated that the GSVD precoding [31] is suboptimal. Alternatively, a gradient descent optimization is proposed in which the precoder matrices are updated with steps proportional to the gradient of the instantaneous secrecy rate. Furthermore, it is shown that transmission along the null-space of the eavesdropper's channel is the optimal secure transmission strategy at the high-SNR regime. This is because with a precoder matrix along the null-space of the eavesdropper's channel, the achievable rate at the eavesdropper is suppressed to zero, and when the SNR is sufficiently high, the rate at the legitimate receiver

approaches the maximum value that can be achieved with the use of specific finite-alphabet inputs, which guarantees that the secrecy rate is maximized. However, it should be noted that, when number of transmit antennas is less than or equal to the number of antennas at the eavesdropper, it is not possible to suppress the information rate at the eavesdropper by transmitting along the null-space of $\mathbf{H}_e$. Therefore, for maximizing secrecy rates, only partial power should be allocated to data transmission. So as to prevent the secrecy rates from dropping to zero, given $N_t > N_{r_b}$, the authors in [32] suggest the use of excess power for transmission of an artificial noise signal along the null-space of $\mathbf{H}_b$.

The structure of the optimal precoders under finite-alphabet input assumption is different from that of the precoders, which are optimal for Gaussian inputs. For example, over MISO multi-antenna eavesdropper (MISOME) channels, the optimal transmission strategy is beamforming along the eigenvector corresponding to the largest generalized eigenvalue of $(\mathbf{H}_b, \mathbf{H}_e)$ [3]. However, these precoders (which correspond to signaling with rank one covariance), when applied to the finite-alphabet inputs, undergo a considerable loss with respect to the precoders optimized under the finite-alphabet input assumption (see, e.g., Fig. 7 in [32]).

As an alternative method to design a suboptimal precoder, one may replace the secrecy capacity with practical metrics such as those based on mean-squared error (MSE). For instance, the authors in [33,34] propose transmit designs which minimize the MSE over the main channel while ensuring that the MSE at the eavesdropper is above a pre-specified level.

2.3.2 Perfect MCSI and Statistical ECSI

Availability of the perfect ECSI at the transmitter may be practical in some limited scenarios. However, in general, it is challenging to obtain the instantaneous CSI of the eavesdropper. A more practical assumption regarding CSIT is the availability of perfect MCSI along with the statistical ECSI at the transmitter. The precoder design in this scenario is not as effective as those carried out with the perfect knowledge of both channels. In other words, in the absence of the

instantaneous ECSI, precoding is not as forceful in suppressing the reception at the eavesdropper. For instance, transmission along the null-space of the eavesdropper's channel is not possible in this scenario. The authors in [35] consider a MISOME channel and define a practical secrecy metric (instead of an information theoretic one), which quantifies the symbol error probability of the confidential data and show that in the absence of artificial noise, secrecy diversity (i.e., the high-SNR slope of their defined metric) vanishes. This result underlines the importance of artificial noise injection in these scenarios.

In order to maximize the secrecy rate, artificial noise-aided precoding strategies are proposed in [32, 36]. Bashar *et al.* employ naive beamforming along with the artificial noise injection while considering single-antenna receivers. The strategy proposed in [32], on the other hand, relies on an iterative maximization of an approximation to the instantaneous secrecy rate. In both of these studies, it is shown that the optimal schemes allocate only a fraction of the total power for signal transmission at high SNRs. Hence, the remaining power can be employed for artificial noise injection.

2.3.3 Perfect MCSI Only

In the scenarios with a passive eavesdropper, a realistic assumption is that the transmitter does not know anything about the eavesdropper's channel. Under this assumption, [37] and [38] propose a secure transmission strategy referred to as directional modulation, in which the amplitude and the phase of the transmit signal are adjusted by varying the length of the reflector antennas for each symbol. This scrambles the PSK symbols in all the directions other than that of the legitimate receiver. Other strategies for securing the communications without the knowledge of the eavesdropper's channel are proposed in [39] and [40]. Zhang *et al.* develop a Tomlinson-Harashima precoding in [39] where the transmitter allocates transmit power in order to achieve a target MSE at the legitimate receiver, and the remaining power is used to transmit artificial noise to degrade the

eavesdropper's reception. In [40], a secure space-time block coding scheme is proposed in which Bob is provided with a separate decoding complexity, while Eve requires an exhaustive search to perform maximum likelihood (ML) decoding. Furthermore, they combine this scheme with artificial noise injection to ensure a high uncoded bit error rate (BER) at Eve.

2.3.4 Statistical MCSI and ECSI

While most of the existing physical layer security solutions rely on the assumption that the transmitter is capable of estimating at least the instantaneous main channel coefficient, in some scenarios (e.g., for fast fading channels), it may be difficult for the transmitter to track the rapidly varying channel coefficients. For these cases, a practical assumption would be that the transmitter is capable of obtaining the statistical MCSI. Only a few articles have studied the scenarios where the transmitter knows only the average statistics of both the legitimate receiver's and the eavesdropper's channels. In [41], it is shown that when the eavesdropper and legitimate channels have i.i.d. Gaussian entries with zero-mean and unit-variance, a circularly symmetric Gaussian input with a diagonal covariance matrix is optimal. Furthermore, [42] proposes an upper-bound on the secrecy capacity with statistical CSIT for fast fading MIMO wiretap channels. To the best of our knowledge, the only article which studies this scenario in the context of finite alphabet inputs is [43] where the authors characterize the achievable secrecy rates for QPSK inputs when both the main and the eavesdropper's channel are only statistically known at the transmitter.

2.4 Secure Simultaneous Wireless Information and Power Transfer

Wireless information and power transfer has received a considerable attention since the seminal work reported in [44]. Radio frequency (RF) based SWIPT has

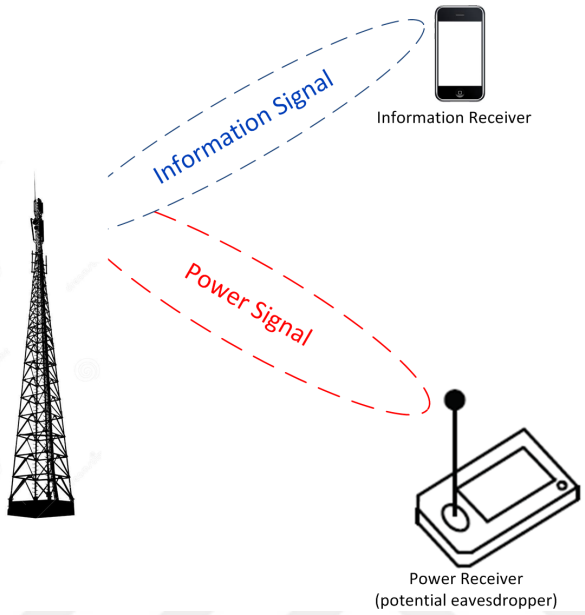

Figure 2.3: A SWIPT scenario with a single IR and a single ER (potential eavesdropper).

been proposed as a complementary technology for mitigating the energy scarcity in energy constrained networks where a central node plays the dual role of information and power transmitter as depicted in Fig. 2.3.

Deployment of a SWIPT system is typically in a manner that the energy receiver (ER) is closer to the source than the information receiver (IR). Therefore, the ER usually enjoys a better channel quality, and if it is malicious, it may successfully decode the information, resulting in high leakage. To address this challenge, providing secure transmission schemes at the physical layer of SWIPT systems has attracted a considerable amount of attention recently (see, e.g., [45] for a survey).

Different secure transmission schemes have been proposed in [46]–[47] for SWIPT with a multi-antenna transmitter, a single-antenna IR and multiple single-antenna ERs. Under the assumption that the perfect CSI of the IR and the ERs is available at the transmitter, [46] proposes a joint information and energy transmit beamforming design and obtains the optimal power allocation between

the data and energy signals. In [48], while assuming that only imperfect CSI of the ERs is available at the transmitter, the authors propose a resource allocation scheme for secure beamforming such that the total transmit power is minimized. The work in [47] studies the transmit signal design for maximizing the minimum harvested energy by ERs while satisfying a secrecy constraint in terms of the signal to interference and noise ratio (SINR) at the IR and the ERs.

2.5 Secure Space Shift Keying Transmission

Spatial modulation and SSK are relatively new MIMO transmission schemes which rely on encoding information into active antenna indices [49]. Similar to the amplitude or phase modulation schemes, in spatial modulation and SSK, the channel inputs are drawn from discrete and finite sets. More specifically, in spatial modulation [50], the data bits are mapped into two information carrying blocks: 1) an antenna index selected from the set of transmit antennas, 2) a symbol drawn from a standard constellation.

The working mechanism of spatial modulation relies on the fact that different transmit-receive antenna pairs experience statistically independent channels. To explain the encoding and decoding processes of spatial modulation, a simple example is given in Fig. 2.4. In this example, we assume that there are 4 transmit antennas, and QPSK modulation is employed. At the transmitter, the data bits are divided into blocks of length 4 bits, the first two bits of which determine the index of the antenna being activated. The second pair of bits in each block is modulated using QPSK and is transmitted via the activated antenna. At the receiver, CSI is used for joint detection of the index of the activated antenna as well as the QPSK symbol.

SSK is a special case of spatial modulation where no amplitude or phase modulation is employed, i.e., the transmit antenna index serves as the only information carrying unit [51]. Rather than PSK or QAM symbols, the transmitter sends reference signals from the activated antenna, and the receiver decodes the

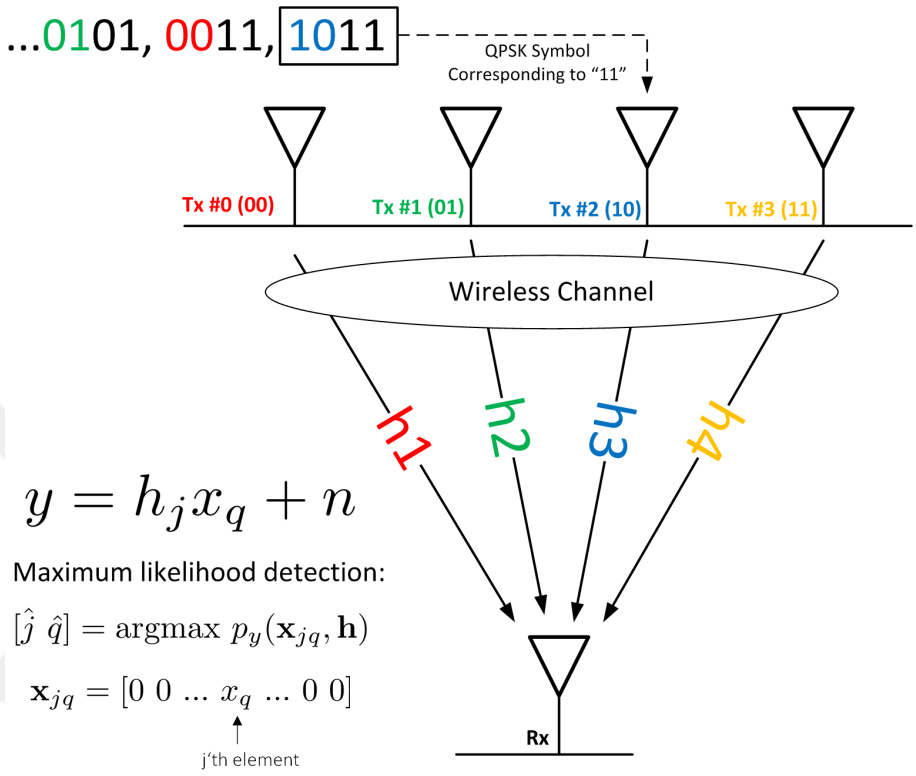

Figure 2.4: The encoding and decoding processes of spatial modulation with $N_t = 4$ and QPSK inputs.

transmitted bits by simply detecting its index with the aid of the CSI.

Various studies have explored the advantages offered by spatial modulation (see [49] for a comprehensive overview). Along with the different application areas of spatial modulation and SSK, their study in the context of physical layer security has been of recent interest. For instance, secrecy capacity of spatial modulation for the case of two transmit antennas has been studied in [52].

2.6 Chapter Summary

In this chapter, we have provided an overview on the fundamental concepts needed for the material covered in the remainder of the thesis. After an introduction on different notions of secrecy and formulation of the secrecy capacity for single-input single-output (SISO) and MIMO wiretap channels, we have given an overview of the literature on MIMO wiretap channels with finite-alphabet inputs. We have also briefly explained the secrecy concerns associated with SWIPT and discussed spatial modulation and SSK as two recently developed MIMO transmission schemes, which are also studied in the context of physical layer security in this thesis.

Chapter 3

Transmit Signal Design for MIMO Wiretap Channel with Finite-Alphabet Inputs

In this chapter, we consider transmit signal design for multi-antenna wiretap channels under the finite-alphabet input assumption. We assume that the transmitter knows the statistics of the eavesdropper's channel. Under two different assumptions on the transmitter's knowledge on the MCSI, we propose secrecy rate maximization algorithms, which rely on optimization of the precoder matrix and artificial noise. We also propose strategies to reduce the complexity of the transmit signal design algorithms.

3.1 System Model and Preliminaries

Consider a general MIMO wiretap channel as depicted in Fig. 3.1. The transmitter, Alice, the legitimate receiver, Bob, and the eavesdropper, Eve, are assumed to be equipped with N_t, N_{r_b} and N_{r_e} antennas, respectively. The received vectors

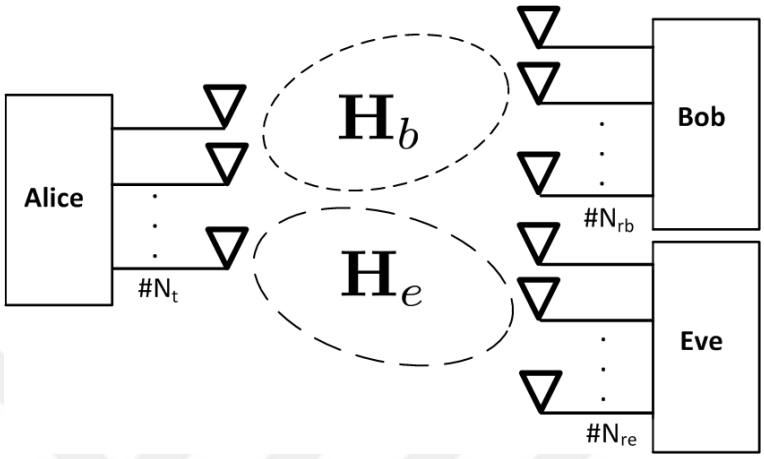

Figure 3.1: The MIMOME setup.

at Bob and Eve are given by

$$\mathbf{y} = \mathbf{H}_b\mathbf{x} + \mathbf{n}_y, \tag{3.1}$$

$$\mathbf{z} = \mathbf{H}_e\mathbf{x} + \mathbf{n}_z, \tag{3.2}$$

where $\mathbf{H}_b$ and $\mathbf{H}_e$ are the $N_{r_b} \times N_t$ and $N_{r_e} \times N_t$ channel matrices corresponding to the legitimate receiver's channel and the eavesdropper's channel, respectively. The AWGN terms, $\mathbf{n}_y$ and $\mathbf{n}_z$ are i.i.d. and they follow circularly symmetric complex Gaussian distributions, $\mathcal{CN}(0, \sigma^2_{\mathbf{n}_y})$ and $\mathcal{CN}(0, \sigma^2_{\mathbf{n}_z})$, respectively. With the objective of maximizing the secrecy rates, the precoded signal is constructed as

$$\mathbf{x} = \mathbf{P}_D\mathbf{s} + \mathbf{P}_{AN}\mathbf{u}, \tag{3.3}$$

where $\mathbf{P}_D \in \mathbb{C}^{N_t \times N_t}$ is the data precoder matrix and $\mathbf{s} \in \mathbb{C}^{N_t \times 1}$ is the transmitted signal vector with zero mean and identity covariance matrix. Each element of $\mathbf{s}$ is drawn equiprobably from an M-ary signal constellation. $\mathbf{P}_{AN}$ denotes the artificial noise precoder matrix.

It is assumed that both the legitimate receiver and the eavesdropper know their own channels perfectly. We model the eavesdropper's channel as a doubly correlated fading MIMO channel, namely,

$$\mathbf{H}_e = \mathbf{\Psi}_{re}^{1/2}\hat{\mathbf{H}}_e\mathbf{\Psi}_{te}^{1/2}, \tag{3.4}$$

where $\mathbf{\Psi}_{re}$ and $\mathbf{\Psi}_{te}$ are the receive and transmit correlation matrices, respectively. $\hat{\mathbf{H}}_e$ is a complex matrix with i.i.d. zero mean unit variance circularly symmetric complex Gaussian entries. We assume that statistical ECSI is available at the transmitter. Specifically, the transmitter is assumed to know the correlation matrices $\mathbf{\Psi}_{re}$ and $\mathbf{\Psi}_{te}$ and the noise variance at the eavesdropper.

Regarding MCSI at the transmitter, we consider two scenarios:

- **Perfect MCSI is available at the transmitter:** In this case, we assume that the elements of the channel matrix $\mathbf{H}_b$ are unit variance i.i.d. circularly symmetric complex Gaussian, i.e., $\mathcal{CN}(0,1)$, and the transmitter knows the realizations of the main channel. Under this CSI assumption, the ergodic secrecy rate is given by

$$\bar{R}_s = \mathbb{E}_{\mathbf{H}_b,\mathbf{H}_e}\Big\{\big[I(\mathbf{s};\mathbf{y}|\mathbf{H}_b) - I(\mathbf{s};\mathbf{z}|\mathbf{H}_e)\big]^+\Big\}, \tag{3.5}$$

  where $I(\mathbf{s};\mathbf{y}|\mathbf{H}_b)$ and $I(\mathbf{s};\mathbf{z}|\mathbf{H}_e)$ are the instantaneous mutual information terms over the main channel and the eavesdropper's channel, respectively.[1]

- **Statistical MCSI is available at the transmitter:** In this scenario, we assume that the main channel is doubly correlated and is modeled as

$$\mathbf{H}_b = \mathbf{\Psi}_{rb}^{1/2}\hat{\mathbf{H}}_b\mathbf{\Psi}_{tb}^{1/2}, \tag{3.6}$$

  where $\mathbf{\Psi}_{tb}$ and $\mathbf{\Psi}_{rb}$ are the corresponding transmit and receive correlation matrices. The transmitter is assumed to know these matrices as well as the noise variance at the legitimate receiver. In this case, the ergodic secrecy rates can be calculated as

$$\bar{R}_s = \Big[\mathbb{E}_{\mathbf{H}_b} I(\mathbf{s};\mathbf{y}|\mathbf{H}_b) - \mathbb{E}_{\mathbf{H}_e} I(\mathbf{s};\mathbf{z}|\mathbf{H}_e)\Big]^+. \tag{3.7}$$

In either of these two scenarios, our objective is to optimize the matrices $\mathbf{P}_D$ and $\mathbf{P}_{AN}$ such that the secrecy rate is maximized. In the following two sections, we formulate and tackle relevant optimization problems.

[1]This notation is different from the standard notation [53] (where $I(\mathbf{s};\mathbf{y}|\mathbf{H})$ stands for the mutual information averaged over $\mathbf{H}$). Here, $I(\mathbf{s};\mathbf{y}|\mathbf{H})$ refers to the instantaneous mutual information conditioned on the channel matrix $\mathbf{H}$.

3.2 Transmit Signal Design with Perfect MCSI

In this section, we assume that the transmitter has access to the channel coefficients of the legitimate receiver and knows the statistics of the eavesdropper's channel. Under this assumption, we propose different strategies for joint optimization of the precoder and artificial noise.

3.2.1 Related Works

Transmit signal design with perfect MCSI and statistical ECSI has been studied in [36] and [32]. In [36], the authors employ a naive beamforming along with artificial noise injection while considering single-antenna receivers. The strategy proposed in [32], on the other hand, relies on iterative maximization of an approximation to the instantaneous secrecy rate. In both of these studies, it has been shown that for maximizing secrecy rates at higher SNRs, it is desirable to allocate only a fraction of the total power for signal transmission and use the remaining power for artificial noise injection. In the remainder of this section we demonstrate that the strategies proposed in [32,36] are suboptimal. More specifically, we show that by jointly optimizing the precoder matrix and artificial noise, higher secrecy rates can be achieved compared to the case of optimization of the precoder matrix only, as done in [32, 36].

3.2.2 Problem Formulation

We consider two scenarios for injection of the artificial noise. First, we consider scenarios with $N_t > N_{r_b}$ where artificial noise is injected along the null space of the main channel with $\mathbf{P}_{AN} = \frac{\alpha_{AN}}{\sqrt{N_t - N_{r_b}}}\mathbf{V}_b$ where $\mathbf{V}_b \in \mathbb{C}^{N_t \times (N_t - N_{r_b})}$ stands for an orthonormal basis for the null space of $\mathbf{H}_b$ and $\mathbf{u}$ denotes the noise term which follows $\mathcal{CN}(0, \mathbf{I}_{N_t - N_{r_b}})$. The portion of the power assigned to the artificial noise is determined by the coefficient α_{AN}. For the scenarios with $N_t \leq N_{r_b}$, in subsection 3.2.6, we consider a generalized artificial noise similar to [54] where $\mathbf{u}$

follows $\mathcal{CN}(0, \mathbf{I}_{N_t})$ and the covariance of the artificial noise $\mathbf{P}_{AN}\mathbf{u}$ is more general. We impose the power constraint

$$\mathrm{tr}(\mathbf{P}_D\mathbf{P}_D^H) + \mathrm{tr}(\mathbf{P}_{AN}\mathbf{P}_{AN}^H) \leq N_t. \tag{3.8}$$

The main user's and the eavesdropper's channels are both block fading. We assume that the channel gains are fixed during each coherence interval and they change independently from one coherence interval to the next. Furthermore, each coherence interval is large enough so that random coding arguments can be invoked, therefore an achievable ergodic secrecy rate can be calculated using (3.5). Irrespective of the precoder design approach, throughout the chapter, we assume that the precoding is adopted along with the random coding and the rate adaptation scheme proposed in [20]. Hence, the ergodic secrecy rates are evaluated using (3.5) the achievability proof of which follows from the proof given in Appendix B in [20].

3.2.3 Precoder and Artificial Noise Design

Let's now focus on the scenarios with $N_t > N_{r_b}$ where artificial noise is injected in the null-space of the main channel. Noting that $\mathbf{P}_{AN} = \frac{\alpha_{AN}}{\sqrt{N_t - N_{r_b}}}\mathbf{V}_b$, with the aid of the instantaneous knowledge of the main channel $\mathbf{H}_b$ and the statistical knowledge of the eavesdropper's channel, we seek to find the optimal $\mathbf{P}_D$ and α_{AN} which maximize the instantaneous secrecy rate given by

$$R_s = \mathbb{E}_{\mathbf{H}_e}\Big\{\big(I(\mathbf{s};\mathbf{y}|\mathbf{H}_b) - I(\mathbf{s};\mathbf{z}|\mathbf{H}_e)\big)^+\Big\}. \tag{3.9}$$

Noting that this is not tractable, we formulate a related optimization problem by considering a lower-bound on R_s, given by

$$R_{s,l} = I(\mathbf{s};\mathbf{y}|\mathbf{H}_b) - \mathbb{E}_{\mathbf{H}_e} I(\mathbf{s};\mathbf{z}|\mathbf{H}_e). \tag{3.10}$$

Therefore, we solve the following problem:

$$\max_{\mathbf{P}_D,\ \alpha_{AN}} \ R_{s,l} \tag{3.11}$$

$$\text{s.t.} \quad \mathrm{tr}(\mathbf{P}_D\mathbf{P}_D^H) + \alpha_{AN}^2 \leq N_t, \tag{3.12}$$

where "s.t." is short for "subject to."

As we will see later, the maximization of this lower-bound is tractable and its solution serves to increase R_s as evidenced by extensive simulations.

We introduce two approaches: the first approach relies on directly maximizing $R_{s,l}$ in (3.10) while the second approach utilizes a cut-off rate based approximation of $R_{s,l}$. After obtaining the optimal precoder matrix $\mathbf{P}_D$ and the artificial noise level α_{AN} from either of these schemes, we evaluate the ergodic secrecy rates using (3.5) to demonstrate the efficacy of the proposed solutions.

3.2.4 Direct Maximization of $R_{s,l}$

Due to the nonconvexity of the problem in (3.11)-(3.12), obtaining a globally optimal closed-form solution is intractable. However, it is possible to implement numerical algorithms which iteratively search for local maxima of the objective function. To solve for the precoder and artificial noise, we first optimize over $\mathbf{P}_D$ for a fixed α_{AN}. In this case, the optimization problem becomes

$$\max_{\mathbf{P}_D} \ (I(\mathbf{s};\mathbf{y}|\mathbf{H}_b) - \mathbb{E}_{\mathbf{H}_e} I(\mathbf{s};\mathbf{z}|\mathbf{H}_e)) \tag{3.13}$$

$$\text{s.t.} \quad \text{tr}(\mathbf{P}_D\mathbf{P}_D^H) \leq N_t - \alpha_{AN}^2, \tag{3.14}$$

where the instantaneous mutual information over the main channel is given by [55]

$$I(\mathbf{s};\mathbf{y}|\mathbf{H}_b) = N_t \log M - \frac{1}{M^{N_t}} \sum_{i=1}^{M^{N_t}} \mathbb{E}_{\mathbf{n}_y} \log \sum_{j=1}^{M^{N_t}} \exp\left(- \frac{\|\mathbf{H}_b\mathbf{P}_D\mathbf{d}_{ij} + \mathbf{n}_y\|^2 - \|\mathbf{n}_y\|^2}{\sigma_{\mathbf{n}_y}^2} \right), \tag{3.15}$$

with $\mathbf{d}_{ij} = \mathbf{s}_i - \mathbf{s}_j$, where $\mathbf{s}_i$ is one of the M^{N_t} possible input vectors for $\mathbf{s} \in \mathbb{C}^{N_t \times 1}$. To compute the second term in (3.13), we note that the received vector at the eavesdropper is given by

$$\mathbf{z} = \mathbf{H}_e\mathbf{P}_D\mathbf{s} + \mathbf{n}_z', \tag{3.16}$$

where $\mathbf{n}_z'$ is the summation of the artificial noise and the thermal noise. When $N_t > N_{r_b}$, the channel input is as given in (3.3), and we have $\mathbf{n}_z' = \alpha_{AN}\mathbf{W}\mathbf{u} + \mathbf{n}_z$

with $\mathbf{W} = \frac{1}{\sqrt{N_t - N_{r_b}}}\mathbf{H}_e\mathbf{V}_b$.

We consider two cases separately. When $N_{r_e} = 1$, $\mathbf{n}'_z$ is a Gaussian random variable and the average mutual information can be written as

$$\mathbb{E}_{\mathbf{H}_e} I(\mathbf{s};\mathbf{z}|\mathbf{H}_e) = N_t \log M - \frac{1}{M^{N_t}} \sum_{m=1}^{M^{N_t}} \mathbb{E}_{\mathbf{H}_e,\mathbf{n}'_z} \log \sum_{k=1}^{M^{N_t}} \exp\left(- \frac{\|\mathbf{H}_e\mathbf{P}_D\mathbf{d}_{mk} + \mathbf{n}'_z\|^2 - \|\mathbf{n}'_z\|^2}{\sigma^2_{\mathbf{n}'_z}} \right), \quad (3.17)$$

where $\sigma^2_{\mathbf{n}'_z} = \sigma^2_{\mathbf{n}_z} + \alpha^2_{AN}\mathbf{w}\mathbf{w}^H$ with $\mathbf{w} = \frac{1}{\sqrt{N_t - N_{r_b}}}\mathbf{h}_e\mathbf{V}_b$. If $N_{r_e} > 1$, $\mathbf{n}'_z$ becomes a zero-mean colored Gaussian noise vector with covariance matrix $\mathbf{K}_{\mathbf{n}'_z} = \mathbf{W}\mathbf{W}^H + \sigma^2_{\mathbf{n}_z}\mathbf{I}_{N_{r_e}}$. Therefore, in order to evaluate $\mathbb{E}_{\mathbf{H}_e} I(\mathbf{s};\mathbf{z}|\mathbf{H}_e)$, one can first whiten the noise term by pre-multiplying the received vector in (3.16) by $\mathbf{K}_{\mathbf{n}'_z}^{-\frac{1}{2}}$ resulting in

$$\mathbf{z}' = \mathbf{K}_{\mathbf{n}'_z}^{-\frac{1}{2}}\mathbf{H}_e\mathbf{P}_D\mathbf{s} + \mathbf{n}''_z, \quad (3.18)$$

where $\mathbf{n}''_z$ is a zero-mean additive white Gaussian noise vector with $\mathbf{K}_{\mathbf{n}''_z} = \mathbf{I}_{N_{r_e}}$, and using the expression

$$\mathbb{E}_{\mathbf{H}_e} I(\mathbf{s};\mathbf{z}'|\mathbf{H}_e) = N_t \log M - \frac{1}{M^{N_t}} \sum_{m=1}^{M^{N_t}} \mathbb{E}_{\mathbf{H}_e,\mathbf{n}''_z} \log \sum_{k=1}^{M^{N_t}} \exp\left(-\|\mathbf{K}_{\mathbf{n}'_z}^{-\frac{1}{2}}\mathbf{H}_e\mathbf{P}_D\mathbf{d}_{mk} + \mathbf{n}''_z\|^2 + \|\mathbf{n}''_z\|^2 \right), \quad (3.19)$$

which is equivalent to $\mathbb{E}_{\mathbf{H}_e} I(\mathbf{s};\mathbf{z}|\mathbf{H}_e)$ as the transformation is one-to-one. The necessary conditions for optimality of the precoder matrix for maximization of $R_{s,l}$ with perfect main channel CSI and statistical CSI of the eavesdropper can be obtained as follows.

Proposition 3. 1. *The solution of the optimization problem (3.13)-(3.14) satisfies the following optimality criteria:*

$$\frac{\log_2 e}{\sigma^2_{\boldsymbol{n}_y}} \left(\boldsymbol{H}_b^H \boldsymbol{H}_b \boldsymbol{P}_D \boldsymbol{\Delta}_b(\boldsymbol{P}_D) \right) - \frac{\log_2 e}{\sigma^2_{\boldsymbol{n}'_z}} \mathbb{E}_{\boldsymbol{H}_e} \left\{ \left(\boldsymbol{H}_e^H \boldsymbol{H}_e \boldsymbol{P}_D \boldsymbol{\Delta}_e(\boldsymbol{P}_D) \right) \right\} = \theta \boldsymbol{P}_D, \quad (3.20)$$

$$\theta \left(tr(\boldsymbol{P}_D \boldsymbol{P}_D^H) + \alpha^2_{AN} - N_t \right) = 0, \quad (3.21)$$

$$\theta \geq 0, \quad (3.22)$$

$$tr(\boldsymbol{P}_D \boldsymbol{P}_D^H) + \alpha^2_{AN} - N_t \leq 0, \quad (3.23)$$

where θ is the Lagrange multiplier corresponding to the constraint in (3.14) and $\boldsymbol{\Delta}_b(\boldsymbol{P}_D)$ and $\boldsymbol{\Delta}_e(\boldsymbol{P}_D)$ are the receive minimum mean square error (MMSE) matrices at the legitimate receiver and the eavesdropper, respectively, and are given by [56]

$$\boldsymbol{\Delta}_b(\boldsymbol{P}_D) = \mathbb{E}\big\{(\boldsymbol{s} - \mathbb{E}\{\boldsymbol{s}|\boldsymbol{y}\})(\boldsymbol{s} - \mathbb{E}\{\boldsymbol{s}|\boldsymbol{y}\})^H\big\}, \tag{3.24}$$

$$\boldsymbol{\Delta}_e(\boldsymbol{P}_D) = \mathbb{E}\big\{(\boldsymbol{s} - \mathbb{E}\{\boldsymbol{s}|\boldsymbol{z}\})(\boldsymbol{s} - \mathbb{E}\{\boldsymbol{s}|\boldsymbol{z}\})^H\big\}. \tag{3.25}$$

Proof. The proof follows from Karush-Kuhn-Tucker (KKT) analysis as given in Appendix A. □

In order to solve the optimization problem in (3.13)-(3.14), a gradient descent algorithm [57] can be employed. In this scheme, the precoder is updated as

$$\mathbf{P}_D(k+1) = \big[\mathbf{P}_D(k) + \mu \nabla_{\mathbf{P}_D} R_{s,l}(k)\big]^{\dagger}_{\mathrm{tr}(\mathbf{P}_D\mathbf{P}_D^H) \leq N_t - \alpha_{AN}^2}, \tag{3.26}$$

where k and μ are the iteration index and the step-size of the update, respectively, and $[.]^{\dagger}_{\mathrm{tr}(\mathbf{P}_D\mathbf{P}_D^H) \leq N_t - \alpha_{AN}^2}$ stands for the normalization which guarantees the feasibility of the solution at each step. More specifically, for cases where the updated precoder matrix $\hat{\mathbf{P}}_{D_k}$ does not satisfy the constraint in (3.14), similar to [56], we adopt a normalization as

$$\hat{\mathbf{P}}_{D_k} = \sqrt{(N_t - \alpha_{AN}^2)/\mathrm{tr}(\hat{\mathbf{P}}_{D_k}\hat{\mathbf{P}}_{D_k}^H)}\hat{\mathbf{P}}_{D_k}, \tag{3.27}$$

which projects the solution onto the feasible set. The optimality of the precoder matrix which is obtained as the solution of gradient descent search can be proved by showing that (3.20) holds for a fixed $\theta \geq 0$.

So as to obtain the optimal $(\alpha_{AN}, \mathbf{P}_D)$, namely, to solve (3.11)-(3.12), we repeat this gradient descent algorithm for different values of α_{AN} and select the best $(\alpha_{AN}, \mathbf{P}_D)$ pair as described in Algorithm 1. For each value of α_{AN}, the algorithm should be repeated with multiple initializations of $\mathbf{P}_D$ to increase the likelihood for the gradient descent algorithm to converge to the globally optimal solution.

Algorithm 1 Gradient Descent for Maximizing $R_{s,l}$

Consider different values for $\alpha_{AN} \in [0\ \sqrt{N_t}]$ **and for each value of** α_{AN}**, repeat**:
Step 1: Initialize $\mathbf{P}_{D_1}$ with constraint $\mathrm{tr}(\mathbf{P}_{D_1}\mathbf{P}_{D_1}^H) \leq N_t - \alpha_{AN}^2$. Set step size μ and min. tolerance μ_{min}
Step 2: Set $k = 1$, compute $R_{s_1} = R_{s,l}(\mathbf{P}_{D_1})$
Step 3: Compute $\nabla_{\mathbf{P}_D} R_{s,l}(\mathbf{P}_D)$
Step 4: If $\mu \geq \mu_{min}$ goto Step 5, otherwise Stop algorithm and return $\mathbf{P}_{D_k}$
Step 5: Calculate $\hat{\mathbf{P}}_{D_k} = \mathbf{P}_{D_k} + \mu \nabla_{\mathbf{P}_D} R_{s,l}(\mathbf{P}_{D_k})$ and if $\mathrm{tr}(\hat{\mathbf{P}}_{D_k}\hat{\mathbf{P}}_{D_k}^H) > N_t - \alpha_{AN}^2$, normalize as $\hat{\mathbf{P}}_{D_k} = \sqrt{\frac{N_t - \alpha_{AN}^2}{\mathrm{tr}(\hat{\mathbf{P}}_{D_k}\hat{\mathbf{P}}_{D_k}^H)}}\hat{\mathbf{P}}_{D_k}$
Step 6: Compute $\hat{R}_s = R_{s,l}(\hat{\mathbf{P}}_{D_k})$; If $\hat{R}_s \geq R_{s_k}$ update $R_{s_{k+1}} = \hat{R}_s$ and $\mathbf{P}_{D_{k+1}} = \hat{\mathbf{P}}_{D_k}$ & goto Step 7, otherwise, let $\mu = 0.5\mu$ and goto Step 4
Step 7: $k = k + 1$ goto Step 3
Select α_{AN} **and the corresponding optimal** $\mathbf{P}_D$ **which result in the maximum** $R_{s,l}$.

Note that the implementation of Algorithm 1 requires evaluation of the gradient of $R_{s,l}$ which is given by [56]

$$\nabla_{\mathbf{P}_D} R_{s,l}(\mathbf{P}_D) = \frac{\log_2 e}{\sigma_{\mathbf{n}_y}^2}\big(\mathbf{H}_b^H \mathbf{H}_b \mathbf{P}_D \boldsymbol{\Delta}_b(\mathbf{P}_D)\big) - \mathbb{E}_{\mathbf{H}_e}\left\{\frac{\log_2 e}{\sigma_{\mathbf{n}'_z}^2}\left(\mathbf{H}_e^H \mathbf{H}_e \mathbf{P}_D \boldsymbol{\Delta}_e(\mathbf{P}_D)\right)\right\}. \tag{3.28}$$

3.2.5 Cut-off Rate Based Approximation for $R_{s,l}$

The instantaneous and average mutual information terms in (3.10) lack closed-form expressions and involve multiple integrals. Specifically, computation of $R_{s,l}$ requires $2N_{r_e}(N_t + 1) + 2N_{r_b}$ integrals to be evaluated. Alternatively, to estimate $I(\mathbf{s}; \mathbf{y}|\mathbf{H}_b)$ and $\mathbb{E}_{\mathbf{H}_e} I(\mathbf{s}; \mathbf{z}|\mathbf{H}_e)$, one can take advantage of Monte Carlo methods, which require averaging over sufficiently large number of noise and channel samples, making it a computationally complex task.

So as to lower the computational complexity associated with the transmit signal design algorithm, closed form approximations of the mutual information can be employed [58, 59]. To this end, we propose to employ a cut-off rate based metric given by

$$R'_{s,l} = R_0^{(B)} - \bar{R}_0^{(E)}, \tag{3.29}$$

where $R'_{s,l}$ is an approximation of the instantaneous secrecy rate, with $R_0^{(B)}$ being the instantaneous cut-off rate for Bob, which is a valid lower-bound on the mutual information, given by [60]

$$R_0^{(B)} = 2N_t \log M - \log \sum_{i=1}^{M^{N_t}} \sum_{j=1}^{M^{N_t}} \exp\Bigg(- \frac{\mathbf{d}_{ij}^H \mathbf{P}_D^H \mathbf{H}_b^H \mathbf{H}_b \mathbf{P}_D \mathbf{d}_{ij}}{4\sigma_{\mathbf{n}_y}^2} \Bigg), \tag{3.30}$$

and $\bar{R}_0{}^{(E)}$ is the average cut-off rate over the eavesdropper's channel. The details of the derivation of $R_0^{(B)}$ is given in Appendix B. If $N_{r_e} = 1$,

$$\bar{R}_0{}^{(E)} = 2N_t \log M - \mathbb{E}_{\mathbf{H}_e} \log \sum_{m=1}^{M^{N_t}} \sum_{k=1}^{M^{N_t}} \exp\Bigg(- \frac{\mathbf{d}_{mk}^H \mathbf{P}_D^H \mathbf{H}_e^H \mathbf{H}_e \mathbf{P}_D \mathbf{d}_{mk}}{4\sigma_{\mathbf{n}'_z}^2} \Bigg), \tag{3.31}$$

where $\sigma_{\mathbf{n}'_z}^2 = \sigma_{\mathbf{n}_z}^2 + \alpha_{AN}^2 \mathbf{w}\mathbf{w}^H$. Similar to the average mutual information, $\bar{R}_0{}^{(E)}$ can also be evaluated for the scenarios with $N_{r_e} > 1$ after noise whitening as in (3.18) resulting in

$$\bar{R}_0{}^{(E)} = 2N_t \log M - \mathbb{E}_{\mathbf{H}_e} \log \sum_{m=1}^{M^{N_t}} \sum_{k=1}^{M^{N_t}} \exp\Bigg(- \frac{\mathbf{d}_{mk}^H \mathbf{P}_D^H \mathbf{H}_e^H \mathbf{K}_{\mathbf{n}'_z}^{-1} \mathbf{H}_e \mathbf{P}_D \mathbf{d}_{mk}}{4} \Bigg). \tag{3.32}$$

Note that $R'_{s,l}$ is not an achievable rate. However, as we will see later, it can be used as an effective design metric to obtain the precoder matrices. Once the solution for the transmit signal with this metric is obtained, the achievable secrecy rates are evaluated using (3.5).

In order to demonstrate that employing the cut-off rate based design metric in (3.29) instead of directly maximizing (3.10) can significantly reduce the computational complexity, we compare the matrix multiplication steps required for evaluation of $R_{s,l}$ and $R'_{s,l}$ in Table 3.1. We assume that N_{samp} is the number of sample points required for an accurate estimation of the expectation operators, $\mathbb{E}_{\mathbf{n}}$ and $\mathbb{E}_{\mathbf{H}_e}$. For instance, it can be observed through numerical experiments that a sufficiently accurate estimation of the average mutual information $\mathbb{E}_{\mathbf{H}_e} I(\mathbf{s}; \mathbf{z}|\mathbf{H}_e)$ requires averaging over at least $N_{\text{samp}} = 500$ realizations of noise and channel coefficients. Accordingly, Table 3.1 reveals that the computational complexity associated with calculation of $R'_{s,l}$ is considerably smaller than that of $R_{s,l}$. This can also be shown by comparing the CPU times required for evaluation

Table 3.1: The number of matrix multiplication steps required for calculation of the secrecy rate and its cut-off rate-based approximation.

$I(\mathbf{s};\mathbf{y}\|\mathbf{H}_b)$	$R_0^{(B)}$	$\mathbb{E}_{\mathbf{H}_e} I(\mathbf{s};\mathbf{z}\|\mathbf{H}_e)$	$\bar{R}_0{}^{(E)}$
$12M^{2N_t}N_{\text{samp}}$	$5M^{2N_t}$	$12M^{2N_t}N_{\text{samp}}^2$	$8M^{2N_t}N_{\text{samp}}$

of these metrics. As an example, for a $4\times 4\times 4$ wiretap channel with $M=2$ and $N_{\text{samp}}=500$, computation of $R_{s,l}$ and $R'_{s,l}$ takes 962.3693 and 0.6598 seconds, respectively, over an Intel Core-i7-4770, 3.4 GHz processor.

In order to maximize $R'_{s,l}$, we jointly optimize $\mathbf{P}_D$ and α_{AN} using Algorithm 1 by replacing $R_{s,l}$ with $R'_{s,l}$. Gradient of $R'_{s,l}$ is given in

$$\nabla_{\mathbf{P}_D} R'_{s,l}(\mathbf{P}_D) = \frac{1}{\kappa_b}\sum_{i=1}^{M^{N_t}M^{N_t}}\sum_{j=1}(\mathbf{H}_b^H\mathbf{H}_b\mathbf{P}_D\mathbf{d}_{ij}\mathbf{d}_{ij}^H)\exp\left(-\frac{\mathbf{d}_{ij}^H\mathbf{P}_D^H\mathbf{H}_b^H\mathbf{H}_b\mathbf{P}_D\mathbf{d}_{ij}}{4\sigma^2_{\mathbf{n}_y}}\right)$$
$$-\sum_{m=1}^{M^{N_t}M^{N_t}}\sum_{k=1}\mathbb{E}_{\mathbf{H}_e}\frac{1}{\kappa_e}(\mathbf{H}_e^H\mathbf{H}_e\mathbf{P}_D\mathbf{d}_{mk}\mathbf{d}_{mk}^H)\exp\left(-\frac{\mathbf{d}_{mk}^H\mathbf{P}_D^H\mathbf{H}_e^H\mathbf{H}_e\mathbf{P}_D\mathbf{d}_{mk}}{4\sigma^2_{\mathbf{n}'_z}}\right), \quad (3.33)$$

where

$$\kappa_b = 4\sigma^2_{\mathbf{n}_y}(\ln(2))\sum_{i'=1}^{M^{N_t}}\sum_{j'=1}^{M^{N_t}}\exp\left(-\frac{\mathbf{d}_{i'j'}^H\mathbf{P}_D^H\mathbf{H}_b^H\mathbf{H}_b\mathbf{P}_D\mathbf{d}_{i'j'}}{4\sigma^2_{\mathbf{n}_y}}\right), \quad (3.34)$$

and

$$\kappa_e = 4\sigma^2_{\mathbf{n}'_z}(\ln(2))\sum_{m'=1}^{M^{N_t}}\sum_{k'=1}^{M^{N_t}}\exp\left(-\frac{\mathbf{d}_{m'k'}^H\mathbf{P}_D^H\mathbf{H}_e^H\mathbf{H}_e\mathbf{P}_D\mathbf{d}_{m'k'}}{4\sigma^2_{\mathbf{n}'_z}}\right). \quad (3.35)$$

The details of this derivation are given in Appendix C.

For finite-alphabet inputs with equal SNR values at the legitimate receiver and the eavesdropper, a lower fraction of the power should be allocated to data transmission at higher SNRs [28], [36], [61]. This is due to the fact that, under finite-alphabet input constraints, transmission at full power for high SNRs allows the eavesdropper to acquire the maximum number of bits per channel use which results in zero secrecy. Hence, it is possible to limit the search space of the optimization in Algorithm 1 according to the SNR values. For higher SNRs, it is

reasonable to search among larger α_{AN} values, whereas, at low SNRs, the search should be carried out among α_{AN}'s near 0.

3.2.6 Generalized Artificial Noise-Aided Precoding

In the subsections 3.2.3–3.2.5, we introduced a precoder and artificial noise design algorithm in which the artificial noise is transmitted in conjunction with the information signal, and is designed to be orthogonal to the intended receiver in such a way that only the eavesdropper suffers a degradation in the receiver performance. However, such artificial noise injection is not applicable when the number of antennas at the legitimate receiver is greater than the number of transmit antennas (i.e., when the null space dimensionality is 0), hence, we need to seek an alternative approach.

For the cases with $N_t \leq N_{r_b}$, we employ a joint precoder and generalized artificial noise design scheme. The notion of generalized artificial noise has been proposed in [54]. Dissimilar to the conventional artificial noise which is only allowed to be transmitted in the null-space of $\mathbf{H}_b$, generalized artificial noise possesses a more flexible covariance matrix.

The received vectors at the legitimate receiver and the eavesdropper are given as

$$\mathbf{y} = \mathbf{H}_b\mathbf{P}_D\mathbf{s} + \mathbf{H}_b\mathbf{P}_{AN}\mathbf{u}' + \mathbf{n}_y, \tag{3.36}$$

$$\mathbf{z} = \mathbf{H}_e\mathbf{P}_D\mathbf{s} + \mathbf{H}_e\mathbf{P}_{AN}\mathbf{u}' + \mathbf{n}_z, \tag{3.37}$$

where $\mathbf{P}_{AN}$ is the $N_t \times N_t$ precoder matrix for the artificial noise signal and $\mathbf{u}'$ follows $\mathcal{CN}(0, \mathbf{I}_{N_t})$. The objective is to obtain optimal $\mathbf{P}_D$ and $\mathbf{P}_{AN}$ by solving the following problem

$$\max_{\mathbf{P}_D,\, \mathbf{P}_{AN}} R_{s,l} \tag{3.38}$$

$$\text{s.t.} \quad \text{tr}(\mathbf{P}_D\mathbf{P}_D^H) + \text{tr}(\mathbf{P}_{AN}\mathbf{P}_{AN}^H) \leq N_t, \tag{3.39}$$

where $R_{s,l}$ is given in (3.10). Since $\mathbf{n}'_y = \mathbf{H}_b\mathbf{P}_{AN}\mathbf{u}' + \mathbf{n}_y$ is colored with covariance $\mathbf{K}_{\mathbf{n}'_y} = \mathbf{H}_b\mathbf{P}_{AN}\mathbf{P}_{AN}^H\mathbf{H}_b^H + \sigma^2_{\mathbf{n}_y}\mathbf{I}_{N_{r_b}}$, the mutual information over the main channel

can be calculated after whitening the noise by pre-multiplying (3.36) by $\mathbf{K}_{\mathbf{n}'_y}^{-\frac{1}{2}}$, i.e., obtaining

$$\mathbf{y}'' = \mathbf{K}_{\mathbf{n}'_y}^{-\frac{1}{2}} \mathbf{H}_b \mathbf{P}_D \mathbf{s} + \mathbf{n}''_y, \tag{3.40}$$

where $\mathbf{n}''_y$ is a zero-mean AWGN with unit variance, resulting in

$$I(\mathbf{s}; \mathbf{y}''|\mathbf{H}_b) = N_t \log M - \frac{1}{M^{N_t}} \sum_{i=1}^{M^{N_t}} \mathbb{E}_{\mathbf{n}''_y} \log \sum_{j=1}^{M^{N_t}} \exp\Big(- \|\mathbf{K}_{\mathbf{n}'_y}^{-\frac{1}{2}} \mathbf{H}_b \mathbf{P}_D \mathbf{d}_{ij} + \mathbf{n}''_y\|^2 + \|\mathbf{n}''_y\|^2 \Big). \tag{3.41}$$

The expression for $\mathbb{E}_{\mathbf{H}_e} I(\mathbf{s}; \mathbf{z}|\mathbf{H}_e)$ is given in (3.19) where $\mathbf{K}_{\mathbf{n}'_z} = \mathbf{H}_e \mathbf{P}_{AN} \mathbf{P}_{AN}^H \mathbf{H}_e^H + \sigma^2_{\mathbf{n}_z} \mathbf{I}_{N_{r_e}}$.

In order to solve (3.38)-(3.39), we compute the Lagrangian of the problem as

$$L(\mathbf{P}_D, \mathbf{P}_{AN}, \lambda) = R_{s,l} + \lambda(N_t - \mathrm{tr}(\mathbf{P}_D \mathbf{P}_D^H) - \mathrm{tr}(\mathbf{P}_{AN} \mathbf{P}_{AN}^H)), \tag{3.42}$$

where λ is the Lagrange dual variable associated with the constraint in (3.39). For a fixed dual variable λ, the dual function is defined as

$$D(\lambda) = \max_{\mathbf{P}_D,\ \mathbf{P}_{AN}} L(\mathbf{P}_D, \mathbf{P}_{AN}, \lambda). \tag{3.43}$$

Then, the dual optimization problem can be written as

$$\min_{\lambda > 0} D(\lambda). \tag{3.44}$$

Noting that $D(\lambda)$ is a convex function in λ, we update the dual variable using the bisection method similar to [62]. That is to say, when the subgradient $\nabla D(\lambda) = N_t - \mathrm{tr}(\mathbf{P}_D \mathbf{P}_D^H) - \mathrm{tr}(\mathbf{P}_{AN} \mathbf{P}_{AN}^H)$ is positive, we decrease λ in the bisection method; otherwise, we increase it. Indeed, we can interpret λ in (3.42) as a price for power which should increase when the power constraint is exceeded, and it should decrease otherwise.

In order to maximize the Lagrangian for a fixed λ, we employ a coordinate descent algorithm which relies on updating $\mathbf{P}_D$ and $\mathbf{P}_{AN}$ in an alternating fashion as described in Algorithm 2. After obtaining the optimal λ, the corresponding $(\mathbf{P}_D, \mathbf{P}_{AN})$ pair is used as the precoders. Obtaining the optimal $\mathbf{P}_D$ with a fixed

$\mathbf{P}_{AN}$, and conversely, obtaining the optimal $\mathbf{P}_{AN}$ with a fixed $\mathbf{P}_D$ is carried out with the aid of gradient descent type solutions. Particularly, with a fixed $\mathbf{P}_{AN}$, the optimal $\mathbf{P}_D$ is obtained by using a similar procedure as described in steps 1 through 7 of Algorithm 1. In this case, the data precoder is updated as

$$\mathbf{P}_D(k+1) = \left[\mathbf{P}_D(k) + \mu \nabla_{\mathbf{P}_D} R_{s,l}(k)\right]^{\dagger}_{\mathrm{tr}(\mathbf{P}_D\mathbf{P}_D^H) \leq N_t - \mathrm{tr}(\mathbf{P}_{AN}\mathbf{P}_{AN}^H)}. \tag{3.45}$$

Similarly, with a fixed $\mathbf{P}_D$, the artificial noise precoder matrix $\mathbf{P}_{AN}$ is updated as

$$\mathbf{P}_{AN}(k+1) = \left[\mathbf{P}_{AN}(k) + \mu \nabla_{\mathbf{P}_{AN}} R_{s,l}(k)\right]^{\dagger}_{\mathrm{tr}(\mathbf{P}_{AN}\mathbf{P}_{AN}^H) \leq N_t - \mathrm{tr}(\mathbf{P}_D\mathbf{P}_D^H)}. \tag{3.46}$$

We note that these steps are considerably simplified by replacing the mutual information with the cut-off rate expression as an approximate solution. The cut-off rate based approximation of the instantaneous secrecy rates can be calculated after whitening the additive noise terms in (3.36) and (3.37). That is to say, $R_0^{(B)}$ and $\bar{R}_0^{(E)}$ are calculated for the equivalent channels in (3.40) and (3.18), respectively. The gradient of the cut-off rate based approximation, $R'_{s,l}$ with respect to $\mathbf{P}_D$ is attained by replacing $\mathbf{H}_b$ and $\mathbf{H}_e$ in (3.33)-(3.35) by $\mathbf{K}_{\mathbf{n}'_y}^{-\frac{1}{2}}\mathbf{H}_b$ and $\mathbf{K}_{\mathbf{n}'_z}^{-\frac{1}{2}}\mathbf{H}_e$, respectively.

By optimizing the matrix $\mathbf{P}_{AN}$, the transmitter can highly suppress the useful signal at the eavesdropper whereas the degradation over the main channel is kept at a limited level as will be further illustrated via examples. The convergence proofs for the Algorithms 1 and 2 are given in Appendix D. It should be

Algorithm 2 Alternating Optimization for Maximizing $R_{s,l}$

Initialize $\lambda_h > \lambda_l = 0$, $\mathbf{P}_D$, $\mathbf{P}_{AN}$ and the convergence criteria ϵ_L and ϵ_λ:
Step 1: update $\lambda = \frac{1}{2}(\lambda_l + \lambda_h)$
Step 2: repeat:
obtain optimal $\mathbf{P}_D$ with fixed $\mathbf{P}_{AN}$ using grad. desc. optimization
obtain optimal $\mathbf{P}_{AN}$ with fixed $\mathbf{P}_D$ using grad. desc. optimization
until: consecutive values of $L(\mathbf{P}_D, \mathbf{P}_{AN}, \lambda)$ differ by less than ϵ_L
Step 3: If $\mathrm{tr}(\mathbf{P}_D\mathbf{P}_D^H) + \mathrm{tr}(\mathbf{P}_{AN}\mathbf{P}_{AN}^H) < N_t$ then update $\lambda_h = \lambda$
If $\mathrm{tr}(\mathbf{P}_D\mathbf{P}_D^H) + \mathrm{tr}(\mathbf{P}_{AN}\mathbf{P}_{AN}^H) > N_t$ then update $\lambda_l = \lambda$
until: two consecutive values of λ differ by less than ϵ_λ.

noted that, since the problem in (3.38)-(3.39) is non-convex, there is no guarantee that there is no duality gap, however, as will be demonstrated using numerical examples in Section 3.2.8, the approach is highly effective.

3.2.7 Per-Group Precoding for Large MIMO Wiretap Channels

The proposed transmit signal design algorithm in Section 3.2.5 possesses a lower complexity with respect to directly maximizing the secrecy rates due to the elimination of the averaging over channel and noise samples. However, this may still be a complex task in evaluation of the mutual information and in obtaining the optimal precoder, especially when N_t is large. With this motivation, we now provide a transmit signal design algorithm which reduces the search space for the optimal precoder and the artificial noise, and hence the complexity.

The basic idea behind the proposed scheme is to decouple the data streams and the artificial noise over parallel equivalent subchannels towards the legitimate receiver and the eavesdropper, and accordingly reduce the dimensionality of the search space for the transmit signal optimization. More specifically, such a decoupling will allow us to group subchannels in pairs and design the precoder and the artificial noise for each pair separately. We note that the idea of per-group precoding has been recently proposed for capacity maximization in MIMO channels [63, 64] and for sum rate maximization of multiple access channels [65]. Here, we extend it to the case of MIMO wiretap channels.

In order to obtain a decoupled structure, we take advantage of GSVD of the pair $(\mathbf{H}_b, \mathbf{\Psi}_t^{1/2})$ which results in [3]

$$\mathbf{H}_b = \mathbf{U}_b \mathbf{\Sigma}_b [\mathbf{\Omega}^{-1} \ \mathbf{0}_{k \times N_t - k}] \mathbf{Q}^H, \tag{3.47}$$

$$\mathbf{\Psi}_t^{1/2} = \mathbf{U}_{\Psi_t} \mathbf{\Sigma}_{\Psi_t} [\mathbf{\Omega}^{-1} \ \mathbf{0}_{k \times N_t - k}] \mathbf{Q}^H, \tag{3.48}$$

where $\mathbf{U}_b \in \mathbb{C}^{N_{r_b} \times N_{r_b}}$, $\mathbf{U}_{\Psi_t} \in \mathbb{C}^{N_t \times N_t}$ and $\mathbf{Q} \in \mathbb{C}^{N_t \times N_t}$ are unitary matrices and $\mathbf{\Omega} \in \mathbb{C}^{k \times k}$ is a nonsingular matrix where $k = \text{rank}([\mathbf{H}_b^H \ \ \mathbf{\Psi}_t^H]^H)$. $\mathbf{\Sigma}_b$ and $\mathbf{\Sigma}_{\Psi_t}$ are

$N_{r_b} \times k$ and $N_t \times k$ matrices as[2]

$$\mathbf{\Sigma}_b = \begin{array}{c} \\ N_{r_b}-p-o \\ o \\ p \end{array} \begin{array}{c} \begin{array}{ccc} k-p-o & o & p \end{array} \\ \begin{bmatrix} \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{D}_b & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{I} \end{bmatrix} \end{array}, \tag{3.49}$$

$$\mathbf{\Sigma}_{\Psi_t} = \begin{array}{c} \\ N_t-p-o \\ o \\ p \end{array} \begin{array}{c} \begin{array}{ccc} k-p-o & o & p \end{array} \\ \begin{bmatrix} \mathbf{I} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{D}_{\Psi_t} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} \end{bmatrix} \end{array}, \tag{3.50}$$

where $p = \dim\left(\text{null}(\mathbf{H}_b)^{\perp} \cap \text{null}(\mathbf{\Psi}_t^{1/2})\right)$ and $o = \dim\left(\text{null}(\mathbf{H}_b) \cap \text{null}(\mathbf{\Psi}_t^{1/2})^{\perp}\right)$. $\mathbf{D}_b$ and $\mathbf{D}_{\Psi_t}$ are diagonal matrices with real and strictly positive entries. Also, by applying eigenvalue decomposition on $\mathbf{\Psi}_r^{1/2}$, we have

$$\mathbf{\Psi}_r^{1/2} = \mathbf{U}_{\Psi_r} \mathbf{\Sigma}_{\Psi_r} \mathbf{U}_{\Psi_r}^H, \tag{3.51}$$

where $\mathbf{U}_{\Psi_r}$ is a unitary matrix whose columns are eigenvectors of $\mathbf{\Psi}_r^{1/2}$, and $\mathbf{\Sigma}_{\Psi_r}$ represents a diagonal matrix whose diagonal entries are the eigenvalues of $\mathbf{\Psi}_r^{1/2}$. We now construct the channel input in (3.3) with the data and artificial noise precoder matrices of the following form

$$\mathbf{P}_D = \mathbf{QBP}_{Dg}, \tag{3.52}$$

$$\mathbf{P}_{AN} = \mathbf{QBP}_{ANg}, \tag{3.53}$$

where

$$\mathbf{B} = \begin{bmatrix} \mathbf{\Omega}_{k\times k} & \mathbf{0}_{l\times l} \\ \mathbf{0}_{l\times k} & \mathbf{0}_{l\times k} \end{bmatrix}, \tag{3.54}$$

where $l = N_t - k$. Hence, the received signal vector at the legitimate receiver is given by

$$\mathbf{y} = \mathbf{U}_b \mathbf{\Sigma}_b \begin{bmatrix} \mathbf{I}_{k\times k} & \mathbf{0}_{k\times l} \end{bmatrix} \left(\mathbf{P}_{Dg}\mathbf{s} + \mathbf{P}_{ANg}\mathbf{u}'\right) + \mathbf{n}_y, \tag{3.55}$$

By pre-multiplying (3.55) by $\mathbf{U}_b^H$, we obtain the following equivalent model

$$\tilde{\mathbf{y}} = \mathbf{\Sigma}_b \begin{bmatrix} \mathbf{I}_{k\times k} & \mathbf{0}_{k\times l} \end{bmatrix} \left(\mathbf{P}_{Dg}\mathbf{s} + \mathbf{P}_{ANg}\mathbf{u}'\right) + \tilde{\mathbf{n}}_y, \tag{3.56}$$

[2]The number of columns and rows of all the sub-matrices are shown explicitly in (3.49) and (3.50).

where $\tilde{\mathbf{n}}_y = \mathbf{U}_b^H \mathbf{n}_y$ which has the same statistics as $\mathbf{n}_y$. Clearly, this strategy converts the main channel to a diagonal MIMO channel. Similarly, we obtain an equivalent diagonal channel towards Eve. To do this, consider the received signal at the eavesdropper

$$\mathbf{z} = \mathbf{U}_{\Psi_r} \mathbf{\Sigma}_{\Psi_r} \mathbf{U}_{\Psi_r}^H \hat{\mathbf{H}}_e \mathbf{U}_{\Psi_t} \mathbf{\Sigma}_{\Psi_t} \Big[\mathbf{I}_{k\times k} \;\; \mathbf{0}_{k\times l} \Big] \big(\mathbf{P}_{Dg}\mathbf{s} + \mathbf{P}_{ANg}\mathbf{u}' \big) + \mathbf{n}_z'. \tag{3.57}$$

Pre-multiplying (3.57) by $\mathbf{U}_{\Psi_r}^H$ results in the following equivalent input-output relationship

$$\tilde{\mathbf{z}} = \mathbf{\Sigma}_{\Psi_r} \tilde{\mathbf{H}}_e \mathbf{\Sigma}_{\Psi_t} \Big[\mathbf{I}_{k\times k} \;\; \mathbf{0}_{k\times l} \Big] \big(\mathbf{P}_{Dg}\mathbf{s} + \mathbf{P}_{ANg}\mathbf{u}' \big) + \tilde{\mathbf{n}}_z, \tag{3.58}$$

where $\tilde{\mathbf{n}}_z = \mathbf{U}_{\Psi_r}^H \mathbf{n}_z$ and $\tilde{\mathbf{H}}_e = \mathbf{U}_{\Psi_r}^H \hat{\mathbf{H}}_e \mathbf{U}_{\Psi_t}$ have same statistics as $\mathbf{n}_z$ and $\hat{\mathbf{H}}_e$, respectively [58].

Proposition 3. 2. *(Taken from [63]) For large-dimensional set-ups, the mutual information corresponding to the virtual channel input-output relationship in (3.58) is approximated as*

$$\mathbb{E}_{\tilde{\boldsymbol{H}}_e} I(\boldsymbol{s}; \tilde{\boldsymbol{z}} | \tilde{\boldsymbol{H}}_e) \approx I(\boldsymbol{x}_{eq}; \boldsymbol{z}_{eq} | \sqrt{\mathbf{\Xi}}) + \log_2 \det(\boldsymbol{I}_{N_{r_e}} + \boldsymbol{R}_{eq}) - \gamma_{eq}\phi_{eq} \log e, \tag{3.59}$$

where $I(\boldsymbol{x}_{eq}; \boldsymbol{z}_{eq} | \sqrt{\mathbf{\Xi}})$ stands for the ergodic mutual information corresponding to the diagonal MIMO relationship

$$\boldsymbol{z}_{eq} = \mathbf{\Xi}^{1/2} \boldsymbol{x}_{eq} + \tilde{\boldsymbol{n}}_z, \tag{3.60}$$

with $\boldsymbol{x}_{eq} = \boldsymbol{P}_{Dg}\boldsymbol{s} + \boldsymbol{P}_{ANg}\boldsymbol{u}'$ and $\mathbf{\Xi}^{1/2}$ is a diagonal matrix which is a function of three auxiliary variables, $\boldsymbol{R}_{eq}$, γ_{eq} and ϕ_{eq} which are the solutions of the following coupled equations:

$$\mathbf{\Xi} = \gamma_{eq} \mathbf{\Sigma}_{\Psi_t}^2, \tag{3.61}$$

$$\boldsymbol{R}_{eq} = \phi_{eq} \mathbf{\Sigma}_{\Psi_r}^2, \tag{3.62}$$

$$\gamma_{eq} = tr((\boldsymbol{I}_{N_{r_e}} + \boldsymbol{R}_{eq})^{-1} \mathbf{\Sigma}_{\Psi_r}^2), \tag{3.63}$$

$$\phi_{eq} = tr(\mathbf{\Gamma}_{eq} \mathbf{\Sigma}_{\Psi_t}^2), \tag{3.64}$$

where $\mathbf{\Gamma}_{eq} = \mathbb{E}\big\{ (\boldsymbol{s} - \mathbb{E}\{\boldsymbol{s}|\boldsymbol{z}_{eq}\})(\boldsymbol{s} - \mathbb{E}\{\boldsymbol{s}|\boldsymbol{z}_{eq}\})^H \big\}$ is the MMSE matrix corresponding to channel (3.60).

Using this result, we focus on the received vectors, $\tilde{\mathbf{y}}$ and $\mathbf{z}_{eq}$ given in (3.56) and (3.60), respectively, and design precoders which can partition the multi-antenna wiretap channel into a number of independent groups. More specifically, by employing precoders in (3.52) with $\mathbf{P}_{D,g}$ and $\mathbf{P}_{AN,g}$ taking the following form

$$\begin{bmatrix} P_{11} & P_{12} & 0 & 0 & \dots & 0 \\ P_{21} & P_{22} & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & \dots & P_{(N_t-1)(N_t-1)} & P_{(N_t-1)N_t} \\ 0 & 0 & \dots & \dots & P_{N_t(N_t-1)} & P_{N_tN_t} \end{bmatrix}, \tag{3.65}$$

we obtain two-by-two paired transmitted data streams. With this structure, the m^{th} data stream is transmitted along the $(2m-1)^{th}$ and $(2m)^{th}$ diagonal entries of $\mathbf{\Sigma}_b$ and $\mathbf{\Xi}^{1/2}$. Hence, we have

$$\tilde{\mathbf{y}}_m = \mathbf{\Sigma}_b \Big[\mathbf{I}_{k\times k} \quad \mathbf{0}_{k\times l} \Big] \big(\mathbf{P}_{Dg_m}\mathbf{s} + \mathbf{P}_{ANg_m}\mathbf{u}' \big) + \tilde{\mathbf{n}}_{y_m}, \tag{3.66}$$

$$\mathbf{z}_{eq_m} = \mathbf{\Xi}^{1/2} \big(\mathbf{P}_{Dg}\mathbf{s} + \mathbf{P}_{ANg}\mathbf{u}' \big) + \tilde{\mathbf{n}}_{z_m}, \tag{3.67}$$

$$\mathbf{P}_{Dg_m} = \begin{bmatrix} P_{D,(2m-1)(2m-1)} & P_{D,(2m-1)(2m)} \\ P_{D,(2m)(2m-1)} & P_{D,(2m)(2m)} \end{bmatrix}, \tag{3.68}$$

$$\mathbf{P}_{ANg_m} = \begin{bmatrix} P_{AN,(2m-1)(2m-1)} & P_{AN,(2m-1)(2m)} \\ P_{AN,(2m)(2m-1)} & P_{AN,(2m)(2m)} \end{bmatrix}, \tag{3.69}$$

where $m = 1, 2, \dots, \frac{N_t}{2}$. Finally, we note that the transmit signal design algorithm proposed in Section 3.2.2 can be applied to each group, separately. This is to say, instead of the original optimization problem in (3.11)-(3.12), the following $N_t/2$ sub-problems can be solved.

$$\max_{\mathbf{P}_{Dg_m},\, \mathbf{P}_{ANg_m}} \quad \tilde{R}_{s_m}, \qquad m = 1, 2, \dots, \frac{N_t}{2} \tag{3.70}$$

$$\text{s.t.} \quad \text{tr}(\mathbf{P}'_{Dg_m}\mathbf{P}'^{H}_{Dg_m}) + \text{tr}(\mathbf{P}'_{ANg_m}\mathbf{P}'^{H}_{ANg_m}) \leq 2, \tag{3.71}$$

where $\mathbf{P}'_{Dg_m}$ is an $N_t \times N_t$ matrix as

$$\mathbf{P}'_{Dg_m} = \mathbf{QB} \begin{bmatrix} \mathbf{P}_{Dg_m} & \mathbf{0}_{2\times(N_t-2)} \\ \mathbf{0}_{(N_t-2)\times 2} & \mathbf{0}_{(N_t-2)\times(N_t-2)} \end{bmatrix}, \tag{3.72}$$

$$\mathbf{P}'_{ANg_m} = \mathbf{QB} \begin{bmatrix} \mathbf{P}_{ANg_m} & \mathbf{0}_{2\times(N_t-2)} \\ \mathbf{0}_{(N_t-2)\times 2} & \mathbf{0}_{(N_t-2)\times(N_t-2)} \end{bmatrix}, \tag{3.73}$$

and $\tilde{R}_{s_m}$ is the difference between the instantaneous mutual information of the m^{th} group in (3.66) and the approximation in (3.59) for the m^{th} group in (3.67). After obtaining $\mathbf{P}_{D,g}$ and $\mathbf{P}_{AN,g}$ we construct the precoder matrices $\mathbf{P}_D$ and $\mathbf{P}_{AN}$ using (3.52) and (3.53). If these matrices do not satisfy the power constraint $\mathrm{tr}(\mathbf{P}_D\mathbf{P}_D^H) + \mathrm{tr}(\mathbf{P}_{AN}\mathbf{P}_{AN}^H) \leq N_t$, we adopt normalizations similar to (3.27) so that $\mathrm{tr}(\mathbf{P}_D\mathbf{P}_D^H) + \mathrm{tr}(\mathbf{P}_{AN}\mathbf{P}_{AN}^H) = N_t$.

Taking advantage of the per-group precoding scheme considerably reduces the computational complexity associated with the evaluation of mutual information or the cut-off rate, and accordingly, it simplifies the transmit signal design. For example, consider a $4 \times 4 \times 4$ MIMO wiretap channel with QPSK inputs. Using the equivalent channels $\tilde{\mathbf{y}}$ and $\mathbf{z}_{eq}$ with precoders in the form of (3.65) reduces the computational complexity (roughly) by a factor of $\frac{4^{2\times 4}}{2\times 4^{2\times 2}} = 128$ [63].

Finally, we emphasize that while we only consider the case of two-by-two pairing of the data streams in (3.65), N_g-by-N_g coupling of the data streams with $N_g > 2$ is also possible and it is expected to improve the precoder performance (with an increase in complexity). Namely, there is a trade-off between performance and complexity where $N_g = N_t$ coincides with the case of complete search adopted in Sections 3.2.2 and 3.2.6.

3.2.8 Numerical Examples

In order to demonstrate the efficacy of the proposed signal design schemes, we provide several numerical examples. Throughout the simulations, equal noise levels are assumed at the legitimate receiver and the eavesdropper. The numerical results are provided for the scenarios with constant and fading main channels, separately. We set $\mu = 0.5$ and $\mu_{min} = 0.01$ in implementation of Algorithm 1, and we consider $\epsilon_L = \epsilon_\lambda = 0.01$ in execution of Algorithm 2.

Constant Main Channel: In this example, we assume that the main channel

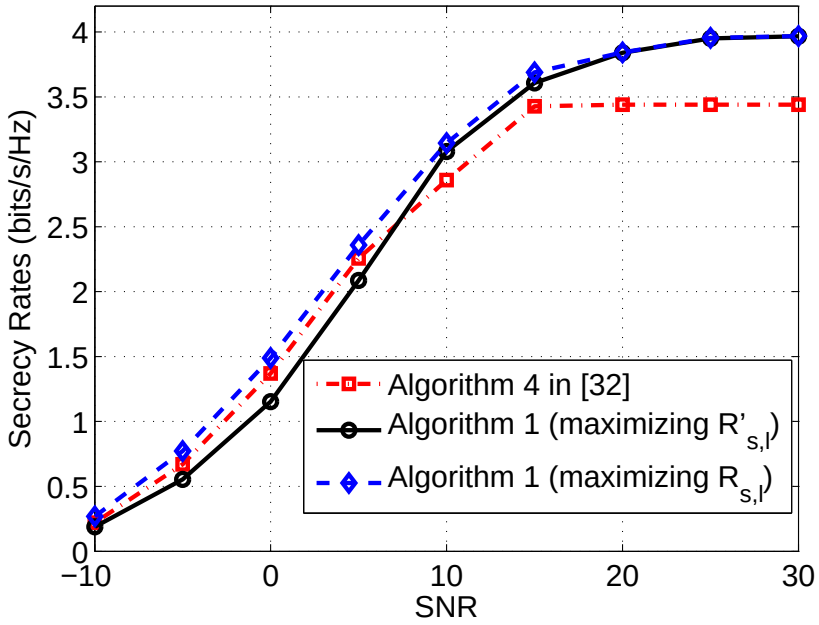

Figure 3.2: Secrecy rates with QPSK inputs for a wiretap channel with $(N_t, N_{r_b}, N_{r_e}) = (2, 1, 1)$ with the main channel given in (3.74) and the eavesdropper channel with $\rho_t = 0.9$ and $\rho_r = 1$.

is fixed throughout the whole transmission period and is given as

$$\mathbf{H}_b = \begin{bmatrix} 0.5128 - 0.3239j & -0.8903 - 0.0318j \end{bmatrix}. \tag{3.74}$$

We consider 500 realizations of $\mathbf{H}_e$ for evaluation of the average mutual information for the eavesdropper and calculate the secrecy rate using (3.9). The eavesdropper's channel is assumed to be correlated according to (3.4) where $\mathbf{\Psi}_t$ and $\mathbf{\Psi}_r$ have exponentially decaying entries, i.e.,

$$[\mathbf{\Psi}_t]_{ij} = \rho_t^{|i-j|}, \quad \text{and} \quad [\mathbf{\Psi}_r]_{ij} = \rho_r^{|i-j|}, \tag{3.75}$$

with $\rho_t = 0.9$ and $\rho_r = 1$.

Fig. 3.2 compares the ergodic secrecy rates for the three different transmit signal design algorithms. In implementation of Algorithm 1, we perform the search among 5 different values of α_{AN} which are selected according to the SNR values and for each value of α_{AN}, we repeat the algorithm for 4 different initialization

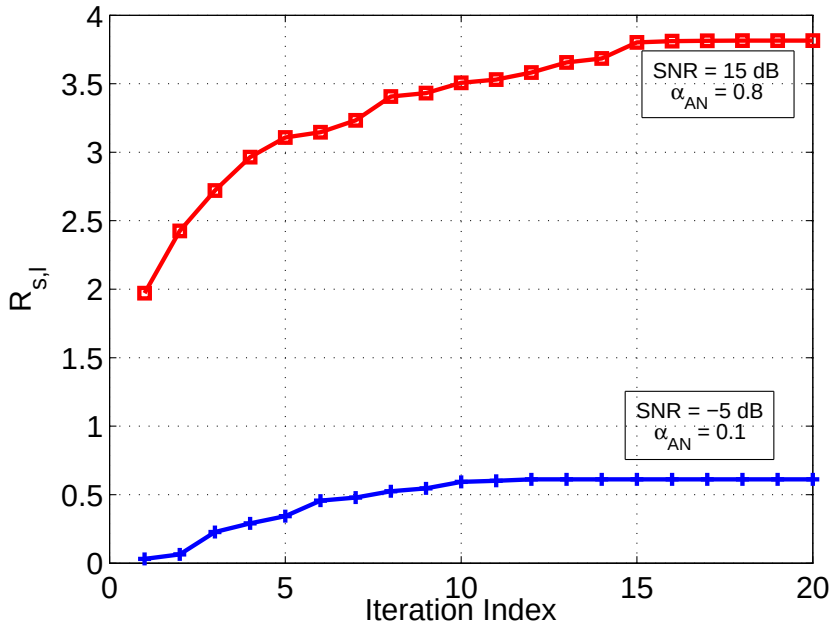

Figure 3.3: Convergence of Algorithm 1 for the same setting as Fig. 3.2.

of $\mathbf{P}_D$. For a fair comparison, we run the algorithm proposed in [32] with 20 initializations. We observe that the maximization of $R_{s,l}$ while jointly optimizing the precoder matrix and the power allocated to the artificial noise, i.e., employing Algorithm 1, yields higher secrecy rates compared to the scheme given in [32] which relies on the precoder optimization only. Furthermore, it can be inferred from Fig. 3.2 that the maximization of the cut-off rate based design metric $R'_{s,l}$ using Algorithm 1 incurs a relatively small loss with respect to the scheme proposed in [32] in low and moderate SNR values. While it is only approximate, the proposed algorithm even outperforms the algorithm in [32] in high SNRs due to the joint optimization of the precoder and artificial noise. We also note that, the cut-off rate based optimization undergoes a loss of 28% and 2% in the achievable secrecy rates at SNR $= -5$ dB and at SNR $= 10$ dB, respectively, and it achieves almost the same performance as the direct maximization method at high SNRs. This comparable performance is achieved with a much lower computational complexity, e.g., for this example, the CPU times is reduced roughly by a factor of 1000.

Fig. 3.3 illustrates the convergence behavior of Algorithm 1 for given values of α_{AN} in different SNRs. Values of $R_{s,l}$ is depicted in each iteration and it can be observed that the proposed algorithm needs only a few iterations to converge. The final output of Algorithm 1 in these examples are as follows. At SNR $= -5$dB, with $\alpha_{AN} = 0.1$,

$$\mathbf{P}_{D_1} = \begin{bmatrix} -0.1438 - 0.8947j & 0.0509 + 0.1416j \\ 0.4118 + 0.9718j & -0.0950 - 0.1522j \end{bmatrix}, \tag{3.76}$$

and at SNR $= 15$dB, the algorithm converges to

$$\mathbf{P}_{D_2} = \begin{bmatrix} 0.3124 - 0.2078j & -0.6076 + 0.4017j \\ -0.2857 + 0.2432j & 0.5536 - 0.4914j \end{bmatrix}, \tag{3.77}$$

with $\alpha_{AN} = 0.8$. The (local) optimality of these results is verified by showing that (3.20) holds as

$$\nabla R_{s,l}(\mathbf{P}_{D_1}) \simeq \theta_1 \mathbf{P}_{D_1}, \quad \nabla R_{s,l}(\mathbf{P}_{D_2}) \simeq \theta_2 \mathbf{P}_{D_2}, \tag{3.78}$$

with $\theta_1 = 0.15$ and $\theta_2 = 0.22$, respectively.

Fading Main Channel: We now consider fading channels towards the legitimate receiver and the eavesdropper. In particular, we assume that the channel gains over both links change independently from one coherence interval to the next and accordingly, optimal $\mathbf{P}_D$ and α_{AN} (or $\mathbf{P}_{AN}$ when employing Algorithm 2) are obtained for each realization of $\mathbf{H}_b$ with the aid of the cut-off rate based approximations and the secrecy rate is averaged over 500 realizations according to (3.5). The eavesdropper's channel is assumed to be correlated as in (3.4) where the transmit and receive correlations follow (3.75).

Fig. 3.4 compares the secrecy rates achieved by transmissions with different channel inputs under two different correlation scenarios for the eavesdropper's channel. We observe that, when the SNR is sufficiently high, the proposed transmit signal design scheme provides achievable secrecy rates close to $N_t \log M$, i.e., the maximum rate which can be attained by the legitimate receiver assuming finite-alphabet inputs. As expected, higher secrecy rates are attained when the eavesdropper's channel is highly correlated. It is also observed that the achievable

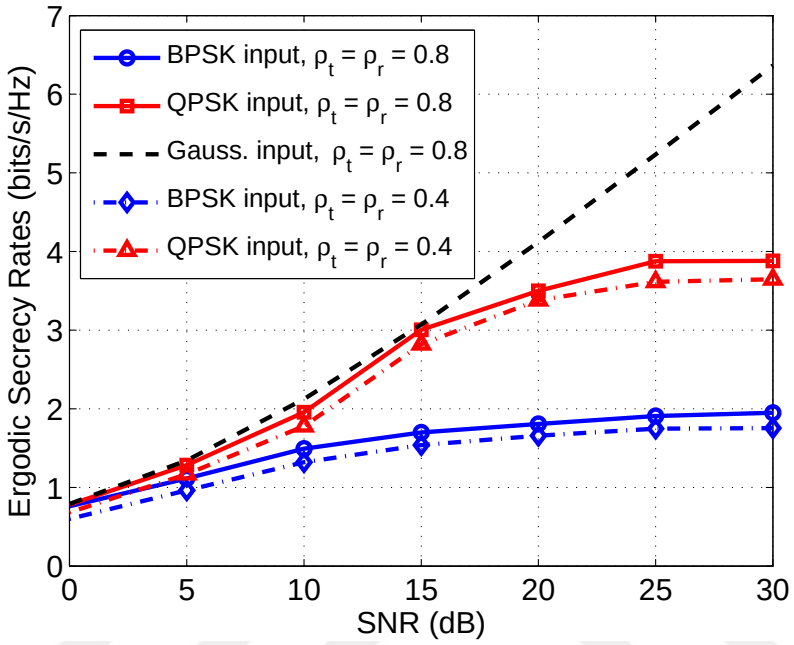

Figure 3.4: Achievable secrecy rates for fading main channel, with different values of M ($N_t = 2$ and $N_{r_e} = N_{r_b} = 1$).

secrecy rates increase with M for a fixed number of transmit and receive antennas. Furthermore, Fig. 3.4 reveals an important difference between the secrecy behavior of the Gaussian vs. finite alphabet inputs. That is, while the achievable secrecy rates with Gaussian inputs increase monotonically with increasing SNR, it saturates for the latter scenario.

The effect of different number of receive antennas on the achievable secrecy rates is demonstrated in Fig. 3.5. The eavesdropper's channel is correlated with correlation matrices given in (3.75) with $\rho_t = 0.8$ and $\rho_r = 0.8$. Clearly, the proposed transmit signal design scheme is capable of providing positive secrecy rates even for the cases where the eavesdropper is equipped with a larger number of antennas than the legitimate receiver. Furthermore, it can be observed that increasing the number of receive antennas at the legitimate receiver results in increased achievable secrecy rates for fixed N_{r_e}. It should be noted that, for the case of $N_{r_b} = 4$, the generalized artificial noise-aided precoding provides higher

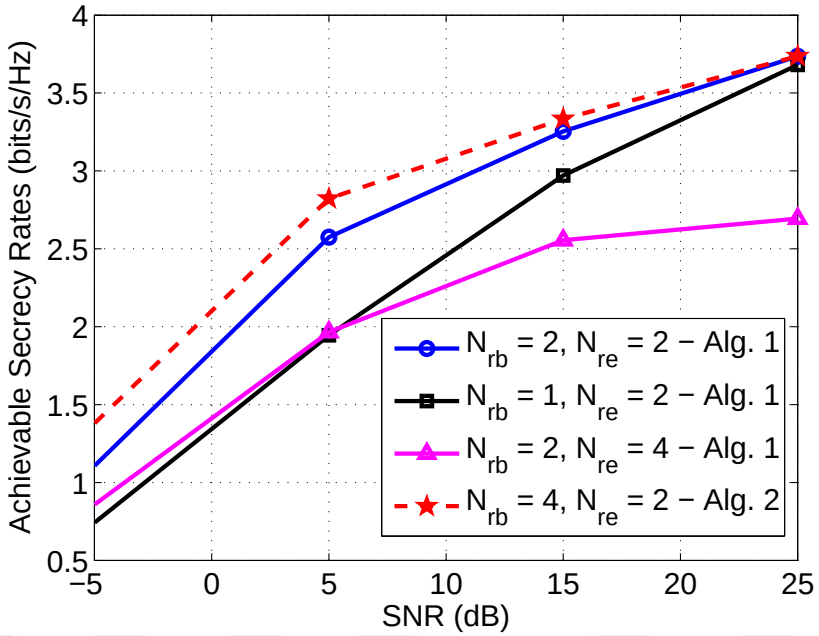

Figure 3.5: Ergodic Secrecy Rates with different number of antennas at the receiver ends ($N_t = 4$, BPSK inputs).

secrecy rates with respect to the cases with $N_{r_b} < 4$ in spite of a leakage of artificial noise at the legitimate receiver. We attribute this to the fact that the more flexible covariance matrix of the generalized artificial noise is more effective than the conventional artificial noise in terms of suppressing the reception at the eavesdropper. Furthermore, thanks to the optimization in Algorithm 2 the leakage of artificial noise at the legitimate receiver is small.

Fig. 3.6 compares the ergodic secrecy rates achieved with the proposed transmit signal design algorithms with and without per-group precoding. It can be inferred from this figure that the secrecy rates achieved by the solution of the relaxed problem undergoes a degradation with respect to the solution without per-group precoding. However, the considerably lower complexity of the per-group precoding technique makes possible obtaining suboptimal data and artificial noise precoding matrices for large set-ups which is intractable by directly employing Algorithms 1 and 2.

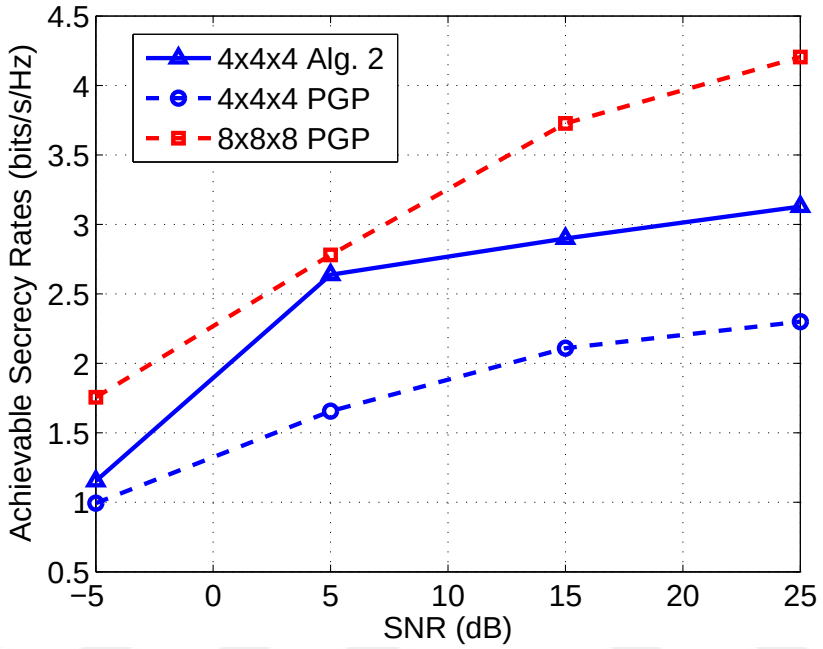

Figure 3.6: Ergodic secrecy rates for BPSK inputs using Algorithm 2 with and without per-group precoding.

3.3 Transmit Signal Design with Statistical MCSI

In this section, we focus on the scenarios where the transmitter is unable to track the instantaneous MCSI, and the transmit and receive correlation matrices are the only CSI available at the transmitter. In this section, both the main and the eavesdropper's channels are modeled as doubly correlated, and the transmit signal design approaches proposed in Section 3.2 are extended to this scenario.

3.3.1 Related Works

A common assumption in many of the studies in the literature of physical layer security is that the transmitter is capable of estimating at least the instantaneous

main channel coefficient. Only a few articles have studied the scenarios where transmitter knows the statistics of the channels only. In [41], it has been shown that when the eavesdropper and legitimate channels have i.i.d. Gaussian entries with zero-mean and unit-variance, a circularly symmetric Gaussian input with diagonal covariance is optimal. Furthermore, [66] and [42] propose upper-bounds on the secrecy capacity with statistical CSIT for fast fading MIMOME and MISOSE wiretap channels, respectively. These upper-bounds are derived by forming degraded wiretap channels and by considering an equivocation constraint which is less stringent than the weak secrecy constraint [1]. Similar to [41], the optimal channel input in the set-ups considered in [66] and [42] is proved to be Gaussian without prefixing.

While the aforementioned studies consider i.i.d. entries for $\mathbf{H}_b$ and $\mathbf{H}_e$, in [21], the authors study MISOSE setup where the channel coefficients corresponding to different transmit-receive antenna pairs are statistically correlated. The optimal input covariance in this scenario has been proved to have the same eigenvectors as the main channel covariance. In [67], Girnyk *et al.* propose sub-optimal algorithms for obtaining optimal covariance matrix for MIMOME channels with transmit correlation.

All the studies above are under Gaussian input assumption. Under finite-alphabet input constraint, however, the only existing results, to the best of our knowledge, have been reported in [43] where the authors have characterized the achievable secrecy rates over a degraded MIMO wiretap channel with QPSK inputs. The results in [43] once again demonstrate the behavioral differences between Gaussian and finite-alphabet inputs over MIMO wiretap channels.

3.3.2 Problem Formulation

Given that the transmitter knows the correlation matrices $\mathbf{\Psi}_{tb}$, $\mathbf{\Psi}_{te}$, $\mathbf{\Psi}_{rb}$, $\mathbf{\Psi}_{re}$ and the noise variances at the receivers, our first objective is to obtain the precoder matrix (in absence of artificial noise, i.e., $\mathbf{P}_{AN} = 0$) which is the optimizer of the

following problem

$$\max_{\mathbf{P}_D} R_{s,l} \tag{3.79}$$

$$\text{s.t.} \quad \text{tr}(\mathbf{P}_D \mathbf{P}_D^H) \leq N_t, \tag{3.80}$$

where $R_{s,l}$ is a lower bound on the ergodic secrecy rates given by

$$R_{s,l} = \mathbb{E}_{\mathbf{H}_b} I(\mathbf{s}; \mathbf{y}|\mathbf{H}_b) - \mathbb{E}_{\mathbf{H}_e} I(\mathbf{s}; \mathbf{z}|\mathbf{H}_e). \tag{3.81}$$

Although in the scenarios with i.i.d. channel coefficients injecting artificial noise with statistical CSIT is a waste of power [68], for the case of doubly correlated channels, injecting artificial noise at a specific direction might result in a less degradation over the main channel than the eavesdropper. To investigate the possible advantages of artificial noise injection, we also tackle the following joint optimization

$$\max_{\mathbf{P}_D,\ \mathbf{P}_{AN}} R_{s,l} \tag{3.82}$$

$$\text{s.t.} \quad \text{tr}(\mathbf{P}_D \mathbf{P}_D^H) + \text{tr}(\mathbf{P}_{AN} \mathbf{P}_{AN}^H) \leq N_t, \tag{3.83}$$

where $R_{s,l}$ is as given in (3.81).

3.3.3 Precoder Optimization

We note that the problem in (3.79)-(3.80) is a non-convex optimization problem similar to the one given in (3.13)-(3.14). In order to obtain optimal $\mathbf{P}_D$, we take advantage of a gradient descent based optimization similar to Algorithm 1. In this scheme, the precoder is updated as

$$\mathbf{P}_{D_{k+1}} = \left[\mathbf{P}_{D_k} + u \nabla_{\mathbf{P}_D} R_{s,l}\right]^{\dagger}_{\text{tr}(\mathbf{P}_D \mathbf{P}_D^H) \leq N_t}, \tag{3.84}$$

where k and u are the iteration index and the step-size of the update, respectively, and $[.]^{\dagger}_{\text{tr}(\mathbf{P}_D \mathbf{P}_D^H) \leq N_t}$ stands for the normalization which guarantees the feasibility of the solution at each step. More specifically, for cases where the updated precoder matrix $\hat{\mathbf{P}}_{D_k}$ does not satisfy the constraint in (3.80), similar to [56], we adopt a

normalization as $\hat{\mathbf{P}}_{D_k} = \sqrt{N_t/\mathrm{tr}(\hat{\mathbf{P}}_{D_k}\hat{\mathbf{P}}_{D_k}^H)}\hat{\mathbf{P}}_{D_k}$, which projects the solution onto the feasible set. In order to evaluate the gradient of $R_{s,l}$, we use the results in [56] to obtain

$$\nabla_{\mathbf{P}_D} R_{s,l} = \mathbb{E}_{\hat{\mathbf{H}}_b}\left\{\frac{\log_2 e}{\sigma^2_{\mathbf{n}_y}}\big(\mathbf{H}_b^H\mathbf{H}_b\mathbf{P}_D\boldsymbol{\Delta}_b(\mathbf{P}_D)\big)\right\} - \mathbb{E}_{\hat{\mathbf{H}}_e}\left\{\frac{\log_2 e}{\sigma^2_{\mathbf{n}'_z}}\left(\mathbf{H}_e^H\mathbf{H}_e\mathbf{P}_D\boldsymbol{\Delta}_e(\mathbf{P}_D)\right)\right\}, \quad (3.85)$$

where $\boldsymbol{\Delta}_b(\mathbf{P}_D)$ and $\boldsymbol{\Delta}_e(\mathbf{P}_D)$ are the MMSE matrices corresponding to estimation of $\mathbf{s}$ upon the observations at the legitimate receiver and the eavesdropper which are given by (3.24) and (3.25).

3.3.4 Joint Precoder and Artificial Noise Optimization

So as to solve (3.82)-(3.83), we employ a joint precoder and artificial noise optimization scheme. Since the instantaneous CSI of the main channel is not known at the transmitter, it is not possible to inject artificial noise in the null-space of $\mathbf{H}_b$. Therefore, we consider injection of a generalized artificial noise which is allowed to be transmitted in all directions spanned by $\mathbf{H}_b$ [54], and we take advantage of Algorithm 2 to obtain the optimal pair of data and artificial noise precoders, which maximize the ergodic secrecy rate.

Particularly, we assume that Alice transmits a signal as

$$\mathbf{x} = \mathbf{P}_D\mathbf{s} + \mathbf{P}_{AN}\mathbf{v}, \quad (3.86)$$

where $\mathbf{s}$ is the data signal and $\mathbf{v}$ stands for the artificial noise signal that follows $\mathcal{CN}(0, \mathbf{I}_{N_t})$. $\mathbf{P}_D$ and $\mathbf{P}_{AN}$ are the precoder matrices for the data and the artificial noise signals, respectively. Although this artificial noise degrades the reception both at the legitimate receiver and the eavesdropper, it is possible to optimize $\mathbf{P}_{AN}$ in a manner that the achievable rate at the eavesdropper is highly suppressed while the mutual information over the main channel undergoes less degradation.

3.3.5 Numerical Results

We now provide ergodic secrecy rates for the scenarios where the channel is driven by finite-alphabet inputs. To exemplify the results, we consider correlation matrices with exponentially decaying entries as $[\mathbf{\Psi}(\rho)]_{ij} = \rho^{|i-j|}$ with $\mathbf{\Psi}_{tb} = \mathbf{\Psi}(\rho_{tb})$, $\mathbf{\Psi}_{rb} = \mathbf{\Psi}(\rho_{rb})$, $\mathbf{\Psi}_{te} = \mathbf{\Psi}(\rho_{te})$ and $\mathbf{\Psi}_{re} = \mathbf{\Psi}(\rho_{re})$.

Fig. 3.7 depicts the ergodic secrecy rates with BPSK inputs over a MIMOME channel with $N_t = 4$, $N_{rb} = 4$ and $N_{re} = 2$. The proposed algorithms are shown to achieve positive ergodic secrecy rates at low and moderate SNRs. However, at high SNRs, under the finite-alphabet input constraint, secrecy rate drops to zero. This is in contrast to the scenarios with Gaussian signaling where achievable secrecy rates increase monotonically by increasing SNR (with $N_{rb} > N_{re}$, e.g., the results in Fig. 3.2).

We also observe that injection of artificial noise provides slight improvements in moderate to high SNR regions. This behavior is different from the cases with uncorrelated channels where injection of artificial noise with statistical CSI is a waste of power [68]. Fig. 3.7 also underlines the importance of availability of the main channel CSI at the transmitter. By jointly optimizing the precoder and the artificial noise using the knowledge of instantaneous CSI of the main channel, considerably higher secrecy rates are attained with respect to the transmit signal design with statistical CSI only. More specifically, in the presence of instantaneous CSI of the main channel, the transmitter is capable of injecting artificial noise in a more efficient manner where the noise leakage at the legitimate receiver is minimal (or zero when artificial noise is injected along null-space of the main channel). Therefore, at high SNRs, the transmitter allocates a considerable portion of the total power to artificial noise which efficiently suppresses the reception at the eavesdropper. However, when the instantaneous CSI of the main channel is not available, due to the leakage of artificial noise at the legitimate receiver, allocating a large portion of the total power to artificial noise does not help, and since at high SNRs the mutual information over both channels approach the saturation value of $N_t \log M$, ergodic secrecy rate drops to zero.

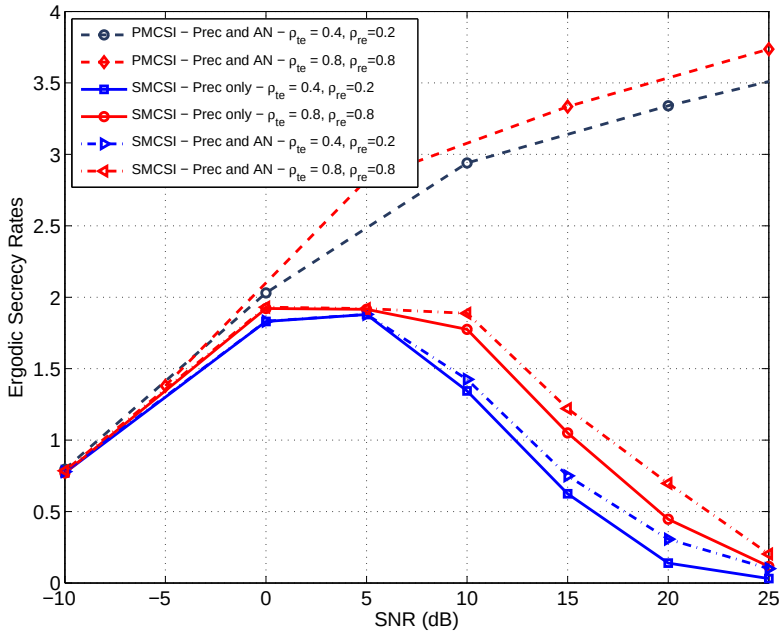

Figure 3.7: Ergodic secrecy rates for BPSK input with different transmit signal design approaches ($\rho_{tb} = 0.9$ and $\rho_{rb} = 0.6$). PMCSI and SMCSI stand for perfect and statistical MCSI, respectively.

3.4 Chapter Summary

In this chapter, we have proposed iterative joint precoder and artificial noise design schemes for maximization of ergodic secrecy rates over MIMO wiretap channels with finite-alphabet inputs under two different CSIT assumptions. We have shown that maximizing a cut-off rate based approximation of the instantaneous secrecy rate is a promising low-complexity alternative to the direct approach. We have also studied generalized artificial noise-aided precoding schemes for the scenarios with perfect MCSI where the dimensionality of the null-space of the main channel is zero as well as for the scenarios where main channel is only statistically known at the transmitter. Our findings demonstrate that the problem of precoder and artificial noise design is considerably simplified for large MIMO wiretap channels by two-by-two pairing of the transmit antennas and obtaining

the optimal solution for each pair, separately. Exemplary numerical results clearly show that the proposed transmit signal design methods provide positive secrecy rates in a variety of scenarios and yield an enhanced secrecy performance compared to the existing solutions in spite of their significantly lower computational complexities. Furthermore, our results underline the importance of availability of the main channel CSI at the transmitter. Injecting artificial noise with statistical CSI provides some improvements in the secrecy rate, however, it does not prevent secrecy rate from dropping to zero at high SNRs.

Chapter 4

Secure Wireless Information and Power Transfer with Constellation-Constrained Inputs

Simultaneous wireless information and power transfer (SWIPT) has been introduced as a promising solution for mitigating the energy scarcity in energy constrained networks. Despite various opportunities SWIPT provides for self-sustainability of the wireless communication systems, ensuring confidentiality of the transmitted data remains as a major concern. To overcome the above concern, many different solutions have been proposed (see [45] for a survey). Among these solutions, multiple-antenna techniques have been shown to exhibit a high potential for enhancing security in SWIPT systems. While the existing works all rely on Gaussian signaling, in this chapter, we focus on secure SWIPT under finite alphabet input constraint. We first review the existing results on the problem of secure transmission in absence of energy harvesting, and on maximizing harvested energy without a secrecy constraint under two different CSI assumptions. Then, we propose transmission algorithms, which achieve the trade-off between them.

4.1 Related Works

The secrecy rate of the SWIPT MIMO wiretap channel has been studied in [69] and [70]. In [69], the authors assume that the transmitter knows only the statistics of the channels, and after deriving an asymptotic expression for the ergodic secrecy rate, they obtain the optimal input structure, which achieves the trade-off between ergodic secrecy rate and harvested energy. On the other hand, the secrecy rates of MIMO SWIPT wiretap channels have been characterized in [70] under a global CSI assumption.

The aforementioned characterizations and designs rely on a Gaussian input assumption. However, practical communication systems employ discrete signaling and the channel inputs are drawn from standard constellations such as PSK and QAM. While the impact of finite-alphabet inputs on the trade-off between the mutual information of the IR and the harvested energy at the ER has been explored in [71], to the best of our knowledge, no study has been reported on secure SWIPT under the finite-alphabet input assumption, motivating the work in this chapter.

4.2 MISO SWIPT Wiretap Channels

In this section, we focus on a MISO SWIPT wiretap channel in which a multi-antenna transmitter with N_t antenna elements wishes to deliver its data to an intended single-antenna IR while transferring energy to a single-antenna ER, as depicted in Fig. 4.1. In the remainder of this section, we first provide the problem formulation, and then, we introduce a framework for transmit signal design under perfect and statistical ECSIT assumptions.

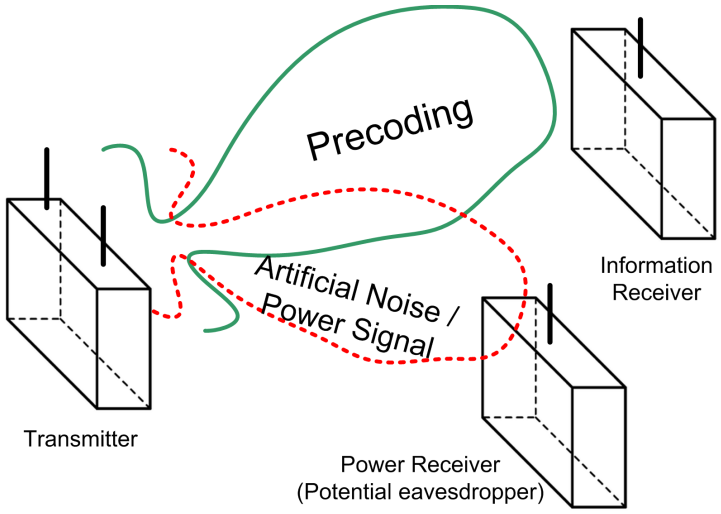

Figure 4.1: The system model.

4.2.1 System Model and Problem Formulation

For the setup under consideration, the received signals at the IR and the ER are given by

$$y = \sqrt{\gamma_y}\mathbf{h}^H\mathbf{x} + n_y, \tag{4.1}$$

$$z = \sqrt{\gamma_z}\mathbf{g}^H\mathbf{x} + n_z, \tag{4.2}$$

where the vectors $\mathbf{h}^H \in \mathbb{C}^{1\times N_t}$ and $\mathbf{g}^H \in \mathbb{C}^{1\times N_t}$ denote the channels corresponding to the IR and the ER, respectively. The distance-dependent path loss over these channels are represented by the coefficients γ_y and γ_z. The $N_t \times 1$ vector $\mathbf{x}$ is the channel input, and n_y and n_z stand for circularly symmetric complex AWGN terms, which follow $\mathcal{CN}(0, \sigma_{n_y}^2)$ and $\mathcal{CN}(0, \sigma_{n_z}^2)$, respectively.

Regarding the availability of the ECSI at the transmitter (ECSIT), we consider two scenarios. In the first case, perfect CSI on both channels is available at the transmitter, and we assume that the channels are independent Rayleigh fading, i.e., we model the channels using vectors, the elements of which are i.i.d. zero-mean and unit-variance circularly symmetric complex Gaussian random variables $\mathcal{CN}(0, 1)$. In the second case, perfect CSI of the channel towards the IR and statistical CSI of the ER's channel are available. In this case, we assume that

the IR's channel is an independent Rayleigh fading channel, however, a transmit correlation exists, namely [69]

$$\mathbf{g}^H = \hat{\mathbf{g}}^H \mathbf{\Psi}_t^{1/2}, \tag{4.3}$$

where $\hat{\mathbf{g}}$ is a complex vector with i.i.d. zero mean unit variance Gaussian entries, and $\mathbf{\Psi}_t$ is the correlation matrix, which can be acquired by the transmitter.

For both scenarios, it is assumed that the ER can act as a potential eavesdropper for the confidential data transmitted to the IR. Our objective is to maximize the number of bits transmitted to the IR while simultaneously guaranteeing that the ER is ignorant about the transmitted information and the harvested power of the ER is larger than a predefined value. The transmit signal is constructed as

$$\mathbf{x} = \mathbf{P}_D \mathbf{s} + \mathbf{u}, \tag{4.4}$$

where $\mathbf{s} \in \mathbb{C}^{N_t \times 1}$ is the information vector with zero mean and identity covariance matrix, the elements of which are assumed to be drawn from standard constellations such as PSK and QAM. $\mathbf{P}_D \in \mathbb{C}^{N_t \times N_t}$ denotes the data precoder matrix. $\mathbf{u}$ is a circularly symmetric complex Gaussian signal, which follows $\mathcal{CN}(0, \mathbf{K_u})$ playing the dual role of the artificial noise and the energy signal.

The IR's and the ER's channels are both ergodic. The channel gains are assumed to be fixed during each coherence interval while they change independently from one coherence interval to the next. Moreover, we assume that the coherence intervals are long enough so that random coding arguments can be invoked. Accordingly, an achievable ergodic secrecy rate is given by [20]

$$\bar{R}_s = \mathbb{E}_{\mathbf{h},\mathbf{g}} \Big\{ \big(I(\mathbf{s}; y|\mathbf{h}) - I(\mathbf{s}; z|\mathbf{g}) \big)^+ \Big\}, \tag{4.5}$$

where the mutual information over the IR's channel is given by

$$\begin{aligned} I(\mathbf{s}; y|\mathbf{h}) &= N_t \log M \\ &\quad - \frac{1}{M^{N_t}} \sum_{i=1}^{M^{N_t}} \mathbb{E}_{n_y} \left\{ \log \sum_{j=1}^{M^{N_t}} \exp \left(- \frac{\|\mathbf{h}^H \mathbf{P}_D \mathbf{d}_{ij} + n_y\|^2 - \|n_y\|^2}{\sigma_{n_y}^2 + \mathbf{h}^H \mathbf{K_u} \mathbf{h}} \right) \right\}, \end{aligned} \tag{4.6}$$

with $\mathbf{d}_{ij} = \mathbf{s}_i - \mathbf{s}_j$. The mutual information over the ER's channel, i.e., $I(\mathbf{s}; \mathbf{z}|\mathbf{g})$, can be calculated in exactly the same way. Average harvested energy at the ER is given by

$$\bar{E}_H = \epsilon\gamma_z \mathbb{E}_{\mathbf{g}}\{\mathbf{g}^H \mathbf{K}_{\mathbf{x}} \mathbf{g}\}, \tag{4.7}$$

where $\mathbf{K}_{\mathbf{x}}$ is the covariance matrix of the channel input $\mathbf{x}$. The constant ϵ in (4.7) denotes the energy conversion rate. For convenience, without loss of generality, we assume that $\epsilon = 1$ [69].

Throughout the chapter, we provide approaches for joint optimization of the precoder matrix $\mathbf{P}_D$ and the covariance matrix $\mathbf{K}_{\mathbf{u}} \in \mathbb{C}^{N_t \times N_t}$ such that the ergodic secrecy rate is maximized subject to a power constraint while guaranteeing that the harvested energy at the ER is larger than a given value. To do this, we utilize the lower bounds on the instantaneous secrecy rates under the perfect and statistical ECSIT given by

$$R_{s,l} = I(\mathbf{s}; y|\mathbf{h}) - I(\mathbf{s}; z|\mathbf{g}), \tag{4.8}$$

$$R'_{s,l} = I(\mathbf{s}; y|\mathbf{h}) - \mathbb{E}_{\mathbf{g}} I(\mathbf{s}; z|\mathbf{g}), \tag{4.9}$$

respectively. Under the full CSI assumption, we use the harvested power conditioned on $\mathbf{g}$, i.e.,

$$E_H = \gamma_z(\mathbf{g}^H \mathbf{P}_D \mathbf{P}_D^H \mathbf{g} + \mathbf{g}^H \mathbf{K}_{\mathbf{u}} \mathbf{g}), \tag{4.10}$$

as our design metric. It should be noted that in (4.10), $\mathbf{g}$ stands for the realization of the ER's channel. Then, the relevant optimization problem under perfect ECSIT becomes

$$\max_{\mathbf{P}_D,\, \mathbf{K}_{\mathbf{u}}} R_{s,l} \tag{4.11}$$

$$\text{s.t.} \quad \text{tr}(\mathbf{P}_D \mathbf{P}_D^H) + \text{tr}(\mathbf{K}_{\mathbf{u}}) \leq N_t P_{tx}, \tag{4.12}$$

$$\text{and} \quad E_H \geq E_0. \tag{4.13}$$

One may note that for particular realizations of the ER's channel, there might be no feasible solution (satisfying (4.13)) to the problem.

Similarly, under statistical ECSIT, the relevant optimization problem is defined

as

$$\max_{\mathbf{P}_D,\, \mathbf{K_u}} R'_{s,l} \tag{4.14}$$

$$\text{s.t.} \quad \text{tr}(\mathbf{P}_D\mathbf{P}_D^H) + \text{tr}(\mathbf{K_u}) \leq N_t P_{tx}, \tag{4.15}$$

$$\text{and} \quad \bar{E}_H \geq E_0, \tag{4.16}$$

where the constraint is on the average harvested power $\bar{E}_H$ given in (4.7).

4.2.2 Secrecy Rate-Harvested Energy Trade-off Under Perfect CSIT

In this subsection, we characterize the trade-off between the ergodic secrecy rate and the harvested energy for the scenarios with perfect CSIT. The assumption of availability of the perfect CSI of the ER at the transmitter is reasonable when the ER is a legitimate user of the network. After reviewing the solutions to the problems of maximizing the secrecy rates without considering the harvested energy constraint and also maximizing the harvested energy without taking into account the secrecy requirement, we introduce an iterative approach for solving the optimization problem in (4.11)-(4.13).

We define the signal $\mathbf{u}$ in (4.4) as

$$\mathbf{u} = \mathbf{P}_E\mathbf{u}_E, \tag{4.17}$$

where $\mathbf{P}_E \in \mathbb{C}^{N_t \times N_t}$ and $\mathbf{u}_E \sim \mathcal{CN}(0, \mathbf{I}_{N_t})$, and therefore, $\mathbf{K_u} = \mathbf{P}_E\mathbf{P}_E^H$, i.e., the optimization of the covariance matrix $\mathbf{K_u}$ reduces to the optimization of $\mathbf{P}_E$. In the following, we discuss the design of the $\mathbf{P}_D$ and $\mathbf{P}_E$ matrices for achieving secrecy rate-harvested energy trade-off.

Proposition 4.1. *[From [32]] Under the assumption that both receivers operate at high-SNR regime, with perfect CSIT, the maximum secrecy rate is achieved by data precoders in the following form*

$$\boldsymbol{P}_D = \boldsymbol{W}_g\tilde{\boldsymbol{P}}_D, \tag{4.18}$$

where $\boldsymbol{W}_g \in \mathbb{C}^{N_t \times N_t - 1}$ *is an orthonormal basis for the null-space of* $\boldsymbol{g}^H$ *and* $\tilde{\boldsymbol{P}}_D \in \mathbb{C}^{N_t - 1 \times N_t}$ *is the precoder matrix which maximizes the mutual information over the effective channel* $\boldsymbol{h}^H \boldsymbol{W}_g$ *under the power constraint* $tr(\tilde{\boldsymbol{P}}_D \tilde{\boldsymbol{P}}_D^H) \leq N_t P_{tx}$.

Proposition 4.2. *[From [72]] When the instantaneous CSI of the ER is available at the transmitter, the optimal transmission strategy for maximizing the harvested power is to use all the available power for transmitting* $\boldsymbol{u}$ *in (4.17) with the precoders of the form* $\boldsymbol{P}_E = \begin{bmatrix} \tilde{\boldsymbol{P}}_E & \boldsymbol{0}_{N_t \times N_t - 1} \end{bmatrix}_{N_t \times N_t}$, *where*

$$\tilde{\boldsymbol{P}}_E = \sqrt{N_t P_{tx}} \frac{\boldsymbol{g}}{\|\boldsymbol{g}\|}. \tag{4.19}$$

Propositions 4.1 and 4.2 reveal that the maximization of the secrecy rate and maximization of the harvested energy are two conflicting objectives. This is because by transmitting on the null-space of the eavesdropper's channel (which is secrecy capacity achieving according to Proposition 4.1), no power is harvested at the ER. Meanwhile, the secrecy rate drops to zero when (only) beamforming the artificial noise (energy signal) in the direction of the ER. Therefore, a solution which provides a good trade-off lies between these two approaches.

In the following, we introduce a framework for joint optimization of $\mathbf{P}_D$ and $\mathbf{P}_E$. In an attempt to solve the optimization problem in (4.11)-(4.13), we formulate a surrogate dual problem in which we combine the two constraints in (4.12) and (4.13) as

$$S(\zeta) = \max_{\mathbf{P}_D,\, \mathbf{P}_E} R_{s,l} \tag{4.20}$$

$$\text{s.t. } (1-\zeta)\big(\text{tr}(\mathbf{P}_D \mathbf{P}_D^H) + \text{tr}(\mathbf{P}_E \mathbf{P}_E^H)\big) - \zeta E_H \leq (1-\zeta) N_t P_{tx} - \zeta E_0, \tag{4.21}$$

where $0 \leq \zeta \leq 1$ and $R_{s,l}$ and E_H are as given in (4.8) and (4.10), respectively. The surrogate dual problem is defined as [73], [71]

$$S(\zeta^*) = \min_{\zeta} S(\zeta). \tag{4.22}$$

By defining $\mathbf{C} = \big((1-\zeta)\mathbf{I}_{N_t} - \zeta \mathbf{g}\mathbf{g}^H\big)^{\frac{1}{2}}$ and $\tilde{P}_{tx} = (1-\zeta) N_t P_{tx} - \zeta E_0$, given that $\frac{\zeta}{1-\zeta} < \frac{1}{\beta}$, where β is the maximal eigenvalue of $\mathbf{g}\mathbf{g}^H$, the optimization problem in (4.20)-(4.21) can be simplified as

$$S(\zeta) = \max_{\mathbf{P}_D,\, \mathbf{P}_E} R_{s,l} \tag{4.23}$$

Algorithm 3 Joint Precoder and Artificial Noise Design

for different values of $\zeta_i \in [0,1]$ **do**
  Initialize $\lambda_u > \lambda_l = 0$, $\mathbf{P}_D$ and $\mathbf{P}_E$
  while difference between two consecutive updates of λ is smaller than ϵ_λ **do**
    update $\lambda = \frac{1}{2}(\lambda_l + \lambda_u)$
    while two consecutive updates of $L(\mathbf{P}_D, \mathbf{P}_E, \lambda)$ differ by less than ϵ_L **do**
      with fixed $\mathbf{P}_E$, update $\mathbf{P}_D$ using the grad.-based rule in (4.28)
      with fixed $\mathbf{P}_D$, update $\mathbf{P}_E$ using the grad.-based rule in (4.29)
    end while
    if $\mathrm{tr}(\mathbf{Q}_D\mathbf{Q}_D^H) + \mathrm{tr}(\mathbf{Q}_E\mathbf{Q}_E^H) < \tilde{P}_{tx}$ **then**
      update $\lambda_u = \lambda$
    else if $\mathrm{tr}(\mathbf{Q}_D\mathbf{Q}_D^H) + \mathrm{tr}(\mathbf{Q}_E\mathbf{Q}_E^H) > \tilde{P}_{tx}$ **then**
      update $\lambda_l = \lambda$
    end if
  end while
  Calculate $S(\zeta_i)$
end for
Obtain $\zeta^* = \mathrm{argmin}_{\zeta_i} S(\zeta)$ and return the corresponding $\mathbf{P}_D$ and $\mathbf{P}_E$.

$$\text{s.t.} \quad \mathrm{tr}(\mathbf{Q}_D\mathbf{Q}_D^H) + \mathrm{tr}(\mathbf{Q}_E\mathbf{Q}_E^H) \leq \tilde{P}_{tx}, \tag{4.24}$$

where $\mathbf{Q}_D = \mathbf{C}\mathbf{P}_D$ and $\mathbf{Q}_E = \mathbf{C}\mathbf{P}_E$. In order to solve (4.23)-(4.24), we define a Lagrange dual optimization problem as follows. The Lagrangian of (4.23) is given as:

$$L(\mathbf{P}_D, \mathbf{P}_E, \lambda) = R_{s,l} + \lambda(\tilde{P}_{tx} - \mathrm{tr}(\mathbf{Q}_D\mathbf{Q}_D^H) + \mathrm{tr}(\mathbf{Q}_E\mathbf{Q}_E^H)), \tag{4.25}$$

where λ is the Lagrange dual variable associated with the constraint in (4.24). The associated dual optimization problem is defined as

$$\min_{\lambda>0} T(\lambda), \tag{4.26}$$

where

$$T(\lambda) = \max_{\mathbf{P}_D,\ \mathbf{P}_E} L(\mathbf{P}_D, \mathbf{P}_E, \lambda). \tag{4.27}$$

In order to solve (4.26), we employ a bisection method as explained in Algorithm 3. For each value of λ, we optimize $\mathbf{P}_D$ and $\mathbf{P}_E$ in an alternating fashion. The optimization of $\mathbf{P}_D$ with fixed $\mathbf{P}_E$ and also the optimization of $\mathbf{P}_E$ with fixed $\mathbf{P}_D$ is carried out using gradient descent based approaches. Particularly, with a fixed $\mathbf{P}_E$, the optimal $\mathbf{P}_D$ is updated by taking steps proportional to the gradient of the objective function as

$$\mathbf{P}_D(k+1) = \left[\mathbf{P}_D(k) + \mu\nabla_{\mathbf{P}_D} R_{s,l}(k)\right]^{\dagger}_{\mathrm{tr}(\mathbf{Q}_D\mathbf{Q}_D^H) \leq \tilde{P}_{tx} - \mathrm{tr}(\mathbf{Q}_E\mathbf{Q}_E^H)}, \tag{4.28}$$

where μ denotes the step size of the update and $[.]^{\dagger}_{\mathrm{tr}(\mathbf{Q}_D\mathbf{Q}_D^H)\leq\tilde{P}_{tx}-\mathrm{tr}(\mathbf{Q}_E\mathbf{Q}_E^H)}$ denotes normalization of $\mathbf{P}_D$ and $\mathbf{P}_E$ (while keeping the ratio $\mathrm{tr}(\mathbf{P}_D\mathbf{P}_D^H)/\mathrm{tr}(\mathbf{P}_E\mathbf{P}_E^H)$ at the same level prior to normalization) such that $\mathrm{tr}(\mathbf{Q}_D\mathbf{Q}_D^H) \leq \tilde{P}_{tx} - \mathrm{tr}(\mathbf{Q}_E\mathbf{Q}_E^H)$ is satisfied.

Similarly, gradient descent based optimization is adopted for optimizing $\mathbf{P}_E$ with a fixed $\mathbf{P}_D$ as

$$\mathbf{P}_E(k+1) = \left[\mathbf{P}_E(k) + \mu\nabla_{\mathbf{P}_E}R_{s,l}(k)\right]^{\dagger}_{\mathrm{tr}(\mathbf{Q}_E\mathbf{Q}_E^H)\leq\tilde{P}_{tx}-\mathrm{tr}(\mathbf{Q}_D\mathbf{Q}_D^H)}. \tag{4.29}$$

The derivations of the gradients $\nabla_{\mathbf{P}_D}R_{s,l}$ and $\nabla_{\mathbf{P}_E}R_{s,l}$ are provided in Appendix E.

In order to obtain the solution for (4.22), we perform a one-dimensional search over multiple values of ζ. One may note that the solution of the surrogate dual problem may not always be feasible in the original problem. When this is the case, the optimization procedure should be repeated with new constraints (e.g., larger values of E_0) until the obtained solution satisfies the original constraints.

4.2.3 Secrecy Rate-Harvested Energy Trade-off with Statistical ECSIT

We now focus on the scenarios where only statistical information on the ER's channel is available at the transmitter. More specifically, we consider a correlated channel towards the ER as in (4.3), and assume that the transmitter knows only the transmit correlation matrix $\mathbf{\Psi}_t$.

Similar to Section 4.2.2, we first review the existing solutions for the problem of maximizing the secrecy rates without any harvested energy constraint as well as the harvested energy maximization problem without any secrecy constraint. No closed-form optimal solution is available for the former problem. However, the framework introduced in Chapter 3 enables obtaining precoder matrices $\mathbf{P}_D$ and $\mathbf{P}_E$ as suboptimal solutions for maximization of the achievable secrecy rate under the power constraint in (4.12). As for the latter problem, the optimal transmit

signal for maximization of the harvested energy without secrecy constraint is as given in the following proposition.

Proposition 4.3. *[From [69]] When the transmitter knows only the statistical CSI of the ER, the optimal transmission strategy for maximizing the harvested energy is to use all transmission power for transmitting* $\boldsymbol{u}$ *on the strongest eigenmode of* $\boldsymbol{\Psi}_t$*. In other words, if we consider the eigenvalue decomposition of the ER's channel as* $\frac{1}{N_t}\boldsymbol{\Psi}_t = \boldsymbol{V}_{\boldsymbol{\Psi}}\boldsymbol{\Sigma}_{\boldsymbol{\Psi}}\boldsymbol{V}_{\boldsymbol{\Psi}}^H$*, the optimal artificial noise (energy signal) precoder matrix is* $\boldsymbol{P}_E = \left[\tilde{\boldsymbol{P}}_E \;\; \boldsymbol{0}_{N_t\times N_t-1}\right]_{N_t\times N_t}$ *where*

$$\tilde{\boldsymbol{P}}_E = \sqrt{N_t P_{tx}}\boldsymbol{v}_{\boldsymbol{\Psi}_1}, \tag{4.30}$$

where $\boldsymbol{v}_{\boldsymbol{\Psi}_1}$ *denotes the first column of* $\boldsymbol{V}_{\boldsymbol{\Psi}}$*.*

Our objective is to solve the optimization problem in (4.14)-(4.16). We employ a similar dual optimization as introduced in Section 4.2.2 via simply replacing $R_{s,l}$ and E_H in (4.20)-(4.21) by the expressions given in (4.9) and (4.7), respectively. The optimization problem in (4.23)-(4.24) is rewritten as

$$S(\zeta) = \max_{\mathbf{P}_D,\, \mathbf{P}_E} R'_{s,l} \tag{4.31}$$

$$\text{s.t.} \quad \text{tr}(\mathbf{Q}'_D\mathbf{Q}'^H_D) + \text{tr}(\mathbf{Q}'_E\mathbf{Q}'^H_E) \leq \tilde{P}_{tx}, \tag{4.32}$$

where $\mathbf{Q}'_D = \left((1-\zeta)\mathbf{I}_{N_t} - \zeta\boldsymbol{\Psi}_t\right)^{\frac{1}{2}}\mathbf{P}_D$ and $\mathbf{Q}'_E = \left((1-\zeta)\mathbf{I}_{N_t} - \zeta\boldsymbol{\Psi}_t\right)^{\frac{1}{2}}\mathbf{P}_E$. This problem is solved using the same steps given in Algorithm 3 where $\mathbf{Q}_D$, $\mathbf{Q}_E$ and $R_{s,l}$ are replaced by $\mathbf{Q}'_D$, $\mathbf{Q}'_E$ and $R'_{s,l}$, respectively. Proof of convergence follows from the same line of arguments given in Appendix D.

4.2.4 Low Complexity Two-Stage Precoder Design

Due to the nature of SWIPT systems, the ER is expected to work at high SNRs. As a result, without taking into account the harvested energy constraint, either with the perfect or the statistical CSI of the ER, existing transmit signal design algorithms over MISO wiretap channels with finite-alphabet inputs (see e.g., [32] for the perfect and [36] for the statistical ECSIT scenario) lead to solutions,

which allocate only a small fraction of total power for data transmission. The reason behind this observation is that, with a higher power transmission, the eavesdropper would be able to decode the transmitted data. In this section, we take advantage of this property to propose a low complexity alternative for the schemes given in Sections 4.2.2 and 4.2.3.

Let us first consider the full CSI case. In the proposed low complexity approach, rather than optimizing the covariance matrix $\mathbf{K_u}$, we propose to construct $\mathbf{u}$ in (4.4) as

$$\mathbf{u} = \alpha_{AN}^2 \mathbf{W}_h \mathbf{v}_{AN} + \alpha_b^2 \mathbf{p}_{BF} v_b', \tag{4.33}$$

where $\mathbf{W}_h \in \mathbb{C}^{N_t \times N_t - 1}$ stands for an orthonormal basis for the null-space of $\mathbf{h}^H$, and for a given channel of the ER, $\mathbf{p}_{BF} = \mathbf{g}/\|\mathbf{g}\|$. In particular, the artificial noise signal $\mathbf{v}_{AN} \sim \mathcal{CN}(0, \mathbf{I}_{N_t-1})$ and the energy signal $v_b' \sim \mathcal{CN}(0,1)$ are transmitted in the null space of the IR's channel and beamformed to the ER, respectively. While the former provides gains in terms of secrecy, the latter is beneficial from an energy harvesting perspective. The scalars α_{AN} and α_b determine the portion of power allocated to each of these signals. The optimization problem can now be stated as

$$\max_{\mathbf{P}_D,\, \alpha_{AN},\, \alpha_b} \quad R_{s,l} \tag{4.34}$$

$$\text{s.t.} \quad \text{tr}(\mathbf{P}_D \mathbf{P}_D^H) + \alpha_{AN}^2 + \alpha_b^2 \leq N_t P_{tx}, \tag{4.35}$$

$$\text{and} \quad E_H \geq E_0, \tag{4.36}$$

where the instantaneous harvested energy (conditioned on $\mathbf{g}$) is given by

$$E_H = \gamma_z(\mathbf{g}^H \mathbf{P}_D \mathbf{P}_D^H \mathbf{g} + \alpha_{AN}^2 \mathbf{g}^H \mathbf{W}_b \mathbf{W}_b^H \mathbf{g} + \alpha_b^2 \|\mathbf{g}\|^2). \tag{4.37}$$

In order to solve (4.34)-(4.36), we propose a two-stage transmit signal design algorithm. In the first stage, without considering (4.36), the precoder matrix $\mathbf{P}_D$ is obtained using the precoder design algorithms given in Algorithm 3 in Chapter 3. Due to the assumption that the ER works at high SNRs, this algorithm leads to precoders with small $\text{tr}(\mathbf{P}_D \mathbf{P}_D^H)$ values. Therefore, the remaining power, $P_{rem} = N_t P_{tx} - \text{tr}(\mathbf{P}_D \mathbf{P}_D^H)$ is divided between the signals $\mathbf{v}$ and v' such that the constraints (4.35) and (4.36) are satisfied. In order to obtain the portion of power

allocated to each artificial noise term, we perform a one-dimensional parameter search to solve

$$\min_{\alpha_b} \alpha_b^2 \tag{4.38}$$

$$\text{s.t. } E_H(\alpha_b) \geq E_0. \tag{4.39}$$

By solving (4.38)-(4.39), we obtain the minimum power which should be allocated to the artificial noise which is beamformed to the ER such that the constraint on the harvested power is satisfied. Since this artificial noise leaks into the IR's channel, it is reasonable to find the minimum power which can be allocated to this signal to satisfy (4.39). The remaining power is allocated for injection of artificial noise in the null-space of the main channel (i.e., $\alpha_{AN}^2 = P_{rem} - \alpha_b^2$), and accordingly, the power constraint in (4.35) is satisfied.

The proposed two-stage precoder design can also be used in the scenarios with statistical ECSIT. In this case, the signal $\mathbf{u}$ is generated using (4.33) with $\mathbf{p}_{BF} = \mathbf{v}_{\mathbf{\Psi}_1}$ where $\mathbf{v}_{\mathbf{\Psi}_1}$ is the first column of the left singular matrix $\mathbf{V}_{\mathbf{\Psi}}$, which is the eigenvector corresponding to the largest eigenvalue of $\mathbf{\Psi}_t$. The optimization problem is constructed by replacing $R_{s,l}$ and E_H in (4.34)-(4.36) by $R'_{s,l}$ and $\bar{E}_H$, respectively. In particular, in this case, the constraint is on the average harvested power, which is given by

$$\bar{E}_H = \mathbb{E}_{\mathbf{g}}\{\gamma_z(\mathbf{g}^H\mathbf{P}_D\mathbf{P}_D^H\mathbf{g} + \alpha_{AN}^2\mathbf{g}^H\mathbf{W}_b\mathbf{W}_b^H\mathbf{g} + \alpha_b^2\mathbf{g}^H\mathbf{p}_{BF})\}. \tag{4.40}$$

The optimization problem is tackled by taking the same steps as explained for the scenarios with full CSI.

4.3 Generalization to MIMO Setups

In the previous section, we have focused on the scenarios where both the ER and the IR are equipped with a single antenna. We now generalize the proposed strategies to the setups with multiple antennas at the receiver nodes.

For a SWIPT wiretap channel with N_r antennas at the IR, and N_e antennas at the ER, the received vectors can be written as

$$\mathbf{y} = \sqrt{\gamma_y}\mathbf{H}\mathbf{x} + \mathbf{n}_y, \tag{4.41}$$

$$\mathbf{z} = \sqrt{\gamma_z}\mathbf{G}\mathbf{x} + \mathbf{n}_z. \tag{4.42}$$

where $\mathbf{H} \in \mathbb{C}^{N_r \times N_t}$ and $\mathbf{G} \in \mathbb{C}^{N_e \times N_t}$ denote the channel matrices corresponding to the IR and the ER, respectively. Similar to (4.1)-(4.2), γ_y and γ_z are the distance-dependent path loss coefficients, and $\mathbf{n}_y$ and $\mathbf{n}_z$ stand for circularly symmetric complex AWGN terms, which follow $\mathcal{CN}(0, \sigma^2_{\mathbf{n}_y})$ and $\mathcal{CN}(0, \sigma^2_{\mathbf{n}_z})$, respectively. The channel input is given by $\mathbf{x} = \mathbf{P}_D\mathbf{s} + \mathbf{P}_E\mathbf{u}_E$. Therefore, the received vectors in (4.41)-(4.42) can be written as

$$\mathbf{y} = \mathbf{H}\mathbf{P}_D\mathbf{s} + \mathbf{H}\mathbf{P}_E\mathbf{u}_E + \mathbf{n}_y, \tag{4.43}$$

$$\mathbf{z} = \mathbf{G}\mathbf{P}_D\mathbf{s} + \mathbf{G}\mathbf{P}_E\mathbf{u}_E + \mathbf{n}_z. \tag{4.44}$$

Under both perfect and statistical ECSIT scenarios, we can employ Algorithm 3 by simply replacing the expressions for the objective functions in (4.8) and (4.9) with the following

$$R_{s,l} = I(\mathbf{s}; \mathbf{y}|\mathbf{H}) - I(\mathbf{s}; \mathbf{z}|\mathbf{G}), \tag{4.45}$$

$$R'_{s,l} = I(\mathbf{s}; \mathbf{y}|\mathbf{H}) - \mathbb{E}_{\mathbf{G}} I(\mathbf{s}; \mathbf{z}|\mathbf{G}). \tag{4.46}$$

Noting that $\mathbf{n}'_y = \mathbf{H}\mathbf{P}_E\mathbf{u}_E + \mathbf{n}_y$ and $\mathbf{n}'_z = \mathbf{G}\mathbf{P}_E\mathbf{u}_E + \mathbf{n}_z$ are colored noise terms with covariance matrices $\mathbf{K}_{\mathbf{n}'_y} = \mathbf{H}\mathbf{P}_E\mathbf{P}_E^H\mathbf{H}^H + \sigma^2_{\mathbf{n}_y}\mathbf{I}_{N_r}$ and $\mathbf{K}_{\mathbf{n}'_z} = \mathbf{G}\mathbf{P}_E\mathbf{P}_E^H\mathbf{G}^H + \sigma^2_{\mathbf{n}_z}\mathbf{I}_{N_e}$, the mutual information terms in (4.45)-(4.46) can be calculated after whitening $\mathbf{n}'_y$ and $\mathbf{n}'_z$. More specifically, in order to calculate $I(\mathbf{s}; \mathbf{y}|\mathbf{H})$, we pre-multiply (4.43) by $\mathbf{K}_{\mathbf{n}'_y}^{-\frac{1}{2}}$ which results in

$$\mathbf{y}'' = \mathbf{K}_{\mathbf{n}'_y}^{-\frac{1}{2}}\mathbf{H}\mathbf{P}_D\mathbf{s} + \mathbf{n}''_y, \tag{4.47}$$

where $\mathbf{n}''_y$ is a zero-mean AWGN with unit variance. As a result, the mutual information is given by

$$I(\mathbf{s}; \mathbf{y}''|\mathbf{H}) = N_t \log M - \frac{1}{M^{N_t}} \sum_{i=1}^{M^{N_t}} \mathbb{E}_{\mathbf{n}''_y} \left\{ \log \sum_{j=1}^{M^{N_t}} \exp\left(- \|\mathbf{K}_{\mathbf{n}'_y}^{-\frac{1}{2}}\mathbf{H}\mathbf{P}_D\mathbf{d}_{ij} + \mathbf{n}''_y\|^2 + \|\mathbf{n}''_y\|^2 \right) \right\}, \tag{4.48}$$

which is equal to $I(\mathbf{s};\mathbf{y}|\mathbf{H})$ as the transformation is one-to-one. Following similar steps, $I(\mathbf{s};\mathbf{z}|\mathbf{G})$ can be calculated as

$$I(\mathbf{s};\mathbf{z}|\mathbf{G}) = N_t \log M - \frac{1}{M^{N_t}} \sum_{i=1}^{M^{N_t}} \mathbb{E}_{\mathbf{n}_z''} \left\{ \log \sum_{j=1}^{M^{N_t}} \exp\left(- \|\mathbf{K}_{\mathbf{n}_z'}^{-\frac{1}{2}} \mathbf{G}\mathbf{P}_D \mathbf{d}_{ij} + \mathbf{n}_z''\|^2 + \|\mathbf{n}_z''\|^2 \right) \right\}, \quad (4.49)$$

where n_z'' is a zero-mean unit variance AWGN term.

In the scenarios where $N_t > N_r$, it is also possible to employ the two-stage precoder design introduced in Section 4.2.4 as a low-complexity approach over MIMO SWIPT wiretap channels. Rather than jointly optimizing $\mathbf{P}_D$ and $\mathbf{P}_E$, one can first obtain the precoder matrix and then perform a power allocation between the signals given in (4.33) where $\mathbf{W}_h \in \mathbb{C}^{N_t \times N_t - N_r}$ stands for an orthonormal basis for the null-space of $\mathbf{H}$ and $\mathbf{p}_{BF}$ is equal to the first column of the left singular matrix of SVDs of $\mathbf{G}$ and $\mathbf{\Psi}_t$ (i.e., the eigenvectors corresponding to the largest eigenvalues) under perfect and statistical ECSIT scenarios. In order to solve (4.34)-(4.36), first, the precoder optimization is carried out using the Algorithms proposed in Chapter 3. Then, a one dimensional parameter search is performed to solve (4.38)-(4.39), and once the optimal α_b^2 is obtained, the remaining power is allocated to artificial noise injection in the null-space of $\mathbf{H}$.

4.4 Numerical Examples

We now provide numerical examples to examine the efficacy of the proposed algorithms. Throughout the simulations, we model the distance-dependent path loss as

$$\gamma = \Gamma_0 \Big(\frac{l}{l_0} \Big)^{-\tau}, \quad (4.50)$$

where $\tau = 2.7$ is the path loss exponent and $\Gamma_0 = 10^{-3}$ is the path loss at the reference distance $l_0 = 1\ m$. We further assume that the ER and the IR's distances from the transmitter are $l_y = 10\ m$ and $l_z = 15\ m$, respectively. The total transmitted power is $N_t P_{tx} = 36\ dBm$ and the power of the noise terms at both receivers is $\sigma_{n_y}^2 = \sigma_{n_z}^2 = -50\ dBm$.

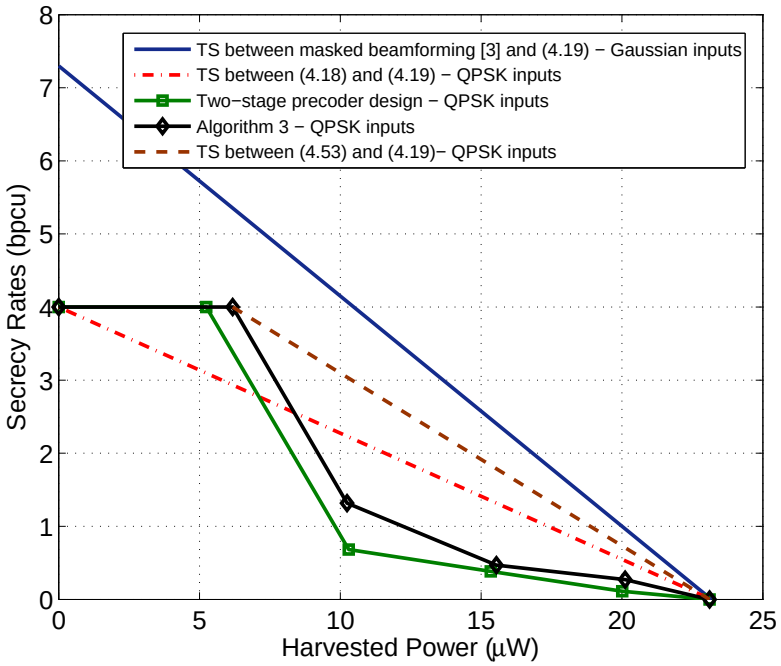

Figure 4.2: Achievable secrecy rates versus harvested power with QPSK and Gaussian inputs for the channels given in (4.51) and (4.52) and with perfect CSI of both channels at the transmitter.

First, we focus on a $2 \times 1 \times 1$ set-up with fixed channel coefficients as

$$\mathbf{h}^H = \begin{bmatrix} 0.5128 - 0.3239j & -0.8903 - 0.0318j \end{bmatrix}, \tag{4.51}$$

$$\mathbf{g}^H = \begin{bmatrix} 0.3880 + 1.2024j & -0.9825 + 0.5914j \end{bmatrix}. \tag{4.52}$$

Fig. 4.2 demonstrates the achievable secrecy rates versus the harvested power for different transmission strategies under the perfect CSI assumption. It is clearly observed that the proposed transmit signal design algorithm achieves high secrecy rates in the scenarios where the required harvested power is not very high. For example, while solving the optimization problem (4.11)-(4.13) for $E_0 = 6$ μW, the following solution is obtained via Algorithm 3:

$$\mathbf{P}_D = \begin{bmatrix} 0.6403 + 1.7981j & -2.0944 - 2.4498j \\ -2.5329 - 0.3699j & 4.2786 - 0.9595j \end{bmatrix},$$

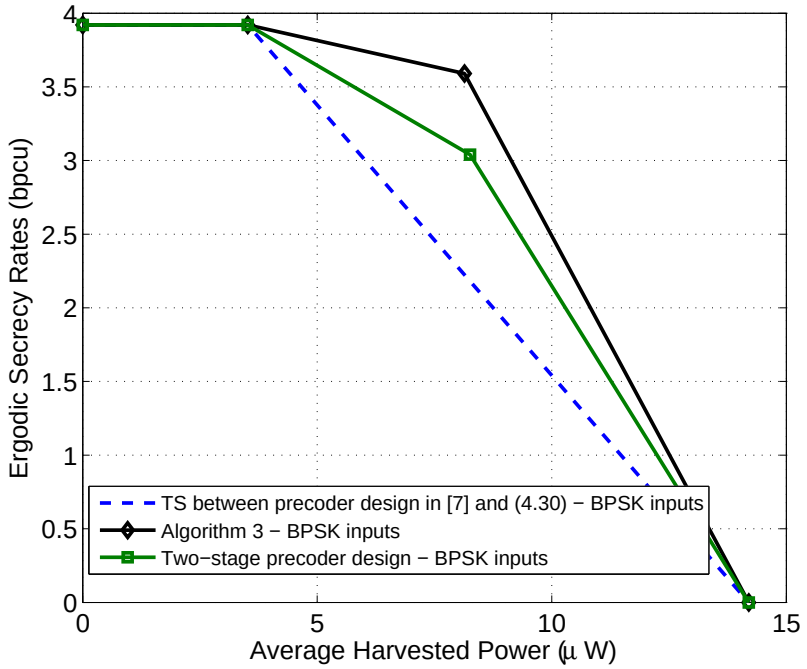

Figure 4.3: Achievable ergodic secrecy rates versus average harvested power over $4 \times 1 \times 1$ channels with BPSK inputs and statistical ECSIT.

$$\mathbf{P}_E = \begin{bmatrix} 5.2938 - 54.5471j & 0 \\ 25.3433 - 17.1919j & 0 \end{bmatrix}, \tag{4.53}$$

which achieves the point $(6.18\ \mu\text{W}, 4\ \text{bpcu})$[1] and time sharing (TS) between this channel input and the one given in (4.19) considerably outperforms the TS between the strategies introduced in Propositions 4.1 and 4.2. Furthermore, it is observed that the two-stage design approach yields a comparable performance to that of Algorithm 3 in spite of its significantly reduced complexity.

Fig. 4.3 demonstrates the trade-off between the ergodic secrecy rates and the average harvested energy for the scenarios where perfect CSI of the IR's channel and only the statistical CSI of the ER are available at the transmitter. We consider a $4 \times 1 \times 1$ setup with BPSK inputs. In order to model the ER's channel, we use (4.3), and consider correlation matrices with exponentially decaying entries

[1] bpcu stands for bits per channel use.

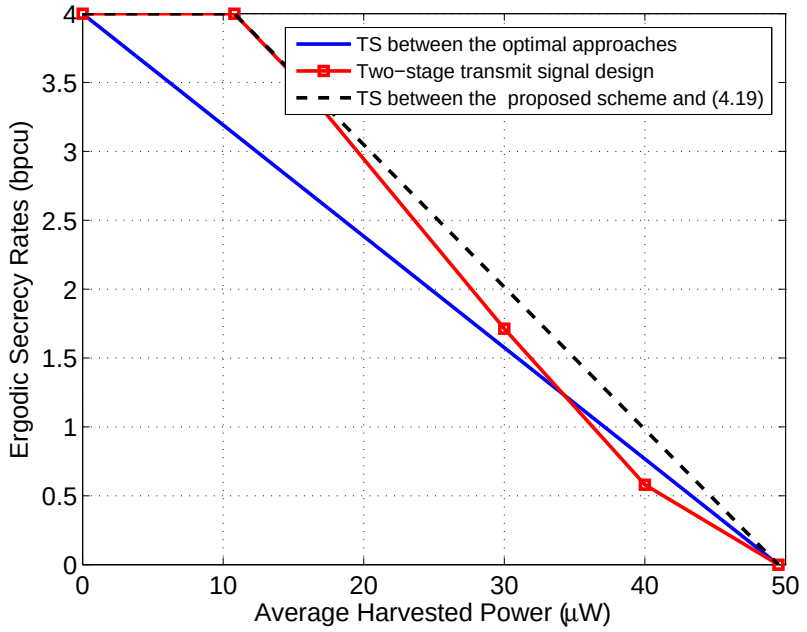

Figure 4.4: Achievable ergodic secrecy rates versus average harvested power over $4 \times 2 \times 2$ channels with BPSK inputs and perfect CSIT.

as

$$[\mathbf{\Psi}_t(\rho)]_{ij} = \rho_t^{|i-j|}, \quad i, j = 1, 2, \ldots, N_t, \tag{4.54}$$

with $\rho_t = 0.8$. The ergodic secrecy rate and the average harvested power are obtained via averaging over 500 channel realizations. Both Algorithm 3 and the two-stage precoder design approach offer substantial gains with respect to the TS in the scenarios with the statistical ECSIT. Furthermore, we observe through our simulations that the two-stage approach possesses a considerably (roughly, two orders of magnitude) lower complexity.

We now focus on a MIMO setup with $N_t = 4$, $N_r = 2$ and $N_e = 2$. The secrecy rate harvested power trade-off with BPSK inputs under the perfect CSIT assumption, is shown in Fig. 4.4. It is clear that the proposed transmit signal design algorithms yield an enhanced performance with respect to the time sharing approach.

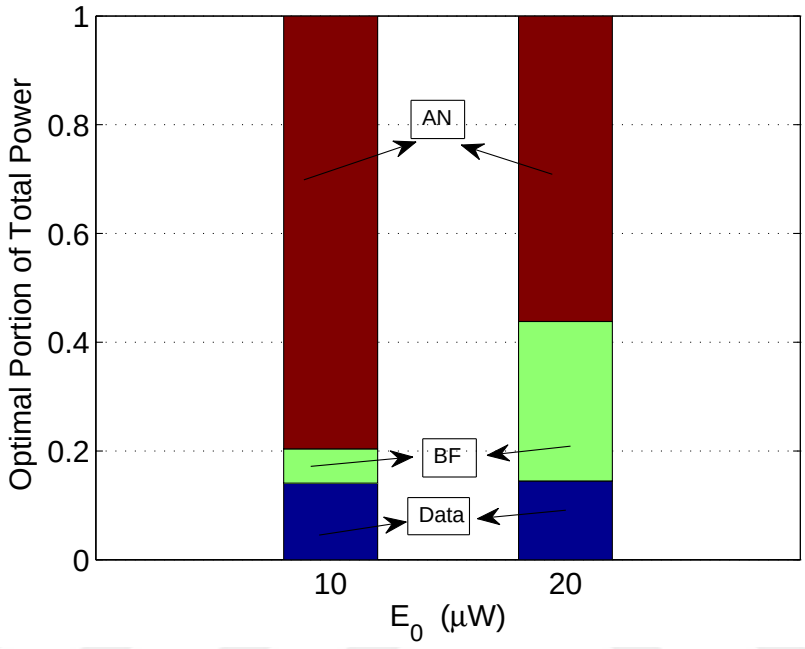

Figure 4.5: The optimal portions of the total power allocated to information bearing signal (denoted by Data), energy signal (denoted by BF) and artificial noise (denoted by AN) in $4 \times 2 \times 2$ channel with perfect CSIT.

Fig. 4.5 represents the portions of the total power allocated to different signals in (4.33), i.e., the data signal, artificial noise and the energy signal, using the two-stage precoding approach with perfect CSI. Expectedly, the portion of power allocated to the energy signal increases for the higher values of E_0. It should be noted that, when perfect ECSIT is available, the optimal data precoder matrices are of the form (4.18). Therefore, no information leakage occurs at the ER and, injecting artificial noise in the null-space of the IR's channel does not improve the secrecy rate. However, it increases the harvested power at the ER without influencing the reception at the IR.

Fig. 4.6 demonstrates the average secrecy rate versus the average harvested power with statistical ECSIT for BPSK over a $4 \times 2 \times 2$ MIMO setup. In this case, we consider a doubly correlated channel towards the ER where the channel

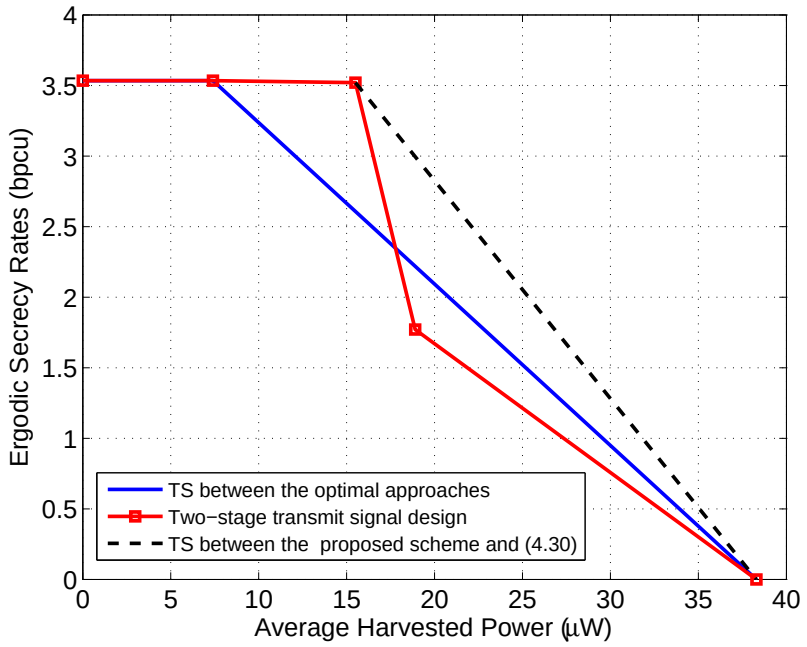

Figure 4.6: Achievable ergodic secrecy rates versus average harvested power over $4 \times 2 \times 2$ channels with BPSK inputs and statistical ECSIT.

coefficients are generated using

$$\mathbf{G} = \mathbf{\Psi}_r^{1/2} \hat{\mathbf{G}} \mathbf{\Psi}_t^{1/2}, \tag{4.55}$$

where $\hat{\mathbf{G}}$ is a complex matrix with i.i.d. zero mean unit variance Gaussian entries, and the receive and transmit correlation matrices $\mathbf{\Psi}_t$ and $\mathbf{\Psi}_r$ are generated using (4.54) with $\rho_t = \rho_r = 0.6$. Time sharing between the proposed transmission scheme and the one given in (4.30) yields the best performance among the existing solutions. Moreover, comparing the rate-energy region given in Fig. 4.6 with that of Fig. 4.4 clearly shows the reduction both in the harvested power and the secrecy rate due to lack of instantaneous channel knowledge of the ER at the transmitter.

Fig. 4.7 presents the portions of the total power allocated to the signals in (4.33) using two-stage precoding with statistical ECSIT. Dissimilar to the results given in Fig. 4.5, a larger part of the power is allocated to the artificial noise, which is transmitted in the null-space of the main channel. This is because, the

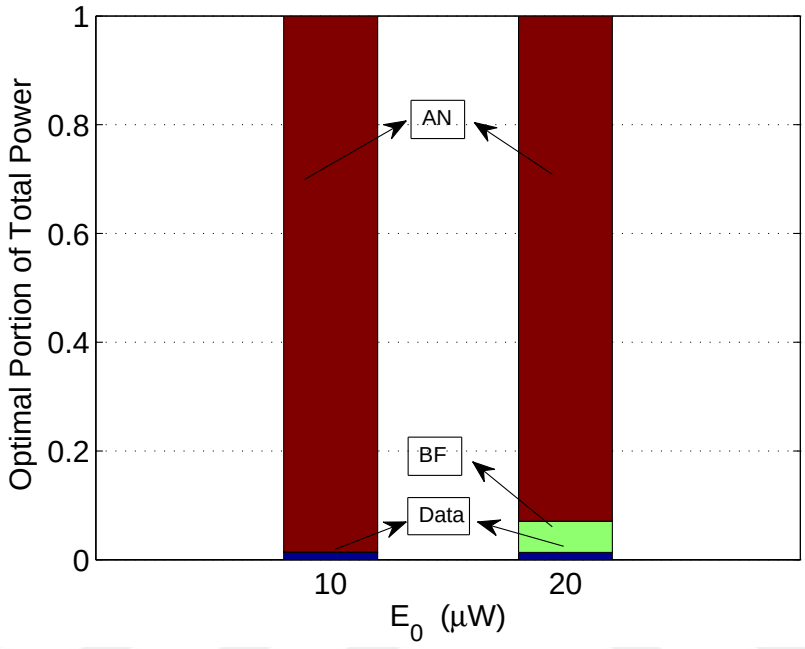

Figure 4.7: The optimal portions of the total power allocated to information bearing signal (denoted by Data), energy signal (denoted by BF) and artificial noise (denoted by AN) in $4 \times 2 \times 2$ channel with statistical ECSIT.

precoder matrix $\mathbf{P}_D$ is not capable of preventing information leakage to the ER. Therefore, artificial noise plays a more vital role in this scenario, and clearly, it is beneficial for both increasing the secrecy rate and the harvested power.

4.5 Chapter Summary

In this chapter, we have characterized the secrecy rate-harvested power trade-off for the scenarios with multi-antenna nodes and discrete signaling. We have demonstrated that maximizing the secrecy rate and maximizing the harvested power are two conflicting objectives. We have proposed a framework for transmit signal design with the objective of maximizing the achievable secrecy rate given that the harvested power at the energy receiver is larger than a pre-specified

value. The proposed solutions rely on joint optimization of data precoder and covariance of the signal (which plays the dual role of artificial noise and energy signal). Exemplary numerical results demonstrate that the proposed schemes achieve an improved trade-off with respect to the time-sharing strategy.

Chapter 5

Physical Layer Security with Space Shift Keying Transmission

Spatial modulation and space shift keying (SSK) represent transmission methods for low-complexity implementation of MIMO wireless systems in which antenna indices are employed for data transmission. So as to realize an SSK transmission, a one-to-one mapping is established between the blocks of information bits to be transmitted and the spatial position of the transmit antenna in the antenna array. At each time instance, among the multiple antennas at the transmitter, only one of them is activated and a reference signal is transmitted to the receiver. This signal goes through a generic wireless channel, which plays the role of a "modulation unit". Since the channels corresponding to different transmit-to-receive wireless links are different, it is possible to detect the index of the activated antenna with the aid of the CSI at the receiver [51]. In spatial modulation, data bits are mapped into two information carrying blocks: 1) an antenna index selected from the set of transmit antennas, 2) a symbol drawn from a standard constellation. More specifically, in spatial modulation, the transmitted signals are drawn from a tridimensional constellation as depicted in Fig. 5.1.

SSK has many unique characteristics, which make it a promising candidate for

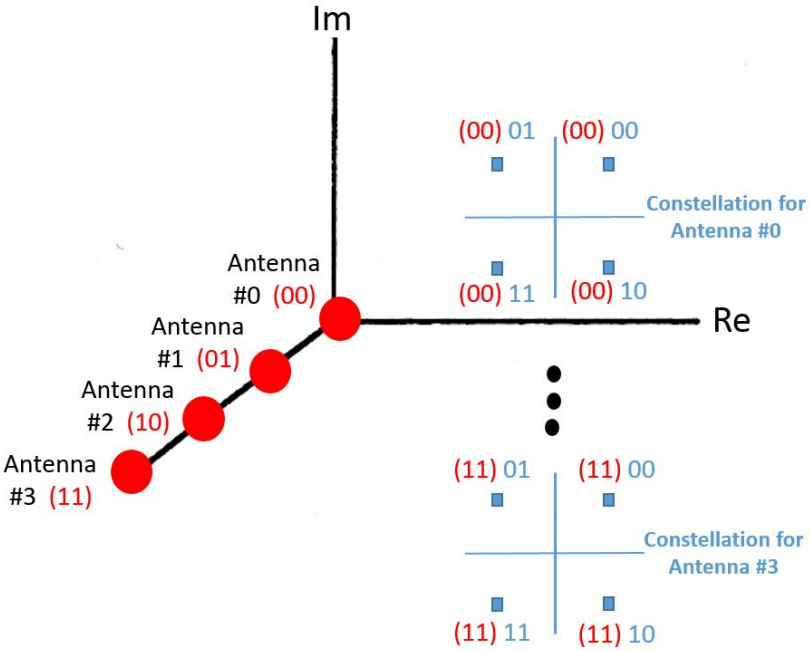

Figure 5.1: Tridimensional signal constellation corresponding to spatial modulation with 4 antennas and QPSK symbols.

future wireless systems. Due to its working mechanism, SSK requires only a single RF front-end chain at the transmitter and avoids the need for inter-antenna synchronization as only a single antenna is activated at each time instance. Furthermore, the receiver complexity is considerably less than the conventional spatial multiplexing techniques such as V-BLAST (vertical Bell laboratories layered-space-time).

Along with the various studies on the performance and applications of SSK [49], some attention has recently been devoted to studying its capabilities in securing communication. In this chapter, we take steps forward studying spatial modulation and SSK in the context of physical layer security. We first derive expressions for the mutual information of spatial modulation and SSK transmission schemes, and characterize their achievable secrecy rates over degraded MIMO wiretap channels in absence of CSIT. Then, we focus on the scenarios where perfect CSI is available at the transmitter, and develop two strategies for precoder

design for secure SSK. Finally, we introduce a secure SSK transmission over reciprocal channels, in which the indices associated with the transmit antennas are assigned dynamically according to the channel towards the legitimate receiver.

5.1 Related Works

A semi-analytical study of secrecy capacity of SSK with two transmit antennas has been provided in [52]. Authors in [74] have formulated the secrecy mutual information for spatial modulation for the scenarios where the legitimate receiver and the eavesdropper are equipped with a single antenna. Among other related works, the authors in [75] and [76] have introduced the idea of employing precoding together with spatial modulation to attain positive secrecy rates along with a low complexity detection at the desired receiver. In [75], this enhanced secrecy is achieved by jointly maximizing the received signal power at the legitimate receiver and minimizing it at the eavesdropper. On the other hand, an artificial noise-aided transmission is utilized in [76].

5.2 Achievable Secrecy Rates

In this section, we formulate the received signals and also define an achievable secrecy rate for two separate cases where SSK and spatial modulation are employed at the transmitter.

5.2.1 System Model and Problem Formulation

We consider a general MIMOME wiretap channel. While Alice transmits a spatially modulated signal to the legitimate receiver, Bob, a third party, Eve, is present with capability of eavesdropping on Alice's signal. Alice, Bob and Eve are assumed to be equipped with N_t, N_{r_b} and N_{r_e} antennas, respectively. Our

objective is to formulate achievable secrecy rates for SSK and spatial modulation transmission schemes. To this end, we first provide the channel input-output relationships under each scheme.

Space Shift Keying: By employing SSK at the transmitter, the received signals $\mathbf{y}$ and $\mathbf{z}$ at the legitimate receiver and the eavesdropper can be represented, respectively, as

$$\mathbf{y} = \mathbf{H}_b\mathbf{x} + \mathbf{n_y} \tag{5.1}$$

$$\mathbf{z} = \mathbf{H}_e\mathbf{x} + \mathbf{n_z}, \tag{5.2}$$

where, $\mathbf{x} \in \{\mathbf{x}_1, \mathbf{x}_2, ..., \mathbf{x}_{N_t}\}$ is the SSK signal vector which is of the form

$$\mathbf{x}_m = [0\ 0\ ...\ 1\ ...\ 0\ 0], \tag{5.3}$$

with the position of "1" indicating the antenna being activated. $\mathbf{n_y}$ and $\mathbf{n_z}$ are i.i.d. additive white Gaussian noise terms which follow circularly symmetric complex Gaussian distributions, $\mathcal{CN}(0, \sigma^2_{\mathbf{n_y}})$ and $\mathcal{CN}(0, \sigma^2_{\mathbf{n_z}})$, respectively. $\mathbf{H}_b$ and $\mathbf{H}_e$ are the channel matrices corresponding to the legitimate channel and the eavesdropper's channel, respectively. The elements of the channel matrices are i.i.d. with distribution $\mathcal{CN}(0, 1)$. Furthermore, $\mathbf{H}_b$, $\mathbf{H}_e$, $\mathbf{n_y}$ and $\mathbf{n_z}$ are independent. It is assumed that the fading process is ergodic. The legitimate receiver and the eavesdropper know their own channels perfectly. However, no CSI is available at the transmitter.

In this section, we focus on the scenarios where $\sigma^2_{\mathbf{n_y}} < \sigma^2_{\mathbf{n_z}}$ and $N_{r_e} \leq N_{r_b}$, where the MIMOME secrecy capacity can be calculated as [42]:

$$C_s = \max_{P_x(\mathbf{x})} \big(\mathbb{E}_{\mathbf{H}_b} I(\mathbf{x}; \mathbf{y}|\mathbf{H}_b) - \mathbb{E}_{\mathbf{H}_e} I(\mathbf{x}; \mathbf{z}|\mathbf{H}_e)\big), \tag{5.4}$$

in which the optimization is over the input distribution. It is well known that for a symmetric discrete memoryless channel, mutual information is maximized with equiprobable inputs [77, p. 94]. With a similar reasoning, it can be claimed that the maximum of $I(\mathbf{x}; \mathbf{y}|\mathbf{H})$ is achieved with a source with equiprobable inputs. Here, we define an achievable secrecy rate as

$$R_s^{SSK} = \big[\mathbb{E}_{\mathbf{H}_b} I(\mathbf{x}; \mathbf{y}|\mathbf{H}_b) - \mathbb{E}_{\mathbf{H}_e} I(\mathbf{x}; \mathbf{z}|\mathbf{H}_e)\big]\big|_{P_x(\mathbf{x})=1/N_t}, \tag{5.5}$$

if $\mathbb{E}_{\mathbf{H}_b} I(\mathbf{x};\mathbf{y}|\mathbf{H}_b) < \mathbb{E}_{\mathbf{H}_e} I(\mathbf{x};\mathbf{z}|\mathbf{H}_e)$ and zero otherwise. This quantifies the information being secretly transmitted with the assumption that the active antennas are selected equiprobably. Indeed, R_s^{SSK} is simply a lower bound on the secrecy capacity given in (5.4) in view of the fact that $P_X(\mathbf{x}) = 1/N_t$ is not necessarily the input distribution which maximizes the expression in (5.4).

Spatial Modulation: While the antenna indices are the only source of information in SSK transmission, spatial modulation additionally employs an amplitude or phase modulation scheme. In this case, the received signals at the legitimate receiver and the eavesdropper can be written as:

$$\mathbf{y}' = \mathbf{H}_b \mathbf{x} s + \mathbf{n}_{y'} \tag{5.6}$$

$$\mathbf{z}' = \mathbf{H}_e \mathbf{x} s + \mathbf{n}_{z'}, \tag{5.7}$$

where $s \in \{s_1, s_2, ..., s_N\}$ denotes the symbol chosen from an equiprobable discrete signal constellation with size N. We assume that a power constraint of unity, i.e., $\mathbb{E}\{|s|^2\} = 1$, holds. In this case, the achievable secrecy rate can be defined as

$$R_s^{SM} = \left[\mathbb{E}_{\mathbf{H}_b} I(\mathbf{x}, s; \mathbf{y}'|\mathbf{H}_b) - \mathbb{E}_{\mathbf{H}_e} I(\mathbf{x}, s; \mathbf{z}'|\mathbf{H}_e)\right]\big|_{P_x(\mathbf{x})=1/N_t, P_s(s)=1/N}, \tag{5.8}$$

which is the difference between the mutual information terms corresponding to the legitimate receiver and the eavesdropper with the assumption that the amplitude or phase modulation symbols are selected equiprobably, $P_s(s) = 1/N$, along with the same assumption for the antenna indices, i.e., $P_x(\mathbf{x}) = 1/N_t$.

5.2.2 Mutual Information and Secrecy Rate

In this section, we separately derive expressions for the mutual information of SSK and spatial modulation. These expressions make possible the evaluation of the secrecy rates in (5.5) and (5.8).

5.2.3 Space Shift Keying

So as to characterize the secrecy rate of SSK, we are required to evaluate the mutual information between the source and the destination, i.e., $I(\mathbf{x};\mathbf{y}|\mathbf{H}_b)$, as well as the mutual information between the source and the eavesdropper, i.e., $I(\mathbf{x};\mathbf{z}|\mathbf{H}_e)$. For $N_r \times N_t$ MIMO channel, $\mathbf{H} \sim \mathcal{CN}(0,1)$, mutual information can be calculated using the following formula [53, Eq. (2.28)]:

$$I(\mathbf{x};\mathbf{y}|\mathbf{H}) = \sum_{\mathbf{x}\in X} \int_{\mathbf{y}} P_{xy|H}(\mathbf{x},\mathbf{y}|\mathbf{H}) \log \frac{P_{xy|h}(\mathbf{x},\mathbf{y}|\mathbf{H})}{P_{x|H}(\mathbf{x}|\mathbf{H}) P_{y|H}(\mathbf{y}|\mathbf{H})}\, dy. \tag{5.9}$$

The N_r-dimensional received signal follows a complex Gaussian distribution with conditional probability density function (PDF) given by:

$$P_{y|xH}(\mathbf{y}|\mathbf{x}_m,\mathbf{H}) = \frac{1}{\pi^{N_r}\sigma_{\mathbf{n}}^{2N_r}} \exp(-\parallel \mathbf{y} - \mathbf{H}\mathbf{x}_m \parallel_F^2 / \sigma_{\mathbf{n}}^2). \tag{5.10}$$

As stated in the previous section, we assume that the antennas are selected equiprobably, i.e., $P_x(\mathbf{x}) = \frac{1}{N_t}$. Note that this is due to the fact that in the absence of CSIT, the active antenna sets are equally likely to be used. We obtain

$$P_{xy|H}(\mathbf{x}_m,\mathbf{y}|\mathbf{H}) = \frac{1}{N_t} P_{y|xH}(\mathbf{y}|\mathbf{x}_m,\mathbf{H}), \tag{5.11}$$

$$P_{x|H}(\mathbf{x}|\mathbf{H}) = \frac{1}{N_t}, \tag{5.12}$$

$$P_{y|H}(\mathbf{y}|\mathbf{H}) = \frac{1}{N_t} \sum_{m=1}^{N_t} P_{y|xH}(\mathbf{y}|\mathbf{x}_m,\mathbf{H}). \tag{5.13}$$

By substituting (5.17)-(5.13) in (5.9), the mutual information for SSK can be derived as:

$$I(\mathbf{x};\mathbf{y}|\mathbf{H}) = \frac{1}{N_t \pi^{N_r}\sigma_{\mathbf{n}}^{2N_r}} \sum_{m=1}^{N_t} \int_{\mathbf{y}} \exp(-\parallel \mathbf{y} - \mathbf{H}\mathbf{x}_m \parallel_F^2 / \sigma_{\mathbf{n}}^2) \times \log \frac{N_t \exp(-\parallel \mathbf{y} - \mathbf{H}\mathbf{x}_m \parallel_F^2 / \sigma_{\mathbf{n}}^2)}{\sum_{m'=1}^{N_t} \exp(-\parallel \mathbf{y} - \mathbf{H}\mathbf{x}_{m'} \parallel_F^2 / \sigma_{\mathbf{n}}^2)}\, d\mathbf{y}. \tag{5.14}$$

5.2.4 Spatial Modulation

For spatial modulation, the mutual information between the two inputs and the output for a fixed channel can be written by using the chain rule [53, Eq. 2.62],

as:

$$I(\mathbf{x}, s; \mathbf{y}') = I(s; \mathbf{y}') + I(\mathbf{x}; \mathbf{y}'|s). \tag{5.15}$$

We first start with obtaining $I(\mathbf{x}; \mathbf{y}'|s)$ which can be obtained using

$$I(\mathbf{x}; \mathbf{y}'|s) = \mathbb{E}_{\mathbf{S}}\Bigg\{ \sum_{\mathbf{x}\in X} \int_{\mathbf{y}'} P_{xy'|s}(\mathbf{x}, \mathbf{y}'|s) \times \log \frac{P_{xy|s}(\mathbf{x}, \mathbf{y}'|s)}{P_{x|s}(\mathbf{x}|s) P_{y'|s}(\mathbf{y}'|s)}\, dy' \Bigg\}. \tag{5.16}$$

Noting that given $\mathbf{x} = \mathbf{x}_m$ and $s = s_n$, the continuous random variable $\mathbf{y}'$ has PDF as

$$P_{y'|xx}(\mathbf{y}'|\mathbf{x}_m, s_m) = \frac{1}{\pi^{N_r} \sigma_{\mathbf{n}}^{2N_r}} \exp(- \parallel \mathbf{y} - \mathbf{H}\mathbf{x}_m s_n \parallel_F^2 / \sigma_{\mathbf{n}}^2), \tag{5.17}$$

we can obtain the following marginal probabilities

$$P_{y'|x}(\mathbf{y}'|\mathbf{x}_m) = \frac{1}{N} \sum_{j=1}^{N} P_{y'|xs}(\mathbf{y}'|\mathbf{x}_m, s_j) \tag{5.18}$$

$$P_{y'|s}(\mathbf{y}'|s_n) = \frac{1}{N_t} \sum_{i=1}^{N_t} P_{y'|xs}(\mathbf{y}'|\mathbf{x}_i, s_n) \tag{5.19}$$

$$P_{y'}(\mathbf{y}') = \frac{1}{NN_t} \sum_{i=1}^{N_t} \sum_{j=1}^{N} P_{y'|xs}(\mathbf{y}'|\mathbf{x}_i, s_j). \tag{5.20}$$

By substitution of the conditional PDFs above in (5.16) we have

$$\begin{aligned} I(\mathbf{x}; \mathbf{y}'|s) &= \log N_t \\ &- \frac{1}{NN_t} \sum_{i=1}^{N_t} \sum_{j=1}^{N} \mathbb{E}_{\mathbf{n}} \log \sum_{k=1}^{N_t} \exp\left(- \frac{\|\mathbf{H}(\mathbf{x}_i - \mathbf{x}_k) + \mathbf{n}\|^2 - \|\mathbf{n}\|^2}{\sigma^2} \right). \end{aligned} \tag{5.21}$$

Taking similar steps, we can obtain $I(s; \mathbf{y}')$ as

$$I(s; \mathbf{y}') = \log N - \frac{1}{NN_t} \sum_{i=1}^{N_t} \sum_{j=1}^{N} \mathbb{E}_{\mathbf{n}} \log \frac{\sum_{k=1}^{N_t} \sum_{l=1}^{N} \exp(-\frac{\|\mathbf{h}_i s_j - \mathbf{h}_k s_l + \mathbf{n}\|^2}{\sigma^2})}{\sum_{k'=1}^{N_t} \exp(-\frac{(\|\mathbf{h}_m - \mathbf{h}_{k'}) s_j + \mathbf{n}\|^2}{\sigma^2})}. \tag{5.22}$$

Hence, the expression for mutual information of spatial modulation can be derived as

$$\begin{aligned} I(\mathbf{x}, s; \mathbf{y}') &= \log NN_t \\ &- \frac{1}{NN_t} \sum_{i=1}^{N_t} \sum_{j=1}^{N} \mathbb{E}_{\mathbf{n}} \log \sum_{k=1}^{N_t} \sum_{l=1}^{N} \exp\left(- \frac{\|\mathbf{h}_i s_j - \mathbf{h}_k s_l + \mathbf{n}\|^2 - \|\mathbf{n}\|^2}{\sigma^2} \right). \end{aligned} \tag{5.23}$$

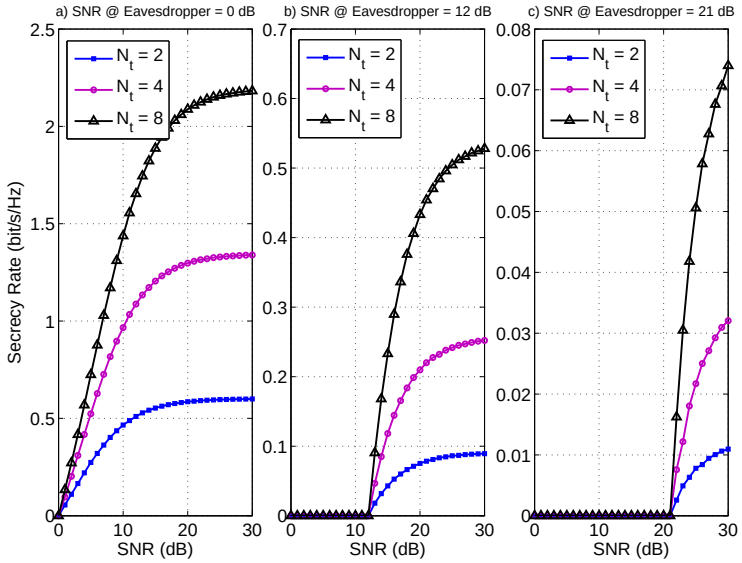

Figure 5.2: Secrecy rate for a SSK system with different number of transmit antennas. $N_{r_e} = N_{r_b} = 1$.

5.2.5 Numerical Examples

In this section, we quantify the achievable secrecy rate of SSK and spatial modulation. For SSK, the secrecy rate is calculated using (5.5) and by numerically evaluating the mutual information expression given in (5.14), for the main channel and the eavesdropper's channel. Fig. 5.2 depicts the secrecy rate for the case with a single receive antenna at the legitimate receiver and the eavesdropper. This rate is evaluated via subtracting the mutual information associated with the eavesdropper's channel from the mutual information corresponding to the legitimate user's channel. In this evaluation, by considering i.i.d. channel coefficients from different transmit antennas, the secrecy rate is averaged over many channel realizations and plotted versus legitimate user's SNR, while it is assumed that the eavesdropper's SNR is fixed at 0, 12 and 21 dB. It can be inferred from Fig. 5.2 that for the case where eavesdropper's SNR is fixed to 0 dB, increasing the number of transmit antennas from 2 to 4 and 8 gives rise to 1 and 2 bits/s/Hz enhancement in the secrecy rate, respectively.

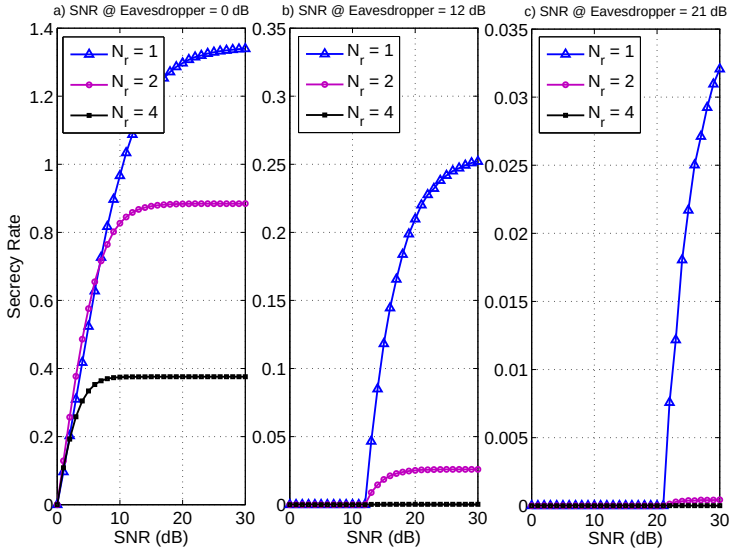

Figure 5.3: Secrecy rate for a SSK system with different number of receiver antennas at the legitimate receiver and the eavesdropper. $N_t = 4, N_{r_e} = N_{r_b} = N_r$.

By comparing the Figures 5.2-(a) , 5.2-(b) and 5.2-(c), it can be observed that the secrecy rates are decreased when we increase the SNR at the eavesdropper. This is to be expected due to the fact that by increasing the Eve's SNR, we decrease the gap between Bob's and Eve's SNRs and this gives rise to a smaller difference between the corresponding mutual informations. Furthermore, it is inferred that for the cases where Eve has higher SNRs, the advantages of larger number of transmit antennas is more apparent.

The effects of increasing the number of receive antennas is shown in Fig. 5.3. Four antennas have been considered at the transmitter and the secrecy capacity has been evaluated by varying the legitimate receiver's SNR for three cases where the eavesdropper's SNR is fixed at 0, 12 and 21 dB, respectively. These results declare that increasing the number of antennas at the legitimate receiver and the eavesdropper results in a decreased secrecy level. This behavior is different from the capacity behavior of SSK in the sense that a higher number of receive antennas results in an increased achievable information rate (see, e.g., Fig. 5

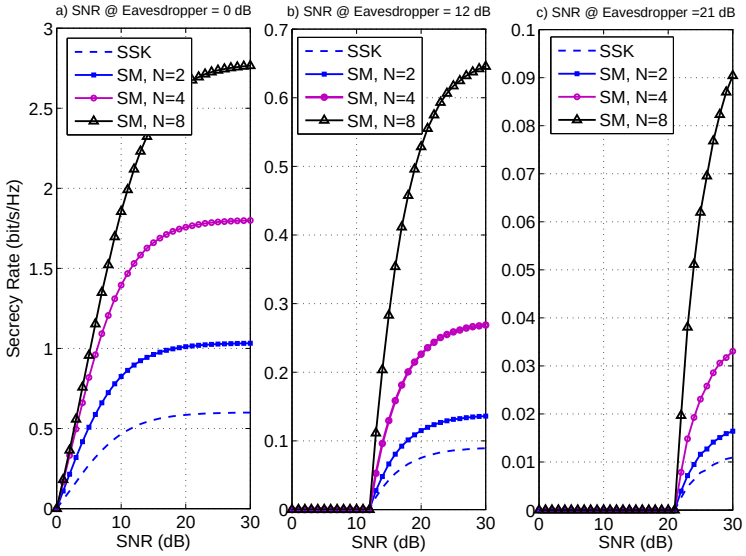

Figure 5.4: Secrecy rate for a spatial modulation system with different underlying signal constellations. $N_t = 2$, $N_{r_e} = N_{r_b} = 1$.

in [78]). This is due to the fact that increasing the number of receive antennas at the legitimate receiver and the eavesdropper leads to a capacity gain for both of the receivers and as a result the behavior of secrecy capacity differs from that of capacity.

In order to characterize the secrecy behavior of spatial modulation, we quantify the secrecy rate using (5.8) and via numerical evaluations of the mutual information expressions for the main channel and the eavesdropper's channel, given in (5.21). Fig. 5.4 shows the secrecy rate for spatial modulation. It can be observed that spatial modulation provides larger secrecy rates than SSK. Also, by increasing the size of the underlying signal constellation, namely N, a better performance is attained for spatial modulation. This is due to the fact that in spatial modulation, utilization of a conventional modulation along with encoding of the data in the antenna index introduces a further randomization which enhances the achievable secrecy rate. Similar to the case for SSK, when Eve's SNR is higher, spatial modulation's secrecy rates are decreased. In these conditions, system benefits more from the increased signal constellation size.

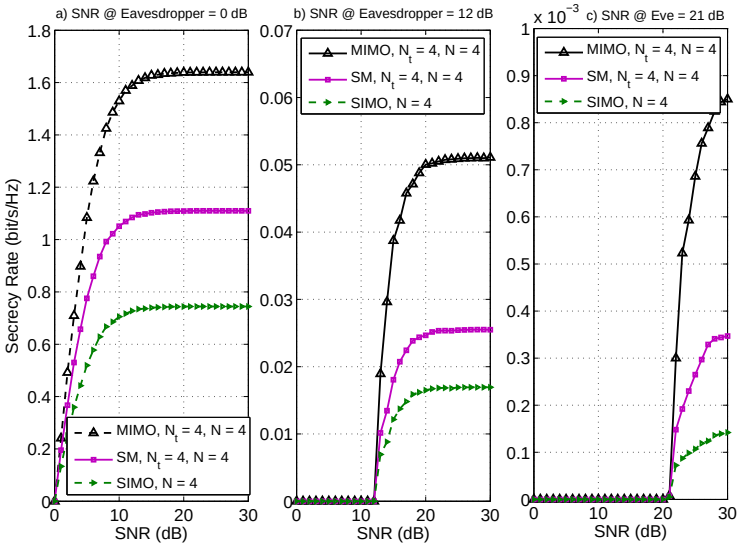

Figure 5.5: Comparison of secrecy rates for spatial modulation and general MIMO and SIMO systems. $N = 4$, $N_{r_e} = N_{r_b} = 2$.

What we can recognize from Fig. 5.4 is that for a fixed number of transmit antennas, employing an amplitude or phase modulation along with the spatial encoding of data can increase the secrecy rate. This increased secrecy rate is attained at the price of increased detection complexity and higher BERs. This is because increasing the order of modulation which is advantageous from a secrecy perspective, on the other hand, gives rise to a decreased minimum distance between the points in the signal-constellation and results in a higher probability of error.

In Fig. 5.5 the secrecy rates of spatial modulation have been compared to those of general MIMO and single-input multiple-output (SIMO) systems with finite alphabet inputs with $N = 4$, namely, using QPSK transmission. The results for the general MIMO have been obtained using [55, Eq. (5)]. Fig. 5.5 clearly shows that spatial modulation can yield an improved secrecy performance with respect to the SIMO case due to taking advantage of multiple transmit antennas. Yet, its secrecy rate is notably less than a general MIMO transmission where all of the transmitted antennas are activated. In fact, this degradation is the price that

should be paid to take advantage of appealing features of spatial modulation in terms of complexity and cost.

5.3 Secure Precoding Algorithms

In this section, we introduce secrecy-enhancing transmit signal design algorithms for SSK with the aid of the CSIT. Unlike [75], where the optimization problem is defined according to a trade-off between the improvement of Bob's reception and the degradation of Eve's signal, we propose an iterative algorithm which directly maximizes the achievable secrecy rates. The proposed iterative approach yields promising performance, however it possesses a relatively high computational complexities. This is mainly due to the fact that the mutual information expression for SSK lacks a tractable and closed form. Hence, we further introduce two lower complexity transmit signal design algorithms.

We show through examples that, when Eve is equipped with a single antenna, it is possible to maximize her level of confusion. This can be done by simply mapping the SSK symbols to a single constellation point from eavesdropper's point of view. Different from the solution provided in [74] which does not satisfy any power constraints, we propose a transmit signal design scheme for which the transmit power does not change with respect to nonprecoded transmission. For scenarios where the number of antennas at the eavesdropper is larger than one, a low-complexity transmission algorithm is proposed which either maximizes the minimum Euclidean distance over the main channel or minimizes it over the eavesdropper's channel.

5.3.1 System Model for Precoded SSK

We consider a MIMO wiretap channel with N_t antennas at the transmitter, Alice. The legitimate receiver, Bob, and the eavesdropper, Eve, are assumed to be equipped with N_{r_b} and N_{r_e} antennas, respectively. The received signals at Bob

and Eve can be written as

$$\mathbf{y} = \mathbf{H}_b \mathbf{X} \mathbf{p} + \mathbf{n}_y, \tag{5.24}$$

$$\mathbf{z} = \mathbf{H}_e \mathbf{X} \mathbf{p} + \mathbf{n}_z, \tag{5.25}$$

respectively, where $\mathbf{X}$ is the $N_t \times N_t$ SSK signal matrix which is of the form $\mathbf{X} = diag(\{0, .., 1, .., 0\})$, with the position of "1" indicating the antenna being activated. $\mathbf{H}_b$ and $\mathbf{H}_e$ are the $N_{r_b} \times N_t$ and $N_{r_e} \times N_t$ channel matrices with independent fading coefficients from the transmitter to the legitimate receiver and to the eavesdropper, respectively. $\mathbf{n_y}$ and $\mathbf{n_z}$ are i.i.d. AWGN terms. It is assumed that the elements of the channel matrices and the noise follow circularly symmetric complex Gaussian distributions, $\mathcal{CN}(0, 1)$ and $\mathcal{CN}(0, \sigma_{\mathbf{n}}^2)$, respectively. $\mathbf{p}$ stands for the $N_t \times 1$ precoding vector. The fading process is ergodic and the channel gains corresponding to both channels remain constant during each coherence interval and vary independently from one interval to the next. Also, the coherence times are assumed to be large enough so that the random coding arguments can be applied as in [20].

Similar to various other studies in the literature, we employ the ergodic secrecy rate to characterize the secrecy behavior, which is given as [20]

$$\bar{R}_s = \mathbb{E}_{\mathbf{H}_b, \mathbf{H}_e} \big(I(\mathbf{X}; \mathbf{y} | \mathbf{H}_b) - I(\mathbf{X}; \mathbf{z} | \mathbf{H}_e) \big)^+, \tag{5.26}$$

where $(a)^+ = \max(a, 0)$ and transmit antennas are assumed to be equally likely to be activated, i.e., $P_x(X) = 1/N_t$. We assume that the instantaneous knowledge of $\mathbf{H}_b$ and $\mathbf{H}_e$ is available at the transmitter, which would be true for active eavesdroppers and also for the cases where the eavesdropper is a participating system user in a wireless system [2].

5.3.2 Precoding for Secrecy Rate Maximization

From 5.14, the average mutual information of SSK transmission, assuming $P_X(X) = 1/N_t$, is given by

$$\mathbb{E}_{\mathbf{H}} I(\mathbf{X};\mathbf{y}|\mathbf{H}) = \log N_t - \frac{1}{N_t}\sum_{i=1}^{N_t}\mathbb{E}_{\mathbf{H},\mathbf{n}} \log \sum_{j=1}^{N_t} \exp\big(-\frac{\parallel \mathbf{H}\mathbf{E}_{ij}\mathbf{p}+\mathbf{n}\parallel^2 - \parallel \mathbf{n}\parallel^2}{\sigma^2_{\mathbf{n}}}\big), \quad (5.27)$$

where $\mathbf{E}_{ij} = \mathbf{X}_i - \mathbf{X}_j$.

For a specific channel realization, we obtain the instantaneous mutual information as

$$I(\mathbf{X};\mathbf{y}|\mathbf{H}) = \log N_t - \mathbb{E}_{\mathbf{n}} \log \exp\big(\frac{\parallel \mathbf{n}\parallel^2}{\sigma^2_{\mathbf{n}}}\big) - \frac{1}{N_t}\sum_{i=1}^{N_t}\mathbb{E}_{\mathbf{n}} \log \sum_{j=1}^{N_t} \exp\big(-\frac{\parallel \mathbf{H}\mathbf{E}_{ij}\mathbf{p}+\mathbf{n}\parallel^2}{\sigma^2_{\mathbf{n}}}\big). \quad (5.28)$$

Accordingly, for specific realizations of $\mathbf{H}_b$ and $\mathbf{H}_e$, the secrecy rate can be written from (5.26) as

$$R_s = \frac{1}{N_t}\Bigg(\sum_{i=1}^{N_t}\mathbb{E}_{\mathbf{n_z}} \log \sum_{j=1}^{N_t} \exp\big(-\frac{\parallel \mathbf{H}_e\mathbf{E}_{ij}\mathbf{p}+\mathbf{n_z}\parallel^2}{\sigma^2_{n_\mathbf{z}}}\big) - \sum_{k=1}^{N_t}\mathbb{E}_{\mathbf{n_y}} \log \sum_{l=1}^{N_t} \exp\Big(-\frac{\parallel \mathbf{H}_b\mathbf{E}_{kl}\mathbf{p}+\mathbf{n_y}\parallel^2}{\sigma^2_{n_\mathbf{y}}}\Big)\Bigg)^+. \quad (5.29)$$

The objective is to solve the following optimization problem

$$\max_{\mathbf{p}} R_s \quad (5.30)$$

$$\text{subject to} \;\; \mathbf{p}^H\mathbf{p} \le N_t. \quad (5.31)$$

The Lagrangian corresponding to this problem can be constructed as

$$L(\mathbf{p},\theta) = -R_s(\mathbf{p}) + \theta(\mathbf{p}^H\mathbf{p} - N_t), \quad (5.32)$$

Algorithm 4 Gradient Descent for Maximizing R_s

Step 1: Initialize $\mathbf{p}_1$ with constraint $\mathbf{p}^H\mathbf{p} \leq N_t$. Set step size u and minimum tolerance u_{min}.
Step 2: Set $k = 1$, compute $R_{s1} = R_s(\mathbf{p}_1)$ using (5.29).
Step 3: Compute $\nabla_{P_1} R_s(\mathbf{p})$.
Step 4: If $u \geq u_{min}$ goto Step 5, otherwise Stop algorithm and return $\mathbf{p}_k$.
Step 5: Calculate $\mathbf{p}'_k = \mathbf{p}_k + u\nabla_{\mathbf{p}_k} R(\mathbf{p})$. Normalize $\mathbf{p}'_k$ so that $\mathbf{p}^H\mathbf{p} \leq N_t$ is satisfied.
Step 6: Compute $R' = R(\mathbf{p}'_k)$.
Step 7: If $R' \geq R_k$ update $R_{k+1} = R'$ and $\mathbf{p}_{k+1} = \mathbf{p}'_k$ and goto Step 8, otherwise let $u = 0.5u$ and goto Step 4.
Step 8: $k = k + 1$ goto Step 3.

where θ is the Lagrange multiplier. The gradient of the Lagrangian is given by

$$-\nabla_{\mathbf{p}} R_s(\mathbf{p}) + \theta\mathbf{p} = 0. \tag{5.33}$$

We solve the optimization problem in (5.30)-(5.31) numerically using the gradient descent method as illustrated in Algorithm 4.

The implementation of Algorithm 4 requires calculation of the gradient of R_s, which can be derived as

$$\nabla_{\mathbf{p}} R_s(\mathbf{p}) = \frac{1}{N_t}\left(\sum_{i=1}^{N_t} \mathbb{E}_{\mathbf{n_z}}\left(\frac{\sum\limits_{j=1,j\neq i}^{N_t} -\nabla_{\mathbf{p}}\Psi_{e,ij}(\mathbf{p})\exp(-\frac{\Psi_{e,ij}(\mathbf{p})}{\sigma^2_{n_\mathbf{z}}})}{\sigma^2_{n_\mathbf{z}}\ln 2\sum\limits_{j=1}^{N_t}\exp(-\frac{\Psi_{e,ij}(\mathbf{p})}{\sigma^2_{n_\mathbf{z}}})}\right)\right.$$
$$\left. - \sum_{k=1}^{N_t} \mathbb{E}_{\mathbf{n_y}}\left(\frac{\sum\limits_{l=1,l\neq k}^{N_t} -\nabla_{\mathbf{p}}\Psi_{b,kl}(\mathbf{p})\exp(-\frac{\Psi_{b,kl}(\mathbf{p})}{\sigma^2_{n_\mathbf{y}}})}{\sigma^2_{n_\mathbf{y}}\ln 2\sum\limits_{l=1}^{N_t}\exp(-\frac{\Psi_{b,kl}(\mathbf{p})}{\sigma^2_{n_\mathbf{y}}})}\right)\right), \tag{5.34}$$

where

$$\Psi_{b,kl}(\mathbf{p}) = \| \mathbf{H}_b\mathbf{E}_{kl}\mathbf{p} + \mathbf{n_y} \|^2, \tag{5.35}$$
$$\Psi_{e,ij}(\mathbf{p}) = \| \mathbf{H}_e\mathbf{E}_{ij}\mathbf{p} + \mathbf{n_z} \|^2 . \tag{5.36}$$

Using the definition of the complex gradient vector which is

$$[\nabla_{\mathbf{g}} f]_i = \frac{\partial f}{\partial [\mathbf{g}^*]_i}, \tag{5.37}$$

where the complex derivative of scalar function f is defined as

$$\frac{\partial f}{\partial g^*} = \frac{\partial Re\{f\}}{\partial g^*} + j\frac{\partial Im\{f\}}{\partial g^*}, \tag{5.38}$$

we obtain

$$\nabla_{\mathbf{p}}\Psi_{b,kl}(\mathbf{p}) = \mathbf{E}_{kl}^H\mathbf{H}_b^H\mathbf{H}_b\mathbf{E}_{kl}\mathbf{p} + \mathbf{E}_{kl}^H\mathbf{H}_b^H\mathbf{n}_{\mathbf{y}}, \tag{5.39}$$

$$\nabla_{\mathbf{p}}\Psi_{e,ij}(\mathbf{p}) = \mathbf{E}_{ij}^H\mathbf{H}_e^H\mathbf{H}_e\mathbf{E}_{ij}\mathbf{p} + \mathbf{E}_{ij}^H\mathbf{H}_e^H\mathbf{n}_{\mathbf{z}}. \tag{5.40}$$

By substituting these expressions in (5.34), we can numerically evaluate the gradient and implement a gradient descent algorithm. Algorithm 4 illustrates the iterative search for the optimal $\mathbf{p}$ using the gradient descent method which is guaranteed to converge to a local optimum. Hence, by repeating the algorithm with different initializations for $\mathbf{p}$, it is possible to obtain improved solutions.

5.3.3 Low Complexity Precoding Schemes

The previous section developed an iterative approach (Algorithm 4) for maximization of the secrecy rate. However, due to the need for many evaluations of the mutual information expression, which requires numerical evaluation of the expectation operator, Algorithm 4 is computationally complex. Hence, in this section, we propose precoding schemes which are of significantly lower complexity in the sense that their implementation are based on closed-form solutions. Both algorithms are based on the observation that, in the high SNR region, the term corresponding to the points with the minimum Euclidean distance is dominant in (5.29). Accordingly, modification of the received constellation vectors which results in an increased minimum Euclidean distance from Bob's point of view and a reduced minimum Euclidean distance at Eve can be an effective transmission scheme.

First, let us consider scenarios where the eavesdropper is equipped with a single antenna. For these scenarios, it is possible to apply precoding with the aid of the instantaneous knowledge on the eavesdropper's channel, which results in

zero information leakage to the eavesdropper. Consider $N_t = 2$, where we have $\mathbf{p} = [\rho_1 \;\; \rho_2]^T$. Let $\rho_i = r_i \exp(j\phi_i)$. For this case, it is straightforward to find ρ_1 and ρ_2 such that

$$\rho_1 h_{e_1} = \rho_2 h_{e_2} \tag{5.41}$$

is satisfied. This increases Eve's confusion to the highest level, as the precoder maps the constellation points to a single point from the eavesdropper's point of view. In order to solve (5.41), we substitute $r_1 = \sqrt{2 - r_2^2}$ and by letting

$$\frac{h_{e_2}}{h_{e_1}} = \lambda \exp(j\varphi), \tag{5.42}$$

we obtain

$$\rho_1 = \sqrt{\frac{2\lambda^2}{1+\lambda^2}} \exp(j\varphi), \quad \rho_2 = \sqrt{\frac{2}{1+\lambda^2}}. \tag{5.43}$$

While the stated approach addresses the signal design for $N_t = 2$, for $N_t > 2$, the set of precoding coefficients can be found by repeatedly applying (5.43) as stated in Algorithm 5. The working principle of the transmit signal design stated in this algorithm is demonstrated in Fig. 5.6. We will show in Section 5.4.7 that, this algorithm which is of the complexity $\mathcal{O}(N_t^3)$ is capable of achieving maximum secrecy rate at sufficiently high SNR values.

Algorithm 5 Low-complexity Algorithm with ($N_{r_e} = 1$)

Step 1: Consider the set of all combinations of N_t as $\mathbf{i}$.
Step 2: For each combination, consider $\mathbf{h}_{e(i_1)}$ and $\mathbf{h}_{e(i_2)}$, namely i_1^{th} and i_2^{th} columns of $\mathbf{H}_e$, and obtain ρ_1 and ρ_2 using (5.43).
Step 3: Consider the precoded channel $\rho_1 \mathbf{h}_{e(i_1)} = \rho_2 \mathbf{h}_{e(i_2)} = \mathbf{h}_{\text{eff}}$.
Step 4: Apply (5.43) to $\mathbf{h}_{\text{eff}}$ and $\mathbf{h}_{e(i_3)}$.
Step 5: Repeat this procedure until all the points are mapped to a single point.
Step 6: Calculate the minimum Euclidean distance over the main channel for each combination and choose $\{\rho_1, \rho_2, \ldots, \rho_{N_t}\}$ corresponding to the combination which results in the maximum minimum Euclidean distance at Bob.

For the scenarios where $N_{r_e} > 1$, finding a precoding vector which results in zero mutual information over the eavesdropper's channel is not possible. Hence, we introduce a low-complexity alternative for Algorithm 4 by modifying the minimum Euclidean distances over the main channel as well as the eavesdropper's channel. Consider $N_t = 2$, where we have $\mathbf{p} = [\rho_1 \;\; \rho_2]^T$. The term to be optimized

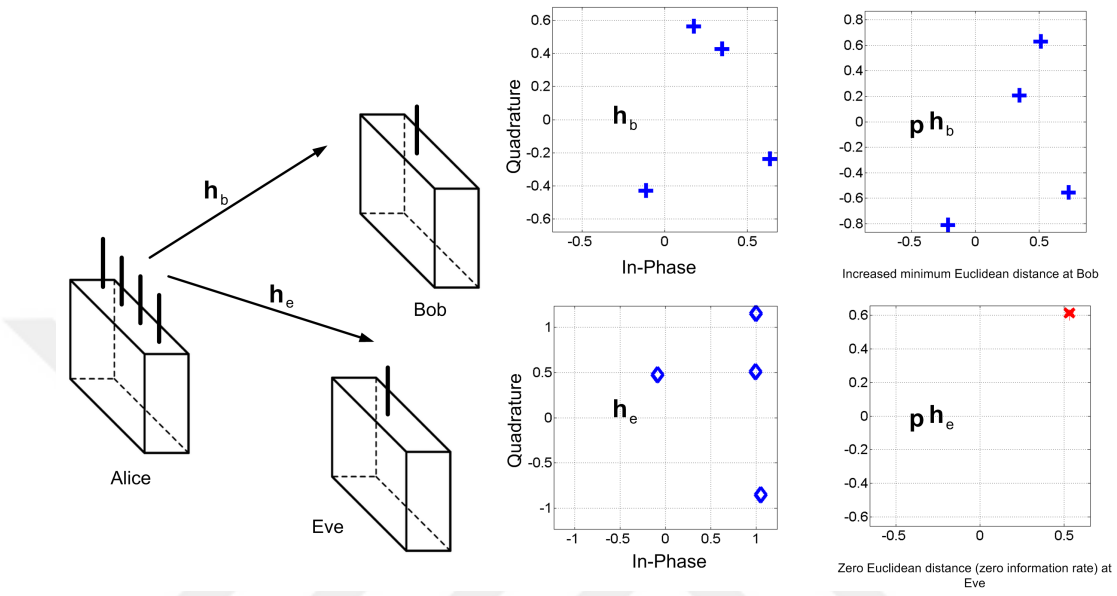

Figure 5.6: An example demonstrating the working principle of Algorithm 5.

can be written as [79]

$$\begin{aligned} d(r_1) &= \|\mathbf{H}\mathbf{E}_{12}\mathbf{p}\|^2 = \|\rho_1\mathbf{h}_1 - \rho_2\mathbf{h}_2\|^2 \\ &= \tau r_1^2 - (2\mu\cos(\psi_1 - \psi_2 + \phi))r_1\sqrt{2 - r_1^2} + 2\|\mathbf{h}_2\|^2, \end{aligned} \tag{5.44}$$

where $\mathbf{h}_2^H\mathbf{h}_1 = \mu\exp(j\phi)$ and $\|\mathbf{h}_1\|^2 - \|\mathbf{h}_2\|^2 = \tau$. In derivation of (5.44), we have used $r_2 = \sqrt{2 - r_1^2}$ which is a result of the constraint in (5.31). So as to derive the conditions under which $d(r_1)$ has a maximum or a minimum, we take the second derivative of (5.44) with respect to r_1, as

$$d''(r_1) = 2\tau - (4\mu\cos(\psi_1 - \psi_2 + \phi))\frac{\sqrt{2 - r_1^2}(r_1^3 - 3r_1)}{r_1^4 - 4r_1^2 + 4}. \tag{5.45}$$

By considering $\cos(\psi_1 - \psi_2 + \phi) = \pm 1$, the second term in (5.45) is dominant in determining the sign of $d''(r_1)$. In order for (5.44) to have a minimum, it is required that $\psi_1 - \psi_2 + \phi = 0$. On the other hand, so as to maximize (5.44), we need to consider $\psi_1 - \psi_2 + \phi = \pi$. By taking into the account these conditions, the optimal value of $d(r_1)$ can be obtained by setting the first derivative of (5.44)

equal to zero, as

$$2\tau r_1 - (2\mu\cos(\psi_1 - \psi_2 + \phi))\frac{2 - 2r_1^2}{\sqrt{2 - r_1^2}} = 0. \tag{5.46}$$

Accordingly, the elements of the optimal $\mathbf{p}$ is attained as

$$\rho_1 = A\exp(j\psi_1), \quad \rho_2 = B\exp(j\psi_2), \tag{5.47}$$

where $d(r_1)$ is maximized with $A = (1+\frac{\tau}{(4\mu^2+\tau^2)^{1/2}})^{1/2}$, $B = (1-\frac{\tau}{(4\mu^2+\tau^2)^{1/2}})^{1/2}$ and $\psi_1 - \psi_2 + \phi = \pi$. Also, minimum of $d(r_1)$ is attained with $A = (1-\frac{\tau}{(4\mu^2+\tau^2)^{1/2}})^{1/2}$, $B = (1+\frac{\tau}{(4\mu^2+\tau^2)^{1/2}})^{1/2}$ and $\psi_1 - \psi_2 + \phi = 0$.

With the aid of the calculations above, we propose a low-complexity signal design algorithm as stated in Algorithm 6. More specifically, in Algorithm 6, the intention is to maximize the minimum Euclidean distance over the main channel (strategy 1) or to minimize it from Eve's point of view (strategy 2). At each time instance, after finding the precoding coefficients corresponding to these two strategies, transmitter selects the strategy which gives rise to a higher secrecy rate.

Algorithm 6 Low-complexity minimum Euclidean distance modification algorithm ($N_t = 2, N_{r_e} > 1$)

Step 1: Apply (5.47) to obtain $\mathbf{p}_1 = [\rho_1^{(b)}\ \rho_2^{(b)}]$ which maximizes (5.44).
Step 2: Apply (5.47) to obtain $\mathbf{p}_2 = [\rho_1^{(e)}\ \rho_2^{(e)}]$ which minimizes (5.44).
Step 3: Using (5.29), calculate the secrecy rates corresponding to $\mathbf{p}_1$ and $\mathbf{p}_2$ and select the precoder which gives rise to the higher R_s.

For the scenarios with $N_{r_e} > 1$ and $N_t > 2$, obtaining a closed-form precoder which maximizes or minimizes the minimum Euclidean distance is not straight forward. In these scenarios, the maximization and the minimization in steps 1 and 2 of the Algorithm 6 can be done using the optimization proposed in [80, Eq. (8)]. Besides serving as low complexity transmit signal design schemes, the solutions attained from Algorithms 5 and 6 are appropriate candidates for initialization of Algorithm 4.

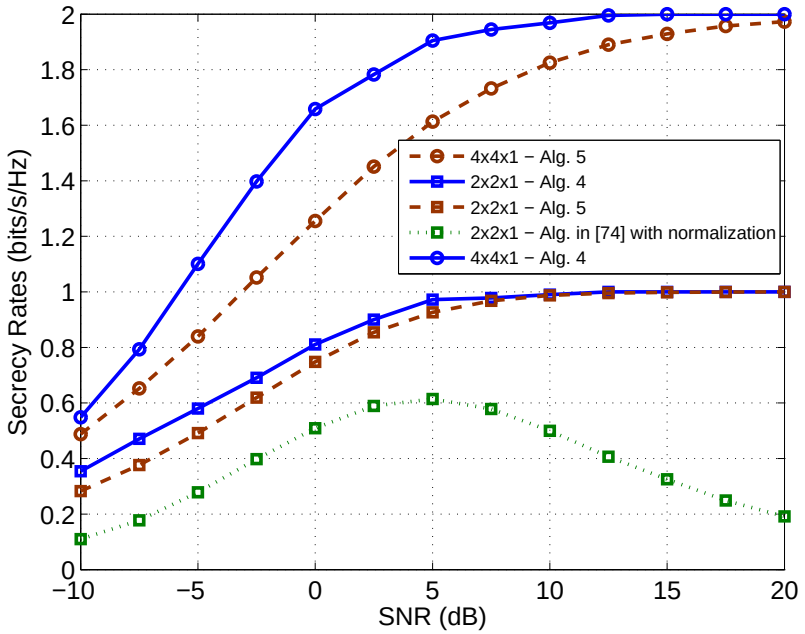

Figure 5.7: Average secrecy rate for precoded SSK with $N_{r_e} = 1$.

5.3.4 Numerical Results

In this section, we quantify the achievable secrecy rates for SSK using the proposed precoding techniques. Throughout the simulations, equal noise power is assumed at Bob and Eve. We consider i.i.d. Rayleigh channel coefficients for the main channel and the eavesdropper's channel, and evaluate the achievable secrecy rates by averaging (5.26) over many channel realizations.

Figure 5.7 denotes the achievable secrecy rates with the aid of the proposed algorithms when the eavesdropper is equipped with a single antenna. An increased secrecy rate is achieved with a higher number of transmit antennas as the rate is increased over the main channel while the transmission rate over the eavesdropper's channel is restricted as a result of the precoding in Algorithms 4 and 5. Figure 5.7 also compares the performance of the algorithms proposed with that of the scheme in [74]. Clearly, the newly proposed algorithms considerably outperform the precoding scheme in [74], when an additional normalization is

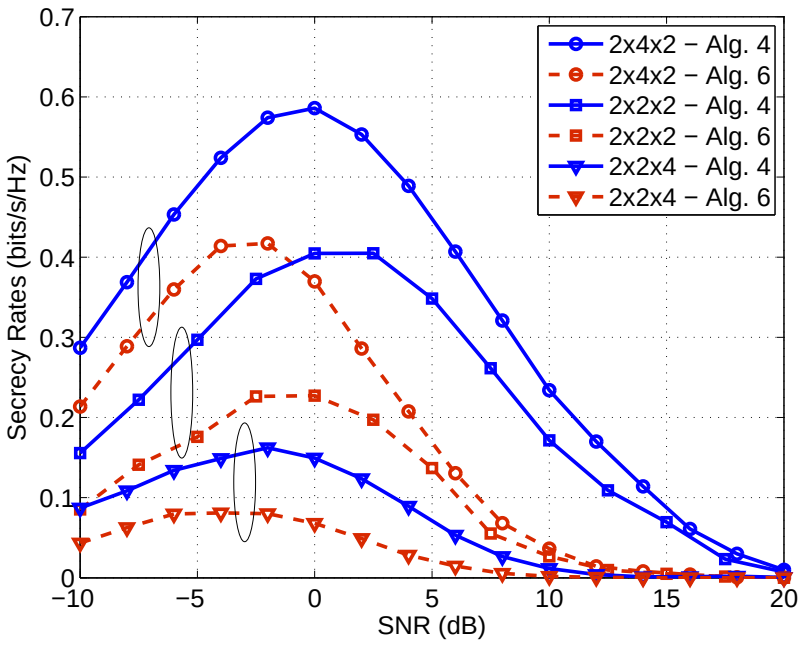

Figure 5.8: Average secrecy rate for precoded SSK with $N_{r_e} > 1$.

carried out on the precoding coefficients obtained to satisfy (5.31).

Figure 5.8 illustrates that, in scenarios where the eavesdropper has more than one antenna, the proposed precoding schemes are not capable of providing positive secrecy rates for high SNRs. This is because, neither of the precoding schemes in Algorithms 4 and 6 have the capability to realize a transmission with no leakage over the eavesdropper's channel. Accordingly, when SNR is sufficiently high, the mutual information over the eavesdropper's channel will also approach the saturation value of $\log N_t$ which results in zero secrecy rate.

The numerical results provided in Fig. 5.7 and Fig. 5.8 reveal the gap between Algorithm 4 and its low complexity alternatives, Algorithms 5 and 6. Finally, we compare the CPU times associated with the implementation of each of the proposed algorithms for a given realization of $\mathbf{H}_b$ and $\mathbf{H}_e$. We assume that Algorithm 4 is repeated with 10 initializations and expectations are estimated using 1000 samples. Table 5.2 clearly shows that the computational complexities associated

Table 5.1: CPU times required for obtaining precoder for secure SSK transmission (Intel Core-i7-4770, 3.4 GHz)

$N_t \times N_{r_b} \times N_{r_e}$	Alg. 4	Alg. 5	Alg. 6
$2 \times 1 \times 1$	2.4476 (s)	0.1299 (s)	–
$2 \times 2 \times 2$	3.0647 (s)	–	0.1386 (s)

with Algorithms 5 and 6 are notably less than that of Algorithm 4.

5.4 Space Shift Keying with Dynamic Antenna Index Assignment

In this section, we propose a new secure transmission scheme which relies on SSK with dynamic antenna index assignment. In particular, we adopt an antenna index assignment scheme which varies from one block of information bits to another according to the channel between the legitimate users. The transmitter assigns the antenna indices according to a decreasing order of the magnitudes of their instantaneous channel gains. If the channel reciprocity holds, the legitimate receiver can simply acquire the antenna index assignment pattern initiated by the transmitter and can detect the transmitted bits accordingly. In contrast, an eavesdropper which is sufficiently far from the legitimate receiver observing a statistically independent channel cannot track the antenna index assignment pattern, and as a result, it fails to detect the message.

We first evaluate the achievable secrecy rates for the scenarios with perfect channel reciprocity and an eavesdropper with an independent channel for high SNRs. We also study the impacts of imperfect reciprocity and presence of a nearby eavesdropper. The imperfect reciprocity results in a mismatched antenna index assignment pattern at the legitimate users and deteriorates the reliability of transmission. Moreover, an eavesdropper who is sufficiently close to the legitimate receiver may observe a channel that is correlated with that of the legitimate

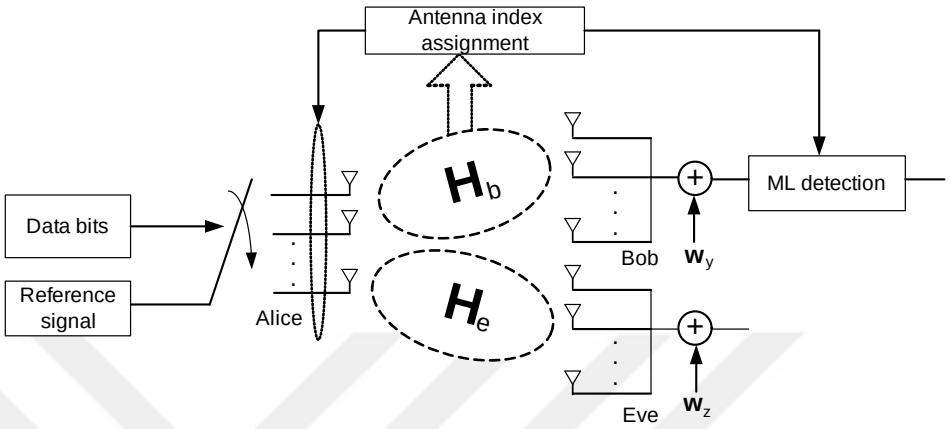

Figure 5.9: SSK with dynamic antenna index assignment.

receiver. In presence of such an eavesdropper the security of the proposed scheme is breached.

So as to resolve the above-mentioned deficiencies, we also propose a practical secure transmission scheme in which antenna index assignment is carried out according to a rotated legitimate channel. Inspired by the channel estimation scheme proposed in [62], we include a training session which is done with reference signals rotated by random unitary matrices selected from a codebook, which is assumed to be known by all the parties including the eavesdropper. The advantages of this approach are two-fold: First, since the specific unitary matrices utilized are only known by the legitimate users, the eavesdropper is unable to acquire the antenna index assignment even if her channel is highly correlated with the legitimate user's channel. The second advantage is that, by selecting the unitary matrix from the codebook in a manner that the minimum channel magnitude difference among the antennas is maximized, the probability of mismatched antenna index assignment pattern at the legitimate users is reduced, and accordingly, we can improve the reliability for the scenarios with imperfect reciprocity.

5.4.1 System Model for SSK with Dynamix Antenna Index Assignment

Consider a general MIMOME wiretap channel as depicted in Fig. 5.9. The transmitter, Alice, the legitimate receiver, Bob, and the eavesdropper, Eve, are assumed to be equipped with N_t, N_{r_b} and N_{r_e} antennas, respectively. We consider the use of SSK for which the antenna indices are employed for embedding user data, therefore a one-to-one mapping is established between the blocks of information bits to be transmitted and the indices of the transmit antennas in the array [51].

The received signals at the legitimate receiver and the eavesdropper are given by

$$\mathbf{y} = \mathbf{H}_b\mathbf{x} + \mathbf{w}_\mathbf{y}, \tag{5.48}$$

$$\mathbf{z} = \mathbf{H}_e\mathbf{x} + \mathbf{w}_\mathbf{z}, \tag{5.49}$$

where $\mathbf{H}_b$ and $\mathbf{H}_e$ are the $N_{r_b} \times N_t$ and $N_{r_e} \times N_t$ channel matrices corresponding to the legitimate channel and the eavesdropper's channel, respectively. The elements of the channel matrices are i.i.d. zero-mean and unit-variance circularly symmetric complex Gaussian random variables $\mathcal{CN}(0, 1)$. We consider a block fading scenario in which $\mathbf{H}_b$ and $\mathbf{H}_e$ remain constant over a block of N_c symbols and vary independently from one block to the next. The transmitted symbol, $\mathbf{x}$, is of the form $[0\ 0\ ...\ 1\ ...\ 0]^T$, with the position of 1 indicating the antenna being activated. In (5.48) and (5.49), $\mathbf{w}_\mathbf{y}$ and $\mathbf{w}_\mathbf{z}$ are additive white Gaussian noise vectors which follow $\mathcal{CN}(0, \sigma_b^2)$ and $\mathcal{CN}(0, \sigma_e^2)$, respectively. Furthermore, $\mathbf{H}_b$, $\mathbf{H}_e$, $\mathbf{w}_\mathbf{y}$ and $\mathbf{w}_\mathbf{z}$ are independent. We assume that the fading process is ergodic. We also assume that the response of the channel from the transmitter to the legitimate receiver is identical to the response in the opposite direction. The legitimate receiver and the eavesdropper estimate their own channels perfectly. However, the transmitter may estimate the main channel correctly or erroneously depending on whether the reciprocity is perfect or imperfect.

5.4.2 CSI-Based Antenna Index Assignment

In this section, we propose an SSK transmission scheme which provides communication confidentiality via not allowing the eavesdropper to determine the indices of antennas activated. In order to realize such a transmission scheme, the transmitter and the legitimate receiver obtain local channel estimates. This is to say, training signals are transmitted from the transmitter to the legitimate receiver and vice versa as depicted in Fig. 5.10. We refer to this scheme as Scheme 1. After estimating the channel, the transmitter sorts the columns of the channel matrix and assigns indices to the antennas in such a way that $\|\mathbf{h}_{b_1}\|^2 \geq \|\mathbf{h}_{b_2}\|^2 \geq \ldots \geq \|\mathbf{h}_{b_{N_t}}\|^2$. Based on channel reciprocity, the legitimate receiver can obtain the antenna index assignment pattern initiated by the transmitter through its local channel estimate, and then decode the transmitted message. In contrast, the eavesdropper receiving the signal through a statistically independent channel cannot track the antenna index assignment pattern, and as a result, fails to detect the message.

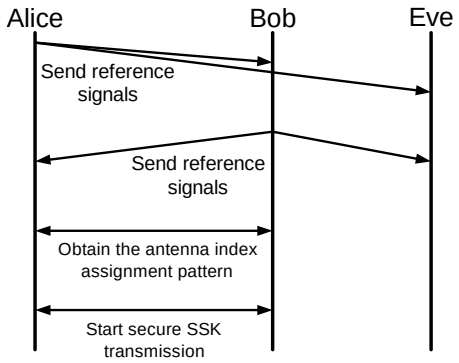

Figure 5.10: CSI-based antenna index assignment (Scheme 1).

5.4.3 Asymptotic Ergodic Secrecy Rates with Perfect Reciprocity

In this section, we perform an information-theoretic analysis of the proposed scheme under the perfect reciprocity assumption. More specifically, we derive the asymptotic secrecy rate for SSK with CSI-based antenna index assignment for high SNRs. With perfect reciprocity, the setup is equivalent to the case of a wiretap channel with the main channel CSI only, and the ergodic achievable secrecy rates are evaluated as [20]

$$R_s = \mathbb{E}_{\mathbf{H}_b,\mathbf{H}_e}\Big\{\big(I(\mathbf{x};\mathbf{y}|\mathbf{H}_b) - I(\mathbf{x};\mathbf{z}|\mathbf{H}_e)\big)^+\Big\}, \tag{5.50}$$

where $I(\mathbf{x};\mathbf{y}|\mathbf{H}_b)$ and $I(\mathbf{x};\mathbf{z}|\mathbf{H}_e)$ are mutual information terms corresponding to the main channel and the eavesdropper's channel, respectively. For an asymptotic analysis, we assume that $\sigma_b \to 0$ and $\sigma_e \to 0$. As a result, both of the receivers are capable of detecting the antennas which have been activated at the transmitter correctly. In this case, the legitimate receiver achieves the maximum rate, i.e., $\log N_t$ bits per transmission. However, the eavesdropper can only make a random guess among the $N_t!$ words of length $n_c = N_c \log N_t$ bits. Hence, the mutual information for the eavesdropper can be calculated as [53]

$$I(\hat{\mathbf{x}}^{n_c};\hat{\mathbf{z}}^{n_c}) = H(\hat{\mathbf{z}}^{n_c}) - H(\hat{\mathbf{z}}^{n_c}|\hat{\mathbf{x}}^{n_c}), \tag{5.51}$$

where $\hat{\mathbf{x}}$ denotes the transmitted bits and $\hat{\mathbf{z}}$ denotes the received bits at the eavesdropper. The mutual information in (5.51) is calculated using

$$H(\hat{\mathbf{z}}^{n_c}) = n_c, \tag{5.52}$$

$$H(\hat{\mathbf{z}}^{n_c}|\hat{\mathbf{x}}^{n_c}) = \sum_{(\hat{\mathbf{x}}^{n_c},\hat{\mathbf{z}}^{n_c})\in\mathcal{X}\times\mathcal{Z}} P_{xz}(\hat{\mathbf{x}}^{n_c},\hat{\mathbf{z}}^{n_c}) \log\left(\frac{1}{P_{xz}(\hat{\mathbf{z}}^{n_c}|\hat{\mathbf{x}}^{n_c})}\right), \tag{5.53}$$

in which,

$$P_{z|x}(\hat{\mathbf{z}}^{n_c}|\hat{\mathbf{x}}^{n_c}) = \frac{1}{N_t!}, \tag{5.54}$$

$$P_{xz}(\hat{\mathbf{x}}^{n_c},\hat{\mathbf{z}}^{n_c}) = P_x(\hat{\mathbf{x}}^{n_c})P_{z|x}(\hat{\mathbf{z}}^{n_c}|\hat{\mathbf{x}}^{n_c}) = \left(\frac{1}{2}\right)^{n_c}\frac{1}{N_t!}. \tag{5.55}$$

As a result, (5.51) becomes

$$I(\hat{\mathbf{x}}^{n_c};\hat{\mathbf{z}}^{n_c}) = n_c - \log(N_t!) \quad \text{(bits)}. \tag{5.56}$$

Therefore, at high SNRs, the mutual information at the eavesdropper, i.e., $I(\mathbf{x};\mathbf{z}|\mathbf{H}_e)$, approaches $\log N_t - \frac{\log(N_t!)}{N_c}$ bits per transmission and the achievable secrecy rate is given by

$$R_{s,asymp} = \frac{\log(N_t!)}{N_c} \quad \text{(bpcu)}, \tag{5.57}$$

where bpcu is short for bits per channel use.

5.4.4 Reliability under Imperfect Reciprocity

Channel estimation errors can result in mismatched antenna indices at the legitimate users. To model such an imperfect channel estimation at the transmitter, we assume that the estimate is a noisy version of the actual channel [81], i.e.,

$$\tilde{\mathbf{h}}_{b_i} = \sqrt{1-\tau^2}\mathbf{h}_{b_i} + \tau\mathbf{q}_i, \tag{5.58}$$

where $\tilde{\mathbf{h}}_{b_i}$ is the estimated channel between the i^{th} transmit antenna and the receive antennas, $\mathbf{q}_i$ is the i^{th} column of an $N_{r_b} \times N_t$ random matrix $\mathbf{Q}$ which follows $\mathcal{CN}(0,\mathbf{I})$, and τ is a parameter which determines the quality of estimation. While in the scenarios with perfect reciprocity, the symbol error probability of the proposed transmission scheme is equal to that of the conventional SSK, in the presence of the channel estimation errors at the transmitter, the mismatched antenna index assignment pattern can increase the symbol error rate (SER). More specifically, the SER of the proposed SSK with the CSI-based antenna index assignment is given by

$$P_{SER} \approx 1 - P_I(1 - P'_{SER}), \tag{5.59}$$

where P'_{SER} denotes the SER of the conventional SSK and P_I stands for the probability of the identical antenna indices at the legitimate users, which can be calculated as

$$P_I = P(\theta_A|\theta_B), \tag{5.60}$$

where θ_A and θ_B stand for the events that $\|\tilde{\mathbf{h}}_{b_1}\|^2 \geq \|\tilde{\mathbf{h}}_{b_2}\|^2 \geq \ldots \geq \|\tilde{\mathbf{h}}_{b_{N_t}}\|^2$ and $\|\mathbf{h}_{b_1}\|^2 \geq \|\mathbf{h}_{b_2}\|^2 \geq \ldots \geq \|\mathbf{h}_{b_{N_t}}\|^2$, respectively. Clearly, the quality of channel

estimation plays a vital role in keeping the probability of error acceptably low. On the other hand, the channels in which the norm squares of the columns are close to each other are more prone to the occurrence of mismatched antenna indices. Consider the simple case of a MISO main channel with $N_t = 2$. Given that $|h_1|^2 \geq |h_2|^2$, the probability of having mismatched antenna indices is equal to

$$P_{MI} = 1 - P_I = P\{|\tilde{h}_1|^2 < |\tilde{h}_2|^2\} = P\{|\tilde{h}_1|^2 - |\tilde{h}_2|^2 < 0\}. \tag{5.61}$$

Noting that from (5.58), conditioned on the actual channel gains, $\tilde{h}_1$ and $\tilde{h}_2$ are distributed as $\mathcal{CN}(\sqrt{1-\tau^2}h_1, \tau^2)$ and $\mathcal{CN}(\sqrt{1-\tau^2}h_2, \tau^2)$, respectively, and $D = |\tilde{h}_1|^2 - |\tilde{h}_2|^2$ is difference of two independent chi-square random variables. Hence, conditioned on h_1 and h_2, the probability of mismatched antenna indices in (5.61) can be evaluated using [82, Eq. (4)] as

$$\begin{aligned} P_{MI} = {} & Q_1\Big(\sqrt{\frac{1-\tau^2}{\tau^2}}|h_2| \ , \ \sqrt{\frac{1-\tau^2}{\tau^2}}|h_1|\Big) \\ & -\frac{1}{2}\exp\Big(-\frac{1-\tau^2}{2\tau^2}(|h_1|^2 + |h_2|^2)\Big) I_0\Big(\frac{1-\tau^2}{\tau^2}|h_1||h_2|\Big), \end{aligned} \tag{5.62}$$

where $Q_1(.,.)$ is the first-order Marcum Q-function

$$Q_1(a,b) = \int_b^\infty u \exp\Big(-\frac{(u^2+a^2)}{2}\Big) I_0(au)du, \tag{5.63}$$

and $I_0(.,.)$ denotes the 0^{th}-order modified Bessel function of the first kind. Defining $\Delta = |h_1|^2 - |h_2|^2$, we can rewrite (5.62) as

$$\begin{aligned} P_{MI} = {} & Q_1\Big(\sqrt{\frac{1-\tau^2}{\tau^2}(|h_1|^2 - \Delta)} \ , \ \sqrt{\frac{1-\tau^2}{\tau^2}}|h_1|\Big) \\ & -\frac{1}{2}\exp\Big(-\frac{1-\tau^2}{2\tau^2}(2|h_1|^2 - \Delta)\Big) I_0\Big(\frac{1-\tau^2}{\tau^2}|h_1|\sqrt{|h_1|^2 - \Delta}\Big). \end{aligned} \tag{5.64}$$

Table 5.2 illustrates the values of P_{MI} obtained from evaluation of (5.64) for different values of $|h_1|^2$ and Δ. It is seen from this table that for a fixed $|h_1|^2$ and a given quality of channel estimation τ, increasing Δ can decrease the probability of antenna index mismatch at the legitimate users, as expected.

Table 5.2: Probability of antenna index mismatch for $\tau = 0.05$.

Δ \ $\lvert h_1 \rvert^2$	0.25	0.5	0.75	1
0.05	0.1462	0.2344	0.2788	0.3066
0.1	0.0123	0.0681	0.1162	0.1527
0.15	0.0001	0.0106	0.0340	0.0596
0.2	0.0000	0.0007	0.0065	0.0175

5.4.5 Threat of a Nearby Eavesdropper

Security of the SSK scheme with a CSI-based antenna index assignment relies on the spatial separation between Bob and Eve. That is, if the wireless channel experienced by Eve is similar to the one experienced by Alice and Bob, the security will easily be breached. It is well known that the channel experienced by a nearby eavesdropper may be highly correlated with the main channel [83]. Denoting the vector representation of the channel matrices $\mathbf{H}_b$ and $\mathbf{H}_e$ as

$$\mathbf{g}_b = \text{vec}(\mathbf{H}_b), \tag{5.65}$$

$$\mathbf{g}_e = \text{vec}(\mathbf{H}_e), \tag{5.66}$$

we model the correlation between $\mathbf{H}_b$ and $\mathbf{H}_e$ using [62, Eq. (31)]

$$\mathbb{E}\{\mathbf{g}_e \mathbf{g}_b^H\} = \rho \mathbf{I}, \tag{5.67}$$

where ρ is a parameter which takes values in the interval $[-1 \;\; 1]$. When $\mathbf{H}_b$ and $\mathbf{H}_e$ are independent, we have $\rho = 0$. However, some recent experiments have shown that an eavesdropper which is sufficiently close to the legitimate receiver can experience a channel, which is correlated with the main channel with a correlation parameter as high as $\rho = 0.99$ [83], which allows the adversary to infer significant portions of the data transmitted using Scheme 1.

5.4.6 Dynamic Antenna Index Assignment based on Rotated Channels

To remedy the problems stated in subsections 5.4.4 and 5.4.5, in this section, we provide an antenna index assignment scheme, which is robust to imperfect reciprocity and also able to mitigate the threat of a nearby eavesdropper. The basic idea is to perform the antenna index assignment according to a rotated channel. So as to avoid wiretapping by an eavesdropper who is potentially close to the legitimate receiver or the transmitter, the rotation matrix should be kept secret. Furthermore, by selecting this rotation matrix in a manner that the magnitude squares of the channel gains are maximally separated, robustness against the channel estimation errors can be enhanced.

The procedure for the proposed dynamic antenna index assignment according to the rotated channel (referred to as Scheme 2) is illustrated in Fig. 5.11. In order for the legitimate users to obtain the rotated channel, the following steps are taken:

- Alice sends a reference signal to Bob which makes it possible for him to estimate the main channel, $\mathbf{H}_b$. Bob then locally generates a codebook of isotropic random unitary matrices (by applying the singular value decomposition (SVD) on zero-mean complex Gaussian matrices).
- Alice generates a secret sequence $\mathbf{s}$ and sends it to Bob.
- Bob selects a rotation matrix $\mathbf{G} \in \mathbb{C}^{N_{rb} \times N_{rb}}$ among the matrices in the codebook which maximizes the minimum distance among the norm squares of the columns of the rotated channel. Bob then multiplies the received signal by $\mathbf{G}$ and echoes it back to Alice.
- Finally, Bob sends a reference signal to Alice which allows her to estimate the main channel, and accordingly retrieve $\mathbf{G}$.

This strategy mitigates the threat of a nearby eavesdropper. This is because the information of the secret sequence is only known by Alice, i.e., she is the only one

who can acquire $\mathbf{G}$. By taking advantage of her knowledge on $\mathbf{s}$ and $\tilde{\mathbf{H}}_b$, Alice can acquire the rotated channel $\mathbf{F}_b = \mathbf{G}\mathbf{H}_b$ from the echoed signal which is given by

$$\mathbf{r}_a = \mathbf{H}_b^H \mathbf{F}_b \mathbf{s} + \mathbf{H}_b^H \mathbf{G} \mathbf{w}_1 + \mathbf{w}_2, \tag{5.68}$$

where $\mathbf{w}_1$ and $\mathbf{w}_2$ are additive white Gaussian noise terms at Bob (echoed back to Alice) and at Alice, respectively. Alice estimates $\mathbf{H}_b^H \mathbf{F}_b$ from (5.68) (e.g., using a least square solution) and hence she acquires the rotated channel $\mathbf{F}_b$ using her knowledge on $\mathbf{H}_b^H$. A nearby Eve, in contrast, cannot acquire any information about $\mathbf{G}$ and as a result, fails to detect the bits transmitted. Moreover, since Bob selects the rotation matrix using the following rule

$$\mathbf{G}_{\hat{k}} = \arg \max_{k} \min_{\forall i,j} \left| \|\mathbf{f}_{b_{ki}}\|^2 - \|\mathbf{f}_{b_{kj}}\|^2 \right| \quad i, j = 1, \ldots, N_t, \quad j \neq i, \tag{5.69}$$

where $\mathbf{f}_{b_{ki}}$ is the i^{th} column of the rotated channel corresponding to the k^{th} rotation matrix (i.e., $\mathbf{F}_{bk}$), the probability of a mismatched antenna index assignment between the legitimate users is reduced. The price to be paid in implementation of Scheme 2 with respect to Scheme 1 is the need for two extra steps in the process of obtaining the antenna index assignment pattern.

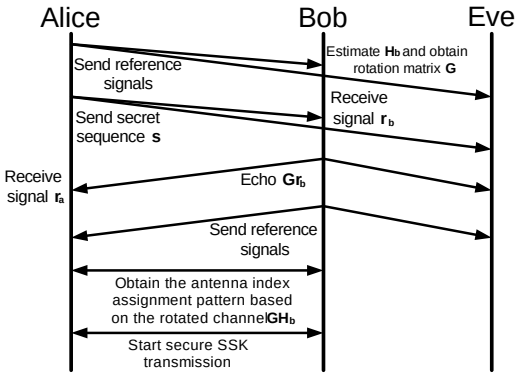

Figure 5.11: Dynamic antenna index assignment to avoid wiretapping by a nearby eavesdropper (Scheme 2).

5.4.7 Numerical Examples

This section provides several numerical examples to demonstrate the efficacy of the proposed transmission schemes. Throughout the simulations, we assume that the main and the eavesdropper's channels follow the same statistics and the additive noise terms at both receivers have equal variances.

Fig. 5.12 demonstrates the asymptotic secrecy rates for the proposed SSK transmission scheme with the CSI-based antenna index assignment. It is assumed that the perfect reciprocity holds, and hence, the achievable secrecy rates for high SNRs are evaluated using (5.57). It can be inferred from the figure that increasing the number of transmit antennas yields considerable gains in terms of the secrecy rates. Since an eavesdropper experiencing an independent channel cannot do any better than a random guess among the $N_t!$ possible word choices, increasing the number of transmit antennas increases her confusion. Furthermore, it is clear from (5.57), and also from the figure, that the secrecy rates are reduced with an increased channel coherence time.

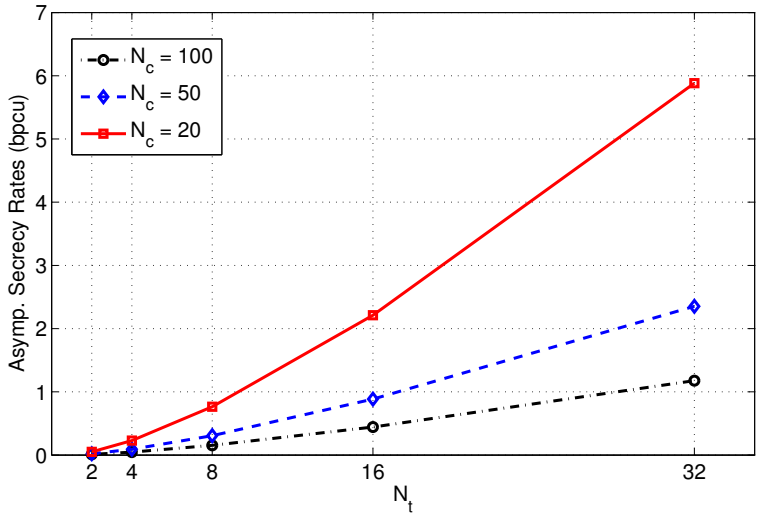

Figure 5.12: Achievable secrecy rates at high SNRs for SSK transmissions with the CSI-based antenna index assignment under perfect reciprocity.

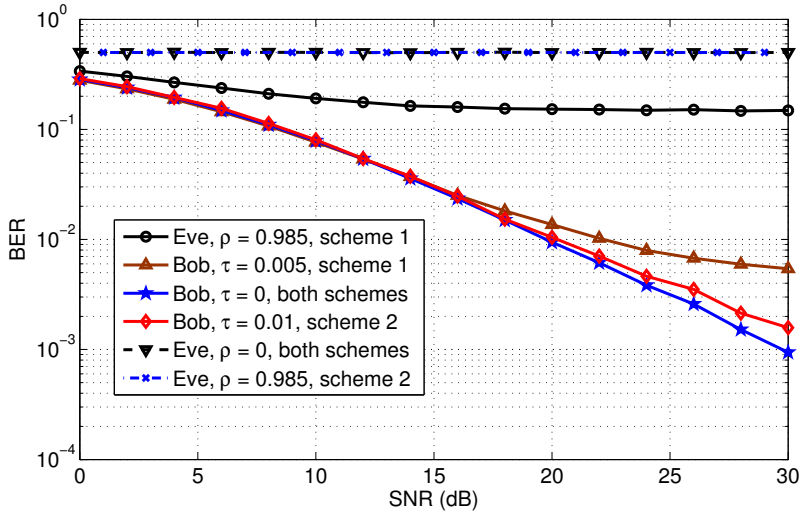

Figure 5.13: BER for SSK with $N_t = 4$, $N_{r_b} = N_{r_e} = 1$ under perfect and imperfect reciprocity, and with and without channel correlation between Bob and Eve.

In order to compare the performance of the two proposed algorithms, we perform Monte Carlo simulations to obtain the BERs[1] at Bob and Eve under perfect and imperfect CSI scenarios. We consider a MIMOME wiretap channel with $(N_t, N_{r,b}, N_{r,e}) = (4, 1, 1)$ employing SSK transmission. We model the imperfect CSI at Alice as follows. When employing Scheme 1, the estimated channel at Alice is given as in (5.58). Similarly, when Scheme 2 is employed, the estimated rotated channel at the transmitter is modeled as $\tilde{\mathbf{f}}_{b_i} = \sqrt{1-\tau^2}\mathbf{f}_{b_i} + \tau\mathbf{q}_i$. Furthermore, the correlation between the main channel and the eavesdropper's channel is modeled using (5.67). A rotation matrix codebook of size 100 is considered for Scheme 2. Fig. 5.13 compares the resulting BERs at the legitimate receiver and the eavesdropper where both receivers are assumed to employ maximum ML detection [51]. It is clear that the SSK scheme with the CSI-based antenna index assignment is capable of providing good reliability and eavesdropping resilience for the scenarios with perfect reciprocity ($\tau = 0$) and uncorrelated eavesdropper's

[1]Although BER is used as a practical metric for quantifying the eavesdropping resilience, it satisfies neither the strong nor the weak secrecy constraints.

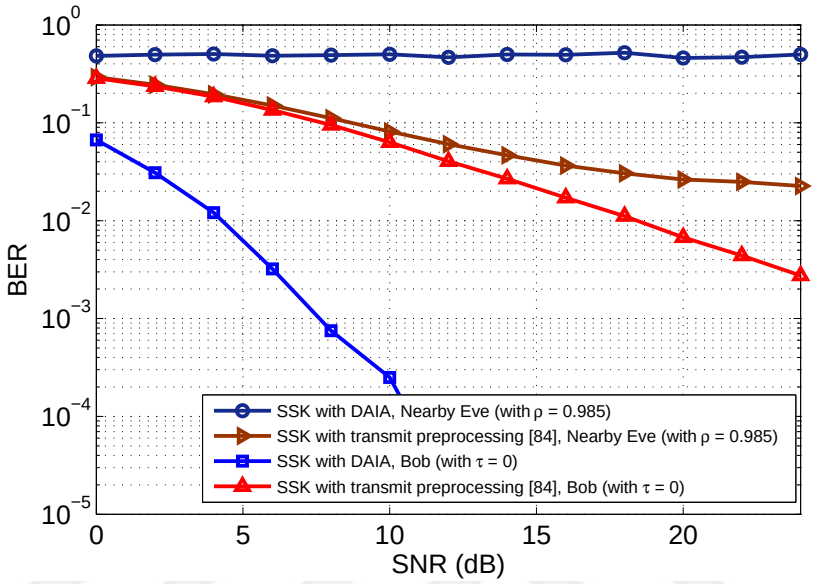

Figure 5.14: SSK with dynamic antenna index assignment (DAIA) versus transmit preprocessing scheme, $(N_t, N_{r_b}, N_{r_e}) = (4, 4, 4)$.

channel ($\rho = 0$). However, an imperfect reciprocity (with $\tau = 0.005$) considerably degrades the BER at Bob, and a correlated eavesdropper (with $\rho = 0.985$) is capable of breaching the security of the system. We also observe that the second scheme, which relies on antenna index assignment according to a rotated channel is more robust to imperfect reciprocity (with $\tau = 0.01$), and also it prevents a correlated eavesdropper (with $\rho = 0.985$) from tracking the antenna index assignment pattern, correctly.

Finally, we compare the performance of the proposed dynamic antenna index assignment technique with that of the secure SSK and spatial modulation scheme proposed in [84], which relies on transmit preprocessing. In the secure transmission scheme of [84], with the assumption that the main channel is reciprocal, the channel estimation is carried out only in the reverse direction (from Bob to Alice). Then, Alice takes advantage of the estimated channel to design transmit preprocessing coefficients, which cancel the effect of fading at Bob so that he can detect the transmitted bits with no need for CSI. For the scenarios with $N_t = N_{r_b}$, these coefficients are attained by normalizing $\mathbf{H}_b^{-1}$. Fig. 5.14

compares the reliability and eavesdropping resilience of this technique with those of Scheme 2 proposed in Section 5.4.6. We depict the BER at Bob and at a nearby Eve (with $\rho = 0.985$) with $N_t = N_{r_b} = N_{r_e} = 4$. It can be inferred from Fig. 5.14 that, unlike the newly proposed scheme, the security of the one in [84] is breached in such scenarios. Moreover, since in the proposed SSK scheme with a dynamic antenna index assignment, the CSI is available at Bob, he can take advantage of the optimal ML detection. As a result, the proposed scheme yields a considerably smaller error probability at the legitimate receiver, and achieves a higher reliability.

5.5 Chapter Summary

In this chapter, we have investigated the potential of spatial modulation and SSK in securing communication at the physical layer. We have derived the mutual information terms and have formulated achievable secrecy rate expressions. We have examined the secrecy rate enhancements that can be attained by applying CSI aided transmit signal design algorithms. We have developed iterative precoder optimization algorithms for maximizing secrecy rates. The merits of the proposed transmit signal design schemes have been depicted via extensive numerical examples. Moreover, in the scenarios where the main channel is reciprocal, we have proposed an eavesdropping resilient transmission scheme using SSK with randomized antenna index assignment. Specifically, exploiting the channel between the legitimate users as a source of common randomness, two algorithms have been introduced for acquiring the indices of transmit antennas. It has been shown that the proposed antenna index assignment algorithm based on the rotated channel is robust to imperfect reciprocity and resolves the threat of nearby eavesdroppers.

Chapter 6

Summary and Conclusions

We conclude the thesis by providing a summary of our contributions, and introducing a number of directions for future studies.

An obligatory step towards practical implementation of physical layer security is understanding the impacts of employing standard constellations on the secrecy performance. The usual approaches for designing secure transmit signals with Gaussian inputs lead to considerable losses when applied to the signals drawn from finite constellations. With this motivation, we have proposed various transmit signal design strategies with the signals drawn from standard constellations for a variety of scenarios.

In Chapter 3, we have studied a MIMO wiretap channel with statistical ECSI, and under perfect and statistical MCSI assumptions, we have proposed different transmit signal design algorithms, which rely on precoding and artificial noise injection. We have also introduced different strategies for reducing the computational complexity associated with the transmit signal design.

The following conclusions can be drawn from our results in Chapter 3. Artificial noise plays an important role in securing communications in the scenarios with finite-alphabet inputs. In many cases (especially, in the absence of the instantaneous ECSI), without artificial noise injection, secrecy rates drop to zero

when transmit power increases. Therefore, injecting artificial noise is crucial for guaranteeing a saturation behavior at high SNRs. We also note that artificial noise injection well-suits the nature of secure transmission with finite-alphabet inputs. This is because, for the signals drawn from standard constellations, the optimal power to be allocated is only a fraction of the total available power for signal transmission at high SNR. Hence, the excess power can be used for injection of artificial noise for signaling with finite alphabet inputs.

The optimal secure transmission scheme under finite-alphabet input constraints is not available in closed-form. This is due to the non-convexity of the objective function (i.e., the secrecy rate). So as to maximize the secrecy rates, we have developed iterative approaches for jointly optimizing the precoder matrix and artificial noise. The transmit signal design algorithms, which rely on direct maximization of secrecy rates are computationally complex mainly due to the fact that the mutual information expression under finite-alphabet inputs lacks closed-form. Therefore, we have also introduced maximization of a cut-off rate based approximation of the secrecy rate as well as a per-group precoding based approach as two techniques for lowering the computational complexity associated with the transmit signal design. It turns out that there is an important trade-off between the achievable secrecy rate and the computational complexity of the proposed solutions.

Our results also reveal that the amount of CSIT plays a central role in determining the secrecy performance of the proposed transmission scheme. Transmission schemes with the aid of full CSI typically have a high capability in simultaneously increasing the information rates at the legitimate receiver and suppressing the reception at the eavesdropper, however, acquiring a perfect instantaneous CSI of the eavesdropper may not be feasible in many scenarios. Although the achievable secrecy rates undergo considerable losses in the absence of instantaneous ECSIT, our numerical examples reveal that high secrecy rates can still be attained with statistical ECSIT. Meanwhile, lack of the instantaneous MCSI at the transmitter is a more critical issue as our results demonstrate that the precoding and artificial noise injection with the aid of the statistical MCSI and ECSI cannot prevent ergodic secrecy rate from dropping to zero at high SNRs.

In Chapter 4, we have studied the trade-off between the secrecy rate and the harvested power in SWIPT systems with finite-alphabet inputs. We have introduced a framework for transmit signal design to achieve this trade-off. We have demonstrated that maximizing the harvested power at the ER (which is also a potential eavesdropper) and maximizing the secrecy rate are two conflicting problems. In other words, the strategies which are beneficial for maximizing secrecy rates (e.g., transmitting data in the null-space of the eavesdropper's channel) are not helpful for achieving high harvested power and vice versa. With this motivation, we have proposed an iterative transmit signal design to achieve the trade-off between the secrecy rate and the harvested power.

Since the iterative approach developed in Chapter 4 possesses a high computational complexity, we have also introduced a two-stage transmit signal design solution as a low-complexity alternative. Due to the nature of SWIPT systems, the ER is expected to work at high SNRs. Therefore, for maximizing the secrecy rate, under finite-alphabet input constraints, only a fraction of the total power should be allocated to data transmission. Hence, in the two-stage transmit signal design approach, once the data precoder is obtained without taking into account the harvested power, the remaining power is assigned for transmission of a signal playing the dual role of the artificial noise and the energy signal. Our numerical results demonstrate that the proposed transmission strategies achieve a better trade-off than time sharing between the schemes, which maximize the secrecy rate and the harvested power separately.

In Chapter 5, we have focused on spatial modulation and SSK in the context of physical layer security. Though originally introduced as low-complexity multi-antenna transmission schemes, the fundamentally different working principle of spatial modulation and SSK opens new avenues for the secure transmission design. To explore these potentials, we have derived the relevant mutual information expressions and formulated achievable secrecy rates. We have also introduced precoder optimization strategies for maximizing the secrecy rate. Our results reveal that transmit precoding with the aid of CSIT is an effective tool for enhancing the secrecy of SSK transmission. In the scenarios with a single receive antenna at the eavesdropper and in the presence of perfect ECSI at the transmitter, it is possible

to completely suppress the reception at the eavesdropper. The precoder structure making this possible is indeed the optimal transmit signal design at the high SNR regime. However, for other scenarios, the optimal precoder is not known in a closed-form, and the maximization of the secrecy rate is carried out with the aid of suitable iterative algorithms. We have also proposed an eavesdropping resilient SSK transmission scheme for the scenarios with reciprocal main channel, which relies on randomized antenna index assignment. Exploiting the channel between the legitimate users as a source of common randomness, two algorithms have been introduced for acquiring the indices of transmit antennas. We have shown that the proposed antenna index assignment algorithm based on a rotated channel is robust to imperfect reciprocity and may resolve the threat of nearby eavesdroppers observing highly correlated channels with that of the legitimate receiver.

We now identify several research directions building on the study conducted in this thesis.

Throughout the thesis, we have focused our attention to a limited set of CSI scenarios (e.g., perfect and statistical CSI assumptions). Some other important scenarios regarding the CSI uncertainty at different nodes, e.g., noisy estimation of CSI, outdated CSI or limited CSI feedback, which are well-investigated under Gaussian input assumption [85], have not been considered for the cases with finite-alphabet inputs. It would be interesting to quantify the losses in the secrecy rates under each of these imperfect CSI assumptions in this framework.

While the artificial noise injection strategies proposed in this thesis rely on transmitting Gaussian distributed noise either by aligning it in the null-space of the main channel or by optimizing its covariance matrix, such artificial noise signals are not necessarily optimal. It has been shown in [86] that the worst case noise for AWGN channels with binary inputs has a discrete distribution. This motivates seeking interference distributions (rather than merely optimizing covariance matrices of Gaussian distributed signals), which maximize secrecy rates.

Recently, some attempts have been made to assess the limits of secure communications in different network scenarios, including multiple access and interference channels [34], smart grid systems [87] and heterogeneous networks [88]. However, many important scenarios have not yet been tackled under the finite-alphabet input assumption. For example, to the best of our knowledge, no results have been reported for finite-input interference channels with secrecy constraints. Studying multi-user and multi-eavesdropper setups under finite-alphabet inputs constitutes an important direction for future research.

Massive MIMO [89] and millimeter wave (mmWave) communication systems [90] have attracted significant interest from researchers in industry and academia. Exploiting large antenna arrays and taking advantage of a spectrum from 30 GHz to 300 GHz away from the almost fully occupied spectral band, have proven to provide various benefits, which make these technologies promising candidates for the next generation wireless systems. Investigating the potentials of massive MIMO and mmWave communications in providing physical layer security has been of recent interest as well (see e.g., [91]). Besides opportunities offered, many challenges arise in secure transmit design, specifically, with finite-alphabet inputs. For instance, the proposed iterative precoder optimization approaches given in Chapter 3 (except the per-group precoding approach) will be intractable when the number of antennas is large. Communicating at mmWave considerably changes the channel model and defines new constraints (e.g., in terms of RF hardware) as well, motivating development of new frameworks for secure transmission designs.

As a final proposal for future research, we suggest investigation of discriminatory channel estimation aided SSK transmission. Since the wireless channel plays the role of the modulation unit in SSK transmission, the corresponding receivers require a perfect CSI to detect the transmitted data. This means that degrading the channel estimation performance of the eavesdropper can be a promising technique for improving secrecy. With this motivation, employing SSK transmission along with discriminatory channel estimation techniques [92], which aim at maximizing the channel estimation quality difference between the legitimate receiver and the eavesdropper, may be an interesting direction for future research.

Bibliography

[1] Y. Liang, H. V. Poor, S. Shamai, *et al.*, "Information theoretic security," *Foundations and Trends® in Communications and Information Theory*, vol. 5, no. 4–5, pp. 355–580, 2009.

[2] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 16, pp. 1550–1573, 3rd Quart., 2014.

[3] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas: Part II: The MIMOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, pp. 5515–5532, Nov. 2010.

[4] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *IEEE Trans. Inf. Theory*, vol. 57, pp. 4961–4972, Aug. 2011.

[5] T. Liu and S. Shamai, "A note on the secrecy capacity of the multiple-antenna wiretap channel," *IEEE Trans. Inf. Theory*, vol. 55, pp. 2547–2553, Jun. 2009.

[6] W. Trappe, "The challenges facing physical layer security," *IEEE Commun. Mag.*, vol. 53, pp. 16–20, Jun. 2015.

[7] S. R. Aghdam and T. M. Duman, "Joint precoder and artificial noise design for MIMO wiretap channels with finite-alphabet inputs based on the cut-off rate," *IEEE Trans. Wireless Commun.*, vol. 16, pp. 3913–3923, Jun. 2017.

[8] S. R. Aghdam and T. M. Duman, "Low complexity precoding for MIMOME wiretap channels based on cut-off rate," in *2016 IEEE Int. Symp. Inf. Theory (ISIT)*, pp. 2988–2992, Jul. 2016.

[9] S. R. Aghdam and T. M. Duman, "Transmit signal design for MIMO wiretap channels with statistical CSI and arbitrary inputs." *accepted in 2017 2017 IEEE 28th Annual Int. Symp. on Pers., Indoor, Mobile Radio Commun. (PIMRC)*, Oct. 2017.

[10] S. R. Aghdam and T. M. Duman, "Secrecy rate and harvested energy trade-off for MISO channels with finite-alphabet inputs." *submitted to 2018 IEEE Int. Conf. Commun. (ICC)*.

[11] S. R. Aghdam and T. M. Duman, "Physical layer security for space shift keying transmission with precoding," *IEEE Wireless Commun. Lett.*, vol. 5, pp. 180–183, Apr. 2016.

[12] S. R. Aghdam, T. M. Duman, and M. D. Renzo, "On secrecy rate analysis of spatial modulation and space shift keying," in *2015 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom)*, pp. 63–67, May 2015.

[13] S. R. Aghdam and T. M. Duman, "Secure space shift keying transmission using dynamic antenna index assignment." *accepted in 2017 IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2017.

[14] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, 1975.

[15] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, no. 4, pp. 656–715, 1949.

[16] U. Maurer and S. Wolf, "From weak to strong information-theoretic key agreement," in *2000 IEEE Int. Symp. Inf. Theory (ISIT)*, pp. 18–19, Jun. 2000.

[17] S. Leung-Yan-Cheong and M. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 24, pp. 451–456, Jul. 1978.

[18] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, pp. 339–348, May 1978.

[19] J. Barros and M. R. D. Rodrigues, "Secrecy capacity of wireless channels," in *2006 IEEE Int. Symp. Inf. Theory (ISIT)*, pp. 356–360, Jul. 2006.

[20] P. K. Gopala, L. Lai, and H. E. Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inf. Theory*, vol. 54, pp. 4687–4698, Oct. 2008.

[21] J. Li and A. P. Petropulu, "On ergodic secrecy rate for Gaussian MISO wiretap channels," *IEEE Trans. Wireless Commun.*, vol. 10, pp. 1176–1187, Apr. 2011.

[22] P. H. Lin and E. Jorswieck, "On the fast fading Gaussian wiretap channel with statistical channel state information at the transmitter," *IEEE Trans. Inf. Forensics Security*, vol. 11, pp. 46–58, Jan. 2016.

[23] Q. Li, M. Hong, H. T. Wai, Y. F. Liu, W. K. Ma, and Z. Q. Luo, "Transmit solutions for MIMO wiretap channels using alternating optimization," *IEEE J. Sel. Areas Commun.*, vol. 31, pp. 1714–1727, Sep. 2013.

[24] S. Loyka and C. D. Charalambous, "An algorithm for global maximization of secrecy rates in Gaussian MIMO wiretap channels," *IEEE Trans. Commun.*, vol. 63, pp. 2288–2299, Jun. 2015.

[25] G. Raghava and B. S. Rajan, "Secrecy capacity of the Gaussian wiretap channel with finite complex constellation input," *arXiv preprint arXiv:1010.1163*, 2010.

[26] M. R. D. Rodrigues, A. Somekh-Baruch, and M. Bloch, "On Gaussian wiretap channels with M-PAM inputs," in *2010 European Wireless Conf. (EW)*, pp. 774–781, Apr. 2010.

[27] E. Biglieri, *Coding for wireless channels*. Springer Science & Business Media, 2005.

[28] Z. Li, R. Yates, and W. Trappe, "Achieving secret communication for fast Rayleigh fading channels," *IEEE Trans. Wireless Commun.*, vol. 9, pp. 2792–2799, Sep. 2010.

[29] R. Negi and S. Goel, "Secret communication using artificial noise," in *VTC-2005-Fall. 2005 IEEE 62nd Veh. Technol. Conf., 2005.*, vol. 3, pp. 1906–1910, Sep. 2005.

[30] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, pp. 2180–2189, Jun. 2008.

[31] S. Bashar, Z. Ding, and C. Xiao, "On secrecy rate analysis of MIMO wiretap channels driven by finite-alphabet input," *IEEE Trans. Commun.*, vol. 60, pp. 3816–3825, Dec. 2012.

[32] Y. Wu, C. Xiao, Z. Ding, X. Gao, and S. Jin, "Linear precoding for finite-alphabet signaling over MIMOME wiretap channels," *IEEE Trans. Veh. Technol.*, vol. 61, pp. 2599–2612, Jul. 2012.

[33] D. Jose, P. Darsana, A. M. Soney, G. Joseph, and R. M. Thomas, "Filter design for MIMO Gaussian wiretap channel," in *2014 Annual International Conference on Emerging Research Areas: Magnetics, Machines and Drives (AICERA/iCMMD)*, pp. 1–3, Jul. 2014.

[34] A. Özçelikkale and T. M. Duman, "Cooperative precoding and artificial noise design for security over interference channels," *IEEE Signal Process. Lett.*, vol. 22, pp. 2234–2238, Dec. 2015.

[35] T. V. Nguyen, T. Q. S. Quek, Y. H. Kim, and H. Shin, "Secrecy diversity in MISOME wiretap channels," in *2012 IEEE Global Commun. Conf. (GLOBECOM)*, pp. 4840–4845, Dec. 2012.

[36] S. Bashar, Z. Ding, and C. Xiao, "On the secrecy rate of multi-antenna wiretap channel under finite-alphabet input," *IEEE Commun. Lett.*, vol. 15, pp. 527–529, May 2011.

[37] A. Kalantari, M. Soltanalian, S. Maleki, S. Chatzinotas, and B. Ottersten, "Secure M-PSK communication via directional modulation," in *2016 IEEE Int. Conf. Acoust., Speech, Signal Process. (ICASSP)*, pp. 3481–3485, Mar. 2016.

[38] A. Kalantari, M. Soltanalian, S. Maleki, S. Chatzinotas, and B. Ottersten, "Directional modulation via symbol-level precoding: A way to enhance security," *IEEE J. Sel. Topics Signal Process.*, vol. 10, pp. 1478–1493, Dec. 2016.

[39] L. Zhang, Y. Cai, B. Champagne, and M. Zhao, "Tomlinson-Harashima precoding design in MIMO wiretap channels based on the MMSE criterion," in *2015 IEEE Int. Conf. on Commun. Workshop (ICCW)*, pp. 470–474, Jun. 2015.

[40] S. A. A. Fakoorian, H. Jafarkhani, and A. L. Swindlehurst, "Secure space-time block coding via artificial noise alignment," in *Forty Fifth Asilomar Asilomar Conf. Signals, Syst., Comput. (ASILOMAR)*, pp. 651–655, Nov. 2011.

[41] Z. Rezki, F. Gagnon, and V. Bhargava, "The ergodic capacity of the MIMO wire-tap channel," *arXiv preprint arXiv:0902.0189*, 2009.

[42] S. C. Lin and C. L. Lin, "On secrecy capacity of fast fading MIMOME wiretap channels with statistical CSIT," *IEEE Trans. Wireless Commun.*, vol. 13, pp. 3293–3306, Jun. 2014.

[43] M. A. Girnyk, M. Vehkapera, J. Yuan, and L. K. Rasmussen, "On the ergodic secrecy capacity of MIMO wiretap channels with statistical CSI," in *2014 Int. Symp. on Inf. Theory and its Applications*, pp. 398–402, Oct. 2014.

[44] P. Grover and A. Sahai, "Shannon meets tesla: Wireless information and power transfer," in *2010 IEEE Int. Symp. Inf. Theory (ISIT)*, pp. 2363–2367, Jun. 2010.

[45] X. Chen, D. W. K. Ng, and H. H. Chen, "Secrecy wireless information and power transfer: challenges and opportunities," *IEEE Wireless Commun*, vol. 23, pp. 54–61, Apr. 2016.

[46] L. Liu, R. Zhang, and K. C. Chua, "Secrecy wireless information and power transfer with MISO beamforming," in *2013 IEEE Global Commun. Conf. (GLOBECOM)*, pp. 1831–1836, Dec. 2013.

[47] M. R. A. Khandaker and K. K. Wong, "Robust secrecy beamforming with energy-harvesting eavesdroppers," *IEEE Wireless Commun. Lett.*, vol. 4, pp. 10–13, Feb. 2015.

[48] D. W. K. Ng, E. S. Lo, and R. Schober, "Robust beamforming for secure communication in systems with wireless information and power transfer," *IEEE Trans. Wireless Commun.*, vol. 13, pp. 4599–4615, Aug. 2014.

[49] M. D. Renzo, H. Haas, A. Ghrayeb, S. Sugiura, and L. Hanzo, "Spatial modulation for generalized MIMO: Challenges, opportunities, and implementation," *Proc. IEEE*, vol. 102, pp. 56–103, Jan. 2014.

[50] R. Y. Mesleh, H. Haas, S. Sinanovic, C. W. Ahn, and S. Yun, "Spatial modulation," *IEEE Trans. Veh. Technol.*, vol. 57, pp. 2228–2241, Jul. 2008.

[51] J. Jeganathan, A. Ghrayeb, L. Szczecinski, and A. Ceron, "Space shift keying modulation for MIMO channels," *IEEE Trans. Wireless Commun.*, vol. 8, pp. 3692–3703, Jul. 2009.

[52] S. Sinanovic, N. Serafimovski, M. D. Renzo, and H. Haas, "Secrecy capacity of space keying with two antennas," in *2012 IEEE Veh. Technol. Conf. (VTC Fall)*, pp. 1–5, Sep. 2012.

[53] T. M. Cover and J. A. Thomas, *Elements of information theory*. John Wiley & Sons, 2012.

[54] P. H. Lin, S. H. Lai, S. C. Lin, and H. J. Su, "On secrecy rate of the generalized artificial-noise assisted secure beamforming for wiretap channels," *IEEE J. Sel. Areas Commun.*, vol. 31, pp. 1728–1740, Sep. 2013.

[55] C. Xiao and Y. R. Zheng, "On the mutual information and power allocation for vector Gaussian channels with finite discrete inputs," in *IEEE Global Commun. Conf. (GLOBECOM 2008)*, pp. 1–5, Nov. 2008.

[56] D. P. Palomar and S. Verdu, "Gradient of mutual information in linear vector Gaussian channels," *IEEE Trans. Inf. Theory*, vol. 52, pp. 141–154, Jan. 2006.

[57] S. Boyd and L. Vandenberghe, *Convex optimization*. Cambridge university press, 2004.

[58] W. Zeng, C. Xiao, M. Wang, and J. Lu, "Linear precoding for finite-alphabet inputs over MIMO fading channels with statistical CSI," *IEEE Trans. Signal Process.*, vol. 60, pp. 3134–3148, Jun. 2012.

[59] A. Yadav, M. Juntti, and J. Lilleberg, "Linear precoder design for doubly correlated partially coherent fading MIMO channels," *IEEE Trans. Wireless Commun.*, vol. 13, pp. 3621–3635, Jul. 2014.

[60] S. G. Wilson, *Digital modulation and coding*. Prentice-Hall, Inc., 1995.

[61] T. Y. Liu, S. C. Lin, and Y. W. P. Hong, "On the role of artificial noise in training and data transmission for secret communications," *IEEE Trans. Inf. Forensics Security*, vol. 12, pp. 516–531, Mar. 2017.

[62] 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 Trans. Wireless Commun.*, vol. 12, pp. 2717–2729, Jun. 2013.

[63] Y. Wu, C. K. Wen, D. W. K. Ng, R. Schober, and A. Lozano, "Low-complexity MIMO precoding with discrete signals and statistical CSI," in *2016 IEEE Int. Conf. Commun. (ICC)*, pp. 1–6, May 2016.

[64] Y. Wu, D. W. K. Ng, C. K. Wen, R. Schober, and A. Lozano, "Low-complexity MIMO precoding for finite-alphabet signals," *IEEE Trans. Wireless Commun.*, vol. 16, pp. 4571–4584, Jul. 2017.

[65] Y. Wu, C. K. Wen, C. Xiao, X. Gao, and R. Schober, "Linear precoding for the MIMO multiple access channel with finite alphabet inputs and statistical CSI," *IEEE Trans. Wireless Commun.*, vol. 14, pp. 983–997, Feb. 2015.

[66] S. C. Lin and P. H. Lin, "On secrecy capacity of fast fading multiple-input wiretap channels with statistical CSIT," *IEEE Trans. Inf. Forensics Security*, vol. 8, pp. 414–419, Feb. 2013.

[67] M. A. Girnyk, F. Gabry, M. Vehkaperä, L. K. Rasmussen, and M. Skoglund, "On the transmit beamforming for MIMO wiretap channels: Large-system analysis," in *International Conference on Information Theoretic Security*, pp. 90–102, Springer, 2013.

[68] A. Zappone, P. H. Lin, and E. Jorswieck, "Energy efficiency of confidential multi-antenna systems with artificial noise and statistical CSI," *IEEE J. Sel. Topics Signal Process.*, vol. 10, pp. 1462–1477, Dec. 2016.

[69] J. Zhang, C. Yuen, C. K. Wen, S. Jin, K. K. Wong, and H. Zhu, "Large system secrecy rate analysis for swipt MIMO wiretap channels," *IEEE Trans. Inf. Forensics Security*, vol. 11, pp. 74–85, Jan. 2016.

[70] K. Banawan and S. Ulukus, "MIMO wiretap channel under receiver-side power constraints with applications to wireless power transfer and cognitive radio," *IEEE Trans. Commun.*, vol. 64, pp. 3872–3885, Sep. 2016.

[71] A. A. Lu, X. Gao, Y. R. Zheng, and C. Xiao, "Linear precoder design for swipt in MIMO broadcasting systems with discrete input signals: Manifold optimization approach," *IEEE Trans. Commun.*, vol. 65, pp. 2877–2888, Jul. 2017.

[72] R. Zhang and C. K. Ho, "MIMO broadcasting for simultaneous wireless information and power transfer," *IEEE Trans. Wireless Commun.*, vol. 12, pp. 1989–2001, May 2013.

[73] F. Glover, "Surrogate constraint duality in mathematical programming," *Operations Research*, vol. 23, no. 3, pp. 434–451, 1975.

[74] X. Guan, Y. Cai, and W. Yang, "On the secrecy mutual information of spatial modulation with finite alphabet," in *2012 International Conference on Wireless Communications and Signal Processing (WCSP)*, pp. 1–4, Oct. 2012.

[75] F. Wu, R. Zhang, L. L. Yang, and W. Wang, "Transmitter precoding-aided spatial modulation for secrecy communications," *IEEE Trans. Veh. Technol.*, vol. 65, pp. 467–471, Jan. 2016.

[76] F. Wu, L. L. Yang, W. Wang, and Z. Kong, "Secret precoding-aided spatial modulation," *IEEE Commun. Lett.*, vol. 19, pp. 1544–1547, Sep. 2015.

[77] R. G. Gallager, *Information theory and reliable communication*, vol. 2. Springer, 1968.

[78] R. Rajashekar, K. V. S. Hari, and L. Hanzo, "Reduced-complexity ml detection and capacity-optimized training for spatial modulation systems," *IEEE Trans. Commun.*, vol. 62, pp. 112–125, Jan. 2014.

[79] M. Maleki, H. R. Bahrami, S. Beygi, M. Kafashan, and N. H. Tran, "Space modulation with CSI: Constellation design and performance evaluation," *IEEE Trans. Veh. Technol.*, vol. 62, pp. 1623–1634, May 2013.

[80] M. C. Lee, W. H. Chung, and T. S. Lee, "Generalized precoder design formulation and iterative algorithm for spatial modulation in MIMO systems with CSIT," *IEEE Trans. Commun.*, vol. 63, pp. 1230–1244, Apr. 2015.

[81] K. S. Ahn, R. W. Heath, and H. K. Baik, "Shannon capacity and symbol error rate of space-time block codes in MIMO Rayleigh channels with channel estimation error," *IEEE Trans. Wireless Commun.*, vol. 7, pp. 324–333, Jan. 2008.

[82] M. K. Simon and M. S. Alouini, "On the difference of two chi-square variates with application to outage probability computation," *IEEE Trans. Commun.*, vol. 49, pp. 1946–1954, Nov. 2001.

[83] M. Edman, A. Kiayias, and B. Yener, "On passive inference attacks against physical-layer key extraction?," in *Proceedings of the Fourth European Workshop on System Security*, p. 8, ACM, 2011.

[84] Q. Li, "Information-guided randomization for wireless physical layer secure transmission," in *MILCOM 2012 - 2012 IEEE Military Communications Conference*, pp. 1–6, Oct. 2012.

[85] A. Hyadi, Z. Rezki, and M. S. Alouini, "An overview of physical layer security in wireless communication systems with CSIT uncertainty," *IEEE Access*, vol. 4, pp. 6121–6132, Oct. 2016.

[86] S. Shamai and S. Verdu, "Worst-case power-constrained noise for binary-input channels," *IEEE Trans. Inf. Theory*, vol. 38, pp. 1494–1511, Sep. 1992.

[87] E. K. Lee, M. Gerla, and S. Y. Oh, "Physical layer security in wireless smart grid," *IEEE Commun. Mag.*, vol. 50, pp. 46–52, Aug. 2012.

[88] H. M. Wang, T. X. Zheng, J. Yuan, D. Towsley, and M. H. Lee, "Physical layer security in heterogeneous cellular networks," *IEEE Trans. Commun.*, vol. 64, pp. 1204–1219, Mar. 2016.

[89] E. G. Larsson, O. Edfors, F. Tufvesson, and T. L. Marzetta, "Massive MIMO for next generation wireless systems," *IEEE Commun. Mag.*, vol. 52, pp. 186–195, Feb. 2014.

[90] T. S. Rappaport, S. Sun, R. Mayzus, H. Zhao, Y. Azar, K. Wang, G. N. Wong, J. K. Schulz, M. Samimi, and F. Gutierrez, "Millimeter wave mobile communications for 5G cellular: It will work!," *IEEE Access*, vol. 1, pp. 335–349, May 2013.

[91] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, and M. D. Renzo, "Safeguarding 5G wireless communication networks using physical layer security," *IEEE Commun. Mag.*, vol. 53, pp. 20–27, Apr. 2015.

[92] T. H. Chang, W. C. Chiang, Y. W. P. Hong, and C. Y. Chi, "Training sequence design for discriminatory channel estimation in wireless MIMO systems," *IEEE Trans. Signal Process.*, vol. 58, pp. 6223–6237, Dec. 2010.

[93] A. Hjorungnes and D. Gesbert, "Complex-valued matrix differentiation: Techniques and key results," *IEEE Trans. Signal Process.*, vol. 55, pp. 2740–2746, Jun. 2007.

Appendix A

Proof of Proposition 3.1

The Lagrangian for the optimization problem (3.13)-(3.14) is given as

$$L(\mathbf{P}_D, \theta) = -R_{s,l}(\mathbf{P}_D) + \theta\big(\mathrm{tr}(\mathbf{P}_D\mathbf{P}_D^H) + \alpha_{AN}^2 - N_t\big). \tag{A.1}$$

By applying the KKT conditions, we can obtain the necessary conditions for optimality as follows

$$\nabla_{\mathbf{P}_D} L(\mathbf{P}_D, \theta) = 0, \tag{A.2}$$

$$\theta\bigg(\mathrm{tr}(\mathbf{P}_D\mathbf{P}_D^H) + \alpha_{AN}^2 - N_t\bigg) = 0, \tag{A.3}$$

$$\theta \geq 0, \tag{A.4}$$

$$\mathrm{tr}(\mathbf{P}_D\mathbf{P}_D^H) + \alpha_{AN}^2 - N_t \leq 0. \tag{A.5}$$

The gradient of the Lagrangian can be obtained as

$$\nabla_{\mathbf{P}_D} L(\mathbf{P}_D, \theta) = -\nabla_{\mathbf{P}_D} R_{s,l} + \nabla_{\mathbf{P}_D}\theta\big(\mathrm{tr}(\mathbf{P}_D\mathbf{P}_D^H) + \alpha_{AN}^2 - N_t\big). \tag{A.6}$$

By replacing the gradient of the secrecy rates from (3.28) into (A.6), and also noting that $\nabla_{\mathbf{P}_D}\theta\big(\mathrm{tr}(\mathbf{P}_D\mathbf{P}_D^H) + \alpha_{AN}^2 - N_t\big) = \theta\mathbf{P}_D$, the condition in (A.2) can be written as

$$\frac{\log_2 e}{\sigma_{\mathbf{n}_y}^2}\big(\mathbf{H}_b^H\mathbf{H}_b\mathbf{P}_D\boldsymbol{\Delta}_b(\mathbf{P}_D)\big) - \mathbb{E}_{\mathbf{H}_e}\left\{\frac{\log_2 e}{\sigma_{\mathbf{n}_z'}^2}\bigg(\mathbf{H}_e^H\mathbf{H}_e\mathbf{P}_D\boldsymbol{\Delta}_e(\mathbf{P}_D)\bigg)\right\} = \theta\mathbf{P}_D, \tag{A.7}$$

where $\boldsymbol{\Delta}_b(\mathbf{P}_D)$ and $\boldsymbol{\Delta}_e(\mathbf{P}_D)$ are as defined in (3.24)-(3.25), completing the proof.

Appendix B

Derivation of the Cut-off Rate Expression in (3.30)

The cut-off rate expression in (3.30) can be derived using the formula given in [60, Eq. (.3.34)], as

$$R_0^{(B)} = -\log \sum_{i=1}^{M^{N_t}} \sum_{j=1}^{M^{N_t}} \frac{1}{M^{2N_t}} \int p(\mathbf{y}|\mathbf{s}_i, \mathbf{H}_b)^{1/2} p(\mathbf{y}|\mathbf{s}_j, \mathbf{H}_b)^{1/2} d\mathbf{y}. \tag{B.1}$$

By substituting $p(\mathbf{y}|\mathbf{s}_i, \mathbf{H}_b)$ and $p(\mathbf{y}|\mathbf{s}_j, \mathbf{H}_b)$ in (B.1). Given $\mathbf{s}_i$ and $\mathbf{H}_b$ and for a fixed $\mathbf{P}_D$, $\mathbf{y}$ is a complex Gaussian random variable with zero-mean and variance $\mathbf{H}_b \mathbf{P}_D \mathbf{s}_i$. Hence, the conditional probability density function can be obtained as

$$p(\mathbf{y}|\mathbf{s}_i, \mathbf{H}_b) = \frac{1}{\pi^{N_{r_b}} \sigma_{\mathbf{n}_y}^{2N_{r_b}}} \exp\Big(- \frac{\|\mathbf{y} - \mathbf{H}_b \mathbf{P}_D \mathbf{s}_i\|^2}{\sigma_{\mathbf{n}_y}^2} \Big). \tag{B.2}$$

By plugging $p(\mathbf{y}|\mathbf{s}_i, \mathbf{H}_b)$ and $p(\mathbf{y}|\mathbf{s}_j, \mathbf{H}_b)$ into (3.30), we get

$$\begin{aligned} R_0^{(B)} &= 2N_t \log M \\ &-\log \sum_{i=1}^{M^{N_t}} \sum_{j=1}^{M^{N_t}} \int \underbrace{\Big[\frac{1}{\pi^{N_{r_b}} \sigma_{\mathbf{n}_y}^{2N_{r_b}}} \exp\Big(- \frac{\|\mathbf{y} - \mathbf{H}_b \mathbf{P}_D \mathbf{s}_i\|^2}{\sigma_{\mathbf{n}_y}^2} \Big) \Big]^{\frac{1}{2}} \Big[\frac{1}{\pi^{N_{r_b}} \sigma_{\mathbf{n}_y}^{2N_{r_b}}} \exp\Big(- \frac{\|\mathbf{y} - \mathbf{H}_b \mathbf{P}_D \mathbf{s}_j\|^2}{\sigma_{\mathbf{n}_y}^2} \Big) \Big]^{\frac{1}{2}}}_{\mathcal{I}_1} d\mathbf{y}. \end{aligned} \tag{B.3}$$

The integrand $\mathcal{I}_1$ can be simplified as follows.

$$\mathcal{I}_1 = \frac{1}{\pi^{N_{r_b}} \sigma_{\mathbf{n}_y}^{2N_{r_b}}} \times \exp\left(-\frac{\|\mathbf{y}\|^2 + \frac{1}{2}\|\mathbf{H}_b\mathbf{P}_D\mathbf{s}_i\|^2 + \frac{1}{2}\|\mathbf{H}_b\mathbf{P}_D\mathbf{s}_j\|^2 - Re\{(\mathbf{H}_b\mathbf{P}_D\mathbf{S}_i)^*\mathbf{y}\} - Re\{(\mathbf{H}_b\mathbf{P}_D\mathbf{S}_j)^*\mathbf{y}\}}{\sigma_{\mathbf{n}_y}^2} \right). \tag{B.4}$$

Then, completion of the square in the exponent and substituting $\mathcal{I}_1$ into (B.3) yields

$$R_0^{(B)} = 2N_t \log M - \log \sum_{i=1}^{M^{N_t}} \sum_{j=1}^{M^{N_t}} \underbrace{\int \left[\frac{1}{\pi^{N_{r_b}} \sigma_{\mathbf{n}_y}^{2N_{r_b}}} \exp\Big(- \frac{\|\mathbf{y} - \mathbf{H}_b\mathbf{P}_D(\frac{\mathbf{s}_i+\mathbf{s}_j}{2})\|^2}{\sigma_{\mathbf{n}_y}^2} \Big) \right] d\mathbf{y}}_{\mathcal{I}_2} \exp\Big(- \frac{\|\mathbf{H}_b\mathbf{P}_D(\frac{\mathbf{s}_i-\mathbf{s}_j}{2})\|^2}{\sigma_{\mathbf{n}_y}^2} \Big). \tag{B.5}$$

The integral $\mathcal{I}_2$ is equal to 1 since the integrand is a multi-variate Gaussian probability density function. Therefore, the final result simplifies to

$$R_0^{(B)} = 2N_t \log M - \log \sum_{i=1}^{M^{N_t}} \sum_{j=1}^{M^{N_t}} \exp\Big(- \frac{\|\mathbf{H}_b\mathbf{P}_D\mathbf{d}_{ij}\|^2}{4\sigma_{\mathbf{n}_y}^2} \Big), \tag{B.6}$$

where $\mathbf{d}_{ij} = \mathbf{s}_i - \mathbf{s}_j$ concluding the derivation of (3.30).

Appendix C

Derivation of $\nabla_{\mathbf{P}_D} R'_{s,l}$

We apply the matrix differentiation technique in [93] to derive the gradient of $R'_{s,l}$. As a first step, we evaluate the derivative of logarithm of sum of exponentials. Accordingly $\nabla R'_{s,l}$ can be written as

$$\nabla_{\mathbf{P}_D} R'_{s,l}(\mathbf{P}_D) = \frac{1}{\kappa_b} \sum_{i=1}^{M^{N_t}} \sum_{j=1}^{M^{N_t}} \left(\nabla_{\mathbf{P}_D} \Upsilon_{b,ij}\right) \exp\left(- \frac{\mathbf{d}_{ij}^H \mathbf{P}_D^H \mathbf{H}_b^H \mathbf{H}_b \mathbf{P}_D \mathbf{d}_{ij}}{4\sigma^2_{\mathbf{n}_y}} \right) - \sum_{m=1}^{M^{N_t}} \sum_{k=1}^{M^{N_t}} \mathbb{E}_{\mathbf{H}_e} \frac{1}{\kappa_e} \left(\nabla_{\mathbf{P}_D} \Upsilon_{e,mk}\right) \exp\left(- \frac{\mathbf{d}_{mk}^H \mathbf{P}_D^H \mathbf{H}_e^H \mathbf{H}_e \mathbf{P}_D \mathbf{d}_{mk}}{4\sigma^2_{\mathbf{n}'_z}} \right). \quad \text{(C.1)}$$

where κ_b and κ_e are as defined in (3.34) and (3.35), and also, $\Upsilon_{b,ij} = \mathbf{d}_{ij}^H \mathbf{P}_D^H \mathbf{H}_b^H \mathbf{H}_b \mathbf{P}_D \mathbf{d}_{ij}$ and $\Upsilon_{e,mk} = \mathbf{d}_{mk}^H \mathbf{P}_D^H \mathbf{H}_e^H \mathbf{H}_e \mathbf{P}_D \mathbf{d}_{mk}$. Using the definition of the complex gradient vector

$$[\nabla_{\mathbf{G}} f]_{ij} = \frac{\partial f}{\partial [\mathbf{G}^*]_{ij}}, \quad \text{(C.2)}$$

where the complex derivative of scalar function f is defined as $\frac{\partial f}{\partial g^*} = \frac{\partial Re\{f\}}{\partial g^*} + j\frac{\partial Im\{f\}}{\partial g^*}$, we obtain

$$\nabla_{\mathbf{P}_D} \Upsilon_{b,ij} = \mathbf{H}_b^H \mathbf{H}_b \mathbf{P}_D \mathbf{d}_{ij} \mathbf{d}_{ij}^H, \quad \text{(C.3)}$$

$$\nabla_{\mathbf{P}_D} \Upsilon_{e,mk} = \mathbf{H}_e^H \mathbf{H}_e \mathbf{P}_D \mathbf{d}_{mk} \mathbf{d}_{mk}^H. \quad \text{(C.4)}$$

By replacing (C.3) and (C.4) in (C.1), (3.33) follows.

Appendix D

Convergence Proofs for Algorithms 1 and 2

Convergence proof for Algorithm 1:

For each value of α_{AN}, Algorithm 1 iterates over precoder matrix in each step increasing $R_{s,l}$ given in (3.10) or its cut-off rate based approximation $R'_{s,l}$ in (3.29). These expressions are upper-bounded under the finite-alphabet constraint and since Algorithm 1 generates increasing sequences which are upper-bounded, the convergence is guaranteed.

It should be noted that, due to the non-convexity of the objective function, in general, Algorithm 1 will find a local maximum of $R_{s,l}$ (or, $R'_{s,l}$). Different initializations can result in distinct solutions at convergence. Hence, running Algorithm 1 for several random initializations increases the probability of the convergence to a global maximum. In other words, it is more likely that one of these several local optima be the global optimum.

Convergence proof for Algorithm 2:

Algorithm 2 consists of inner iterations and outer iterations. Inner iterations alternatingly update precoder matrices $\mathbf{P}_D$ and $\mathbf{P}_{AN}$, and each outer iteration

updates the Lagrange multiplier λ. Convergence of the subproblems in the inner iterations can be justified as follows. Noting that the $R_{s,l}$ is upper-bounded under the finite-alphabet constraint and since by updating $\mathbf{P}_D$ and $\mathbf{P}_{AN}$ increasing sequences of $R_{s,l}$ are generated which are upper-bounded, the convergence is guaranteed.

Convergence of the outer iterations is proved as follows. Noting that the dual objective function, i.e., $D(\lambda)$, is convex in λ, we employ a bisection method to update λ at each iteration. Let $[\lambda_{l,n} \quad \lambda_{h,n}]$ with $n \geq 0$ denote the successive intervals in the bisection process. Clearly, we have

$$\lambda_{l,0} \leq \lambda_{l,1} \leq \lambda_{l,2} \leq \cdots \leq \lambda_{h,0}, \tag{D.1}$$

$$\lambda_{h,0} \geq \lambda_{h,1} \geq \lambda_{h,2} \geq \cdots \geq \lambda_{l,0}. \tag{D.2}$$

We observe that the sequence $\lambda_{l,n}$ is monotonically increasing and bounded above and the sequence $\lambda_{h,n}$ is monotonically decreasing and bounded below. Hence, these sequences converge, concluding the convergence proof for Algorithm 2.

Appendix E

Derivation of $\nabla_{\mathbf{P}_D} R_{s,l}$ and $\nabla_{\mathbf{P}_E} R_{s,l}$

In order to derive $\nabla_{\mathbf{P}_D} R_{s,l}$, we use the results in [56] where it has been shown that the gradient of the mutual information expression (i.e., Equation (4.6)) can be calculated via calculating the minimum mean-square error (MMSE) matrices $\boldsymbol{\Delta}_y(\mathbf{P}_D)$ and $\boldsymbol{\Delta}_z(\mathbf{P}_D)$ as

$$\nabla_{\mathbf{P}_D} I(\mathbf{s};\mathbf{y}|\mathbf{h}) = \frac{\log_2 e}{\sigma_{n_y}^2 + \mathbf{h}^H \mathbf{P}_E \mathbf{P}_E^H \mathbf{h}} \big(\mathbf{h}\mathbf{h}^H \mathbf{P}_D \boldsymbol{\Delta}_y(\mathbf{P}_D)\big), \tag{E.1}$$

$$\nabla_{\mathbf{P}_D} I(\mathbf{s};\mathbf{z}|\mathbf{g}) = \frac{\log_2 e}{\sigma_{n_z}^2 + \mathbf{g}^H \mathbf{P}_E \mathbf{P}_E^H \mathbf{g}} \big(\mathbf{g}\mathbf{g}^H \mathbf{P}_D \boldsymbol{\Delta}_z(\mathbf{P}_D)\big), \tag{E.2}$$

where

$$\boldsymbol{\Delta}_y(\mathbf{P}_D) = \mathbb{E}\big\{(\mathbf{s} - \mathbb{E}\{\mathbf{s}|\mathbf{y}\})(\mathbf{s} - \mathbb{E}\{\mathbf{s}|\mathbf{y}\})^H\big\}, \tag{E.3}$$

$$\boldsymbol{\Delta}_z(\mathbf{P}_D) = \mathbb{E}\big\{(\mathbf{s} - \mathbb{E}\{\mathbf{s}|\mathbf{z}\})(\mathbf{s} - \mathbb{E}\{\mathbf{s}|\mathbf{z}\})^H\big\}. \tag{E.4}$$

The gradient $\nabla_{\mathbf{P}_D} R_{s,l}$ is obtained via subtracting (E.2) from (E.1).

In order to obtain $\nabla_{\mathbf{P}_E} R_{s,l}$, we first calculate the derivative of logarithm of

sum of exponentials as

$$\nabla_{\mathbf{P}_E} R_{s,l}(\mathbf{P}_E) = \sum_{i=1}^{M^{N_t}} \mathbb{E}_{n_y} \left\{ \frac{\sum_{j=1}^{M^{N_t}} \left(\nabla_{\mathbf{P}_E} \Upsilon_{y,ij}\right) \exp(-\Upsilon_{y,ij})}{\ln 2 \sum_{j'=1}^{M^{N_t}} \exp(-\Upsilon_{y,ij'})} \right\}$$
$$- \sum_{m=1}^{M^{N_t}} \mathbb{E}_{n_z} \left\{ \frac{\sum_{k=1}^{M^{N_t}} \left(\nabla_{\mathbf{P}_E} \Upsilon_{z,mk}\right) \exp(-\Upsilon_{z,mk})}{\ln 2 \sum_{k'=1}^{M^{N_t}} \exp(-\Upsilon_{z,mk'})} \right\}, \quad \text{(E.5)}$$

where

$$\Upsilon_{y,ij} = \frac{\|\mathbf{h}^H \mathbf{P}_D \mathbf{d}_{ij} + n_y\|^2 - \|n_y\|^2}{\sigma_{n_y}^2 + \mathbf{h}^H \mathbf{P}_E \mathbf{P}_E^H \mathbf{h}}, \quad \text{(E.6)}$$

$$\Upsilon_{z,mk} = \frac{\|\mathbf{g}^H \mathbf{P}_D \mathbf{d}_{mk} + n_z\|^2 - \|n_z\|^2}{\sigma_{n_z}^2 + \mathbf{g}^H \mathbf{P}_E \mathbf{P}_E^H \mathbf{g}}. \quad \text{(E.7)}$$

Finally, computing $\nabla_{\mathbf{P}_E} \Upsilon_{y,ij}$ and $\nabla_{\mathbf{P}_E} \Upsilon_{z,mk}$ using the definition of the complex gradient vector, i.e.,

$$[\nabla_{\mathbf{P}_E} f]_{ij} = \frac{\partial f}{\partial [\mathbf{P}_E^*]_{ij}}, \quad \text{(E.8)}$$

where the complex derivative of scalar function f is defined as $\frac{\partial f}{\partial p^*} = \frac{\partial Re\{f\}}{\partial p^*} + j\frac{\partial Im\{f\}}{\partial p^*}$. This concludes the derivation.