

UNIVERSITY OF CALIFORNIA,
IRVINE

Competition, Coexistence, and Confidentiality
in Multiuser Multi-antenna Wireless Networks

DISSERTATION

submitted in partial satisfaction of the requirements
for the degree of

DOCTOR OF PHILOSOPHY

in Electrical and Computer Engineering

by

Amitav Mukherjee

Dissertation Committee:
Professor A. Lee Swindlehurst, Chair
Professor Ender Ayanoglu
Professor Hamid Jafarkhani

2012

DEDICATION

To my parents, and Shri S. K. Chatterji.

TABLE OF CONTENTS

	Page
LIST OF FIGURES	vi
ACKNOWLEDGMENTS	vii
CURRICULUM VITAE	viii
ABSTRACT OF THE DISSERTATION	x
1 Introduction	1
1.1 Coexistence in Wireless Networks	2
1.1.1 Open Problems	3
1.2 Confidentiality at the Physical Layer	4
1.2.1 Open Problems	6
1.3 Contributions	7
1.3.1 Organization	7
2 Models and Assumptions	10
2.1 Underlay and Interweave MIMO CR Networks	10
2.2 MIMO Wiretap Channel	12
3 MIMO CR Precoding with Completely Unknown Primary CSI	15
3.1 Background	15
3.2 System Model	17
3.3 A Rank Minimization strategy for CSI-Unaware Underlay Transmission	20
3.4 Solutions for the Rank Minimization Design	23
3.4.1 FWF Approach	24
3.4.2 Nuclear Norm and Log-det Heuristic	25
3.5 Underlay CR Downlink	29
3.6 Primary Outage Probability	31
3.6.1 Interference Temperature Outage Probability	34
3.6.2 Interference Leakage Outage Probability	39
3.7 Numerical Results	40
3.7.1 Single Underlay Receiver Scenario	40
3.7.2 MIMO Underlay Downlink Scenario	44
3.8 Summary	47

4	Prescient Precoding in Heterogeneous CR Networks	49
4.1	Motivation	49
4.2	Mathematical Model	50
4.2.1	Signal and Network Model	50
4.2.2	ICR Spectrum Sensing	52
4.2.3	ICR Performance Prediction at UCT	54
4.3	Prescient Downlink Precoding	56
4.3.1	Direct UCR Sum Rate Maximization	58
4.3.2	Algorithm Based on Convex Optimization	61
4.3.3	Combined Downlink and Multicast Beamforming	63
4.4	Multi-antenna Underlay Receivers	64
4.5	Simulation Results	66
4.6	Summary	69
5	Robust Beamforming in the MIMO Wiretap Channel	71
5.1	System Model With Perfect CSI	74
5.1.1	Artificial Interference	75
5.1.2	Performance Metrics	77
5.2	Fixed-SINR Beamforming With Perfect CSI	79
5.2.1	Unknown Eavesdropper CSI	79
5.2.2	Known Eavesdropper CSI	82
5.3	Impact Of Imperfect CSI	83
5.4	Robust Beamforming Approaches	92
5.4.1	Robust Beamforming - FDD Case	92
5.4.2	Robust Beamforming - TDD Case	93
5.5	Simulation Results	95
5.5.1	Effects of Eavesdropper CSI	96
5.5.2	SINR Degradation Analysis	97
5.5.3	Robust Beamforming Results	98
5.6	Summary	102
6	Jamming Games in the MIMO Wiretap Channel	103
6.1	Background	103
6.2	Signal and CSI Model	104
6.3	Rate Thresholds	108
6.3.1	Asymptotic MIMO Rates	109
6.3.2	MIMO Secrecy Rate Analysis	112
6.4	Strategic Wiretap Game	116
6.4.1	Pure-strategy Equilibria	117
6.4.2	Mixed-strategy Equilibria	119
6.4.3	Wiretap Channel Parameters	121
6.5	Extensive Form Wiretap Game	123
6.5.1	Perfect Information	123
6.5.2	Imperfect Information	126
6.6	Simulation Results	127

6.7	Summary	131
7	Robust MIMO CR Transmissions for Primary Secrecy	133
7.1	Background	133
7.2	Mathematical Model	134
7.2.1	Network Model	134
7.2.2	CR Transmission with Perfect CSI	137
7.3	Robust CR Transmission	138
7.4	Numerical Results	142
7.5	Summary	145
8	Remarks	146
8.1	Recapitulation	146
8.2	Future Directions	149
	Bibliography	151

LIST OF FIGURES

		Page
2.1	Heterogeneous MIMO DSA network with UCRs, ICRs, and PRs. . . .	11
2.2	MIMO wiretap channel with multi-antenna terminals	12
3.1	Downlink CR network with MIMO underlay transmitter.	17
3.2	Power and dimension allocation versus UCR desired rate.	40
3.3	Achieved PU rate versus UCT desired rate.	41
3.4	Two metrics of PR Interference versus UCR desired rate.	42
3.5	Empirical cdf of interference temperature and leakage rate.	43
3.6	Empirical cdf of PR rate under CWF and FWF.	44
3.7	Achieved PR rate versus per-UCR desired rate.	45
3.8	Achieved PR rate versus UCT transmit power.	46
3.9	Two metrics of PR interference versus UCT transmit power.	47
4.1	ROC curve for ED comparing prescient precoding with RCI.	67
4.2	Underlay sum rate for prescient algorithms and RCI precoding. . . .	68
4.3	Underlay sum rate for prescient and conventional block-diagonalization.	69
5.1	SINR versus number of antennas for Eve.	96
5.2	Second-order naive SINR approximations.	98
5.3	Measured SINR values versus desired SINR for Bob and Eve.	99
5.4	Secrecy rate versus desired SINR for Bob with perfect/imperfect CSI.	100
5.5	Average SINR for Bob and Eve as a function of σ_H	101
6.1	Comparison of exact and asymptotic MIMO secrecy rate outcomes. .	115
6.2	Payoff matrix \mathbf{R} of the strategic MIMO wiretap game.	117
6.3	Game value in mixed strategies as the mixing probabilities are varied.	120
6.4	Extensive form game tree where Alice moves first.	123
6.5	Extensive form game tree where Eve moves first.	126
6.6	Strategic MIMO wiretap game versus transmit power.	128
6.7	Payoff versus antenna ratio N_e/N_a for fixed transmit powers.	129
6.8	Extensive-form games with perfect information.	130
6.9	Single-antenna wiretap channel.	131
7.1	Primary secrecy rate versus UCT CSI error.	143
7.2	Primary secrecy rate versus UCT transmit power.	144

ACKNOWLEDGMENTS

This manuscript and related research contributions owe their compilation to a number of mentors and colleagues. First and foremost, my gratitude goes to Prof. Lee Swindlehurst for his steadfast guidance over the years. His combination of technical acuity and personal affability ensured that the Ph.D. process was both enjoyable and deeply engaging. Thanks LS for taking a chance on a student who randomly walked into your office one fall afternoon in 2008!

I appreciate Prof. Ayanoglu's and Prof. Jafarkhani's willingness to serve as committee members. Thanks are also due to Prof. H. Kwon for setting me down this path with his encouragement and guidance. It has also been a pleasure to work with and learn from mentors at Intel, Nokia Research Center, MERL, and Qualcomm, and for the support from colleagues at California and Kansas, especially Jing Huang for collaborations on physical-layer security. The financial support of my research from the National Science Foundation under grant CCF-0916073 and the Army Research Office under MURI grant W911NF-07-1-0318 is gratefully acknowledged.

On a more personal note, not enough mention can be made of the endless support and encouragement from family and my parents.

CURRICULUM VITAE

Amitav Mukherjee

EDUCATION

Doctor of Philosophy in Electrical and Computer Engineering University of California, Irvine	2012 <i>Irvine, California</i>
Master of Science in Electrical Engineering Wichita State University	2007 <i>Wichita, Kansas</i>
Bachelor of Science in Electrical Engineering University of Kansas	2005 <i>Lawrence, Kansas</i>

WORK EXPERIENCE

Senior Researcher Nokia Research Center	June 2012 – <i>Berkeley, California</i>
Graduate Technical Intern Intel Corporation	Jan.–May 2012 <i>Santa Clara, California</i>
Research Intern Nokia Research Center	June – Sep. 2011 <i>Helsinki, Finland</i>
Research Intern Mitsubishi Electric Research Labs (MERL)	Oct. – Dec. 2010 <i>Cambridge, Massachusetts</i>
Interim Engineering Intern Qualcomm	June – Sep. 2010 <i>San Diego, California</i>
Graduate Student Researcher University of California Irvine	Oct. 2008 – Mar. 2012 <i>Irvine, California</i>

SELECTED HONORS AND AWARDS

IEEE Signal Processing Society ICASSP Travel Grant	2011, 2012
IEEE SPAWC Best Student Paper Award	2010

REFEREED JOURNAL PUBLICATIONS

- J-1 A. Mukherjee, M. Pei, and A. L. Swindlehurst, “Blind MIMO Underlay Cognitive Radio Precoding with Completely Unknown Primary CSI,” submitted to *IEEE Journal on Selected Areas in Communication*, 2012.
- J-2 A. Mukherjee, J. Huang, and A. L. Swindlehurst, “Robust MIMO CR Transmissions for Primary Secrecy Under Imperfect CSI,” submitted to *IEEE Wireless Communications Letters*, 2012.
- J-3 A. Mukherjee and A. L. Swindlehurst, “Jamming Games in The MIMO Wiretap Channel With an Active Eavesdropper,” submitted to *IEEE Transactions on Signal Processing*, 2012.
- J-4 A. Mukherjee and A. L. Swindlehurst, “Modified Waterfilling Algorithms for MIMO Spatial Multiplexing with Asymmetric CSI,” *IEEE Wireless Communications Letters*, vol. 1, no. 2, pg. 89-92, April 2012.
- J-5 A. Mukherjee and A. L. Swindlehurst, “Robust Beamforming for Secrecy in MIMO Wiretap Channels with Imperfect CSI,” *IEEE Transactions on Signal Processing*, vol. 59, no. 1, pg. 351-361, Jan. 2011.
- J-6 A. Mukherjee and H. M. Kwon, “General Auction-Theoretic Strategies for Distributed Partner Selection in Asymmetric Cooperative Wireless Networks,” *IEEE Transactions on Communications*, vol. 58, no. 10, pg. 2903-2915, Oct. 2010.
- J-7 D. Torrieri, A. Mukherjee, and H. M. Kwon, “Coded DS-CDMA Systems with Iterative Channel Estimation and No Pilot Symbols,” *IEEE Transactions on Wireless Communications*, vol. 9, no. 6, pg. 2012-2021, June 2010.

PROFESSIONAL MEMBERSHIPS

IEEE Communications and Signal Processing Societies

Complete CV available at <http://newport.eecs.uci.edu/~amukherj/>

ABSTRACT OF THE DISSERTATION

Competition, Coexistence, and Confidentiality
in Multiuser Multi-antenna Wireless Networks

By

Amitav Mukherjee

Doctor of Philosophy in Electrical and Computer Engineering

University of California, Irvine, 2012

Professor A. Lee Swindlehurst, Chair

Competition for limited bandwidth, power, and time resources is an intrinsic aspect of multi-user wireless networks. There has been a recent move towards optimizing coexistence and confidentiality at the physical layer of multi-user wireless networks, mainly by exploiting the advanced capabilities of multiple-input multiple-out (MIMO) signal processing methods. Coexistence of disparate networks is made possible via interference mitigation and suppression, and is exemplified by the current interest in cognitive radio (CR) systems. On the other hand, MIMO communications that are secure at the physical layer without depending upon network-layer encryption are achieved by redirecting jamming or multi-user interference to unauthorized receivers, while minimizing that to legitimate receivers. In all cases, the accuracy of the channel state information (CSI) available at the transmitters plays a crucial role in determining the degree of interference mitigation and confidentiality that is achieved.

This dissertation seeks to examine the development of multi-antenna transmission techniques for interference mitigation and/or secure communication in multi-user wireless networks, with emphasis on robust designs for scenarios with imperfect channel state information. Commencing with coexistence in MIMO CR networks, we de-

sign novel precoding algorithms for the novel scenario where the CSI of the primary users is completely unknown to the CR, and for a novel network where the primary users coexist with both underlay and spectrum-sensing CRs.

The latter half of the thesis considers the secure communication problem in the so-called MIMO wiretap channel with a passive eavesdropper. We first examine the impact of imperfect knowledge of the legitimate channel on the achievable secrecy rate of the MIMO wiretap channel, and design two robust beamforming schemes that are able to recover a large fraction of the secrecy rate lost due to the channel estimation errors. We then consider a more formidable adversary capable of either eavesdropping or jamming in the MIMO wiretap channel. We formulate the interactions between the multi-antenna transmitter and the dual-mode eavesdropper/jammer as a zero-sum game with the MIMO ergodic secrecy rate as the payoff function, and deduce the existence and properties of steady-state Nash Equilibria for a variety of game-theoretic scenarios.

The culmination of this dissertation is to bring together the coexistence and confidentiality aspects by considering a MIMO cognitive radio network where the CR transmissions serve a dual purpose of jamming the eavesdropper while communicating meaningful information to the underlay receivers, but the CR interference to the primary receiver (PR) must also be limited to a prescribed threshold. When only imperfect CSI is available to the CRs, the primary link security is severely degraded since the CR interference to the PR cannot be effectively controlled, and the jamming signals cannot accurately target the eavesdropper. Therefore, we devise robust CR transmission schemes that reduce the degradation in primary secrecy rate under imperfect CSI.

Chapter 1

Introduction

Competition for limited bandwidth and power resources is an intrinsic aspect of multi-user wireless communications, with ramifications in tactical *ad hoc* networks, legacy GSM cellular systems, forthcoming 4G Long-Term Evolution networks, and many more. Based on the continuing enhancement in microprocessor capabilities, there has been a recent move towards optimizing coexistence and confidentiality at the physical layer of multi-user wireless networks, mainly by exploiting the advanced capabilities of multiple-input multiple-out (MIMO) signal processing methods. Coexistence of disparate networks is made possible via interference mitigation and suppression at both transmitters and receivers, and is exemplified by the current interest in cognitive radio (CR) systems. On the other hand, MIMO communications that are secure at the physical layer without depending upon network-layer encryption are achieved by redirecting interference to unauthorized receivers, while minimizing that to legitimate receivers. Therefore, the aspects of competition, coexistence, and confidentiality are usually conflicting, but on occasion may be complementary depending upon the specific application. In all cases, the accuracy of the channel state information (CSI) available at the transmitters plays a crucial role in determining the degree of inter-

ference mitigation and confidentiality that is achieved.

1.1 Coexistence in Wireless Networks

Dynamic spectrum access (DSA) is emerging as a promising solution to enable better utilization of the radio spectrum, especially in bands that are currently under-utilized [1]. DSA partitions wireless terminals into categories of primary (licensed) and secondary (cognitive radio) users, where the primary users have priority in accessing the shared spectrum. Furthermore, the two most prevalent classifications of secondary users are underlay cognitive radios and interweave cognitive radios (ICRs), following the terminology of [2]. Regardless of the precise nature of the cognition possessed by the secondary users, it is imperative that they eliminate or minimize the interference they cause to the primary user network.

Specifically, the underlay paradigm mandates that concurrent secondary and primary transmissions may occur only if the interference generated by the underlay cognitive transmitters (UCTs) at the primary receivers (PRs) is below some acceptable threshold. In contrast, ICRs are allowed to opportunistically use the spectrum only when it is not occupied by a primary transmitter (PT) which has priority. In the absence of standard control channels or coordinated medium access between the primary and secondary users, the ICRs must periodically sense the spectrum for the presence of PTs [3] and cease transmission upon detection. Inevitably, imperfect ICR spectrum sensing due to channel fading and other impairments will lead to unintentional interference at the underlay cognitive receivers (UCRs) and PRs. Underlay and ICR networks have been studied separately in extensive detail for both single-antenna and MIMO terminals [1,2].

Therefore, in underlay systems a fundamental challenge for the UCT is to balance between maximizing its own transmit rate and minimizing the interference it causes to the PRs. In CR networks with single-antenna nodes, this is usually achieved by exploiting some knowledge of the interfering cross-channels to the PRs at the UCT and performing some admission control algorithms with power control [4]. If UCTs are equipped with multiple antennas, the available spatial degrees of freedom can be used to mitigate interference to the PRs during transmission to the underlay receivers. Multi-antenna CR networks have recently received extensive attention, assuming some knowledge of the interfering cross-channels to the PRs at the UCT, either perfect PR cross-channel state information (CSI) [5]-[6], perturbed PR CSI [7]-[8], or statistical PR CSI [9]-[10]. The use of multiple antennas in ICRs has been suggested for improved spectrum sensing capabilities by means of receive diversity [11]-[12].

1.1.1 Open Problems

While the information-theoretic limits of CR networks are still being explored, we list several uninvestigated problems of interest from a signal processing perspective.

- The design of interference-mitigating MIMO precoding schemes in underlay networks where both the realizations and distribution of the interfering channels to the PRs are completely unknown at the UCT is a novel problem. This is a critical issue since the primary system can not deliberately coordinate the collection of CSI for the CR system, and in this scenario none of the previously listed UCT precoding studies are applicable.
- There is no prior art that examines heterogeneous MIMO DSA networks with *both* UCTs and ICRs attempting to coexist simultaneously with primary users.

Since the UCTs must now counter-balance the PR interference with the possibility of ICR interference due to imperfect spectrum sensing, once again none of the existing conventional CR precoding algorithms are optimal.

- The design of MIMO UCT precoding algorithms that simultaneously transmit to UCRs and preserve primary user secrecy in underlay networks infiltrated by eavesdroppers remains unresolved. As an example of the union of the coexistence and confidentiality aspects, this calls for the design of new precoding algorithms that are also robust to imperfections in transmit-side CSI.

1.2 Confidentiality at the Physical Layer

The two fundamental characteristics of the wireless medium, namely *broadcast* and *superposition*, present different challenges in ensuring secure and reliable communications in the presence of adversaries. The broadcast nature of wireless communications makes it difficult to shield transmitted signals from unintended recipients, while superposition can lead to the overlapping of multiple signals at the receiver. As a result, adversarial users are commonly modeled either as (1) a passive *eavesdropper* that tries to listen in on an ongoing transmission without being detected, or (2) a malicious transmitter (*jammer*) that tries to degrade the signal quality at the intended receiver.

While jamming and counter-jamming physical layer strategies have been of long-standing interest especially in military networks, the security of data transmission has traditionally been entrusted to key-based enciphering (cryptographic) techniques at the network layer [13]. However, in dynamic wireless networks this raises issues such as key distribution for symmetric cryptosystems, and high computational complexity of asymmetric cryptosystems. More importantly, all cryptographic measures

are based on the premise that it is computationally infeasible for them to be deciphered without knowledge of the secret key, which remains mathematically unproven. The information-theoretic aspects of secrecy at the physical layer have experienced a resurgence of interest only in the past decade or so.

A network consisting of a transmitter-receiver pair and a passive eavesdropper is commonly referred to as the *wiretap* channel. The information-theoretic aspects of this scenario have been explored in some detail [14–16]. In particular, this work led to the development of the notion of *secrecy capacity*, which quantifies the maximal rate at which a transmitter can reliably send a secret message to the receiver, without the eavesdropper being able to decode it. Ultimately, it was shown that a non-zero secrecy capacity can only be obtained if the eavesdropper’s channel is of lower quality than that of the intended recipient. The secrecy capacity metric for the multiple-input multiple-output (MIMO) wiretap channel, where all nodes may possess multiple antennas, has been studied in [17]–[18], for example. There are two primary categories of secure transmission strategies for the MIMO wiretap channel, depending on whether the instantaneous channel realization of the eavesdropper is known or unknown at the transmitter. In this thesis we assume that this information is not available, and thus the transmitter incorporates an “artificial noise” signal [19]–[20] along with the secret message in an attempt to degrade the eavesdropper’s channel. The artificial noise is transmitted in conjunction with the information signal, and is ideally designed to be orthogonal to the intended receiver, such that only the eavesdropper suffers a degradation in channel quality.

The impact of malicious jammers on the quality of a communication link is another problem of particular interest, especially in mission-critical and military networks. A common approach is to model the transmitter and the jammer as players in a game-theoretic formulation with the mutual information as the payoff function, and

to identify the optimal transmit strategies for both parties [21]-[22]. Recent work has extended this technique to compute the optimal spatial power allocation for MIMO and relay channels with various levels of CSI available to the transmitters [23]-[24].

1.2.1 Open Problems

- No prior work exists on the impact of imperfect knowledge of the channel to the legitimate receiver on the secrecy of the MIMO wiretap channel. Robust secure transmission schemes need to be developed in order to avoid severely degrading the secrecy rate due to misdirected artificial noise.
- Despite the analysis of wiretap and jamming channels over the past five decades, there is no prior work on the MIMO wiretap channel where an evolved eavesdropper is also capable of jamming the legitimate communication link.
- Detecting the presence of a passive eavesdropper is an open problem, which is complicated by the fact that a passive eavesdropper never transmits by definition. At the same time, it is imperative that the presence of a passive eavesdropper be determined before the transmitter can deploy robust secrecy-encoding schemes as a countermeasure.
- The joint optimization of artificial noise parameters and downlink transmit beamformers for security in a multi-antenna broadcast channel is a necessary yet unsolved extension of the three-user wiretap channel.
- Cross-layer procedures such as user selection in the presence of eavesdroppers are needed, whereby secrecy is now considered in the design of the scheduling algorithm.
- The impact of intelligent ‘spoofing’ attacks in closed-loop multi-user MIMO networks is yet to be investigated, where malicious users deliberately report

false CSI back to the base station in order to degrade the system performance of the legitimate users.

1.3 Contributions

We have addressed all of the aforementioned open problems in our research efforts, a partial list of which is given by papers J-1 to J-5 listed on page (ix). In order to sharpen the focus of this dissertation, for the confidentiality topic we present the details of the robust secure beamforming and dual-capable active eavesdropper problems. The remaining aspects of passive eavesdropper detection, secure downlink beamforming, secure user selection, and malicious CSI feedback have been described in the publications [25], [26], [27], and [28], respectively.

1.3.1 Organization

The remainder of this dissertation is organized as follows. A unified overview of the mathematical models of the CR and wiretap channels considered in this thesis is given in Chapter 2. In Chapter 3, as an example of the coexistence issue, we examine a novel underlay MIMO cognitive radio network where the CR has a complete lack of knowledge of its interfering channels to primary receivers. We then propose a rank minimization precoding strategy for such uninformed underlay MIMO CR systems, assuming a minimum information rate must be guaranteed on the CR main channel. We then present a novel heterogeneous CR network in Chapter 4 where the primary users coexist with both underlay (UCRs) and interweave cognitive radios (ICRs); all terminals being potentially equipped with multiple antennas. We investigate the design of MIMO precoding algorithms for the UCRs so as to increase the detection

probability at the ICRs, while simultaneously meeting a desired Quality-of-Service target to its own receivers and constraining interference leaked to PUs. The objective of such a proactive approach, referred to as *prescient* precoding, is to minimize the probability of interference from ICRs to the UCR and PU receivers due to imperfect spectrum sensing.

In Chapter 5 we examine the impact of imperfect knowledge of the legitimate channel on the achievable secrecy rate of the MIMO wiretap channel. To reduce the impact of the CSI errors, we propose two robust beamforming schemes that are able to recover a large fraction of the SINR lost due to the channel estimation errors. In Chapter 6, we consider a more advanced adversary capable of either eavesdropping or jamming in the MIMO wiretap channel. We formulate the interactions between the multi-antenna transmitter and the dual-mode eavesdropper/jammer as a zero-sum game with the MIMO ergodic secrecy rate as the payoff function.

Finally, in Chapter 7 we consider a MIMO multiple-access cognitive radio network where the CR transmissions serve a dual purpose of jamming the eavesdropper while communicating meaningful information to the underlay receivers, but the CR interference to the primary receiver (PR) must also be limited to a prescribed threshold. Under the assumption that only imperfect CSI is available to the CRs, the primary link security is severely degraded since the CR interference to the PR cannot be effectively controlled, and the jamming signals cannot accurately target the eavesdropper. Therefore, we devise robust CR transmission schemes for more general multi-antenna networks that reduce the degradation in primary secrecy rate under imperfect CSI.

Notation: Bold lowercase letters represent vectors, while bold uppercase letters denote matrices. All logarithms are to the base 2. We will use $\mathcal{CN}(\mathbf{0}, \mathbf{Z})$ for a circularly symmetric complex Gaussian distribution with zero mean and covariance matrix \mathbf{Z} , $\mathcal{E}\{\cdot\}$ to denote expectation, $I(\cdot; \cdot)$ mutual information, $(\cdot)^T$ the transpose,

$(\cdot)^H$ the Hermitian transpose, $(\cdot)^{-1}$ the matrix inverse, $\text{vec}(\cdot)$ the matrix column stacking operator, \otimes the Kronecker product, $\text{Tr}(\cdot)$ the trace operator, $|\cdot|$ or \det the matrix determinant, $\|\cdot\|_{\mathcal{F}}$ the Frobenius norm, $\|\cdot\|_2$ the Euclidean norm, $\text{diag}(\mathbf{a})$ a diagonal matrix with the elements of \mathbf{a} on the main diagonal, $|\mathbf{A}|_{i,j}$ the (i, j) element of \mathbf{A} , $\Gamma(x)$ the gamma function, and \mathbf{I} an identity matrix of appropriate dimension.

Chapter 2

Models and Assumptions

In this chapter we provide a unified overview of the CR and wiretap network models considered in this thesis. The mathematical analyses in the subsequent chapters adhere to the system models given here unless specified otherwise. In general, we will always assume that all receivers have perfect receive CSI, and any inaccuracies are restricted to the CSI available at the transmitters. This is partly justified by the requirement of CSI feedback from receivers in general FDD systems or periodic training in TDD systems, inevitably leading to quantization and delay errors.

2.1 Underlay and Interweave MIMO CR Networks

We begin with the most general DSA network possible: a heterogeneous network with underlay and interweave cognitive radios simultaneously coexisting with primary users. All terminals are potentially equipped with multiple antennas: we will assume a N_a -antenna UCT, K_u UCRs with N_s antennas each as its intended destinations where $K_u \leq N_a$, K multi-antenna ICRs with N_I antennas each, and a single PT-

PR pair with N_p and N_r antennas, respectively. A pictorial representation of such a network for the special case of single-antenna ($N_s = 1$) UCRs is shown in Fig. 2.1. This represents the model initially considered in Chapter 4.

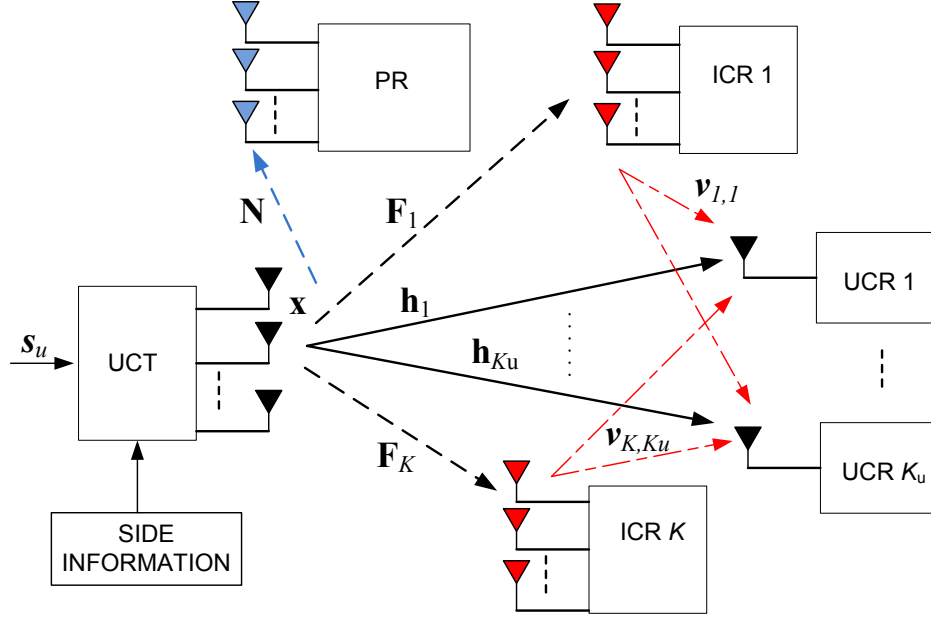


Figure 2.1: Cognitive radio network with a multi-antenna underlay transmitter, K_u underlay receivers, a single MIMO primary receiver, and K spectrum-sensing multi-antenna interweave cognitive radios. The primary transmitter and ICR-to-PR interfering links are not shown for clarity.

Two variants of the above network model are also considered in this work. In the next chapter, we study a homogeneous DSA network where ICRs are absent. In Chapter 7, we consider another homogeneous DSA network without ICRs, with multiple UCTs (up to K_s in number) communicating to a common UCR as a multiple-access channel in the presence of a N_e -antenna eavesdropper that seeks to decode the PT signal. For clarity, the received signal models for each of these different DSA scenarios are enumerated in the associated chapters.

2.2 MIMO Wiretap Channel

We will study a MIMO wiretap channel with an N_a -antenna transmitter (Alice), an N_b -antenna receiver (Bob), and a malicious user (Eve) with N_e antennas, as depicted in Fig. 2.2. Eve need not be a single receiver with colocated antennas; our definition of “Eve” in this context could be multiple receivers in scattered locations who are able to coherently coordinate their received data.

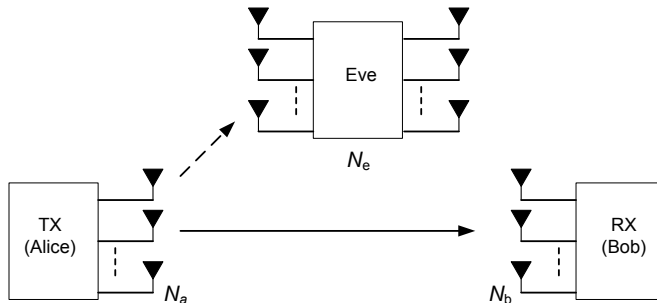


Figure 2.2: Generic MIMO wiretap channel with legitimate transmitter Alice, intended receiver Bob, and unauthorized passive eavesdropper Eve.

We assume that Alice does not have knowledge of the instantaneous CSI of the eavesdropper, only the statistical distribution of its channel, which is assumed to be zero-mean with a scaled-identity covariance. The lack of instantaneous eavesdropper CSI at Alice precludes the joint diagonalization of the main and eavesdropper channels [18]. Instead, as we will show, Alice has the option of utilizing all her power for transmitting data to Bob, regardless of channel conditions or potential eavesdroppers, or optimally splitting her power and simultaneously transmitting the information vector and an “artificial interference” signal that jams any unintended receivers other than Bob. The artificial interference scheme does not require knowledge of Eve’s instantaneous CSI, which makes it suitable for deployment against passive eavesdroppers [18, 19], [29]–[30].

In general, an active eavesdropper Eve also has two options for disrupting the se-

cret information rate between Alice and Bob: she can either eavesdrop on Alice or jam Bob, under a half-duplex constraint. The extension to the full-duplex active eavesdropper scenario is shown in [31]. For the special case of passive eavesdropping studied in Chapters 5 and 7, Eve is assumed to be capable of only listening and never transmits.

The signal received by Bob from Alice while simultaneously being jammed by Eve is

$$\mathbf{y}_b = \mathbf{H}_{ba}\mathbf{x}_a + \sqrt{g_2}\mathbf{H}_{be}\mathbf{x}_e + \mathbf{n}_b, \quad (2.1)$$

while the received signal at Eve when eavesdropping can be represented as

$$\mathbf{y}_e = \sqrt{g_1}\mathbf{H}_{ea}\mathbf{x}_a + \mathbf{n}_e \quad \text{if Eve eavesdrops} \quad (2.2a)$$

$$\mathbf{y}_e = \mathbf{z} \quad \text{if Eve jams} \quad (2.2b)$$

where \mathbf{x}_a is the signal vector transmitted by Alice, \mathbf{x}_e is the Gaussian jamming signal from Eve, \mathbf{z} is an arbitrary variable (possibly 0) independent of the message \mathbf{x}_a , $\mathbf{n}_b, \mathbf{n}_e$ are the naturally occurring additive noise at Bob and Eve, respectively, and $\mathbf{H}_{ba}, \mathbf{H}_{be}, \mathbf{H}_{ea}$ are the corresponding $N_b \times N_a, N_b \times N_e, N_e \times N_a$ channel matrices whose elements are independent and drawn from the complex Gaussian distribution $\mathcal{CN}(0, 1)$. The receive and transmit channels of the eavesdropper have gain factors $\sqrt{g_1}$ and $\sqrt{g_2}$, respectively. These scale factors may be interpreted as an indicator of the relative distances between Eve and the other nodes. The background noise at all receivers is assumed to be spatially white and zero-mean complex Gaussian: $\mathcal{E}\{\mathbf{n}_k\mathbf{n}_k^H\} = \sigma_k^2\mathbf{I}$, where $k = b, e$ indicates Bob or Eve, respectively.

Alice's transmit power is assumed to be fixed at P_a :

$$\mathcal{E}\{\mathbf{x}_a \mathbf{x}_a^H\} = \mathbf{Q}_a \quad \text{Tr}(\mathbf{Q}_a) = P_a ,$$

and similarly Eve has a fixed power of P_e when in jamming mode.

Chapter 3

MIMO CR Precoding with Completely Unknown Primary CSI

3.1 Background

If underlay cognitive transmitters (UCTs) are equipped with multiple antennas, the available spatial degrees of freedom can be used to mitigate interference to the PRs during transmission to the underlay receivers. Multi-antenna CR networks have recently received extensive attention, assuming some knowledge of the interfering cross-channels to the PRs at the UCT, either perfect PR cross-channel state information (CSI) [5]-[6], perturbed PR CSI [7]-[8], or statistical PR CSI [9]-[10]. However, the UCT may not have the luxury of knowing the CSI of the cross links to the PRs, as the primary system would not deliberately coordinate the collection of CSI for the CR system.

In this chapter, we consider the novel scenario where both the realizations and distribution of the PR cross-channels are *completely unknown* at the CR, thereby preclud-

ing the overwhelming majority of existing spectrum underlay schemes in the literature [5]-[32]. Such a scenario of completely-unknown PR CSI is relevant in a number of instances, for example, when the PR transmits intermittently and therefore stymies attempts to learn the cross-channel, when channels are varying rapidly over time, when the PT and PR do not employ time-division duplexing as assumed in [33, 34] among others, or when there are a plurality of active PTs/UCTs and it is impossible to indirectly estimate specific channels.

Specifically, we propose a rank minimization transmission strategy for the UCT while maintaining a minimum information rate on the CR link, and we present a simple solution referred to as frugal waterfilling (FWF) that uses the least amount of power required to achieve the rate constraint with a minimum-rank covariance matrix. In the context of MIMO interference channels (for which the CR underlay network is a special case), rank-minimization has been shown to be a reinterpretation of interference alignment [35], but this approach requires knowledge of interfering cross-channels and treats the overall system sum rate or degrees-of-freedom as the performance metric, assumptions which are both markedly different from the underlay CR scenario we consider.

We also describe two heuristic approaches that have been used in prior work to transform rank minimization problems (RMP) into problems that can be solved via convex optimization. These approaches approximate the rank objective function with two relaxations, one based on the nuclear norm [36], and the other on a log-determinant function [37]. We show theoretically and via numerical simulation that minimizing the rank of the UCT spatial covariance matrix leads to the highest PR throughput in general Rayleigh-fading channels, compared with spreading the transmit power over more dimensions. Furthermore, our simulations indicate that FWF provides a higher PR throughput than the nuclear-norm and log-det heuristic solutions, even though

FWF has a higher interference “temperature” (IT). This suggests that the commonly used IT metric does not accurately capture the impact of the CR interference on PR performance. Instead, we propose a metric based on interference leakage (IL) rate that more accurately reflects the influence of the CR interference.

This chapter is organized as follows. The underlay system model is introduced in Section 3.2. PR CSI-unaware UCT transmit strategies for a single UCR are presented in Section 3.3. The generalization to the underlay downlink with multiple UCRs is shown in Section 3.5. A random matrix-theoretic analysis of the primary outage probability due to the proposed strategies is given in Section 3.6. The penultimate Section 3.7 presents numerical simulations for various underlay scenarios, and we conclude in Section 3.8.

3.2 System Model

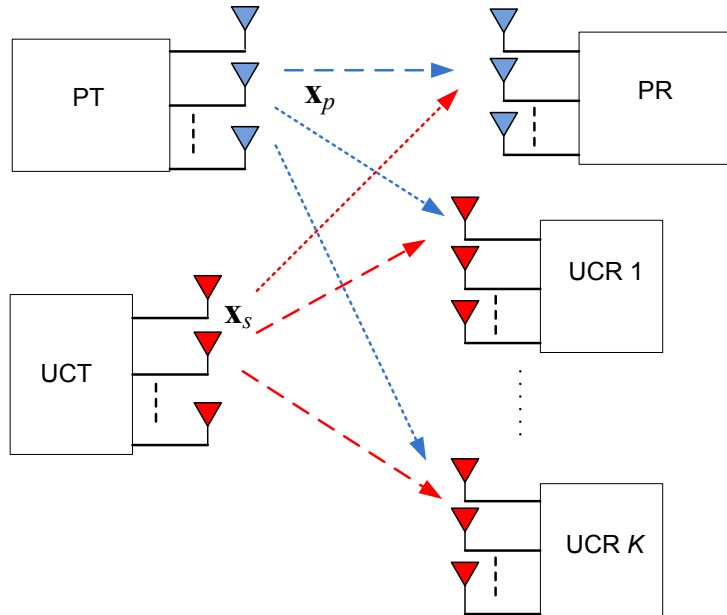


Figure 3.1: Cognitive radio network with a multi-antenna underlay CR transmitter, K_u underlay receivers, and a single MIMO PT-PR pair.

A homogeneous MIMO underlay CR network with K_u multi-antenna underlay receivers is shown in Fig. 1, where a primary system and an underlay CR system share the same spectral band. Since the UCT transmit strategies are independent of the cross-channels to primary users, the numbers of PRs and PTs and their array sizes can be made arbitrary; however to simplify notation we will consider a solitary multi-antenna PT-PR pair. To introduce the problem we first consider the scenario with a single UCR, and generalize to the case of $K_u > 1$ in Sec. 3.5.

Given the model in Chap. 2, the UCR observes

$$\mathbf{y}_s = \mathbf{G}_1 \mathbf{x}_s + \mathbf{G}_2 \mathbf{x}_p + \mathbf{n}_s, \quad (3.1)$$

where $\mathbf{G}_1 \in \mathbb{C}^{N_s \times N_a}$, $\mathbf{G}_2 \in \mathbb{C}^{N_s \times N_p}$ are the complex MIMO channels from the UCT and PT, and $\mathbf{n}_s \sim \mathcal{CN}(\mathbf{0}, \sigma_s^2 \mathbf{I})$ is complex additive white Gaussian noise. We assume Gaussian signaling with zero mean and second-order statistics $\mathcal{E}\{\mathbf{x}_s \mathbf{x}_s^H\} = \mathbf{Q}_s$, and the average UCT transmit power is assumed to be bounded:

$$\text{Tr}(\mathbf{Q}_s) \leq P_s.$$

The signal at the PR is given by

$$\mathbf{y}_p = \mathbf{H}_1 \mathbf{x}_p + \mathbf{H}_2 \mathbf{x}_s + \mathbf{n}_p, \quad (3.2)$$

where $\mathbf{H}_1 \in \mathbb{C}^{N_p \times N_r}$, $\mathbf{H}_2 \in \mathbb{C}^{N_r \times N_a}$ are the channels from the PU and CR transmitters (assumed to be full-rank), and $\mathbf{n}_p \sim \mathcal{CN}(\mathbf{0}, \sigma_p^2 \mathbf{I})$ is complex additive white Gaussian noise. The primary signal is also modeled as a zero-mean complex Gaussian signal with covariance matrix \mathbf{Q}_p and average power constraint $\text{Tr}(\mathbf{Q}_p) \leq P_p$. We will assume \mathbf{Q}_p is fixed and the channels are mutually independent and each composed of i.i.d. zero-mean circularly symmetric complex Gaussian entries, and focus our

attention on the design of the UCT transmit signal.

We assume there is no cooperation between the PT and UCT during transmission, and that both receivers treat interfering signals as noise. The network is essentially an asymmetric 2-user MIMO interference channel, where the UCT attempts to minimize the interference to the PR, but no such reciprocal gesture is made by the PT. The interference covariance matrix at the PR is

$$\mathbf{K}_p = \mathbf{H}_2 \mathbf{Q}_s \mathbf{H}_2^H. \quad (3.3)$$

Define the interference temperature at the PR as [5]-[10]

$$T_p(\mathbf{Q}_s) = \text{Tr}(\mathbf{K}_p). \quad (3.4)$$

Without knowledge of \mathbf{H}_2 or its distribution, the UCT cannot directly optimize the PR interference temperature or outage probability as in existing underlay proposals [5]-[10]. To our best knowledge, precoding strategies and performance analyses for MIMO underlay systems with completely unknown primary CSI have not been presented in the literature thus far. In addition to [5]-[38] not being applicable, the blind interference alignment method for the 2-user MIMO interference channel [39] is also precluded since it requires knowledge of the cross-channel coherence intervals, which we assume is also unknown. In [38], a blind underlay precoding scheme is proposed where the MIMO CR iteratively updates its spatial covariance by observing the transmit power of a solitary PT. The UCT attempts to infer the least-harmful spatial orientation towards the PR, but requires that the PT employ a power control scheme monotonic in the interference caused by the CR, and that the cross-channel remains constant during the learning process. In contrast, we investigate simple non-iterative CR precoding strategies which do not impose any restrictions on the PT transmission

strategy or number of PTs, or cross-channel coherence intervals.

The PT achieves the following rate on its link:

$$R_p(\mathbf{Q}_s) = \log_2 \left| \mathbf{I} + \mathbf{H}_1 \mathbf{Q}_p \mathbf{H}_1^H (\mathbf{K}_p + \sigma_p^2 \mathbf{I})^{-1} \right|. \quad (3.5)$$

Similarly, the achievable rate on the CR link is

$$R_s(\mathbf{Q}_s) = \log_2 \left| \mathbf{I} + \mathbf{G}_1 \mathbf{Q}_s \mathbf{G}_1^H (\mathbf{K}_s + \sigma_s^2 \mathbf{I})^{-1} \right| \quad (3.6)$$

where $\mathbf{K}_s = \mathbf{G}_2 \mathbf{Q}_p \mathbf{G}_2^H$ represents the interference from the PT.

3.3 A Rank Minimization strategy for CSI-Unaware Underlay Transmission

We now expound on the fundamental motivation underlying the UCT transmission strategies proposed in this work. As we have seen, due to a lack of knowledge of \mathbf{H}_2 or its distribution, the UCT cannot directly optimize the PU interference temperature. Hence, we propose an alternative transmission strategy where the UCT tries to minimize a measure of the interference caused to the PR in a “best-effort” sense, while achieving a target data rate to the UCR. Assuming that \mathbf{Q}_p is fixed, we first show that in the clairvoyant case where the UCT has some knowledge of the channel to the PR (\mathbf{H}_2), a rank-1 UCT covariance matrix \mathbf{Q}_s causes least interference to the primary link, which is described in the following proposition.

Proposition 1 *The optimal solution to the clairvoyant problem*

$$\max_{\mathbf{Q}_s} \mathcal{E} \{R_p(\mathbf{Q}_s)\} \quad (3.7a)$$

$$\text{s.t. } R_s(\mathbf{Q}_s) = R_b \quad (3.7b)$$

$$\text{Tr}(\mathbf{Q}_s) \leq P_s \quad (3.7c)$$

$$\mathbf{Q}_s \succeq \mathbf{0}. \quad (3.7d)$$

that maximizes the average PR rate is of rank one, i.e., $\text{rank}(\mathbf{Q}_s^*) = 1$.

Proof: Since $\mathbf{Q}_s \succeq \mathbf{0}$, it can be expressed as $\mathbf{Q}_s = \mathbf{U}\mathbf{\Lambda}\mathbf{U}^H$, where $\mathbf{\Lambda}$ is the diagonal matrix of eigenvalues of \mathbf{Q}_s and \mathbf{U} is the unitary matrix with columns consisting of the eigenvectors of \mathbf{Q}_s . Defining $\tilde{\mathbf{H}}_2 = \mathbf{H}_2\mathbf{U}$, it follow from Lemma 5 in [40] that the distribution of $\tilde{\mathbf{H}}_2$ is the same as that of \mathbf{H}_2 . As a result, the average PU rate can be expressed as

$$\begin{aligned} R_p(\mathbf{Q}_s) &= \Phi(\mathbf{\Lambda}) \\ &= \mathcal{E} \left\{ \log_2 \left[\det \left(\mathbf{I} + \mathbf{H}_1 \mathbf{Q}_p \mathbf{H}_1^H \left(\tilde{\mathbf{H}}_2 \mathbf{\Lambda} \tilde{\mathbf{H}}_2^H + \sigma_p^2 \mathbf{I} \right)^{-1} \right) \right] \right\} \end{aligned}$$

Thus, the problem we considered is essentially equivalent to constructing the diagonal matrix $\mathbf{\Lambda}$ with real nonnegative entries so as to maximize $\Phi(\mathbf{\Lambda})$ under the constraint $\text{Tr}(\mathbf{\Lambda}) = P_s$.

From [23, Lemma 3],[41], we have that $\Phi(\mathbf{\Lambda})$ is a convex function of $\mathbf{\Lambda}$. Note that given any permutation matrix $\mathbf{\Pi}$, we see (using Lemma 5 in [40] again) that

$$\Phi(\mathbf{\Pi}\mathbf{\Lambda}\mathbf{\Pi}^H) = \Phi(\mathbf{\Lambda}).$$

From convexity, we have

$$\Phi \left(\frac{1}{N_a!} \sum_{\mathbf{\Pi}} \mathbf{\Pi} \mathbf{\Lambda} \mathbf{\Pi}^H \right) \leq \frac{1}{N_a!} \sum_{\mathbf{\Pi}} \Phi(\mathbf{\Pi} \mathbf{\Lambda} \mathbf{\Pi}^H) = \Phi(\mathbf{\Lambda})$$

where we have used Jensen's inequality. From the transmit power constraint, we have $\frac{1}{N_a!} \sum_{\mathbf{\Pi}} \mathbf{\Pi} \mathbf{\Lambda} \mathbf{\Pi}^H = (P_s/N_a) \mathbf{I}_{N_a}$. Thus, we have proved that the least PU rate is obtained by $\mathbf{\Lambda} = (P_s/N_a) \mathbf{I}_{N_a}$. Further, due to convexity, we can argue that the largest PU rate is obtain by a point farthest away from $\mathbf{\Lambda} = (P_s/N_a) \mathbf{I}_{N_a}$. Thus, we want $\mathbf{\Lambda}^* = \text{diag}(\lambda_1^*, \dots, \lambda_{N_a}^*)$ that satisfy [42]

$$\max \sum_{i=1}^{N_a} \left(\lambda_i - \frac{P_s}{N_a} \right)^2 \quad \text{s. t.} \quad \sum_{i=1}^{N_a} \lambda_i = P_s$$

Now,

$$\begin{aligned} \sum_{i=1}^{N_a} \left(\lambda_i - \frac{P_s}{N_a} \right)^2 &= \sum_{i=1}^{N_a} \lambda_i^2 - 2 \frac{P_s}{N_a} \sum_{i=1}^{N_a} \lambda_i + \frac{P_s^2}{N_a} \\ &= P_s^2 \left(\sum_{i=1}^{N_a} \left(\frac{\lambda_i}{P_s} \right)^2 - \frac{1}{N_a} \right) \\ &\leq P_s^2 \left(\sum_{i=1}^{N_a} \frac{\lambda_i}{P_s} - \frac{1}{N_a} \right) \\ &= P_s^2 \left(1 - \frac{1}{N_a} \right) \end{aligned}$$

where we used $\sum_{i=1}^{N_a} \left(\frac{\lambda_i}{P_s} \right)^2 \leq \sum_{i=1}^{N_a} \frac{\lambda_i}{P_s} = 1$, and the equality is satisfied by any $(\lambda_1^*, \dots, \lambda_{N_a}^*)$ with all zeros except for one nonzero entry. Hence, we conclude that $\text{rank}(\mathbf{Q}_s^*) = \text{rank}(\mathbf{\Lambda}^*) = 1$. ■

Therefore, in the clairvoyant case where the UCT has some knowledge of the primary CSI, a rank-1 \mathbf{Q}_s causes least interference to the primary link and full-rank \mathbf{Q}_s causes most interference¹. Of course, the optimal \mathbf{Q}_s will depend on the PR CSI, which

¹This notion has been echoed in prior art on MIMO interference channels [43, 44]

we have assumed is unavailable. Still, the result motivates the use of a low-rank transmit covariance at the UCT. It is evident that the UCT does not actually require knowledge of the PR CSI to minimize the rank of \mathbf{Q}_s needed to achieve a rate target R_b on the CR link. To exploit this observation, we henceforth pose the UCT precoder design problem when the PR CSI is completely unknown as

$$(P0) : \quad \min \quad \text{rank}(\mathbf{Q}_s) \tag{3.8a}$$

$$\text{s.t.} \quad R_s(\mathbf{Q}_s) = R_b \tag{3.8b}$$

$$\text{Tr}(\mathbf{Q}_s) \leq P_s \tag{3.8c}$$

$$\mathbf{Q}_s \succeq \mathbf{0}. \tag{3.8d}$$

This is a rank-minimization problem (RMP), and in general is computationally hard to solve since the rank function is quasi-concave and not convex. As explained below, however, in this case a simple waterfilling solution can be obtained. In [45], the mutual information of the CR link is maximized subject to an interference temperature constraint and arbitrary transmit covariance rank constraints, which implies knowledge of PR CSI and thus differs from this work.

3.4 Solutions for the Rank Minimization Design

Notice that the design problem (P0) is ill-posed in the sense that there are potentially an infinite number of solutions. Suppose that we find one minimum-rank solution to (P0) such that $\mathbf{Q}_s = \mathbf{U}\mathbf{\Lambda}\mathbf{U}^H$ for some unitary matrix \mathbf{U} and diagonal matrix $\mathbf{\Lambda}$ satisfies $R_s(\mathbf{Q}_s) = R_b$, $\text{Tr}(\mathbf{\Lambda}) \leq P_s$. If the required power $\text{Tr}(\mathbf{\Lambda})$ is strictly smaller than P_s , then we could find an infinite number of solutions by making small perturbations to \mathbf{U} , which while leading to a higher power requirement, still would require less

power than P_s . Obviously, the solution with least power is more desirable for our underlay CR system in order to minimize the interference caused to the PR, and this solution can easily be found using the *Frugal Waterfilling* (FWF) approach described next.

3.4.1 FWF Approach

The FWF solution seeks to find the least amount of power required to achieve the CR rate target of R_b with the minimum rank transmit covariance \mathbf{Q}_s . The optimization problem can be solved using a combination of the classic waterfilling (CWF) algorithm and a simple bisection line search. The description for FWF is outlined as Algorithm IV-A.1 below. In brief, FWF cycles through the possible number of transmit dimensions in ascending order starting with a rank-one \mathbf{Q}_s , and at each step computes the transmit power required to meet the rate constraint R_b based on CWF. This requires a simple line search over the transmit power for each step. Once a solution is found that satisfies the transmit power constraint, the algorithm terminates. If no feasible solution is found for all N_a transmit dimensions, the CR link will be in outage.

The FWF algorithm was presented in brief without analysis by the authors in [46], and through simulation were shown to be an effective transmission strategy in conventional downlink, wiretap, and underlay networks. While FWF finds an efficient solution to (P0), in general rank minimization problems are difficult to solve and often require exponential-time complexity. Consequently, heuristic approximations to the matrix rank have been proposed as alternatives in order to yield simpler optimization problems. In particular, the nuclear norm [36] and log-determinant [37] heuristics have been proposed in order to convexify RMP problems like (P0) and

Algorithm 3.4.1.1 Frugal Waterfilling for UCT Rank/Power Tradeoff [46]

Require: $P_s > 0, R_b > 0$

set $r = \text{rank}(\mathbf{G}_1)$

for $M = 1$ to r **do**

Solve:

$$p(M) = \min \text{Tr}(\mathbf{Q}_s)$$

$$\text{s. t. } \log_2 \left| \mathbf{I} + \mathbf{G}_1 \mathbf{Q}_s \mathbf{G}_1^H (\mathbf{K}_s + \sigma_s^2 \mathbf{I})^{-1} \right| = R_b .$$

end for

if $p(r) > P_s$ **then**

Declare outage

else

CWF solution: $N = \arg \min_M p(M)$;

FWF solution: $N = \arg \min_M M$;

\mathbf{Q}_s determined by waterfilling $p(N)$ over N largest singular values of $(\mathbf{K}_s + \sigma_s^2 \mathbf{I})^{-1/2} \mathbf{G}_1$

end if

provide approximate solutions with polynomial-time complexity. In the discussion below, we show how these approximations can be applied to the RMP we consider in this chapter.

3.4.2 Nuclear Norm and Log-det Heuristic

The *nuclear norm heuristic* is based on the fact the nuclear norm (sum of the singular values of a matrix) is the convex envelope of the rank function on the unit ball. When the matrix is positive semidefinite, the nuclear norm is the same as the trace function.

As a result, the design problem (P0) can be formulated as follows:

$$\begin{aligned}
\text{(P1):} \quad & \min \quad \text{Tr}(\mathbf{Q}_s) \\
& \text{s.t.} \quad R_s(\mathbf{Q}_s) = R_b \\
& \quad \quad \text{Tr}(\mathbf{Q}_s) \leq P_s \\
& \quad \quad \mathbf{Q}_s \succeq \mathbf{0}.
\end{aligned} \tag{3.9}$$

The nuclear norm heuristic (P1) is a convex optimization problem and can be solved using the CWF algorithm together with a bisection line search (similar to FWF). It is well known that under the CWF algorithm, the lowest transmit power is achieved when $\text{rank}(\mathbf{Q}_s)$ is chosen as large as possible (up to $\text{rank}(\mathbf{G}_1)$). This is clearly contrary to the rank-minimization design formulation, which indicates that the nuclear norm approach for this problem is a poor approximation.

Using the function $\log \det(\mathbf{Q}_s + \delta \mathbf{I})$ as a smooth surrogate for $\text{rank}(\mathbf{Q}_s)$, the *log-det heuristic* can be described as follows:

$$\begin{aligned}
\text{(P2):} \quad & \min \quad \log \det(\mathbf{Q}_s + \delta \mathbf{I}) \\
& \text{s.t.} \quad R_s(\mathbf{Q}_s) = R_b \\
& \quad \quad \text{Tr}(\mathbf{Q}_s) \leq P_s \\
& \quad \quad \mathbf{Q}_s \succeq \mathbf{0},
\end{aligned} \tag{3.10}$$

where $\delta \geq 0$ can be interpreted as a small regularization constant (we choose $\delta = 10^{-6}$ for numerical examples). Since the surrogate function $\log \det(\mathbf{Q}_s + \delta \mathbf{I})$ is smooth on the positive definite cone, it can be minimized using a local minimization method. We use iterative linearization to find a local minimum to the optimization problem (P2) [37]. Let $\mathbf{Q}_s^{(k)}$ denote the k th iteration of the optimization variable \mathbf{Q}_s . The

first-order Taylor series expansion of $\log \det(\mathbf{Q}_s + \delta \mathbf{I})$ about $\mathbf{Q}_s^{(k)}$ is given by

$$\begin{aligned} \log \det(\mathbf{Q}_s + \delta \mathbf{I}) &\approx \log \det(\mathbf{Q}_s^{(k)} + \delta \mathbf{I}) + \\ &\quad \text{Tr}[(\mathbf{Q}_s^{(k)} + \delta \mathbf{I})^{-1}(\mathbf{Q}_s - \mathbf{Q}_s^{(k)})]. \end{aligned} \quad (3.11)$$

Hence, we could attempt to minimize $\log \det(\mathbf{Q}_s + \delta \mathbf{I})$ by iteratively minimizing the local linearization (3.11). This leads to

$$\mathbf{Q}_s^{(k+1)} = \text{argmin} \text{Tr}[(\mathbf{Q}_s^{(k)} + \delta \mathbf{I})^{-1} \mathbf{Q}_s]. \quad (3.12)$$

If we choose $\mathbf{Q}_s^{(0)} = \mathbf{I}$, the first iteration of (3.12) is equivalent to minimizing the trace of \mathbf{Q}_s . Therefore, this heuristic can be viewed as a refinement of the nuclear norm heuristic. As a result, we always pick $\mathbf{Q}_s^{(0)} = \mathbf{I}$, so that $\mathbf{Q}_s^{(1)}$ is the result of the trace heuristic, and the iterations that follow try to reduce the rank of $\mathbf{Q}_s^{(1)}$ further.

Note that at each iteration we will solve a weighted trace minimization problem, which is equivalent to the following optimization problem

$$\begin{aligned} \text{(P2-1)} : \quad &\min \quad \text{Tr}(\mathbf{F}^H \mathbf{A} \mathbf{F}) \\ &\text{s.t.} \quad \log_2 \det(\mathbf{I} + \mathbf{F}^H \mathbf{R} \mathbf{F}) = R_b \\ &\quad \text{Tr}(\mathbf{F}^H \mathbf{F}) \leq P_s. \end{aligned} \quad (3.13)$$

where $\mathbf{A} = (\mathbf{Q}_s^{(k)} + \delta \mathbf{I})^{-1}$, $\mathbf{R} = \mathbf{G}_1^H (\mathbf{G}_2 \mathbf{Q}_p \mathbf{G}_2^H + \sigma_s^2 \mathbf{I})^{-1} \mathbf{G}_1$. This is a Schur-concave optimization problem with multiple trace/log-det constraints. From Theorem 1 in [45], the optimal solution to problem (3.13) is $\mathbf{F}^* = \mathbf{A}^{-1/2} \mathbf{U} \mathbf{\Sigma}$, and $\mathbf{Q}_s^{(k+1)} = \mathbf{F}^* \mathbf{F}^{*H}$ is an optimal solution to (3.12), where $\mathbf{A}^{-1/2} = \mathbf{U}_\mathbf{A} \mathbf{\Lambda}_\mathbf{A}^{-1/2} \mathbf{U}_\mathbf{A}^H$, $\mathbf{U}_\mathbf{A}$ and $\mathbf{\Lambda}_\mathbf{A}$ are defined in the eigen-decomposition $\mathbf{A} = \mathbf{U}_\mathbf{A} \mathbf{\Lambda}_\mathbf{A} \mathbf{U}_\mathbf{A}^H$, \mathbf{U} is a unitary matrix, and $\mathbf{\Sigma} = \text{diag}(\sqrt{\mathbf{p}})$ is a rectangular diagonal matrix.

Substituting the optimal solution structure \mathbf{F}^* into (3.13), we have the following equivalent problem

$$\begin{aligned}
\text{(P2-2):} \quad & \min \quad \text{Tr}(\boldsymbol{\Sigma}\boldsymbol{\Sigma}^H) \\
& \text{s.t.} \quad \log_2 \det(\mathbf{I} + \boldsymbol{\Sigma}^H \mathbf{U}^H \tilde{\mathbf{R}} \mathbf{U} \boldsymbol{\Sigma}) = R_b \\
& \quad \text{Tr}(\mathbf{U}^H \mathbf{A}^{-1} \mathbf{U} \boldsymbol{\Sigma} \boldsymbol{\Sigma}^H) \leq P_s
\end{aligned} \tag{3.14}$$

where $\tilde{\mathbf{R}} = \mathbf{A}^{-1/2} \mathbf{R} \mathbf{A}^{-1/2}$. It is found that the equivalent problem (3.14) is essentially equivalent to the converse formulation

$$\begin{aligned}
\text{(P2-3):} \quad & \max \quad \log_2 \det(\mathbf{I} + \boldsymbol{\Sigma}^H \mathbf{U}^H \tilde{\mathbf{R}} \mathbf{U} \boldsymbol{\Sigma}) \\
& \text{s.t.} \quad \text{Tr}(\boldsymbol{\Sigma}\boldsymbol{\Sigma}^H) = P_0 \\
& \quad \text{Tr}(\mathbf{U}^H \mathbf{A}^{-1} \mathbf{U} \boldsymbol{\Sigma} \boldsymbol{\Sigma}^H) \leq P_s.
\end{aligned} \tag{3.15}$$

This is because both formulations (3.14) and (3.15) describe the same tradeoff curve of performance versus power. Therefore, the quality-constrained problem (P2-2) can be numerically solved by iteratively solving the power-constrained problem (P2-3), combined with the bisection method.

The problem formulation in (P2-3) is a Schur-convex optimization problem with two trace constraints. Using Theorem 1 in [45] again, if we let $\tilde{\mathbf{R}} = \mathbf{U}_{\tilde{\mathbf{R}}} \boldsymbol{\Lambda}_{\tilde{\mathbf{R}}} \mathbf{U}_{\tilde{\mathbf{R}}}^H$ denote the eigen-decomposition of $\tilde{\mathbf{R}}$, then the optimal unitary matrix \mathbf{U} will be chosen as $\mathbf{U}_{\tilde{\mathbf{R}}}$. Denoting $\mathbf{a} = \text{diag}(\mathbf{U}^H \mathbf{A}^{-1} \mathbf{U})$ and letting $\lambda_{\tilde{\mathbf{R}},1} \geq \lambda_{\tilde{\mathbf{R}},2} \geq \dots \geq \lambda_{\tilde{\mathbf{R}},N_a}$ represent the diagonal elements of $\boldsymbol{\Lambda}_{\tilde{\mathbf{R}}}$, the optimal power allocation can be shown to have the form of a *multilevel* waterfilling solution:

$$p_i = \left(\frac{1}{\mu + a_i \nu} - \frac{1}{\lambda_i} \right)^+, \quad i = 1, \dots, N_a \tag{3.16}$$

where a_i is the i th element of \mathbf{a} , and μ, ν can be shown to be the nonnegative Lagrange

multipliers associated with the two power constraints. The algorithmic description for the log-det heuristic approach is outlined in Algorithm 3.4.2.1.

Algorithm 3.4.2.1 Iterative log-det heuristic Algorithm for rank-minimization problem

Require: $P_s > 0, R_b > 0,$

set $\delta = 10^{-6}, \Delta = 10^{-3}, k = 0,$

$$\mathbf{Q}_s^{(0)} = \mathbf{I}, \mathbf{R} = \mathbf{G}_1^H (\mathbf{K}_s + \sigma_s^2 \mathbf{I})^{-1} \mathbf{G}_1.$$

repeat

$$\mathbf{A} = (\mathbf{Q}_s^{(k)} + \delta \mathbf{I})^{-1}, \tilde{\mathbf{R}} = \mathbf{A}^{-1/2} \mathbf{R} \mathbf{A}^{-1/2},$$

$$\text{eig}(\tilde{\mathbf{R}}) = \mathbf{U}_{\tilde{\mathbf{R}}} \boldsymbol{\Lambda}_{\tilde{\mathbf{R}}} \mathbf{U}_{\tilde{\mathbf{R}}}^H.$$

$$\text{set } \mathbf{U} = \mathbf{U}_{\tilde{\mathbf{R}}}, \mathbf{a} = \text{diag}(\mathbf{U}^H \mathbf{A}^{-1} \mathbf{U}).$$

Solve:

$$\min \mathbf{1}^T \mathbf{p}$$

$$\text{s. t. } \log_2 \left(\prod_i (1 + p_i \lambda_{\tilde{\mathbf{R}},i}) \right) = R_b$$

$$\mathbf{a}^T \mathbf{p} \leq P_s.$$

$$\boldsymbol{\Sigma} = \text{diag}(\mathbf{p})$$

$$\mathbf{F} = \mathbf{A}^{-1/2} \mathbf{U} \boldsymbol{\Sigma}$$

$$\mathbf{Q}_s^{(k+1)} = \mathbf{F} \mathbf{F}^H$$

until $\log_2(\det(\mathbf{Q}_s^{(k)} + \delta \mathbf{I})) - \log_2(\det(\mathbf{Q}_s^{(k+1)} + \delta \mathbf{I})) < \Delta$

if $\mathbf{a}^T \mathbf{p} > P_s$ **then**

Declare outage

else

$$\rho = \mathbf{a}^T \mathbf{p} / P_s; \quad \mathbf{Q}_s = \mathbf{Q}_s^{(k+1)}$$

end if

3.5 Underlay CR Downlink

In this section we extend the blind underlay precoding paradigm to a MIMO underlay downlink network with K_u UCRs. We consider a modified block-diagonalization precoding strategy [47] where multiple data streams are transmitted to each UCR. Let each UCR be equipped with N_s antennas for simplicity, although the proposed precoding schemes hold for heterogeneous receiver array sizes as long as the total

number of receive antennas does not exceed N_a . The extension to the case where the UCT serves N_a spatial streams regardless of the total number of receive antennas can be made using the coordinated beamforming approach [47], for example. The received signal at UCR k is now

$$\mathbf{y}_k = \mathbf{G}_{k,1} \mathbf{W}_k \mathbf{s}_{u,k} + \sum_{j \neq k}^{K_u} \mathbf{G}_{k,1} \mathbf{W}_j \mathbf{s}_{u,j} + \mathbf{G}_{k,2} \mathbf{s}_p + \mathbf{n}_k \quad (3.17)$$

where $\mathbf{G}_{k,1} \in \mathbb{C}^{N_s \times N_a}$ is the main channel, $\mathbf{W}_k \in \mathbb{C}^{N_a \times l_k}$ is the precoding matrix applied to signal $\mathbf{s}_{u,k} \in \mathbb{C}^{l_k \times 1}$ for user k , \mathbf{s}_p is the PT signal received over interfering channel $\mathbf{G}_{k,2} \in \mathbb{C}^{N_s \times N_p}$, and $\mathbf{n}_k \sim \mathcal{CN}(0, \sigma_k^2 \mathbf{I})$ is additive Gaussian noise. The UCT transmit covariance per UCR is now $\mathbf{Q}_{k,s} = \mathbf{W}_k \mathbf{W}_k^H$, and the overall UCT transmit covariance assuming independent messages is $\mathbf{Q}_s = \sum_{k=1}^{K_u} \mathbf{Q}_{k,s}$.

We assume each UCR has a desired information rate of R_k , and adopt the ‘‘BD for power control’’ approach in [47, Sec. II-B]. Letting $\mathbf{W}_k = \mathbf{T}_k \mathbf{\Lambda}_k^{1/2}$, it is possible to separately design the beamforming matrix \mathbf{T}_k and diagonal power allocation matrix $\mathbf{\Lambda}_k$ per user to achieve rate R_k in a two-step process. Let

$$\mathbf{G}_{-k} = \begin{bmatrix} \mathbf{G}_{1,1} & \cdots & \mathbf{G}_{k-1,1} & \mathbf{G}_{k+1,1} & \cdots & \mathbf{G}_{K_u,1} \end{bmatrix}$$

represent the the overall UCR downlink channel excluding the k^{th} user. First, a closed-form solution for the unit-power beamforming matrix \mathbf{T}_k of user k is obtained from the nullspace of \mathbf{G}_{-k} . To achieve this, from the SVD $\mathbf{G}_{-k} = \mathbf{U}_{-k} \mathbf{\Sigma}_{-k} \begin{bmatrix} \mathbf{V}_{-k,1} & \mathbf{V}_{-k,0} \end{bmatrix}^H$, the last $(N_a - l_k)$ right singular vectors contained in $\mathbf{V}_{-k,0}$ can be used to construct \mathbf{T}_k [47]. The BD strategy therefore completely eliminates intra-UCR interference on the underlay downlink, and the residual interference-plus-noise covariance matrix at

UCR k is

$$\mathbf{Z}_k = \mathbf{G}_{k,2} \mathbf{Q}_p \mathbf{G}_{k,2}^H + \sigma_s^2 \mathbf{I}. \quad (3.18)$$

Proceeding to the power allocation step, let $\text{rank}(\mathbf{G}_{k,1} \mathbf{T}_k) = r_k$ for user k 's effective channel, and assume $l_k = r_k$. Consider the SVD of user k 's pre-whitened effective channel

$$\mathbf{Z}_k^{-1/2} \mathbf{G}_{k,1} \mathbf{T}_k = \mathbf{U}_k \mathbf{\Lambda}_k \mathbf{V}_k^H$$

where $\mathbf{\Lambda}_k = \text{diag}(\lambda_{k,1}, \dots, \lambda_{k,r_k})$ is the power allocation matrix. While [47] computes $\mathbf{\Lambda}_k$ using the classic waterfilling algorithm in order to minimize the power required to achieve rate R_k , we can instead apply any of the other schemes discussed in Sec. 3.3 such as FWF. Due to the subadditivity of the rank function, reducing the rank of the per-user transmit covariances via FWF effectively reduces the rank of the overall UCT transmit covariance \mathbf{Q}_s , which in turn mitigates the interference caused to the PR according to Proposition 1.

3.6 Primary Outage Probability

In this section we characterize the impact of the classic and frugal waterfilling methods on the primary receiver performance assuming independent Rayleigh fading on all channels. Herein, the channels are mutually independent and are each composed of i.i.d. zero-mean circularly symmetric complex Gaussian entries, i.e., $\text{vec}(\mathbf{G}_1) \sim \mathcal{CN}(\mathbf{0}, \mathbf{I})$, and the same distribution holds for $\mathbf{H}_1, \mathbf{H}_2$, and \mathbf{G}_2 .

A first approach would be to directly analyze the PR rate outage probability $I_r =$

$\Pr(R_p(\mathbf{Q}_s) \leq T)$ for a target rate T , which is equivalent to

$$I_r = \Pr\left(\log_2\left|\mathbf{I} + \mathbf{H}_1\mathbf{Q}_p\mathbf{H}_1^H(\mathbf{K}_p + \sigma_p^2\mathbf{I})^{-1}\right| \leq T\right) \quad (3.19)$$

where \mathbf{Q}_s and \mathbf{Q}_p are obtained via one of the waterfilling methods on their noise-prewhitened channels and are therefore functions of random matrices $\{\mathbf{G}_1, \mathbf{G}_2\}$ and $\{\mathbf{H}_1, \mathbf{H}_2\}$, respectively. Unfortunately, the computation of (3.19) is prohibitively complex since it is a non-linear function of the eigenvalues of four complex Gaussian random matrices (even if the PT applies uniform power allocation instead), and is an open problem to our best knowledge. Previous studies on the statistical distribution of MIMO capacity under interference usually circumvent this difficulty by assuming the MIMO transmitter and interferer adopt uniform or deterministic power allocation [48–50], which reduces the problem to one involving two complex Gaussian random matrices. As such, we are not aware of prior work on the statistics of MIMO capacity under interference where either one or both transmitters employ waterfilling as in our model.

In light of the above, it is of interest to develop more tractable PR performance measures. One such candidate is the PR interference temperature outage probability (ITOP), which is the probability that $T_p(\mathbf{Q}_s)$ [cf. (3.4)] exceeds a threshold η :

$$I_p(\mathbf{Q}_s, \eta) = \Pr\left(\text{Tr}(\mathbf{H}_2\mathbf{Q}_s\mathbf{H}_2^H) \geq \eta\right). \quad (3.20)$$

The ITOP is appealing since the interference temperature metric is widely used in underlay systems, and can be considered to be the MIMO counterpart of efforts to characterize the statistical distribution of aggregate UCT interference in single-antenna networks as in [51]. Paradoxically, however, it is seen in Sec. 3.7 that FWF causes the highest ITOP, even though the average primary rate is the highest and

the PR rate outage is the lowest when \mathbf{Q}_s is computed using FWF. Therefore, a more accurate surrogate for the PR rate outage I_r is the interference leakage-rate outage probability (ILOP), defined as

$$I_l(\mathbf{Q}_s, \eta) = \Pr(\log_2 |\sigma_p^2 \mathbf{I} + \mathbf{H}_2 \mathbf{Q}_s \mathbf{H}_2^H| \geq \eta), \quad (3.21)$$

and it is verified in Sec. 3.7 that UCT transmission schemes with the lowest ILOP also minimize I_r . This is because the leakage rate has a direct impact on the PR rate: $R_p(\mathbf{Q}_s)$ in (3.5) can be rewritten as

$$\begin{aligned} R_p(\mathbf{Q}_s) &= \log_2 |\sigma_p^2 \mathbf{I} + \mathbf{H}_1 \mathbf{Q}_p \mathbf{H}_1^H + \mathbf{K}_p| \\ &\quad - \log_2 |\sigma_p^2 \mathbf{I} + \mathbf{K}_p| \end{aligned} \quad (3.22)$$

where the first term is the sum rate of the virtual PT/UCT multiple access channel (MAC) with optimal successive detection, and the second term is the leakage rate from the UCT. For the worst-case scenario where the PT is decoded first in the virtual MAC, decreasing the leakage rate improves the detection of the PT signal in the first term and simultaneously reduces the second term, thereby decreasing I_r . On the other hand, the link between interference temperature and PR rate is more tenuous.

Assume the UCT transmit covariance matrix \mathbf{Q}_s is of rank k , $1 \leq k \leq \min(N_a, N_s)$, where k is determined by the choice of waterfilling scheme to achieve rate R_b over the pre-whitened UCT channel $\tilde{\mathbf{G}}_1 \triangleq (\mathbf{K}_s + \sigma_s^2 \mathbf{I})^{-1/2} \mathbf{G}_1$. Assume $\tilde{\mathbf{G}}_1^H \tilde{\mathbf{G}}_1$ is of rank d' , with non-zero ordered eigenvalues $\{\alpha_i\}_{i=1}^{d'}$. Waterfilling yields a diagonal \mathbf{Q}_s with

entries [40]

$$[\mathbf{Q}_s]_{i,i} = \left[\mu - \frac{\sigma_s^2}{\alpha_i} \right]^+, \quad i = 1, \dots, N_a, \quad (3.23)$$

where the waterfilling level μ is a function of P_s , σ_s^2 , and $\boldsymbol{\alpha} = (\alpha_1, \dots, \alpha_{d'})$ [52, 53].

Similar arguments hold for the underlay downlink covariance \mathbf{Q}_s designed for sum-rate target $\sum_k R_k$ and aggregate channel $\tilde{\mathbf{G}} = \left[\left(\mathbf{z}_1^{-1/2} \mathbf{G}_{1,1} \mathbf{T}_1 \right)^T \quad \dots \quad \left(\mathbf{z}_{K_u}^{-1/2} \mathbf{G}_{K_u,1} \mathbf{T}_{K_u} \right)^T \right]$.

3.6.1 Interference Temperature Outage Probability

Noting that the ITOP and ILOP (3.20)-(3.21) are still functions of four complex Gaussian matrices, we first develop bounds on the ITOP as follows. We assume \mathbf{H}_2 is full rank such that $\text{rank}(\mathbf{H}_2) = d = \min(N_r, N_a)$, which holds with probability 1 under i.i.d. Rayleigh fading. Define $r = \min(k, d)$ and let $\lambda_i(\mathbf{A})$ denote the i^{th} ordered eigenvalue of \mathbf{A} in descending order. Starting with the commutativity of the trace operator,

$$I_p = \Pr \left(\text{Tr} \left(\mathbf{H}_2^H \mathbf{H}_2 \mathbf{Q}_s \right) \geq \eta \right) \quad (3.24)$$

$$\leq \Pr \left(\text{Tr} \left(\mathbf{H}_2^H \mathbf{H}_2 \mathbf{Q}_s |_{\mathbf{Q}_p = (P_p/N_p) \mathbf{I}} \right) \geq \eta \right) \quad (3.25)$$

$$= \Pr \left(\sum_{i=1}^r \lambda_i \left(\mathbf{H}_2^H \mathbf{H}_2 \mathbf{Q}_s \right) \geq \eta \right) \quad (3.26)$$

$$\approx \Pr \left(\sum_{i=1}^r \lambda_i \left(\mathbf{H}_2^H \mathbf{H}_2 \tilde{\mathbf{Q}}_s \right) \geq \eta \right) \quad (3.27)$$

$$\leq \Pr \left(\sum_{i=1}^r \lambda_i \left(\mathbf{H}_2^H \mathbf{H}_2 \right) \lambda_i \left(\tilde{\mathbf{Q}}_s \right) \geq \eta \right) \quad (3.28)$$

$$\leq \Pr \left(\lambda_1 \left(\tilde{\mathbf{Q}}_s \right) \sum_{i=1}^r \lambda_i \left(\mathbf{H}_2^H \mathbf{H}_2 \right) \geq \eta \right) \quad (3.29)$$

where in (3.25) we eliminate dependence on \mathbf{H}_1 by assuming the PT adopts uniform power allocation ($\mathbf{Q}_p = (P_p/N_p)\mathbf{I}$) such that $\mathbf{K}_s = (P_p/N_p)\mathbf{G}_2\mathbf{G}_2^H$, which is a worst-case interference scenario at the UCR according to Proposition 1 and potentially increases the power expended by the UCT; in (3.27) $\tilde{\mathbf{Q}}_s$ is the statistical waterfilling solution where μ in (3.23) is a function of the statistics of $\{\alpha_i\}_{i=1}^d$ and offers nearly the same performance as instantaneous waterfilling [52]-[53]; and the inequality in (3.28) follows from the bound on the trace of a product of Hermitian matrices [54].

We now define the ordered eigenvalue vectors $\mathbf{h} = (\lambda_1(\mathbf{H}_2^H\mathbf{H}_2), \dots, \lambda_r(\mathbf{H}_2^H\mathbf{H}_2))$ and $\mathbf{q} = (\lambda_1(\tilde{\mathbf{Q}}_s), \dots, \lambda_r(\tilde{\mathbf{Q}}_s))$. Observe that the overall joint density of these random eigenvalues is given by the product of the individual joint densities: $f_{\mathbf{h},\mathbf{q}}(\mathbf{h}, \mathbf{q}) = f_{\mathbf{h}}(\mathbf{h})f_{\mathbf{q}}(\mathbf{q})$ due to the independence of the associated channel matrices. Thus, the bound in (3.29) can be rewritten as

$$I_p \leq E_{\mathbf{h}} \left\{ 1 - F_{q_1} \left(\eta / \sum_{i=1}^r h_i \right) \right\} \quad (3.30)$$

where $F_{q_1}(x)$ is the cumulative distribution function (cdf) of the largest eigenvalue q_1 . From (3.23) we obtain $F_{q_1}(x) = F_{\alpha_1}(\sigma_s^2/(\tilde{\mu} - x))$ where $\tilde{\mu}$ is the statistical water level. The cdf of α_1 , the largest eigenvalue of $\tilde{\mathbf{G}}_1^H\tilde{\mathbf{G}}_1$, is given next for the scenario $N_s \geq N_a, N_s \geq N_p$.

Lemma 1 [55] *Given complex Gaussian matrices $\mathbf{X} \in \mathbb{C}^{N_s \times N_a}, \mathbf{Y} \in \mathbb{C}^{N_s \times N_p}$, and $(N_p \times N_p)$ diagonal matrix $\mathbf{P} = \text{diag}(\rho, \dots, \rho)$, the cdf of the largest eigenvalue α_{max} of the quadratic form $\mathbf{X}^H (\mathbf{Y}\mathbf{P}\mathbf{Y}^H + \sigma^2\mathbf{I}) \mathbf{X}$ when $N_s \geq N_a, N_s \geq N_p$ is*

$$F_{\alpha_{max}}(x) = K_1 \left| \tilde{\Delta}_1(x) \right| \quad (3.31)$$

where $\tilde{\Delta}_1(x) = \left[\tilde{\mathbf{Y}}(x)^T \quad \mathbf{Z}^T \right]^T$,

$$\left[\tilde{\mathbf{Y}}(x) \right]_{i,j} = \begin{cases} \Gamma(i) I_{N_a-i}(\rho) - \Gamma(i) e^{-x} \\ \times \sum_{k=0}^{i-1} \frac{x^k}{k!} I_{N_a-i} \left(\frac{\rho}{1+\rho x} \right), & i = 1, \dots, N_a, \\ (-1)^{N_s-j} I_{N_a+N_s-i}(\rho), & i = N_a + 1, \dots, N_s, \end{cases}$$

$I_a(b) = \sum_{k=0}^a \binom{a}{k} b^{j+k} \Gamma(j+k)$, and the normalization constant K_1 [55, eq. (25)] and the entries $[\mathbf{Z}]_{i,j}$ [55, eq. (27)] are functions of the array dimensions independent of x .

The cdf $F_{\alpha_1}(x)$ for other antenna array dimensions is of a similar form and can be found in [55]. Now, in order to compute the expectation over \mathbf{h} in (3.30), we exploit the Gaussian distribution of \mathbf{H}_2 based on the following lemma.

Lemma 2 [40, 56] *If \mathbf{X} is a $(N_r \times N_a)$ matrix with i.i.d. zero-mean unit-variance complex Gaussian elements, then $\mathbf{W} = \mathbf{X}\mathbf{X}^H$ follows a central complex Wishart distribution if $N_r \leq N_a$, otherwise $\mathbf{W} = \mathbf{X}^H\mathbf{X}$ is Wishart-distributed if $N_r > N_a$. Given $c \triangleq \max(N_r, N_a)$ and $m \triangleq \min(N_r, N_a)$, the joint density of all m ordered eigenvalues of \mathbf{W} is*

$$f_{\Lambda}(\lambda_1, \dots, \lambda_m) = K_w |\mathbf{V}_1(\boldsymbol{\lambda})|^2 \prod_{i=1}^m \frac{e^{-\lambda_i}}{(\lambda_i)^{m-c}}, \quad (3.32)$$

where $\mathbf{V}_1(\boldsymbol{\lambda})$ is a Vandermonde matrix with entries $[\mathbf{V}_1(\boldsymbol{\lambda})]_{i,j} = \lambda_j^{i-1}$, and K_w is a normalization constant independent of $\boldsymbol{\lambda}$ [56, eq. 7].

For the case where $\text{rank}(\tilde{\mathbf{Q}}_s) = k$ is greater than $\text{rank}(\mathbf{H}_2) = d$, i.e., $r = d$, the term $\sum_{i=1}^r h_i$ in (3.30) involves all d ordered eigenvalues $\{h_1, \dots, h_d\}$ and the associated

joint density function $f_{\mathbf{h}}(\mathbf{h})$ is given in Lemma 2. Thus (3.30) yields

$$I_p \leq 1 - K \int \dots \int_{\mathfrak{D}} \left| \tilde{\Delta}_1(\bar{h}) \right| |\mathbf{V}_1(\mathbf{h})| \prod_{i=1}^d \xi(h_i) d\mathbf{h} \quad (3.33)$$

where $K = K_1 K_w$, $\bar{h} = \sigma_s^2 / \left(\tilde{\mu} - \eta / \sum_{i=1}^d h_i \right)$, $\xi(h_i) = \frac{e^{-h_i}}{(h_i)^{m-c}}$, and the integration region is $\mathfrak{D} = \{\infty \geq h_1 \geq h_2 \geq \dots \geq h_d \geq 0\}$. This multidimensional integral has a closed-form solution obtained from the following generalized Cauchy-Binet identity.

Lemma 3 [57, Lemma 2] For $\mathbf{x} = \{x_1, \dots, x_M\}$, arbitrary integrable functions $c_i(\cdot)$, $u_i(\cdot)$, and $\varphi(\cdot)$, $N \times N$ matrix $\Phi(\mathbf{x})$ and $M \times M$ matrix $\Psi(\mathbf{x})$ ($M \leq N$), where $\Phi(\mathbf{x}) = \begin{bmatrix} \mathbf{C}_1(\mathbf{x})^T & \mathbf{C}_2^T \end{bmatrix}^T$, with entries $[\mathbf{C}_1(\mathbf{x})]_{i,j} = c_i(x_j)$ for $i = 1, \dots, N - M; j = 1, \dots, N$, $[\mathbf{C}_2]_{i,j} = c_{2i,j}$ (constant scalars) for $i = N - M + 1, \dots, N; j = 1, \dots, N$, and $[\Psi(\mathbf{x})]_{i,j} = u_i(x_j)$, the following integral identity over domain $\mathfrak{D} = \{b \geq x_1 \geq x_2 \geq \dots \geq x_N \geq a\}$ holds:

$$\int \dots \int_{\mathfrak{D}} |\Phi(\mathbf{x})| \cdot |\Psi(\mathbf{x})| \prod_{k=1}^N \varphi(x_k) d\mathbf{x} = M! \det \mathbf{B} \quad (3.34)$$

where

$$[\mathbf{B}]_{i,j} = \begin{cases} \int_a^b \varphi(x) c_j(x) u_i(x) dx, & i = 1, \dots, N - M; \forall j \\ c_{2i,j}, & i = N - M + 1, \dots, N; \forall j. \end{cases} \quad (3.35)$$

A compact solution to (3.33) is then obtained by setting $\Phi = \tilde{\Delta}_1(\bar{h})$ with $\rho = P_p/N_p$, $\Psi(\mathbf{x}) = \mathbf{V}_1(\mathbf{h})$, and $\varphi(x) = \xi(h)$ in Lemma 3:

$$I_p \leq 1 - d! K |\mathbf{B}_1|; \quad (3.36)$$

$$[\mathbf{B}_1]_{i,j} = \begin{cases} \int_0^\infty \xi(x) x_j^{i-1} [\tilde{\mathbf{Y}}(x)]_{i,j} dx, & i = 1, \dots, N - M; \forall j \\ [\mathbf{Z}]_{i,j}, & i = N - M + 1, \dots, N; \forall j. \end{cases} \quad (3.37)$$

and requires a computationally-inexpensive one-dimensional numerical integration of the product of elementary functions in (3.37).

On the other hand, when $r = k < d$, only the k largest eigenvalues are included in the term $\sum_{i=1}^r h_i$ in (3.30), which necessitates invoking the corresponding joint density function given below in Lemma 4.

Lemma 4 [58] *The joint density function of the ordered subset of the s largest eigenvalues of Wishart matrix \mathbf{W} having m non-zero eigenvalues in total is*

$$f_{\lambda_1, \dots, \lambda_s}(\lambda) = K_w \sum_{\mathbf{n}, \mathbf{m}, s} \sum_{\mathbf{m}, m, s} \text{sgn}(\mathbf{n}, \mathbf{m}) |\mathbf{D}(\lambda_s)| \times \prod_l^s e^{-1} \lambda_l^{N_r - N_a + n_l - m_l + 2} \quad (3.38)$$

where $\mathbf{n} = \mathbf{m} = \{1, \dots, s\}$, each summation is a N_r -fold nested sum over permutations $r_{i,\mathbf{n}}, r_{j,\mathbf{m}}$ of the index sets as defined in [58, eq. (16)] with sign determined by $\text{sgn}(\mathbf{n}, \mathbf{m}) \in \{\pm 1\}$ [58, eq. (17)],

$$[\mathbf{D}(\lambda_s)]_{i,j} = \gamma(N_a - N_r + r_{i,\mathbf{n}} + r_{j,\mathbf{m}}, \lambda_s), \quad (3.39)$$

and $\gamma(a, b)$ is the incomplete gamma function [55].

Substituting $\varphi(x_k) = x_k^{N_r - N_a + n_l - m_l + 2}$ and associated expressions into (3.30) and invoking Lemma 3 provides

$$I_p \leq 1 - \frac{k!K}{e^k} \sum_{\mathbf{n}, d, k} \sum_{\mathbf{m}, d, k} \text{sgn}(\mathbf{n}, \mathbf{m}) |\mathbf{B}_2| \quad (3.40)$$

where

$$[\mathbf{B}_2]_{i,j} = \begin{cases} \int_0^\infty \varphi(x_k) [\mathbf{D}(x)]_{i,j} [\tilde{\mathbf{Y}}(x)]_{i,j} dx, & i = 1, \dots, d - k, \\ [\mathbf{Z}]_{i,j}, & i = d - k + 1, \dots, N; \forall j. \end{cases} \quad (3.41)$$

Since $\gamma(a, b)$ is a standard function in MATLAB, the numerical integration of its product with two elementary functions in (3.41) is straightforward.

3.6.2 Interference Leakage Outage Probability

Turning our attention to the ILOP, starting with the definition of I_l we have

$$\begin{aligned} I_l(\mathbf{Q}_s, \eta) &= \Pr \left(\sum_{i=1}^r \log_2 (\sigma_p^2 + \lambda_i (\mathbf{Q}_s \mathbf{H}_2^H \mathbf{H}_2)) \geq \eta \right) \\ &\approx \Pr \left(\log_2 \prod_{i=1}^r \lambda_i (\mathbf{Q}_s \mathbf{H}_2^H \mathbf{H}_2) \geq \eta \right) \end{aligned} \quad (3.42)$$

$$\leq \Pr \left(\prod_{i=1}^r \lambda_i (\tilde{\mathbf{Q}}_s) \lambda_i (\mathbf{H}_2 \mathbf{H}_2^H) \geq 2^\eta \right) \quad (3.43)$$

$$\leq \Pr \left((q_1)^r \prod_{i=1}^r h_i \geq 2^\eta \right) \quad (3.44)$$

$$= E_{\mathbf{h}} \left\{ 1 - F_{q_1} \left(2^\eta / \prod_{i=1}^r h_i \right)^{1/r} \right\} \quad (3.45)$$

where in (3.42) we consider the interference-limited scenario which is of interest, and (3.43) is due to [54].

The computation of (3.45) closely parallels that of (3.30), by again separating the cases $r = d < k$ and $r = k < d$, followed by invoking Lemmas 1–3 for the former and Lemmas 1,4 and 3 for the latter case, respectively. Therefore, the resulting closed-form bounds for the ILOP are of the form in (3.36) and (3.40), with $\bar{h} = (2^\eta / \prod_{i=1}^r h_i)^{1/r}$ and all other terms being unchanged.

3.7 Numerical Results

In this section, we present some numerical examples to demonstrate the performance of the proposed rank-minimization UCT transmit covariance designs in MIMO cognitive radio networks. We consider MIMO cognitive radio networks with one primary user and one or more underlay receivers. In all simulations, the channel matrices and background noise samples were assumed to be composed of independent, zero-mean Gaussian random variables with unit variance. In situations where the desired rate for UCT cannot be achieved with the given P_s , rather than indicate an outage, we simply assign all power to transmit signals. The performance is evaluated by averaging over 1000 independent channel realizations.

3.7.1 Single Underlay Receiver Scenario

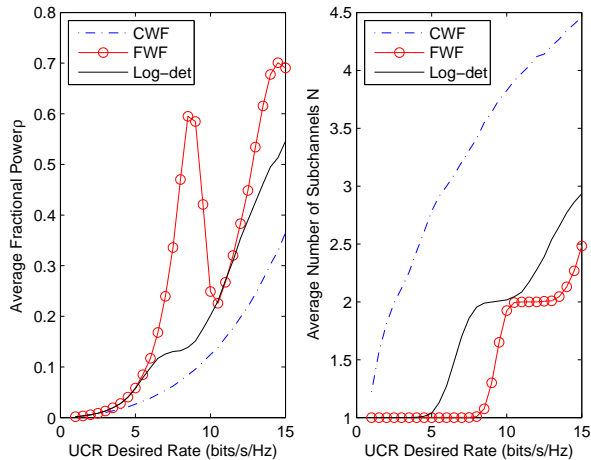


Figure 3.2: Power and dimension allocation versus UCR desired rate.

We first consider the single UCR scenario, where each node is equipped with 6 antennas, and $P_s = 100$, $P_p = 10$. Fig. 7.1 illustrates the average fractional power ρ and the average number of subchannels N required to achieve the UCR desired rates by *CWF*, *FWF* and *log-det heuristic* algorithms. It is shown that the trace and rank

of the UCT transmit covariance matrix \mathbf{Q}_s are two competing objectives, and any scheme which requires more power occupies fewer spatial dimensions. Among the three methods, CWF demands the largest spatial footprint, while the FWF scheme offers the smallest feasible number of transmit dimension. We should point out that the log-det heuristic algorithm for matrix rank minimization does not always provide the smallest transmit dimension, compared to FWF. This is because the log-det algorithm is an approximate heuristic and can only give a local minimum.

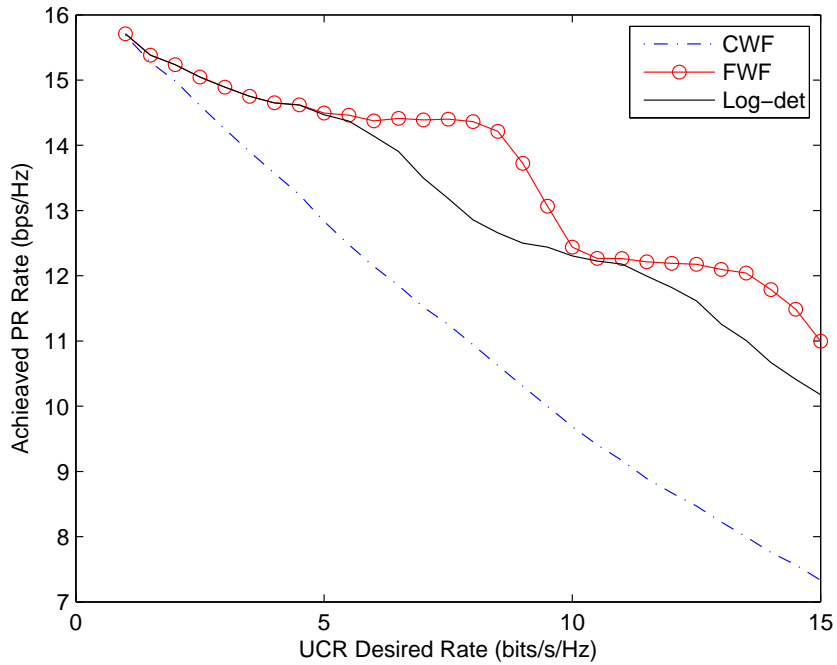


Figure 3.3: Achieved PU rate versus UCT desired rate.

The achieved average primary user data rates for all the methods is depicted in Fig. 7.2. As expected, the lower-rank UCT transmit covariance will cause lesser degradation on average to the PU communication link, thus resulting a higher PR rate in accordance with Proposition 1. Compared to CWF, either of the proposed modified waterfilling algorithms or the log-det heuristic lead to more desirable PR rates, with the advantage of FWF being more pronounced as R_b increases.

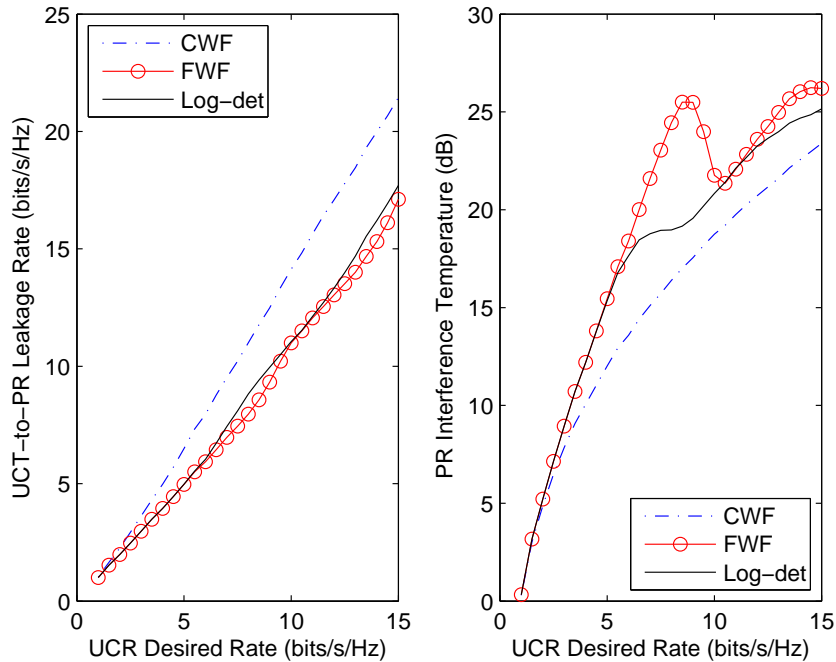


Figure 3.4: Two metrics of PR Interference versus UCR desired rate.

To obtain greater insight, Fig. 3.4 compares two metrics of interference at PR using different algorithms, where one is the newly-defined UCT-PR leakage rate, the other one is the commonly-used interference temperature. We notice that an interesting phenomenon: the two metrics gives the opposite trend. It is worth to point out that the commonly-used interference temperature metric does not accurately capture the interference impact caused by the UCT on the primary mutual information, while the interference leakage rate remedies this defect.

For the statistical characterization of the proposed schemes, we exhibit the empirical complementary cdfs and select analytical upper bounds from Sec. 3.6 of the interference temperature and leakage rate metrics in Fig. 3.5, for 6 antennas at all users and $P_s = 200, R_b = 8, P_p = 40$. An immediate observation is the conflicting trends of the leakage and temperature metrics: FWF causes a much greater interference temperature outage and much smaller leakage rate outage compared to CWF, and

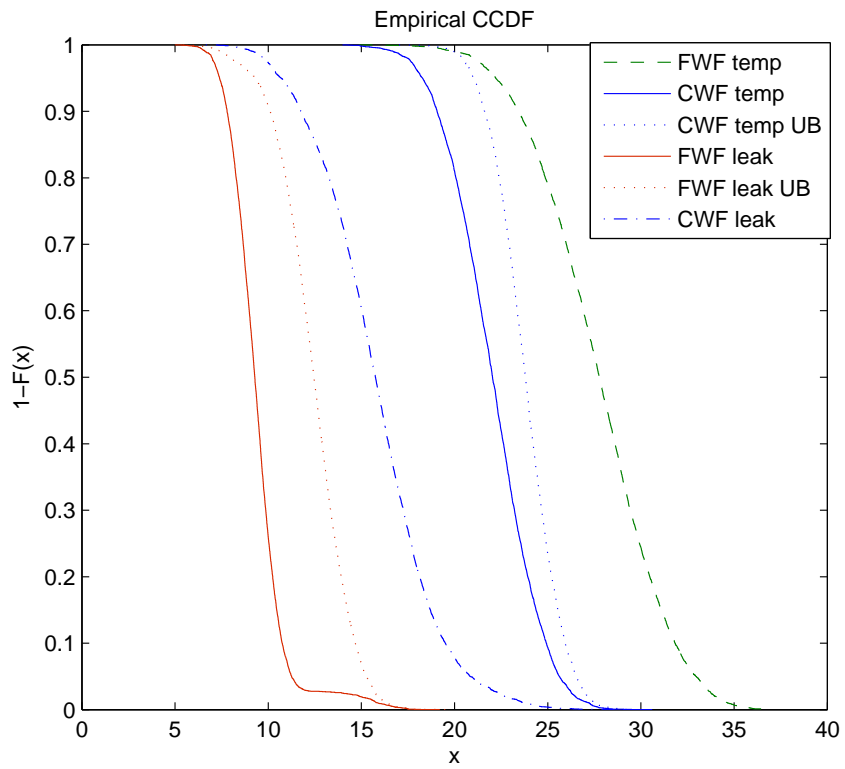


Figure 3.5: Empirical ccdf of interference temperature and leakage rate under CWF and FWF.

the superiority of one versus the other is not apparent. To resolve this dilemma, the corresponding empirical PR rate ccdfs are shown in Fig. 3.6, and it is clear that employing FWF leads to a very significant reduction in PR rate outage probability as compared to CWF. Furthermore, the interference temperature outage is again seen to be misleading regarding the true impact on the PR rate outage probability. Thus, FWF outperforms CWF in terms of both average PR rate and PR rate outage probability.

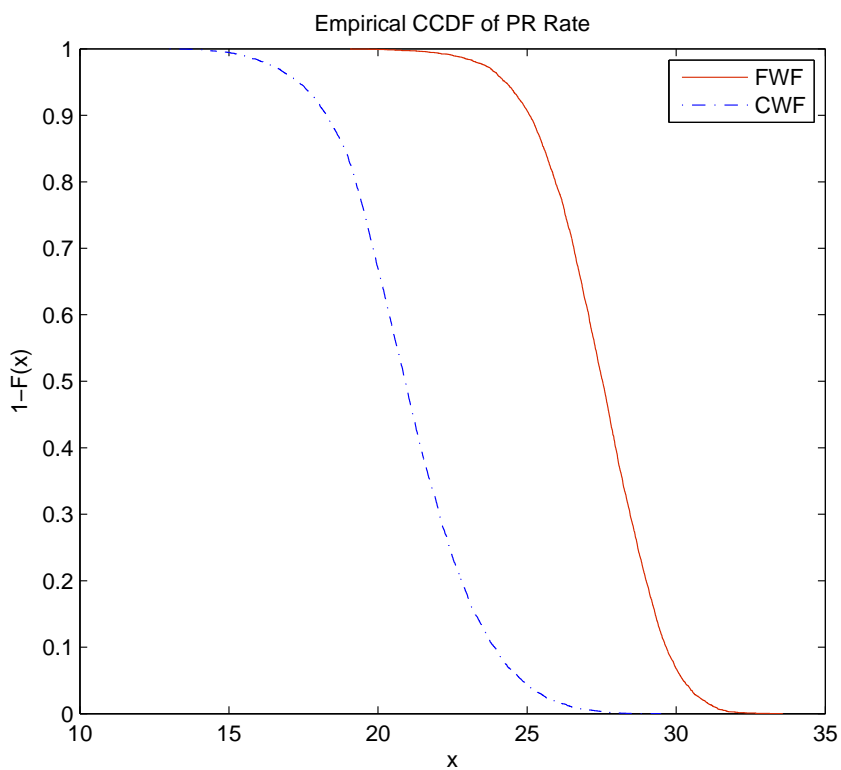


Figure 3.6: Empirical ccdf of PR rate under CWF and FWF.

3.7.2 MIMO Underlay Downlink Scenario

Next, we evaluate the performance of the proposed algorithms with the modified BD strategy of Sec. 3.5 for a MIMO underlay downlink system, where there are $K_u = 3$

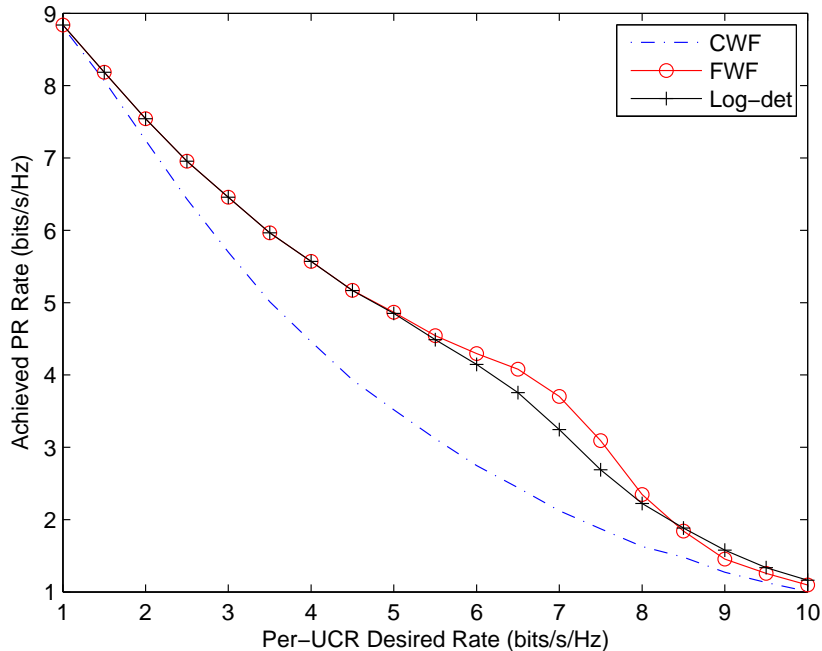


Figure 3.7: Achieved PR rate versus per-UCR desired rate in MIMO underlay downlink, $P_s = 20dB$, $P_p = 10dB$.

UCRs, and $N_a = 12$, $N_p = N_r = N_s = 4$. Without loss of generality it is assumed that the desired rate targets for all UCRs are the same, i.e. $R_1 = R_2 = R_3$. Fig. 3.7 illustrates the achieved PU rate versus per UCT desired rate, when $P_s = 100$ or $20dB$ and $P_p = 10$ or $10dB$. The benefit of minimizing the transmit covariance rank is seen to hold even for the multi-user downlink scenario.

It is also of interest to see how the achieved PR rates under the various designs vary with the UCT transmit power, when the desired rate for each UCT is fixed. The simulation settings are the same as above, except that we fix $R_1 = R_2 = R_3 = 5$ and $P_s \in [10dB, 20dB]$. The results are shown in Fig. 3.8, with the corresponding leakage rate and interference temperature metrics in Fig. 3.9. Once again, FWF offers the optimal average PR rate and PR rate outage probability in the downlink scenario.

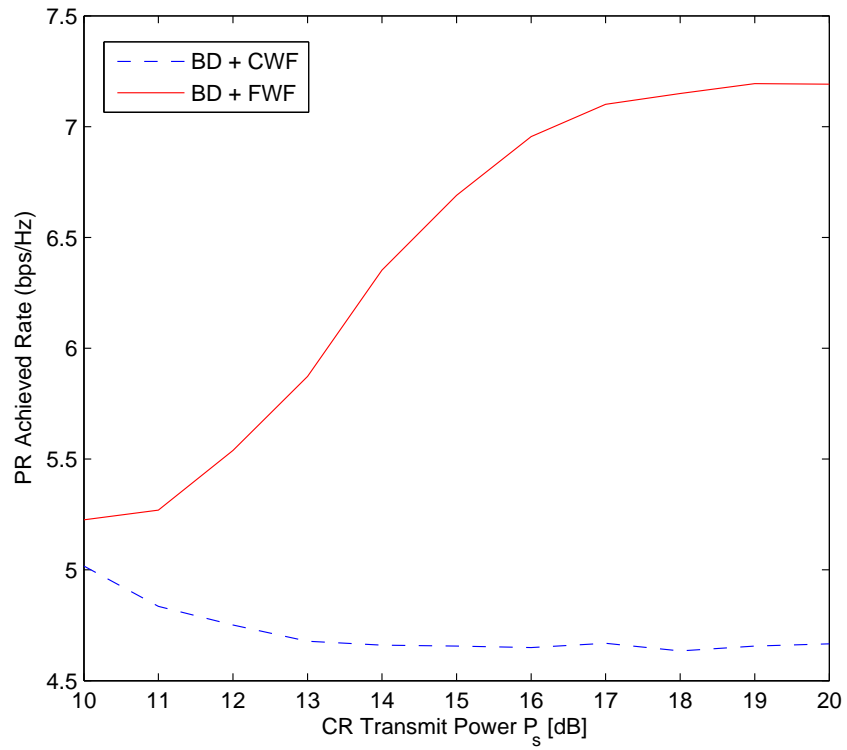


Figure 3.8: Achieved PR rate versus UCT transmit power in MIMO downlink system with identical target rates $R_1 = R_2 = R_3 = 5\text{bits/s/Hz}$.

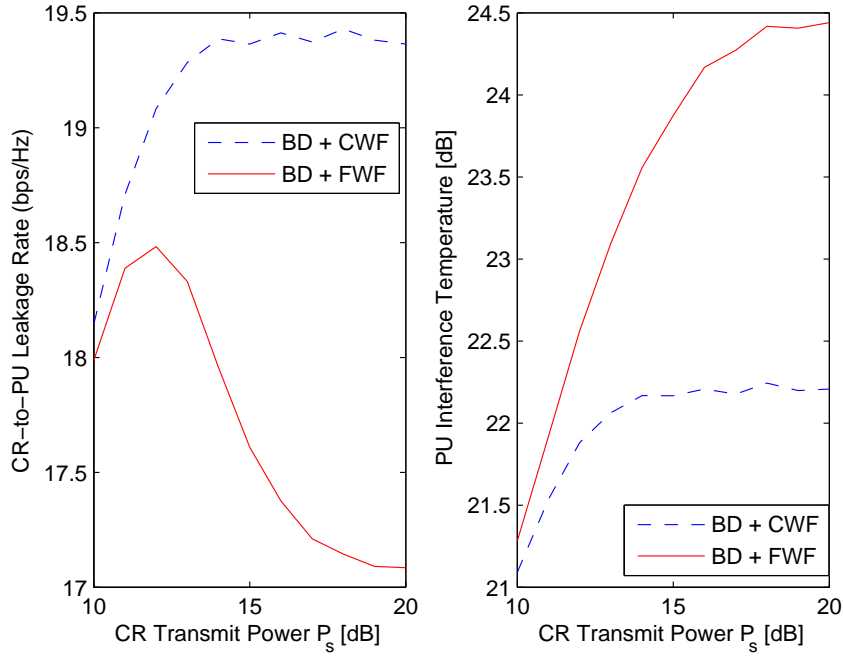


Figure 3.9: Two metrics of PR interference versus UCT transmit power in MIMO underlay downlink with identical target rates $R_1 = R_2 = R_3 = 5$.

3.8 Summary

This chapter has proposed a rank minimization precoding strategy for underlay MIMO CR systems with completely unknown primary CSI, assuming a minimum information rate must be guaranteed on the CR main channel. We presented a simple waterfilling approach can be used to find the minimum rank transmit covariance that achieves the desired CR rate with minimum power. We also presented two alternatives to FWF that are based on convex approximations to the minrank criterion, one that leads to conventional waterfilling for our CR problem, and another based on a log-det heuristic. The CWF approach turns out to be a poor approximation to the min-rank objective, while the log-det approach provides performance similar to FWF, although FWF consistently leads to the highest throughput for the primary link. We also observed that reducing the interference temperature metric is surprisingly not

consistent with improving the PR throughput; in particular, FWF has the highest interference temperature of the algorithms studied, but also leads to the highest PR rate. As an alternative, we proposed an interference leakage metric that is a better indicator of the impact of the CR on the primary link.

Chapter 4

Prescient Precoding in Heterogeneous CR Networks

4.1 Motivation

This chapter examines a fundamentally novel heterogeneous DSA network where the primary users share their spectrum with both UCRs and ICRs; all terminals being potentially equipped with multiple antennas. Specifically, we investigate the design of MIMO precoding algorithms for a underlay downlink network with multiple UCRs and interweave radios. The heterogeneous DSA network presents a myriad of conflicting objectives for the underlay transmitter, since it must mitigate the multi-user interference among its own UCRs, constrain the interference leaked to PRs, and ensure that the detection probability of the ICRs is high so as to preemptively avoid interference from them. Note that such a scenario is radically different from hybrid secondary users that are capable of both underlay and interweave cognition [59, 60]. Consequently, this chapter is devoted to the design of novel precoding algorithms,

collectively referred to as *prescient* precoding, that balance these competing objectives. The aim of prescient precoding is to reduce the probability of interference due to imperfect spectrum sensing from ICRs to the underlay and primary receivers, while simultaneously meeting their QoS/interference temperature requirements.

The chapter is organized as follows. Section 4.2 summarizes the mathematical model of the DSA network and the spectrum sensing performance of the ICRs. Prescient downlink beamforming algorithms for the case of single-antenna underlay receivers are proposed in Section 4.3. Section 4.4 outlines a prescient block-diagonalization algorithm for a MIMO downlink channel with multi-antenna underlay receivers. Selected numerical examples are shown in Section 4.5, and we conclude in Section 4.6.

4.2 Mathematical Model

4.2.1 Signal and Network Model

We consider the heterogeneous DSA network described in Chapter 2, beginning with the case of single-antenna UCRs. The scenario with multi-antenna UCRs is presented in Sec. 4.4. Multiple PRs can be accommodated in the model by aggregating them into a single virtual PR.

Assuming linear precoding, the UCT downlink transmit signal at time index t is written as

$$\mathbf{x}(t) = \sum_{k=1}^{K_u} \mathbf{w}_k s_{u,i}(t) = \mathbf{W} \mathbf{s}_u(t), \quad (4.1)$$

where $\mathbf{W} \in \mathbb{C}^{N_a \times K_u} = \begin{bmatrix} \mathbf{w}_1 & \dots & \mathbf{w}_{K_u} \end{bmatrix}$ is the precoding matrix with its columns

representing individual beamforming vectors, and $\mathbf{s}_u(t) \in \mathbb{C}^{K_u \times 1}$ is the collection of the i.i.d. underlay information symbols drawn from an M -ary constellation with second-order statistics $E\{\mathbf{s}_u \mathbf{s}_u^H\} = \mathbf{I}$. The UCT designs its transmit signal so as to ensure that the interference temperature at the PR remains below a pre-specified threshold ξ_p , as explained in Sec. 4.3.

Suppressing the time index, the overall underlay downlink signal model in the *absence* of ICR interference (i.e., with perfect spectrum sensing) is

$$\begin{bmatrix} y_1 \\ \vdots \\ y_{K_u} \end{bmatrix} = \begin{bmatrix} \mathbf{h}_1 \\ \vdots \\ \mathbf{h}_{K_u} \end{bmatrix} \mathbf{W} \mathbf{s}_u + \begin{bmatrix} n_1 \\ \vdots \\ n_{K_u} \end{bmatrix} \quad (4.2)$$

where y_k is the scalar signal received at the k^{th} UCR, $\mathbf{h}_k \in \mathbb{C}^{1 \times N_a}$ is the corresponding complex channel vector from the UCT, and n_k is a circularly symmetric zero-mean complex Gaussian noise sample with variance σ_k^2 which includes interference from the PT.

We list below the major assumptions regarding the heterogeneous DSA network.

- We assume a *partial CSI* model at the UCT, which is defined to mean that the UCT always has knowledge of the instantaneous realizations of all the downlink channels ($\{\mathbf{h}_k\}_{k=1}^{K_u}$) and UCT-PR ($\{\mathbf{h}_k\}_{k=1}^K$) channels, but may know only the distribution of its channels to the ICRs and the ICR-to-UCR channels.
- The UCT has knowledge of the ICR transmit powers and the parameters of the spectrum sensing scheme deployed at the ICRs, which in practice are likely to be pre-defined by spectrum regulatory agencies.
- There is no coordination between the UCT and ICRs. The UCT and PRs have a

limited coordination with respect to exchange of CSI and tolerable interference temperatures.

- All ICRs are half-duplex, which precludes for example simultaneous data transmission and spectrum sensing. We only consider in-band spectrum sensing, i.e., sensing is conducted on the same band that is used for data transmission.
- The UCRs employ single-user decoding and treat all ICR/PT interference as noise. The interference from the ICRs is assumed to be instantaneous, i.e., the processing delay due to spectrum sensing is neglected.

4.2.2 ICR Spectrum Sensing

The ICRs attempt to individually determine the presence of the PT and UCT in the shared channel by means of non-cooperative spectrum sensing, and we define the alternative hypothesis \mathcal{H}_1 as the scenario when *both* of them are deemed to be present. This is because the case where only the PT is active is irrelevant to the UCT precoder design, and by definition the UCT always transmits concurrently with the PT. In contrast, the ICRs must strictly refrain from transmitting while the PT and UCT are active. The binary hypothesis test for spectrum sensing based on \tilde{M} discrete-time samples at antenna j of the i^{th} ICR, $i = 1, \dots, K$, is

$$\mathcal{H}_0 : z_{i,j}[n] = m_{i,j}[n], \quad j = 1, \dots, N_I; n = 0, \dots, \tilde{M} - 1 \quad (4.3a)$$

$$\mathcal{H}_1 : z_{i,j}[n] = \mathbf{f}_{i,j} \mathbf{W} \mathbf{s}_u[n] + \mathbf{d}_{i,j} \mathbf{s}_p[n] + m_{i,j}[n], \quad j = 1, \dots, N_I; n = 0, \dots, \tilde{M} - 1 \quad (4.3b)$$

where channels $\mathbf{f}_{i,j} \in \mathbb{C}^{1 \times N_a}$ from the UCT and $\mathbf{d}_{i,j} \in \mathbb{C}^{1 \times N_p}$ from the PT are assumed to be invariant over the \tilde{M} samples, $\mathbf{s}_p \in \mathbb{C}^{N_p \times 1}$ is the PT transmit signal with

total power P_t , and $m_{i,j}[n] \sim \mathcal{CN}(0, \epsilon_i^2)$ is additive complex Gaussian noise. The \tilde{M} complex samples are composed of $2\tilde{M}$ independent real and imaginary components [61]. We assume that the background noise at the ICRs is temporally uncorrelated.

A broad range of spectrum sensing algorithms with varying levels of complexity and requisite *a priori* information have been proposed in the literature [11]-[12]. The optimal matched-filter detector has the most prohibitive CSI and PT signal information requirements on one hand, non-coherent energy detection is the simplest possible detector on the other hand since it only requires an accurate estimate of the noise variance ϵ_i^2 , while a range of composite generalized likelihood ratio test (GLRT) and feature detectors lie in between these extremes. Without loss of generality we assume the ICRs employ non-coherent energy detection due to its simplicity and the lack of a need to distinguish between UCT and PT signals.

The test statistic for the energy detector is given by [62]

$$T_i = \sum_{n=0}^{\tilde{M}-1} \sum_{j=1}^{N_I} |z_{i,j}[n]|^2; \quad T_i \underset{\mathcal{H}_0}{\overset{\mathcal{H}_1}{\gtrless}} \lambda_i \quad (4.4)$$

where λ_i is the detection threshold. We begin our development by analyzing the detection probability $P_{D,i}$ at ICR i for deterministic incoming channels and signals from the UCT and PT. Under the null hypothesis \mathcal{H}_0 , we see from (4.3a) that $z_{i,j}[n] \sim \mathcal{CN}(0, \epsilon_i^2)$, whereas under the alternative hypothesis \mathcal{H}_1 we have $z_{i,j}[n] \sim \mathcal{CN}(\mu_{i,j}[n] = \mathbf{f}_{i,j} \mathbf{W} \mathbf{s}_u[n] + \mathbf{d}_{i,j} \mathbf{s}_p[n], \epsilon_i^2)$. Therefore, the test statistic T_i is the sum of the squares of $2\tilde{M}N_I$ independent real zero-mean Gaussian variables and has the following distributions under the two hypotheses:

$$\begin{aligned} T_i &\sim \frac{\epsilon_i^2}{2} \chi_{2\tilde{M}N_I}^2 && \text{under } \mathcal{H}_0 \\ T_i &\sim \frac{\epsilon_i^2}{2} \chi_{2\tilde{M}N_I}'^2(\rho) && \text{under } \mathcal{H}_1 \end{aligned} \quad (4.5)$$

where the noncentrality parameter $\rho = \epsilon_i^{-2} \sum_{n=0}^{\tilde{M}-1} \sum_{j=1}^{N_I} |\mu_{i,j}[n]|^2$ is a function of \mathbf{W} .

Since we have an even number of samples \tilde{M} (real and imaginary components of each sample), the false alarm probability follows immediately from the central chi-square cdf as [63]

$$P_{FA,i} = e^{-\frac{\lambda_i}{\epsilon_i^2}} \sum_{r=0}^{\tilde{M}N_I-1} \frac{1}{r!} \left(\frac{\lambda_i}{\epsilon_i^2} \right)^r. \quad (4.6)$$

where $\lambda_i = \epsilon_i^2 Q_{\chi_{2\tilde{M}N_I}^2}^{-1}(P_f)$ (P_f) is chosen to satisfy a target false alarm rate P_f , and $Q_{\chi_{2\tilde{M}N_I}^2}(\cdot)$ is the complementary cdf of the central chi-square distribution. The detection probability is given by

$$P_{D,i} = Q_{\tilde{M}N_I} \left(\sqrt{\rho}, \sqrt{\frac{2\lambda_i}{\epsilon_i^2}} \right), \quad (4.7)$$

where $Q_M(\cdot, \cdot)$ is the generalized Marcum Q -function [64]. As the number of samples \tilde{M} grows large, T_i approaches a Gaussian random variable in distribution by the central limit theorem (CLT). Under hypothesis \mathcal{H}_1 the CLT yields $T_i \sim \mathcal{N}(\epsilon_i^2 \tilde{M}N_I + \rho, \epsilon_i^4 \tilde{M}N_I + 2\epsilon_i^2 \rho)$ and the corresponding detection probability

$$P_{D,i} \simeq Q \left(\frac{\lambda_i - \epsilon_i^2 \tilde{M}N_I - \rho}{\epsilon_i \sqrt{\epsilon_i^2 \tilde{M}N_I + 2\rho}} \right), \quad (4.8)$$

where $Q(\cdot)$ is the Gaussian Q -function.

4.2.3 ICR Performance Prediction at UCT

The ability of the UCT to predict the spectrum-sensing performance of the ICRs is an important ingredient of the prescient precoding paradigm. Under the partial CSI assumption, it is highly unlikely that the UCT has knowledge of the PT-to-

ICR channel realizations and signals required to compute (4.7) or (4.8). A more plausible scenario is that the UCT knows the realizations of its channels $\{\mathbf{F}_i\}$ to the ICRs, and assumes the PT-to-ICR channels undergo Rayleigh fading with distribution $\mathbf{d}_{i,j} \sim \mathcal{CN}(\mathbf{0}, \sigma_{d,i}^2 \mathbf{I}) \forall i, j$.

Going one step further, the UCT may not have knowledge of the instantaneous realizations of its channels to the ICRs either. In order to gauge the energy detection performance of the ICRs, the UCT assumes a Rayleigh fading scenario such that $\mathbf{f}_{i,j} \sim \mathcal{CN}(\mathbf{0}, \sigma_{f,i}^2 \mathbf{I}) \forall i, j$, and $\mathbf{d}_{i,j} \sim \mathcal{CN}(\mathbf{0}, \sigma_{d,i}^2 \mathbf{I})$ as before. Furthermore, the UCT and PT signals are each assumed to be drawn with uniform probability from a complex M -ary constellation, and all channels, signals, and AWGN samples are mutually independent. Given these assumptions, the ICR samples $z_{i,j}[n]$ are distributed as independent Gaussian random variables [62] for both hypotheses. The false-alarm rate is clearly identical to that in (4.6) since it is channel-independent. Under \mathcal{H}_1 , $E\{z_{i,j}[n]\} = 0$ and $\sigma_{z,i}^2 \triangleq \text{var}\{z_{i,j}[n]\} = 2\sigma_{f,i}^2 \text{Tr}(\mathbf{W}\mathbf{W}^H) + 2P_t N_p \sigma_{d,i}^2 + \varepsilon_i^2$. Thus, $T_i \sim \frac{\sigma_{z,i}^2}{2} \chi_{2\tilde{M}N_I}^2$ and the corresponding average detection probability is

$$\bar{P}_{D,i} = e^{-\frac{\lambda_i}{\sigma_{z,i}^2}} \sum_{r=0}^{\tilde{M}N_I-1} \frac{1}{r!} \left(\frac{\lambda_i}{\sigma_{z,i}^2}\right)^r. \quad (4.9)$$

From the UCT's perspective, a missed detection (Type II error) at any of the ICRs leads to interference at the underlay receivers, and this phenomenon plays a pivotal role in the prescient precoding principle. It will be useful to define the Bernoulli-distributed indicator function F_i as

$$F_i = \begin{cases} 1 & \text{with probability } (1 - P_{D,i}) \\ 0 & \text{with probability } (P_{D,i}). \end{cases} \quad (4.10)$$

F_i therefore models the likelihood that ICR i unintentionally causes interference to

the underlay and primary receivers, and is a function of \mathbf{W} via $P_{D,i}$.

Having defined the impact of missed detections by the ICRs on the performance of the UCRs, we see that it is in the UCT's interest to ensure that the probability of missed detection at the ICRs is made as small as possible, or equivalently, that the probability of detection is made as large as possible. To this end, we introduce the paradigm of prescient precoding in the next section in order to improve the reliability of the underlay downlink.

4.3 Prescient Downlink Precoding

It has been elegantly established that the capacity region of a conventional non-cognitive multi-antenna downlink channel without structured interference is achieved through non-linear dirty-paper coding, since all transmitted signals are known non-causally to the transmitter [65]. However, linear precoding schemes for the multiuser downlink have been extensively studied due to their significantly lower complexity and near-capacity performance in certain regimes, and thus we focus on linear transmit preprocessing at the UCT. By definition, the UCT must limit the (instantaneous or average) interference it causes to the PR to a predefined threshold ξ_p :

$$\text{Tr}(\mathbf{N}\mathbf{W}\mathbf{W}^H\mathbf{N}^H) \leq \xi_p \tag{4.11}$$

if the instantaneous channel $\mathbf{N} \in \mathbb{C}^{N_r \times N_a}$ to the PR is known.

The signal at an arbitrary UCR inclusive of ICR interference due to missed detections

can be written as

$$y_k = \mathbf{h}_k \mathbf{w}_k s_{u,k} + \underbrace{\sum_{j \neq k}^{K_u} \mathbf{h}_k \mathbf{w}_j s_{u,j}}_{\text{intra - UCR interference}} + \underbrace{\sum_{i=1}^K F_i \mathbf{v}_{k,i} \mathbf{s}_{I,i}}_{\text{ICR interference}} + n_k, \quad k = 1, \dots, K_u, \quad (4.12)$$

where $\mathbf{v}_{k,i} \sim \mathcal{CN}(\mathbf{0}, \sigma_{v,i}^2 \mathbf{I})$ and $\mathbf{s}_{I,i} \in \mathbb{C}^{N_I \times 1}$ represent the $(1 \times N_I)$ interfering channel and signal vector of power P_i from ICR i .

We are interested in the characteristics of the aggregate ICR interference power at the k^{th} UCR, defined as

$$I_k(\mathbf{W}) = \sum_{i=1}^K F_i \|\mathbf{v}_{k,i}\|^2 P_i. \quad (4.13)$$

Taking the expectation of the ICR interference power in (4.13) with respect to indicator functions $\{F_i\}_{i=1}^K$ and the ICR-UCR channels $\{\mathbf{v}_{k,i}\}_{i=1}^K$ yields

$$\bar{I}_k(\mathbf{W}) = \sum_{i=1}^K (1 - P_{D,i}) P_i N_I \sigma_{v,i}^2. \quad (4.14)$$

The UCR SINR that can be computed at the UCT is then approximated as

$$\gamma_k = \frac{|\mathbf{h}_k \mathbf{w}_k|^2}{\sum_{j \neq k}^{K_u} |\mathbf{h}_k \mathbf{w}_j|^2 + \bar{I}_k(\mathbf{W}) + \sigma_k^2}, \quad k = 1, \dots, K_u, \quad (4.15)$$

where the aggregate ICR interference $I'_k(\mathbf{W})$ is a function of \mathbf{W} via the spectrum-sensing detection probabilities.

In the remainder of this section, we present several prescient design solutions for \mathbf{W} that provide a tradeoff between complexity and underlay downlink performance. The attribute of ‘‘prescience’’ derives from the fact that the UCT anticipates interference at the PR from SUs due to imperfect spectrum sensing and takes preemptive measures

to avoid the same. Each of these schemes can be implemented either with partial or statistical CSI, therefore to avoid repetition we shall illustrate each scheme for one of these CSI assumptions alone.

4.3.1 Direct UCR Sum Rate Maximization

A suitable performance metric for any UCT precoding scheme is the underlay network sum rate given by

$$R_s = \sum_{k=1}^{K_u} \log_2(1 + \gamma_k). \quad (4.16)$$

A wide variety of choices for \mathbf{W} for conventional non-cognitive and underlay-only downlink channels have been explored in the literature. For example, a naïve transmission scheme that disregards ICR CSI would be to apply a modified regularized channel inversion (RCI) precoder [66], with $\mathbf{W}_{CI} = \frac{1}{\sqrt{\zeta}} \mathbf{H}_u^H (\mathbf{H}_u \mathbf{H}_u^H + \alpha \mathbf{I})^{-1}$ and $\mathbf{H}_u \triangleq \begin{bmatrix} \mathbf{h}_1^T & \dots & \mathbf{h}_{K_u}^T \end{bmatrix}^T$, given a scale factor ζ that is chosen as the smaller of the two scaling factors required to preserve the UCT transmit power and PR interference temperature constraints, and a loading factor $\alpha = K_u/P$. However, the naïve RCI precoder does not account for the potential ICR interference \bar{I}_k , which can severely degrade the underlay sum-rate performance when \bar{I}_k is the dominant term of the denominator in (4.15).

A more efficient usage of the side information available to the UCT is the direct

sum-rate maximization approach that exploits knowledge of the ICR channels:

$$\max_{\mathbf{W}} \sum_{k=1}^{K_u} \log_2 (1 + \gamma_k) \quad (4.17a)$$

$$\text{s.t. } \text{Tr} (\mathbf{N}\mathbf{W}\mathbf{W}^H\mathbf{N}^H) \leq \xi_p \quad (4.17b)$$

$$\text{Tr} (\mathbf{W}\mathbf{W}^H) \leq P. \quad (4.17c)$$

The above problem is novel since the co-channel ICR interference term in the SINR is a function of the transmit signal itself. This is in sharp contrast with conventional single-cell [67], multi-cell [68], and underlay-only [5]-[9] downlink beamforming problems where the co-channel interference is inevitably modeled as independent noise. While signal-dependent interference is a well-studied problem in radar signal processing, see for example [69], in our case this dependence manifests itself in a much more complicated and non-linear fashion involving exponential terms. We are faced with a non-convex objective function with multiple non-linear constraints, and at this point an analytical solution for \mathbf{W} therefore appears to be intractable.

Therefore, we propose an iterative numerical solution for the sum-rate maximization problem based on a gradient projection (GP) algorithm, which will converge to at least a locally-optimal stationary point. To compute the gradient of the UCR sum rate, we define the leakage term

$$L_{k,j} = \sum_{j \neq k} |\mathbf{h}_k \mathbf{w}_j|^2 + \bar{I}_k(\mathbf{W}) + \sigma_k^2, \quad (4.18)$$

and exploit $\nabla_{\mathbf{W}}(R_s) = \left[\nabla_{\mathbf{w}_1}^T(R_s) \quad \dots \quad \nabla_{\mathbf{w}_{K_u}}^T(R_s) \right]^T$ where

$$\begin{aligned} \nabla_{\mathbf{w}_k}(R_s) &= \frac{1}{\ln 2} \left(1 + \frac{|\mathbf{h}_k \mathbf{w}_k|^2}{L_{k,j}} \right)^{-1} \frac{2\mathbf{h}_k^H \mathbf{h}_k \mathbf{w}_k L_{k,j} - |\mathbf{h}_k \mathbf{w}_k|^2 \left(\frac{\partial \bar{I}_k(\mathbf{W})}{\partial \mathbf{w}_k} \right)}{(L_{k,j})^2} \\ &+ \sum_{l \neq k} \frac{1}{\ln 2} \left(1 + \frac{|\mathbf{h}_l \mathbf{w}_l|^2}{L_{l,m}} \right)^{-1} \frac{\left(-2\mathbf{h}_k^H \mathbf{h}_k \mathbf{w}_k - \frac{\partial \bar{I}_l(\mathbf{W})}{\partial \mathbf{w}_k} \right)}{(L_{l,m})^2}, \end{aligned} \quad (4.19)$$

$$\frac{\partial \bar{I}_k(\mathbf{W})}{\partial \mathbf{w}_k} = - \sum_{i=1}^K P_i N_I \sigma_{v,i}^2 \frac{\partial \bar{P}_{D,i}}{\partial \mathbf{w}_k} \quad (4.20)$$

$$= - \frac{2\sigma_{f,i}^2 \mathbf{w}_k}{\sigma_{z,i}^2} e^{\left(-\frac{\lambda_i}{\sigma_{z,i}^2} \right)} \left(\sum_{r=0}^{\infty} \frac{\lambda_i^r}{r!} \frac{(1-r)}{(\sigma_{z,i}^2)^{r+1}} \right) \quad (4.21)$$

and the differential on the RHS of (4.20) is taken with respect to the average detection probability in (4.9) which is computable at the UCT.

At the k^{th} iteration of the GP process, the updated precoding matrix $\mathbf{W}^{(k)}$ in the direction of the gradient computed above is likely to no longer satisfy the UCT transmit power and PR interference temperature constraints. The projection step of the GP algorithm therefore projects the iterate $\mathbf{W}^{(k)}$ back onto the feasible constraint set $\Omega_+(P, \xi_p)$, defined as $\Omega_+(P, \xi_p) \triangleq \{ \mathbf{W} \mid \text{Tr}(\mathbf{W}\mathbf{W}^H) \leq P, \text{Tr}(\mathbf{N}\mathbf{W}\mathbf{W}^H\mathbf{N}^H) \leq \xi_p \}$. Nominally, this is achieved by determining a feasible $\mathbf{W}_0 \in \Omega_+(P, \xi_p)$ that is closest to $\mathbf{W}^{(k)}$ in terms of Frobenius norm, i.e., by minimizing the squared distance $d^2(\mathbf{W}_0, \mathbf{W}^{(k)}) = \text{Tr} \left((\mathbf{W}_0 - \mathbf{W}^{(k)})^H (\mathbf{W}_0 - \mathbf{W}^{(k)}) \right)$ as

$$\min_{\mathbf{W}_0} d^2(\mathbf{W}_0, \mathbf{W}^{(k)}) \quad (4.22a)$$

$$\text{s.t.} \quad \text{Tr}(\mathbf{W}_0 \mathbf{W}_0^H) \leq P \quad (4.22b)$$

$$\text{Tr}(\mathbf{N}\mathbf{W}_0 \mathbf{W}_0^H \mathbf{N}^H) \leq \xi_p. \quad (4.22c)$$

However, instead of numerically solving the above problem, a potentially suboptimal

but much simpler approach is to scale $\mathbf{W}^{(k)}$ such that both (4.22b) and (4.22c) are satisfied. This approach is partly motivated by the observation that the solution to (4.22a) cannot satisfy both constraints with equality for general channel $\mathbf{N} \neq \mathbf{I}$, and one of the constraints is guaranteed to be an inequality.

A summary of the GP approach for underlay prescient sum rate maximization is shown in Algorithm 4.3.1.1, where the step sizes s_k and α_k are chosen using well-defined criteria such as Armijo's rule [70, Sec. 2.3].

Algorithm 4.3.1.1 Prescient Gradient Projection Method

Initialization:

Set iteration index $k = 0$.

Choose initialization $\mathbf{W}^{(0)} = [\mathbf{w}_1^{(0)} \quad \mathbf{w}_2^{(0)} \quad \dots \quad \mathbf{w}_{K_u}^{(0)}]$.

Main Loop:

1. Calculate the gradient $\nabla_{\mathbf{W}^{(k)}} (R_s)$.
 2. Choose an appropriate step size s_k . Let $\mathbf{W}'^{(k)} = \mathbf{W}^{(k)} + s_k \nabla_{\mathbf{W}^{(k)}} (R_s)$.
 3. Let $\bar{\mathbf{W}}^{(k)}$ be the projection of $\mathbf{W}'^{(k)}$ onto $\Omega_+(P, \xi_p)$, where $\Omega_+(P, \xi_p) \triangleq \{\mathbf{W} \mid \text{Tr}(\mathbf{W}\mathbf{W}^H) \leq P, \text{Tr}(\mathbf{N}\mathbf{W}\mathbf{W}^H\mathbf{N}^H) \leq \xi_p\}$.
 4. Choose appropriate step size α_k . Let $\mathbf{W}^{(k+1)} = \mathbf{W}^{(k)} + \alpha_k(\bar{\mathbf{W}}^{(k)} - \mathbf{W}_i^{(k)})$.
 5. $k = k + 1$. If the maximum absolute value of the elements in $\mathbf{W}^{(k)} - \mathbf{W}^{(k-1)} < \epsilon$, then stop; else go to step 1.
-

4.3.2 Algorithm Based on Convex Optimization

While the iterative algorithm described above returns at least a locally optimal prescient beamforming matrix, it is desirable to investigate designs based on simpler optimization procedures. We first define the partial UCR SINR β_k as

$$\beta_k = \frac{|\mathbf{h}_k \mathbf{w}_k|^2}{\sum_{j \neq k}^{K_u} |\mathbf{h}_k \mathbf{w}_j|^2 + \sigma_k^2}, \quad k = 1, \dots, K_u, \quad (4.23)$$

where the ICR interference term in the denominator of (4.15) is omitted.

As a second sub-optimal approach, we can attempt to maximize the minimum partial UCR SINR subject to a set of constraints $\{\eta_i\}_{i=1}^K$ on the total UCT signal power

received by the ICRs, as follows:

$$\max_{\mathbf{W}} \min_k \beta_k \quad (4.24a)$$

$$\text{s.t. } \text{Tr}(\mathbf{W}\mathbf{W}^H) \leq P \quad (4.24b)$$

$$\text{Tr}(\mathbf{W}\mathbf{W}^H \mathbf{F}_i^H \mathbf{F}_i) \geq \eta_i, i = 1, \dots, K \quad (4.24c)$$

$$\text{Tr}(\mathbf{N}\mathbf{W}\mathbf{W}^H \mathbf{N}^H) \leq \xi_p \quad (4.24d)$$

The idea is to maximize the partial underlay SINR accounting for intra-UCR and PR interference, while making a best-effort attempt to limit the expected ICR interference by ensuring a minimum level of signal power leakage to them.

This can be posed as a convex optimization problem as follows. Let $\mathbf{J}_k \triangleq \mathbf{w}_k \mathbf{w}_k^H \forall k$. Applying a change of variable and relaxing the rank-1 constraints on \mathbf{J}_k , we have the reformulation

$$\max_{\{\mathbf{J}_k\}_{k=1}^{K_u}} t \quad (4.25a)$$

$$\text{s.t. } t \left(\sum_{j \neq i} \text{Tr}(\mathbf{h}_i^H \mathbf{h}_i \mathbf{J}_j) + \sigma_i^2 \right) - \text{Tr}(\mathbf{h}_k^H \mathbf{h}_k \mathbf{J}_k) \leq 0 \quad (4.25b)$$

$$\text{Tr} \left(\left(\sum_{k=1}^{K_u} \mathbf{J}_k \right) \mathbf{F}_i^H \mathbf{F}_i \right) \geq \eta_i, i = 1, \dots, K \quad (4.25c)$$

$$\sum_{k=1}^{K_u} \text{Tr}(\mathbf{J}_k) \leq P \quad (4.25d)$$

$$\text{Tr} \left(\mathbf{N} \left(\sum_{k=1}^{K_u} \mathbf{J}_k \right) \mathbf{N}^H \right) \leq \xi_p \quad (4.25e)$$

$$t \geq 0, \mathbf{J}_k \succeq \mathbf{0}, k = 1, \dots, K_u. \quad (4.25f)$$

In this case, however, dropping the rank constraints on $\{\mathbf{J}_i\}_{i=1}^{K_u}$ still does not lead to a semidefinite program (SDP), since the K_u underlay SNR inequality constraints in (4.25b) are non-linear due to the fact that t is a variable. Therefore, a two-stage solution strategy is required where the outer-loop carries out a one-dimensional

bisection search over t , while the inner loop solves (4.25a) for a given value of t , if feasible [71].

4.3.3 Combined Downlink and Multicast Beamforming

We finally present an approach with a semi-analytical expression for \mathbf{W} , motivated by the simple observation that the detection probabilities of energy or GLRT-based detectors increase monotonically with the received SNR at the SUs for a given false alarm rate $P_{FA,i}$. This is clearly seen from (4.7) for energy detection. Consider the following two extreme cases for the choice of \mathbf{W} :

- Disregard ICRs, focus only on UCRs: If the UCT disregards the presence of the ICRs and focuses only on its intended receivers, a suitable choice for \mathbf{w} is the naïve channel-inversion precoder \mathbf{W}_{CI} .
- Disregard downlink, focus only on ICRs: At this extreme, the UCT ignores its downlink and focuses only on improving the signal strength at the ICRs (particularly those that could produce the most interference). This is similar to a MIMO multicast (MC) downlink scenario, where priority is given to certain key users. A reasonable choice for the transmit precoder in this case would maximize the weighted average of the SNRs at the ICRs:

$$\mathbf{W}_{MC} = \arg \max_{\mathbf{W}} \sum_{i=1}^K P_i N_I \sigma_{v,i}^2 \text{Tr}(\mathbf{F}_i \mathbf{W} \mathbf{W}^H \mathbf{F}_i^H), \quad (4.26)$$

where the weight $P_i N_I \sigma_{v,i}^2$ measures the interference impact of the i th ICR at the UCRs. The solution to (4.26) is given by the dominant singular vectors of $\mathbf{F}_S^H \mathbf{\Sigma}_g \mathbf{F}_S^H$ scaled by \sqrt{P} , where $\mathbf{F}_S = \sum_i^K \mathbf{F}_i$ and $\mathbf{\Sigma}_g$ is a diagonal matrix with entries $P_i N_I \sigma_{v,i}^2, i = 1, \dots, K$.

Given that the prescient beamforming objective is to balance these two competing goals, a sensible approach would be to choose \mathbf{W} as some *linear combination* of the solutions:

$$\mathbf{W}_l = \alpha \mathbf{W}_{CI} + (1 - \alpha) \mathbf{W}_{MC} \quad 0 \leq \alpha \leq 1, \quad (4.27)$$

where the optimal value of $\alpha \in [0, 1]$ can be found by a simple line search.

4.4 Multi-antenna Underlay Receivers

In this section we extend the prescient downlink precoding paradigm to the case of multi-antenna UCRs with multiple data streams transmitted to each of them. Let each UCR be equipped with N_s antennas for simplicity, although the proposed prescient precoding schemes hold for heterogeneous receiver array sizes as long as the total number of receive antennas does not exceed N_a . The extension to the case where the UCT serves N_a spatial streams regardless of the total number of receive antennas can be made using the coordinated beamforming approach [47], for example. The received signal at UCR k is now

$$\mathbf{y}_k = \mathbf{H}_k \mathbf{W}_k \mathbf{s}_{u,k} + \sum_{j \neq k}^{K_u} \mathbf{H}_k \mathbf{W}_j \mathbf{s}_{u,j} + \sum_{i=1}^K F_i \mathbf{V}_{k,i} \mathbf{s}_{I,i} + \mathbf{n}_k \quad (4.28)$$

where $\mathbf{H}_k \in \mathbb{C}^{N_s \times N_a}$ is the main channel, $\mathbf{W}_k \in \mathbb{C}^{N_a \times l_k}$ is the beamforming matrix applied to signal $\mathbf{s}_{u,k} \in \mathbb{C}^{l_k \times 1}$ for user k , F_i is the ICR indicator function as before, $\mathbf{s}_{I,i}$ is the i^{th} ICR signal over interfering channel $\mathbf{V}_{k,i} \in \mathbb{C}^{N_s \times N_I}$, and $\mathbf{n}_k \sim \mathcal{CN}(0, \sigma_k^2 \mathbf{I})$ is additive Gaussian noise. The transmit covariance matrix for each UCR is given by $\mathbf{Q}_k = \mathbf{W}_k \mathbf{W}_k^H$. We adopt a prescient block-diagonalization (PBD) strategy on the underlay downlink [47, 72] to completely eliminate intra-UCR interference, as shown

below.

In the first approach, the transmit covariance matrices $\{\mathbf{Q}_k\}_{k=1}^{K_u}$ are computed jointly so as to optimize the underlay system sum rate while subject to constraints on the PR interference and the minimum power leaked to the ICRs. The proposed PBD scheme is succinctly described as

$$\max_{\mathbf{Q}_1, \dots, \mathbf{Q}_{K_u}} \sum_{k=1}^{K_u} \log_2 |\mathbf{I} + \mathbf{H}_k \mathbf{Q}_k \mathbf{H}_k^H| \quad (4.29a)$$

$$\text{s.t. } \mathbf{H}_k \mathbf{Q}_j \mathbf{H}_k^H = \mathbf{0}, \forall k \neq j \quad (4.29b)$$

$$\text{Tr} \left(\mathbf{N} \left(\sum_{k=1}^{K_u} \mathbf{Q}_k \right) \mathbf{N}^H \right) \leq \xi_p \quad (4.29c)$$

$$\text{Tr} \left(\mathbf{F}_i \left(\sum_{k=1}^{K_u} \mathbf{Q}_k \right) \mathbf{F}_i^H \right) \geq \eta_i \quad (4.29d)$$

$$\text{Tr} \left(\sum_{k=1}^{K_u} \mathbf{Q}_k \right) \leq P, \mathbf{Q}_k \succeq \mathbf{0}, k = 1, \dots, K_u. \quad (4.29e)$$

Note that this is not equivalent to direct maximization of the UCR sum rate since the ICR interference is not included in the objective function. However, this decoupling renders the problem convex since the objective function is jointly concave and all constraints are linear in $\{\mathbf{Q}_k\}$, and the leakage constraints η_i can be adjusted appropriately to diminish the probability of missed detections at the ICRs.

As an alternative PBD strategy, it is possible to separately design the precoding and power allocation matrices per user in a two-step process. Let

$$\mathbf{H}_{-k} = \begin{bmatrix} \mathbf{H}_1 & \cdots & \mathbf{H}_{k-1} & \mathbf{H}_{k+1} & \cdots & \mathbf{H}_{K_u} \end{bmatrix}$$

represent the the overall UCR downlink channel excluding the k^{th} user. First, a closed-form solution for the unit-power precoding matrix of user k is obtained from the nullspace of \mathbf{H}_{-k} . For example, from the SVD $\mathbf{H}_{-k} = \mathbf{U}_{-k} \mathbf{\Sigma}_{-k} \begin{bmatrix} \mathbf{V}_{-k,1} & \mathbf{V}_{-k,0} \end{bmatrix}^H$, the last $(N_a - l_k)$ right singular vectors contained in $\mathbf{V}_{-k,0}$ can be used to con-

struct \mathbf{W}_k [47]. However, unlike the conventional BD algorithm, the power allocated over the l_k spatial modes of user k is now no longer obtained via waterfilling. Let $\text{rank}(\mathbf{H}_k \mathbf{W}_k) = r_k$ for user k 's effective channel, and assume $l_k = r_k$. Consider the SVD of user k 's effective channel $\mathbf{H}_k \mathbf{W}_k = \mathbf{U}_k \mathbf{\Sigma}_k \mathbf{V}_k^H$ where $\mathbf{\Sigma}_k = \text{diag}(\epsilon_{k,1}, \dots, \epsilon_{k,r_k})$ is a $r_k \times r_k$ diagonal matrix, and define $\mathbf{\Lambda}_k = \text{diag}(\lambda_{k,1}, \dots, \lambda_{k,r_k})$ as the power allocation matrix. The overall downlink power allocation matrix is therefore $\mathbf{\Lambda}_u = \text{blkdiag}(\mathbf{\Lambda}_1, \dots, \mathbf{\Lambda}_{K_u})$. The PR interference and ICR signal power constraints are accommodated in the power allocation step based on a numerical optimization:

$$\max_{\lambda_{1,1}, \dots, \lambda_{K_u, r_{K_u}}} \sum_{k=1}^{K_u} \sum_{m=1}^{l_k} \log_2(1 + \varepsilon_{k,m}^2 \lambda_{k,m}) \quad (4.30a)$$

$$\text{s.t.} \quad \sum_{c=1}^{N_r} \sum_{k=1}^{K_u} \sum_{m=1}^{l_k} \|\mathbf{n}_c \mathbf{w}_{k,m}\|_2^2 \lambda_{k,m} \geq \xi_p \quad (4.30b)$$

$$\sum_{n=1}^{N_I} \sum_{k=1}^{K_u} \sum_{m=1}^{l_k} \|\mathbf{f}_{i,n} \mathbf{w}_{k,m}\|_2^2 \lambda_{k,m} \geq \eta_i, i = 1, \dots, K, \quad (4.30c)$$

$$\sum_{k=1}^{K_u} \sum_{m=1}^{l_k} \|\mathbf{w}_{k,m}\|_2^2 \lambda_{k,m} \leq P \quad (4.30d)$$

where \mathbf{n}_c is the c^{th} row of \mathbf{N} , $\mathbf{f}_{i,n}$ is the n^{th} row of \mathbf{F}_i , and $\mathbf{w}_{k,m}$ is the m^{th} column of \mathbf{W}_k . The leakage and power constraints (4.30b)-(4.30d) are equivalent to (4.29c)-(4.29e). This is a convex program since the objective function is concave and all constraints are linear in $\{\lambda_{k,i}\}$, and is solvable efficiently using interior-point methods. It must be noted however that a separate design of the underlay precoding and power allocation matrices is potentially suboptimal compared to the joint design of (4.29).

4.5 Simulation Results

In this section, we present the results of several numerical experiments to verify the improvement in primary link performance with prescient beamforming. To avoid repetition, unless specified otherwise, all results in this section are based on the partial

CSI model with instantaneous CSI of the downlink and UCT-ICR links, and only statistical CSI of the ICR-to-UCR links available to the underlay transmitter. Each channel realization for all terminals is drawn from a zero-mean circularly symmetric complex Gaussian distribution, and all results are averaged over 1000 channel realizations. The background AWGN variance at all receivers is assumed to be unity, and the primary antenna array sizes are fixed as $N_p = N_r = 4$. The convex programs are solved numerically using the `cvx` MATLAB toolbox [73]. At the ICRs we set the transmit power to $P_i = 20dB$, false alarm rate target $P_{FA,i} = 10^{-3}\forall i$, and sample size of $M = 4$. The prescient GP algorithm is run 5 times for each set of channel realizations with four random initializations and an initialization based on the naïve RCI precoder to reduce the likelihood of a local maximum; the best-performing precoding solution is chosen as the result.

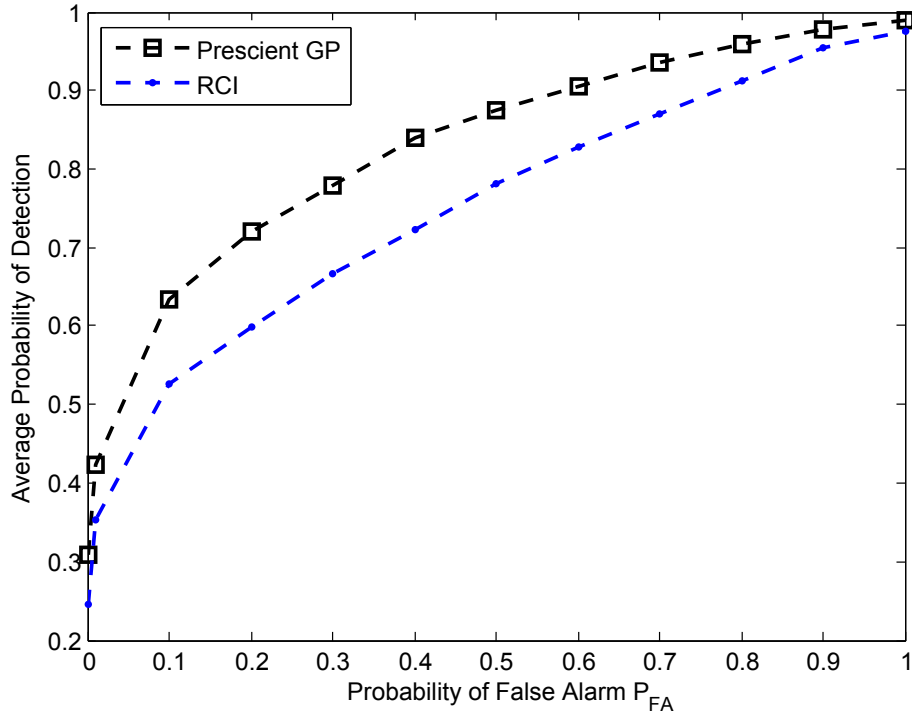


Figure 4.1: ROC curve for energy detection comparing prescient precoding with regularized channel inversion, $N_a = K_u = 3, N_I = K = 2, P = 5dB$.

We first examine the energy detection receiver-operating-characteristic at an arbi-

trary ICR for prescient GP precoding compared to RCI transmission with $K_u = 3$ single-antenna UCRs in Fig. 4.1. The UCT transmit power is fixed at $P = 10dB$ with $N_a = 3$ antennas, and $K = 2$ ICRs are present with $N_I = 2$ antennas each. We observe that prescient precoding provides a significant improvement in energy detection performance for the entire range of P_{FA} , and consequently reduces the likelihood of ICR missed detections.

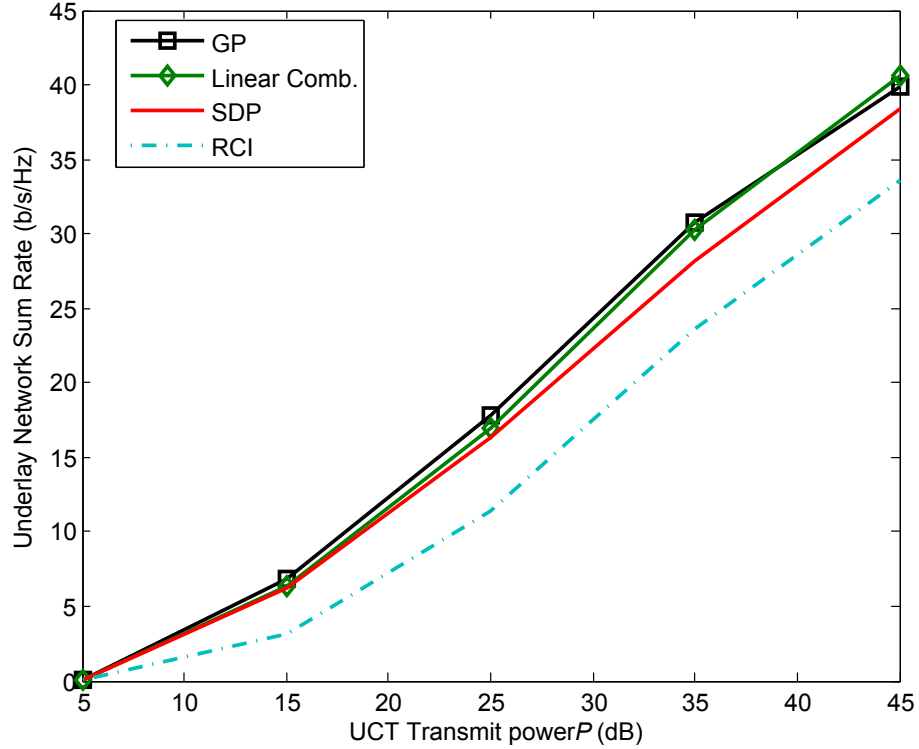


Figure 4.2: Underlay sum rate for prescient algorithms and RCI precoding with $N_a = K_u = K = 3, N_I = 2$.

Sum rate results for the single-antenna UCR downlink versus UCT transmit power with $N_a = K_u = K = 3, N_I = 2$ are shown in Fig. 4.3. The prescient schemes improve markedly upon the naive RCI precoder since each ICR with a missed detection interferes with multiple UCRs. The linear combination scheme is observed to be a very competitive alternative compared to the computationally intensive GP solution. The SDP-based prescient scheme suffers from the difficulty of optimally choosing leakage power thresholds η_i . The proposed prescient GP precoder provides an increase of up

to 7 (bits/s/Hz) in spectral efficiency compared to the RCI scheme, which highlights the significant benefit of preemptively mitigating secondary user interference.

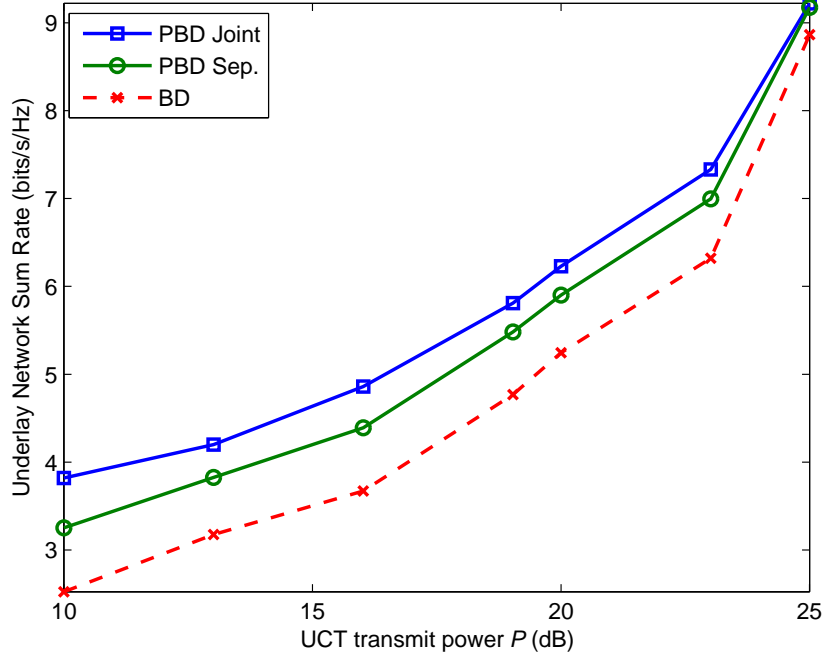


Figure 4.3: Underlay sum rate for prescient and conventional block-diagonalization with $N_a = 8, K_u = 4, K = N_I = N_s = 2$.

We now consider prescient versus conventional block-diagonalization schemes for the multi-antenna UCR downlink with $N_s = 2$. The greatest benefit of the PBD schemes is observed at low to intermediate SNRs, while the sum rate of all three algorithms gradually converge at high SNR. This is because the diversion of transmit power to the ICRs under PBD now has a greater penalty in terms of spatial multiplexing loss to the multi-antenna UCRs.

4.6 Summary

This chapter examined a novel heterogeneous dynamic spectrum access network where the primary users (PUs) coexist with both underlay (UCRs) and interweave cognitive

radios (ICRs); all terminals being potentially equipped with multiple antennas. We investigate the design of MIMO precoding algorithms for the UCRs so as to increase the detection probability at the ICRs, while simultaneously meeting a desired Quality-of-Service target to its own receivers and constraining interference leaked to PUs. The objective of such a proactive approach, referred to as *prescient* precoding, is to minimize the probability of interference from ICRs to the UCR and PU receivers due to imperfect spectrum sensing. We begin with three different downlink prescient precoding algorithms for a plurality of single-antenna UCR and multi-antenna PUs/ICRs. We then present prescient block-diagonalization algorithms for the MIMO underlay downlink where spatial multiplexing is performed for multiple multi-antenna UCR receivers. Numerical experiments demonstrate that prescient precoding by the UCR preemptively mitigates missed detections at the ICRs, and provides a significantly pronounced performance gain in underlay sum rate compared to conventional precoding strategies.

Chapter 5

Robust Beamforming in the MIMO Wiretap Channel

In this chapter, we investigate methods for reducing the likelihood that a message transmitted between two multi-antenna nodes is intercepted by an undetected eavesdropper. In particular, we focus on the judicious transmission of artificial interference to mask the desired signal at the time it is broadcast. Unlike previous work that assumes some prior knowledge of the eavesdropper's channel and focuses on maximizing secrecy capacity, we consider the case where no information regarding the eavesdropper is available, and we use signal-to-interference-plus-noise-ratio (SINR) as our performance metric. Specifically, we focus on the problem of maximizing the amount of power available to broadcast a jamming signal intended to hide the desired signal from a potential eavesdropper, while maintaining a prespecified SINR at the desired receiver. The jamming signal is designed to be orthogonal to the information signal when it reaches the desired receiver, assuming both the receiver and the eavesdropper employ optimal beamformers and possess exact channel state information (CSI). In practice, the assumption of perfect CSI at the transmitter is often difficult

to justify. Therefore, we also study the resulting performance degradation due to the presence of imperfect CSI, and we present robust beamforming schemes that recover a large fraction of the performance in the perfect CSI case. Numerical simulations verify our analytical performance predictions, and illustrate the benefit of the robust beamforming schemes.

A key consideration in the MIMO wiretap problem is what information is available about the eavesdropper. In principle, to compute the secrecy rate, one must know the eavesdropper's channel state information (CSI), or at least its distribution. Such information is unlikely to be available in many scenarios, especially those involving purely passive eavesdroppers. As a result, in this chapter we take a different approach in which the transmitter minimizes the transmit power required to guarantee a certain Quality of Service (QoS) at the desired receiver, and uses the remaining resources to transmit an artificial interference signal that jams any eavesdroppers that are present [29, 74]. The use of artificial interference has been considered by a number of others even for the case where the eavesdropper's CSI is known, although such an approach is known to be suboptimal. For example, assuming that the transmitter has more antennas than the intended recipient so that the corresponding channel has a non-trivial nullspace, one of the approaches taken in [19] is to broadcast artificial interference in this nullspace. Such interference will have no impact on the receiver, but will in general degrade the eavesdropper's channel since its nullspace (if any) will be different. The high-SNR performance of this type of technique was shown to be nearly optimal in [75], and the optimal power distribution between data and interference has been examined in [30]. While [19] studied the case where only the distribution of the eavesdropper's channel was known, [75] focused on the situation where the transmitter has access to the eavesdropper's instantaneous CSI, and developed an algorithm to optimally exploit such information for the case where the intended recipient has a single antenna.

Another key consideration is the accuracy of the available CSI. The impact of imperfect CSI on the secrecy rate of the single-antenna wiretap channel has been investigated in [76,77]. As we illustrate, techniques based on knowledge of the eavesdropper's channel in the multiple antenna case are very sensitive to even slight perturbations in the CSI. If unaccounted for, imprecise CSI for the primary channel also causes interference leakage to the desired recipient when artificial noise is used to jam the eavesdropper, resulting in significant degradation in the desired user's performance. Consequently, we are interested in developing robust schemes that are insensitive to CSI errors. As such, we assume the transmitter uses beamforming rather than spatial multiplexing to communicate with the desired receiver. Beamforming is known to provide higher capacity than spatial multiplexing in many situations where the CSI at the transmitter is in the form of a mean and covariance (similar to the case considered here), even when the receiver has perfect CSI [78]. When the receiver CSI is also subject to errors, recent work has shown that beamforming is optimal even for small channel perturbations [79].

Since we focus on transmission of a single data stream using beamforming, and we let the received signal-to-interference-plus-noise-ratio (SINR) of the data stream at the desired receiver serve as our QoS metric. We design robust algorithms that minimize the transmit power required for the desired receiver to achieve the target QoS in the presence of CSI errors. This in turn maximizes the power available to transmit a jamming signal that disrupts the ability of the eavesdroppers to recover the desired signal. The robust algorithms rely on knowledge of the statistics of the CSI errors, and use a second-order perturbation analysis of the primary channel's singular value decomposition to account for the effects of the perturbation on the desired data stream. As a result, the algorithms provide the following benefits: (1) they minimize the effect of the jamming interference at the desired receiver when CSI errors are present, which means that (2) they require less transmit power to achieve the desired

QoS, which in turn (3) maximizes the power available for degrading the channel of the eavesdroppers. Our simulations demonstrate that the resulting secrecy capacity is significantly improved compared with what would be obtained by a naive scheme that did not take CSI errors into account. We note that a similar approach can be taken to study the impact of imperfect CSI on schemes that make use of relays or neighboring users to jam eavesdroppers [80]-[81].

The chapter is organized as follows. In the next section, the assumed mathematical model is presented, and the capabilities of the transmitter, receiver and eavesdropper are detailed. We also discuss the use of artificial interference, and examine the use of secrecy capacity and SINR as performance metrics. Fixed-QoS beamforming algorithms are described in Section 5.2 for the perfect CSI case, and the effects of imperfect CSI are analytically evaluated in Section 5.3. Robust beamforming methods that compensate for the degradation in SINR are then developed in Section 5.4. The resulting SINR performance for a range of antenna configurations and CSI perturbations is studied via simulation in Section 5.5, and conclusions are drawn in Section 5.6.

5.1 System Model With Perfect CSI

We assume a scenario with two cooperating nodes, Alice and Bob, and a passive eavesdropper Eve, as described in Ch. 2.2. By the term “cooperating,” we mean that Alice and Bob share information with each other about channel state information, desired link quality and coding/decoding strategies. Eve is non-cooperative in the sense that Alice and Bob are unaware of Eve’s operating parameters, including her channel state information, number of antennas, *etc.* Alice is attempting to communicate a message to Bob in the presence of Eve, who is able to overhear Alice’s transmissions.

In this chapter we set the eavesdropper scale factors to unity: $g_1 = g_2 = 1$. Without loss of generality, we also normalize \mathbf{H}_{ba} so that its elements have unit-average gain (excess energy available from \mathbf{H}_{ba} is assumed to be included in P):

$$\begin{aligned}\frac{\|\mathbf{H}_{ba}\|_F^2}{N_b N_a} &= 1 \\ \frac{\|\mathbf{H}_{ea}\|_F^2}{N_e N_a} &= \gamma_{ea}^2.\end{aligned}$$

5.1.1 Artificial Interference

Techniques that employ artificial interference devote a fraction of Alice's power to the transmission of a noise-like waveform, in an attempt to degrade the ability of Eve to intercept the signal destined for Bob. Since we are focusing on a beamforming scenario, Alice's signal is split into two components: one being a scalar data stream denoted as z that contains the message for Bob, and one that contains the jamming signal, which we denote by the $N_a \times 1$ vector \mathbf{z}' . Bob therefore receives

$$\mathbf{y}_b = \mathbf{H}_{ba} \mathbf{t} z + \mathbf{H}_{ba} \mathbf{z}' + \mathbf{n}_b, \tag{5.1}$$

where \mathbf{t} is the $N_a \times 1$ transmit beamformer used for the information signal. Similarly, Eve sees

$$\mathbf{y}_e = \mathbf{H}_{ea} \mathbf{t} z + \mathbf{H}_{ea} \mathbf{z}' + \mathbf{n}_e. \tag{5.2}$$

Assume $\mathbf{t}^H \mathbf{t} = 1$ and let $E\{|z|^2\} = \rho P$, where $0 < \rho \leq 1$ is the fraction of the power devoted to the information signal, so that

$$\begin{aligned} E\{\mathbf{z}'\mathbf{z}'^H\} &= \mathbf{Q}'_z \\ \text{Tr}(\mathbf{Q}'_z) &= (1 - \rho)P. \end{aligned}$$

The QoS experienced by Bob and the probability of Eve intercepting the message intended for Bob will be determined by Alice's choice of the following parameters: the covariance matrix \mathbf{Q}'_z , the transmit beamformer \mathbf{t} , and the power allocation parameter ρ . The impact of these parameters on secrecy capacity and SINR are discussed in Sec. 5.1.2.

It is important to note that the design of a complete transmission strategy for secrecy must also involve the construction of a “secrecy codebook” that is comprised of sub-codebooks for both the secret message and a randomization message intended to confuse the eavesdropper [82]. This is true even for situations where little or no information about the eavesdropper is present; in such cases, one can design the codebook using a set of worst-case assumptions about the eavesdropper. In a sense, the beamforming techniques discussed here represent a version of this idea in the spatial domain, where the secret and random messages are assigned to different spatial precoders (beamformers) with different transmit powers. An optimal design would presumably involve the joint construction of encoding schemes in both space and time, but such an effort is beyond the scope of this chapter.

5.1.2 Performance Metrics

Early work on the wiretap channel [14–16] led to the concept of secrecy capacity, which is defined to be the maximum rate at which Alice and Bob can communicate without allowing the eavesdropper to obtain any information about the transmitted message. In [17], it was shown that for the case where the background noise for Bob and Eve is of equal power (and no artificial interference is generated, $\mathbf{z}' = 0$), the secrecy capacity for the MIMO wiretap channel is given by

$$\begin{aligned} C_{sec} &= \max_{\mathbf{Q}_a \geq 0} I(\mathbf{X}_a; \mathbf{Y}_b) - I(\mathbf{X}_a; \mathbf{Y}_e) \\ &= \max_{\mathbf{Q}_a \geq 0} \log |\mathbf{I} + \mathbf{H}_{ba} \mathbf{Q}_a \mathbf{H}_{ba}^H| - \log |\mathbf{I} + \mathbf{H}_{ea} \mathbf{Q}_a \mathbf{H}_{ea}^H|, \end{aligned} \quad (5.3)$$

where $I(\cdot; \cdot)$ represents mutual information, and where \mathbf{Y}_b , \mathbf{Y}_e and \mathbf{X}_a are the random variable counterparts to the specific realizations \mathbf{y}_b , \mathbf{y}_e and \mathbf{x}_a , respectively. The secrecy-capacity-achieving choice for \mathbf{Q}_a was derived in [17] for the case where the transmitter has knowledge of both \mathbf{H}_{ba} and \mathbf{H}_{ea} , which were assumed to be fixed.

The use of secrecy capacity as the performance metric with artificial interference was studied in [19], where knowledge of only the distribution of \mathbf{H}_{ea} was assumed and the expected value of (5.4) was maximized to obtain the ergodic secrecy capacity. The approach of [19] allowed for the transmission of multiple data streams to Bob, but restricted attention to the case where $N_a > N_b$, and forced Alice to choose a transmit covariance matrix according to the standard water-filling solution without regard to the possibility of an eavesdropper. The expected value of (5.4) was then maximized over ρ , where the expectation was taken over the distribution of eavesdropper channels, and it was assumed that $\sigma_e^2 = 0$. Note that, although this approach obviates the need for knowledge of Eve’s instantaneous channel, optimization over ρ still re-

quires knowledge of the number of antennas Eve possesses and the strength of Eve's channel relative to Bob's (inherent in the assumption that the channel distribution is available).

Without any information about \mathbf{H}_{ea} , the above maximization problem is ill-posed, although (5.4) can still be used to quantify the secrecy rate of a given transmission scheme. In our work, we restrict attention to situations where Alice transmits only a single data stream to Bob since (1) we will focus on cases where the CSI is imperfectly known, and (2) we can develop methods that make beamforming robust to CSI errors. As a result, we choose to work directly with SINR rather than capacity. We will calculate the SINR assuming that both Bob and Eve use linear receive beamforming, recognizing the fact that both could use more sophisticated nonlinear techniques for decoding Alice's signal. The SINR achieved by linear beamforming will nonetheless provide an indication of the relative ability of Bob and Eve to determine the transmitted signal regardless of which decoding approach is used.

Let $\mathbf{w}_b, \mathbf{w}_e$ respectively denote the $N_b \times 1, N_e \times 1$ beamformers employed by Bob and Eve to determine z , so that

$$\hat{z}_b = \mathbf{w}_b^H \mathbf{y}_b = \mathbf{w}_b^H (\mathbf{H}_{ba} \mathbf{t} z + \mathbf{H}_{ba} \mathbf{z}' + \mathbf{n}_b) \quad (5.4)$$

$$\hat{z}_e = \mathbf{w}_e^H \mathbf{y}_e = \mathbf{w}_e^H (\mathbf{H}_{ea} \mathbf{t} z + \mathbf{H}_{ea} \mathbf{z}' + \mathbf{n}_e). \quad (5.5)$$

The resulting SINR available for Bob and Eve to decode z will be given by

$$\text{SINR}_b = \frac{\rho P |\mathbf{w}_b^H \mathbf{H}_{ba} \mathbf{t}|^2}{\mathbf{w}_b^H (\mathbf{H}_{ba} \mathbf{Q}'_z \mathbf{H}_{ba}^H + \sigma_b^2 \mathbf{I}) \mathbf{w}_b} \quad (5.6)$$

$$\text{SINR}_e = \frac{\rho P |\mathbf{w}_e^H \mathbf{H}_{ea} \mathbf{t}|^2}{\mathbf{w}_e^H (\mathbf{H}_{ea} \mathbf{Q}'_z \mathbf{H}_{ea}^H + \sigma_e^2 \mathbf{I}) \mathbf{w}_e}. \quad (5.7)$$

Intuitively, as long as $\text{SINR}_b > \text{SINR}_e$, there will exist modulation and coding schemes that allow Bob but not Eve to reliably decode z .

5.2 Fixed-SINR Beamforming With Perfect CSI

In many applications, it is impractical to assume that any information about the eavesdropper's CSI is available. To increase communications security in such cases, we propose an approach that attempts to achieve the following two performance objectives: (1) maintain a certain guaranteed level of link quality (*e.g.*, SINR) for the intended receiver, and (2) maximize the power available for a jamming signal that makes the unintended reception of the signal more difficult. Obviously, the performance of such a scheme cannot be guaranteed; a fortuitous eavesdropper in the right location could end up with a better quality signal. Here the goal is to reduce the likelihood of such an event. Note that this approach does not imply that a low-power transmission from Alice to Bob will be more secure; reducing the power of the desired signal may allow one to better degrade Eve's channel, but it also reduces the requirements for Eve to decode the signal as well. To illustrate the proposed artificial interference concept, we assume here that the CSI is perfectly known by all parties, Alice, Bob and Eve. The case where Bob and Alice have imperfect or perturbed CSI is examined in Section 5.3.

5.2.1 Unknown Eavesdropper CSI

The proposed approach can be generally outlined as follows, using SINR as the QoS metric:

1. Specify a target SINR for Bob.
2. Allocate the smallest possible fraction ρ of the available transmit power to achieve the desired SINR (if possible) assuming Bob experiences no interference other than the background noise of power σ_b^2 .
3. Allocate all of Alice's remaining power to a jamming signal that is uniformly distributed in space, subject to the constraint that when the interference is received by Bob, it lies in a subspace orthogonal to the desired signal.

Obviously, a given \mathbf{H}_{ba} may not support the desired SINR with a total transmit power P ; in such cases, the link is assumed to be in outage.

Let S denote the target SINR for Bob. To minimize the fraction of the transmit power required to achieve S , Alice should choose \mathbf{t} to be the right singular vector of \mathbf{H}_{ba} with largest singular value, and Bob should choose $\mathbf{w}_b = \mathbf{H}_{ba}\mathbf{t}$ as his receive beamformer. Using this approach, we have

$$\rho = \frac{\sigma_b^2 S}{\mathbf{t}^H \mathbf{H}_{ba}^H \mathbf{H}_{ba} \mathbf{t} P} = \frac{\sigma_b^2 S}{\sigma_1^2 P}, \quad (5.8)$$

where σ_1 is the largest singular value of \mathbf{H}_{ba} . As long as $\rho < 1$, Alice has power available for generating artificial interference.

Since the CSI of the eavesdropper is unknown, the best option available to Alice is to uniformly spread the remaining transmit power along spatial dimensions that will produce no interference for Bob. In particular, we require that

$$\mathbf{H}_{ba}\mathbf{t} \perp \mathbf{H}_{ba}\mathbf{z}' \quad (5.9)$$

for all \mathbf{z}' . With \mathbf{t} chosen as above, it is easy to see that \mathbf{z}' must be chosen as a linear combination of the $N_a - 1$ right singular vectors of \mathbf{H}_{ba} with smallest singular values, which we denote by \mathbf{T}' . Uniformly distributing the remaining transmit power over these vectors yields the following transmit covariance for the artificial interference:

$$\mathbf{Q}'_z = \frac{(1 - \rho)P}{N_a - 1} \mathbf{T}' \mathbf{T}'^H. \quad (5.10)$$

As a consequence, the optimal (in the maximum SINR sense) receive beamformer for Bob is simply the maximal ratio combiner, $\mathbf{w}_b = \mathbf{H}_{ba} \mathbf{t}$, since Bob experiences only white noise. For Eve, the beamformer that maximizes SINR is given by

$$\mathbf{w}_e = (\mathbf{H}_{ea} \mathbf{Q}'_z \mathbf{H}_{ea}^H + \sigma_e^2 \mathbf{I})^{-1} \mathbf{H}_{ea} \mathbf{t}, \quad (5.11)$$

where \mathbf{Q}'_z is given by (5.10). The use of an optimal beamformer here presumes that Eve is aware of $\mathbf{H}_{ea} \mathbf{t}$, as well as the spatial covariance matrix of the transmitted interference. With this choice for \mathbf{w}_e , the SINR experienced by Eve can be expressed as

$$\text{SINR}_e = \rho P \mathbf{t}^H \mathbf{H}_{ea}^H (\mathbf{H}_{ea} \mathbf{Q}'_z \mathbf{H}_{ea}^H + \sigma_e^2 \mathbf{I})^{-1} \mathbf{H}_{ea} \mathbf{t}. \quad (5.12)$$

Since ρ is proportional to σ_b^2 , two observations are immediate for the case of low background noise ($\sigma_b^2, \sigma_e^2 \rightarrow 0$):

1. If $\mathbf{H}_{ea} \mathbf{Q}'_z \mathbf{H}_{ea}^H$ is full rank, which will generically be true if Alice has more antennas than Eve, then

$$\lim_{\sigma_b^2 \rightarrow 0} \text{SINR}_e = 0,$$

regardless of σ_e^2 .

2. If $\mathbf{H}_{ea} \mathbf{Q}'_z \mathbf{H}_{ea}^H$ is rank deficient, for example if Eve has more antennas than Alice, then

$$\lim_{\sigma_e^2 \rightarrow 0} (\mathbf{H}_{ea} \mathbf{Q}'_z \mathbf{H}_{ea}^H + \sigma_e^2 \mathbf{I})^{-1} = \frac{1}{\sigma_e^2} \mathbf{R} \mathbf{R}^H ,$$

where \mathbf{R} is an orthonormal basis for the subspace orthogonal to $\mathbf{H}_{ea} \mathbf{Q}'_z^{1/2}$. In this case, if $\sigma_b^2 \rightarrow 0$ but $\sigma_b/\sigma_e \simeq O(1)$, then in general SINR_e remains non-zero.

5.2.2 Known Eavesdropper CSI

While our focus is on the case where Eve's CSI is unknown, it is useful to compare the performance of the artificial noise scheme with the optimal transmission strategy that takes knowledge of Eve's CSI into account. If perfect CSI of the eavesdropper's channel is available, then it is known that the use of artificial interference is suboptimal. The optimal approach to the problem posed in this chapter is for Alice to transmit with full power using the beamformer that minimizes the eavesdropper's SINR given that the intended receiver's SINR is S :

$$\begin{aligned} \min_{\mathbf{t}} \text{SINR}_e \\ \text{s.t. } \text{SINR}_b = S. \end{aligned} \tag{5.13}$$

It is straightforward to show that the solution to (5.13) is the generalized eigenvector \mathbf{t} corresponding to the largest generalized eigenvalue λ_{max} in the equation

$$\mathbf{H}_{ba}^H \mathbf{H}_{ba} \mathbf{t} = \lambda_{max} \mathbf{H}_{ea}^H \mathbf{H}_{ea} \mathbf{t} , \tag{5.14}$$

where \mathbf{t} is scaled to ensure that $\text{SINR}_b = S$, provided that the transmit power P is large enough. Clearly, if $N_e < N_a$, then \mathbf{t} will lie in the nullspace of \mathbf{H}_{ea} and $\text{SINR}_e = 0$. In such cases, it is preferable from a numerical point of view to calculate \mathbf{t} as the generalized eigenvector with the smallest generalized eigenvalue in this equation:

$$\mathbf{H}_{ea}^H \mathbf{H}_{ea} \mathbf{t} = \lambda_{\min} \mathbf{H}_{ba}^H \mathbf{H}_{ba} \mathbf{t} . \quad (5.15)$$

5.3 Impact Of Imperfect CSI

The assumption of perfect CSI at the transmitter is obviously impossible to achieve in practice. CSI uncertainty at Alice can be due to a number of different phenomena, including estimation error, quantized feedback, or channel mobility. CSI at the receiver is typically much more accurate, due to the receiver's ability to employ rapid channel tracking techniques based on, for example, decision direction. In this section, we examine the effect of inaccurate or mismatched CSI between Alice and Bob using a second-order perturbation analysis of the singular value decomposition (SVD) of \mathbf{H}_{ba} , assuming that the channel error is described as a zero-mean random matrix with a given covariance. In the simulation section, we will demonstrate two important aspects of our analysis. First, we will show that the analysis accurately captures the effect of imperfect CSI even for relatively large channel errors, where the magnitude of the perturbation approaches that of the elements of the channel matrix itself. Second, our analysis will show that the previously proposed beamforming algorithms are very sensitive to imperfect CSI, and result in large degradations in SINR even when the channel perturbation is relatively small. This provides motivation for us to consider beamforming schemes that are robust to CSI errors, as developed in Section 5.4.

For the analysis, we assume that \mathbf{H}_{ba} is of full rank $F = \min(N_b, N_a)$, and we define

the singular value decomposition of the unperturbed channel as follows:

$$\mathbf{H}_{ba} = \mathbf{U}\mathbf{\Sigma}\mathbf{V}^H \quad (5.16)$$

$$= [\mathbf{U}_s \ \mathbf{u}_F] \begin{bmatrix} \mathbf{\Sigma}_s & 0 \\ 0 & \sigma_F \end{bmatrix} [\mathbf{V}_s \ \mathbf{v}_F]^H \quad (5.17)$$

$$= \mathbf{U}_s \mathbf{\Sigma}_s \mathbf{V}_s^H + \sigma_F \mathbf{u}_F \mathbf{v}_F^H, \quad (5.18)$$

where $\mathbf{U}_s, \mathbf{V}_s$ contain respectively the first $F - 1$ left and right singular vectors whose singular values are found in the diagonal matrix $\mathbf{\Sigma}_s$, and $\mathbf{u}_F, \mathbf{v}_F$ are respectively the left and right singular vectors corresponding to the smallest singular value σ_F . The partitioning of the SVD will be useful as we use the perturbation analysis of [83].

For purposes of our analysis, we assume that the CSI error is confined to Alice, who is assumed to have available the following perturbed channel estimate:

$$\tilde{\mathbf{H}}_{ba} = \mathbf{H}_{ba} + \Delta\mathbf{H}_{ba} \quad (5.19)$$

where $\Delta\mathbf{H}_{ba}$ is modeled as a zero-mean circularly-symmetric random matrix with covariance matrix given by

$$\mathbf{C}_{\Delta\mathbf{H}_{ba}} = E \left\{ (\text{vec}(\Delta\mathbf{H}_{ba})) (\text{vec}(\Delta\mathbf{H}_{ba}))^H \right\},$$

and $\text{vec}(\cdot)$ denotes the column stacking operator. The singular value decomposition of the perturbed channel can be written as

$$\tilde{\mathbf{H}}_{ba} = \tilde{\mathbf{U}}_s \tilde{\mathbf{\Sigma}}_s \tilde{\mathbf{V}}_s^H + \tilde{\sigma}_F \tilde{\mathbf{u}}_F \tilde{\mathbf{v}}_F^H, \quad (5.20)$$

where

$$\begin{aligned}
\tilde{\mathbf{U}}_s &= \mathbf{U}_s + \Delta\mathbf{U}_s & \tilde{\mathbf{u}}_F &= \mathbf{u}_F + \Delta\mathbf{u}_F \\
\tilde{\Sigma}_s &= \Sigma_s + \Delta\Sigma_s & \tilde{\sigma}_F &= \sigma_F + \Delta\sigma_F \\
\tilde{\mathbf{V}}_s &= \mathbf{V}_s + \Delta\mathbf{V}_s & \tilde{\mathbf{v}}_F &= \mathbf{v}_F + \Delta\mathbf{v}_F,
\end{aligned} \tag{5.21}$$

and quantities preceded by Δ are perturbations to those in (5.18). The analysis of [83] assumes either a fat or square matrix ($N_a \geq N_b$ in our case), so we perform our derivation for this case. A similar analysis holds when $N_b > N_a$, except that we would work with the transpose of the channel matrix, and we would focus on perturbations to the left rather than right singular vectors.

It will be convenient for our analysis to also define $\Delta\sigma_1$ and $\Delta\mathbf{v}_1$ as the perturbation to the largest singular value and the corresponding right singular vector \mathbf{v}_1 , respectively. Furthermore, we define $\Delta\mathbf{T}'$ as the perturbation to the $N_a - 1$ right singular vectors of \mathbf{H}_{ba} with smallest singular values. With $\Delta\sigma_1$ defined, the perturbed power allocation factor can be expressed as:

$$\tilde{\rho} = \frac{\sigma_b^2 S}{\tilde{\sigma}_1^2 P} = \rho \frac{1}{\left(1 + \frac{2\sigma_1 \Delta\sigma_1 + \Delta\sigma_1^2}{\sigma_1^2}\right)} \tag{5.22}$$

$$\approx \rho \left(1 - \frac{2\Delta\sigma_1}{\sigma_1} - \frac{\Delta\sigma_1^2}{\sigma_1^2}\right), \tag{5.23}$$

If Alice has an inaccurate estimate of the CSI and both Alice and Bob are unaware of the CSI mismatch, then the SINR for Bob is expected to be significantly degraded. There are three factors that contribute to this degradation:

1. Alice will incorrectly allocate power for data and artificial noise based on $\tilde{\rho} = (\sigma_b^2 S)/(\tilde{\sigma}_1^2 P)$.
2. Alice continues to use (5.10) to generate the interference signal, although with imperfect CSI the artificial noise covariance matrix becomes

$$\tilde{\mathbf{Q}}'_z = \frac{(1 - \tilde{\rho})P}{N_a - 1} (\mathbf{T}' + \Delta\mathbf{T}')(\mathbf{T}' + \Delta\mathbf{T}')^H . \quad (5.24)$$

3. Alice will use $\mathbf{t} = \tilde{\mathbf{v}}_1 = \mathbf{v}_1 + \Delta\mathbf{v}_1$ as the transmit beamformer, whereas Bob continues to use $\mathbf{w}_b = \mathbf{H}_{ba}\mathbf{v}_1$ as his receive beamformer. Bob's beamformer will no longer cancel the artificial interference, causing a significant loss of SINR and the bulk of the resulting performance degradation.

This case of mismatched beamformers and erroneous power allocation due to imperfect CSI is referred to as the “*naive*” scheme.

In the presence of CSI errors, Bob's average SINR can be approximated as the ratio of the expected value of the received signal power to the expected value of the received noise and interference power. This approximation is valid to the order of the perturbation analysis assumed in [83], and its accuracy will be demonstrated later in our simulation results. Using this approximation, the average SINR achieved by Bob under the naive scheme can be expressed as

$$\text{SINR}_b^{\text{naive}} = \frac{PE \left\{ \tilde{\rho} |\mathbf{v}_1^H \mathbf{H}_{ba}^H \mathbf{H}_{ba} (\mathbf{v}_1 + \Delta\mathbf{v}_1)|^2 \right\}}{E \left\{ \mathbf{v}_1^H \mathbf{H}_{ba}^H \left(\mathbf{H}_{ba} \tilde{\mathbf{Q}}'_z \mathbf{H}_{ba}^H + \sigma_b^2 \mathbf{I} \right) \mathbf{H}_{ba} \mathbf{v}_1 \right\}}, \quad (5.25)$$

where the remaining expectation is with respect to $\Delta\mathbf{H}_{ba}$. Based on the distribution

of $\Delta \mathbf{H}_{ba}$, we can compute

$$\begin{aligned}
E \left\{ \mathbf{v}_1^H \mathbf{H}_{ba}^H \mathbf{H}_{ba} \tilde{\mathbf{Q}}'_z \mathbf{H}_{ba}^H \mathbf{H}_{ba} \mathbf{v}_1 \right\} &= \sigma_1^4 \tilde{\beta} E \left\{ \mathbf{v}_1^H \tilde{\mathbf{T}}' \left(\tilde{\mathbf{T}}' \right)^H \mathbf{v}_1 \right\} \\
&= \sigma_1^4 \tilde{\beta} E \left\{ \mathbf{v}_1^H \left(\mathbf{I} - \tilde{\mathbf{v}}_1 \tilde{\mathbf{v}}_1^H \right) \mathbf{v}_1 \right\} \\
&\approx -\sigma_1^4 \beta E \left\{ \mathbf{v}_1^H \Delta \mathbf{v}_1 + \Delta \mathbf{v}_1^H \mathbf{v}_1 \right\},
\end{aligned} \tag{5.26}$$

where $\tilde{\beta} = (1 - \tilde{\rho})P/(N_a - 1)$ and $\beta = (1 - \rho)P/(N_a - 1)$.

Let $\Upsilon = \frac{2\Delta\sigma_1}{\sigma_1} + \frac{\Delta\sigma_1^2}{\sigma_1^2}$. Using the familiar relations $\mathbf{H}_{ba}\mathbf{v}_1 = \sigma_1\mathbf{u}_1$ and $\mathbf{H}_{ba}^H\mathbf{u}_1 = \sigma_1\mathbf{v}_1$, and after dropping higher-order perturbation terms from the numerator and denominator, we obtain the following expression for $\text{SINR}_b^{\text{naive}}$:

$$\frac{\sigma_1^2 \rho P \left[1 + E \left\{ \mathbf{v}_1^H \Delta \mathbf{v}_1 \right\} + E \left\{ \Delta \mathbf{v}_1^H \mathbf{v}_1 \right\} - E \left\{ \Upsilon \right\} \right]}{-\sigma_1^2 \beta \left[E \left\{ \mathbf{v}_1^H \Delta \mathbf{v}_1 \right\} + E \left\{ \Delta \mathbf{v}_1^H \mathbf{v}_1 \right\} \right] + \sigma_b^2}. \tag{5.27}$$

It is apparent that when perfect CSI is available at Alice (i.e., $\Delta \mathbf{v}_1 \rightarrow 0$ and $\Delta \sigma_1 \rightarrow 0$), (5.27) reduces to (5.8).

Next, we obtain the expected values of the perturbation terms $\mathbf{v}_1^H \Delta \mathbf{v}_1$, $\Delta \sigma_1$, and $\Delta \sigma_1^2$ in (5.27) as follows. Define $\mathbf{D} \triangleq (\boldsymbol{\Sigma}_s \boldsymbol{\Sigma}_s^H - \sigma_F^2 \mathbf{I})^{-1}$, as well as the following matrices:

$$\mathbf{E}_{ss} \triangleq \mathbf{U}_s^H \Delta \mathbf{H}_{ba} \mathbf{V}_s \tag{5.28}$$

$$\mathbf{E}_{sn} \triangleq \mathbf{U}_s^H \Delta \mathbf{H}_{ba} \mathbf{v}_F \tag{5.29}$$

$$\mathbf{E}_{ns} \triangleq \mathbf{u}_F^H \Delta \mathbf{H}_{ba} \mathbf{V}_s \tag{5.30}$$

$$\mathbf{E}_{nn} \triangleq \mathbf{u}_F^H \Delta \mathbf{H}_{ba} \mathbf{v}_F. \tag{5.31}$$

Using the results of [83], the perturbation in \mathbf{V}_s can be approximated up to second

order in $\Delta\mathbf{H}_{ba}$ as

$$\Delta\mathbf{V}_s = \mathbf{v}_F\bar{\mathbf{P}}_1 + \mathbf{V}_s\bar{\mathbf{P}}_2 \quad (5.32)$$

where $\bar{\mathbf{P}}_1 \approx -\bar{\mathbf{Q}}_1^H$ and $\bar{\mathbf{P}}_2 \approx -\frac{1}{2}\bar{\mathbf{F}}\bar{\mathbf{F}}^H$, and

$$\bar{\mathbf{F}} = -\sigma_F\mathbf{D}\mathbf{E}_{ns}^H - \sigma_F^2\Sigma_s^{-1}\mathbf{D}\mathbf{E}_{sn} - \Sigma_s^{-1}\mathbf{E}_{sn}, \quad (5.33)$$

$$\begin{aligned} \bar{\mathbf{Q}}_1 \approx & \mathbf{D}(\mathbf{E}_{ss}\mathbf{D}\Sigma_s\mathbf{E}_{ns}^H - \sigma_F\mathbf{D}\mathbf{E}_{ns}^H\mathbf{E}_{nn}^H)\Sigma_n \\ & - \mathbf{D}\mathbf{E}_{ns}^H\mathbf{E}_{nn} + \sigma_F^2\mathbf{D}(\mathbf{E}_{ss}^H\mathbf{D}\mathbf{E}_{sn} - \mathbf{D}\mathbf{E}_{ns}^H\mathbf{E}_{nn}) \\ & + \sigma_F^2\Sigma_s^{-1}\mathbf{D}(\mathbf{E}_{ss}\Sigma_s^{-1}\mathbf{E}_{sn} - \mathbf{D}\mathbf{E}_{sn}\Sigma_n^H\mathbf{E}_{nn} + \dots \\ & \dots + \sigma_F^2\mathbf{E}_{ss}\Sigma_s^{-1}\mathbf{D}\mathbf{E}_{sn}) \\ & + \Sigma_s^{-1}\mathbf{E}_{ss}\Sigma_s^{-1}(\mathbf{E}_{sn} + \sigma_F^2\mathbf{D}\mathbf{E}_{sn}) - \sigma_F\Sigma_s^{-1}\mathbf{D}\mathbf{E}_{sn}\mathbf{E}_{nn} \\ & + \sigma_F\Sigma_s^{-1}\mathbf{D}(\sigma_F^2\mathbf{E}_{ss}\mathbf{D}\mathbf{E}_{ns}^H - \sigma_F^2\mathbf{D}\mathbf{E}_{sn}\mathbf{E}_{nn}^H - \mathbf{E}_{sn}\mathbf{E}_{nn}^H) \\ & + \sigma_F\Sigma_s^{-1}\mathbf{E}_{ss}\mathbf{D}\mathbf{E}_{ns}^H + \bar{\mathbf{F}}. \end{aligned} \quad (5.34)$$

Exploiting the circular symmetry of $\Delta\mathbf{H}_{ba}$ in (5.35) leads to

$$\begin{aligned} E\{\bar{\mathbf{P}}_1\} = & (1 + \sigma_F^2)E\{\mathbf{E}_{nn}^H\mathbf{E}_{ns}\}\mathbf{D}^H \\ & + \sigma_F^2E\{\mathbf{E}_{sn}^H\mathbf{D}^H\mathbf{E}_{ss}\}\mathbf{D}^H \\ & - \sigma_F E\{\mathbf{E}_{ns}\mathbf{D}^H\mathbf{E}_{ss}^H\}(\mathbf{I} + \sigma_F^2\mathbf{D}^H)\Sigma_s^{-1} \\ & + \sigma_F E\{\mathbf{E}_{nn}\mathbf{E}_{sn}^H\}\mathbf{D}^H(\sigma_F^2\mathbf{D}^H + \mathbf{I})\Sigma_s^{-1}. \end{aligned} \quad (5.35)$$

Next, recall that $\mathbf{V}_s \perp \mathbf{v}_F$ and $\mathbf{V}_s^H \mathbf{V}_s = \mathbf{I}$, so that $\mathbf{V}_s^H \Delta \mathbf{V}_s = \bar{\mathbf{P}}_2$. After some manipulations based on the circular symmetry of $\Delta \mathbf{H}_{ba}$, we obtain

$$\begin{aligned}
E [\mathbf{V}_s^H \Delta \mathbf{V}_s] &= -\frac{\sigma_F^2}{2} \boldsymbol{\Sigma}_s^{-1} ((\sigma_F^2 + 1) \mathbf{D} E \{ \mathbf{E}_{sn} \mathbf{E}_{sn}^H \} \mathbf{D}^H + \dots \\
&\quad \dots + E \{ \mathbf{E}_{sn} \mathbf{E}_{sn}^H \} \mathbf{D}^H + E \{ \mathbf{E}_{sn} \mathbf{E}_{sn}^H \}) \boldsymbol{\Sigma}_s^{-1} \\
&\quad - \frac{\sigma_F^2}{2} \mathbf{D} E \{ \mathbf{E}_{ns}^H \mathbf{E}_{ns} \} \mathbf{D}^H.
\end{aligned} \tag{5.36}$$

The perturbation to the singular values $\boldsymbol{\Sigma}_s$ can be approximated as

$$\begin{aligned}
E \{ \Delta \boldsymbol{\Sigma}_s \} &\approx (\sigma_F^2 E \{ \mathbf{E}_{sn} \mathbf{E}_{sn}^H \} \mathbf{D}^H + E \{ \mathbf{E}_{sn} \mathbf{E}_{sn}^H \}) \boldsymbol{\Sigma}_s^{-1} \\
&\quad + E \{ \boldsymbol{\Sigma}_s \bar{\mathbf{P}}_2 - \mathbf{P}_2 \boldsymbol{\Sigma}_s \},
\end{aligned} \tag{5.37}$$

where $\mathbf{P}_2 \approx -\frac{1}{2} \mathbf{F} \mathbf{F}^H$ is a component of the perturbation in $\Delta \mathbf{U}_s$, and

$$\mathbf{F} = -\mathbf{D} (\boldsymbol{\Sigma}_s \mathbf{E}_{ns}^H + \sigma_F \mathbf{E}_{sn}). \tag{5.38}$$

From the expression for \mathbf{P}_2 :

$$\begin{aligned}
E \{ \mathbf{P}_2 \boldsymbol{\Sigma}_s \} &= \mathbf{D} (\boldsymbol{\Sigma}_s E \{ \mathbf{E}_{ns}^H \mathbf{E}_{ns} \} \boldsymbol{\Sigma}_s \\
&\quad + \sigma_F^2 E \{ \mathbf{E}_{sn} \mathbf{E}_{sn}^H \}) \mathbf{D}^H \boldsymbol{\Sigma}_s.
\end{aligned} \tag{5.39}$$

It remains to express (5.35) and (5.37) in terms of the second-order statistics of $\Delta \mathbf{H}_{ba}$. Let $\mathbf{C}_{ij} = E \{ (\Delta \mathbf{H}_{ba})_{:,i} (\Delta \mathbf{H}_{ba})_{:,j}^H \}$ represent the covariance of the i th and j th

columns of $\Delta\mathbf{H}_{ba}$. It is straightforward to show that

$$\begin{aligned} E \{ \mathbf{E}_{sn} \mathbf{E}_{sn}^H \} &= \mathbf{U}_s^H E [\Delta\mathbf{H}_{ba} \mathbf{v}_F \mathbf{v}_F^H \Delta\mathbf{H}_{ba}^H] \mathbf{U}_s \\ &= \mathbf{U}_s^H \mathbf{G} \mathbf{U}_s \end{aligned} \quad (5.40)$$

$$E \{ \mathbf{E}_{ns}^H \mathbf{E}_{ns} \} = \mathbf{V}_s^H \mathbf{G}'' \mathbf{V}_s \quad (5.41)$$

$$E \{ \mathbf{E}_{nn} \mathbf{E}_{sn}^H \} = \mathbf{u}_F^H \mathbf{G} \mathbf{U}_s \quad (5.42)$$

$$E \{ \mathbf{E}_{nn}^H \mathbf{E}_{ns} \} = \mathbf{v}_F^H \mathbf{G}'' \mathbf{V}_s \quad (5.43)$$

$$E \{ \mathbf{E}_{ns} \mathbf{D}^H \mathbf{E}_{ss}^H \} = \mathbf{u}_F^H \mathbf{G}' \mathbf{U}_s \quad (5.44)$$

$$E \{ \mathbf{E}_{sn}^H \mathbf{D}^H \mathbf{E}_{ss} \} = \mathbf{v}_F^H \mathbf{G}'' \mathbf{V}_s, \quad (5.45)$$

where the (i, j) entry of \mathbf{G} is $[\mathbf{G}]_{i,j} = \mathbf{v}_F^H \mathbf{C}_{ij} \mathbf{v}_F$, $[\mathbf{G}']_{i,j} = \text{Tr} (\mathbf{V}_s \mathbf{D}^H \mathbf{V}_s^H \mathbf{C}_{ij})$, and $[\mathbf{G}'']_{i,j} = \text{Tr} (\mathbf{U}_s \mathbf{D}^H \mathbf{U}_s^H \mathbf{C}_{ij})$.

For convenience, let $\mathbf{C}_{ij} = E \{ (\Delta\mathbf{H}_{ba})_{:,i} (\Delta\mathbf{H}_{ba})_{:,j}^H \}$ represent the covariance of columns i and j from $\Delta\mathbf{H}_{ba}$, i.e., \mathbf{C}_{ij} is the (i, j) block of $\mathbf{C}_{\Delta\mathbf{H}_{ba}}$. We also define the matrix \mathbf{G} whose (i, j) entry is given by $[\mathbf{G}]_{i,j} = \mathbf{v}_F^H \mathbf{C}_{ij} \mathbf{v}_F$. The expressions needed to evaluate

Bob's SINR are given in (5.46)-(5.52):

$$E \{ [\mathbf{V}_s^H \Delta \mathbf{V}_s] \} = -\frac{\sigma_F^2}{2} \mathbf{D} \mathbf{V}_s^H \mathbf{G} \mathbf{V}_s \mathbf{D} \quad (5.46)$$

$$- \frac{\sigma_F^2}{2} \Sigma_s^{-1} \mathbf{D} \left([(\sigma_F^2 + 1) \mathbf{I} + \mathbf{D}^{-1}] \times \right. \\ \left. \dots \times \mathbf{U}_s^H \mathbf{G} \mathbf{U}_s \mathbf{D} + \mathbf{D}^{-1} \mathbf{U}_s^H \mathbf{G} \mathbf{U}_s \right) \Sigma_s^{-1}$$

$$E \{ \Delta \Sigma_s \} \approx (\sigma_F^2 \mathbf{U}_s^H \mathbf{G} \mathbf{U}_s \mathbf{D} + \mathbf{U}_s^H \mathbf{G} \mathbf{U}_s) \Sigma_s^{-1} \quad (5.47)$$

$$- \mathbf{D} (\Sigma_s \mathbf{V}_s^H \mathbf{G} \mathbf{V}_s \Sigma_s + \dots$$

$$\dots + \sigma_F^2 \mathbf{U}_s^H \mathbf{G} \mathbf{U}_s) \mathbf{D} \Sigma_s$$

$$+ \Sigma_s E [\mathbf{V}_s^H \Delta \mathbf{V}_s]$$

$$E \{ \mathbf{v}_1^H \Delta \mathbf{v}_1 \} = E \{ [\mathbf{V}_s^H \Delta \mathbf{V}_s] \}_{1,1} \quad (5.48)$$

$$\mathbf{D} = (\Sigma_s \Sigma_s^H - \sigma_F^2 \mathbf{I})^{-1} \quad (5.49)$$

$$E \{ \Delta \sigma_1 \} = E \{ [\Delta \Sigma_s]_{1,1} \} \quad (5.50)$$

$$E \{ \Delta \sigma_1^2 \} = [\mathbf{U}_s^H \mathbf{K} \mathbf{U}_s]_{1,1} \quad (5.51)$$

$$[\mathbf{K}]_{i,j} = \text{Tr} (\mathbf{V}_s^H \mathbf{C}_{ij} \mathbf{V}_s) . \quad (5.52)$$

Therefore, the naive SINR at Bob expressed in terms of the second-order statistics of $\Delta \mathbf{H}_{ba}$ is obtained by substituting the expected values in (5.48), (5.50), and (5.48) into (5.27). For the special case of i.i.d CSI errors where $\mathbf{C}_{\Delta H_{ba}} = \sigma_H^2 \mathbf{I}$, the expressions above simplify considerably since in this case $\mathbf{G} = \sigma_H^2 \mathbf{I}$.

Note that Alice's use of imperfect transmit beamformers does not implicitly impact the SINR available to Eve. As far as Eve is concerned, use of $\mathbf{v}_1 + \Delta \mathbf{v}_1$ rather than \mathbf{v}_1 as the transmit beamformer for the desired signal, and $\mathbf{T}' + \Delta \mathbf{T}'$ rather than \mathbf{T}' as the interference precoder, has on average no effect on her performance since we assume that \mathbf{H}_{ba} and \mathbf{H}_{ea} are unrelated.

5.4 Robust Beamforming Approaches

While the instantaneous CSI perturbation cannot be determined, if Bob has information about the statistics of the perturbation, then he may take remedial measures to overcome at least some of the significant SINR degradation that occurs with the naive scheme. In particular, if Bob has knowledge of $\mathbf{C}_{\Delta\mathbf{H}_{ba}}$, then the spatial covariance of the artificial interference that impacts Bob can be calculated, and incorporated into the maximum SINR beamformer. In this section, we examine two such approaches for the case where Alice does not possess CSI for Eve. The first case corresponds to a frequency-division duplex (FDD) scenario where Bob estimates the CSI, quantizes it, and sends this information to Alice via a feedback channel. In this case, Bob is aware of the CSI used by Alice for her transmission parameters. In the second case, which corresponds to a time-division duplex (TDD) scenario, Alice and Bob obtain individual channel estimates on their own, and neither is aware of the other's CSI. In both cases, we assume that (1) Alice's transmission allows Bob to obtain an exact estimate of the current CSI \mathbf{H}_{ba} (the estimation error will be negligible compared with errors due to quantization and channel time variations), and that (2) Bob informs Alice of the power fraction ρ needed to obtain his desired SINR.

5.4.1 Robust Beamforming - FDD Case

When Alice has imperfect CSI for Bob and applies a mismatched transmit beamformer, the interference-plus-noise portion of Bob's received signal is, from (5.1),

$$\tilde{\mathbf{n}}_b = \mathbf{H}_{ba}\mathbf{z}' + \mathbf{n}_b ,$$

with covariance

$$E \{ \tilde{\mathbf{n}}_b \tilde{\mathbf{n}}_b^H \} = \mathbf{Q}_{int} . \quad (5.53)$$

In the FDD case, Bob is aware of the value of $\tilde{\mathbf{H}}_{ba}$ since this was information he computed and fed back to Alice. He can thus determine the exact value of \mathbf{Q}_{int} as follows:

$$\mathbf{Q}_{int} = \tilde{\mathbf{H}}_{ba} \tilde{\mathbf{Q}}'_z \tilde{\mathbf{H}}_{ba}^H + \sigma_b^2 \mathbf{I} , \quad (5.54)$$

as well as the exact beamformer $\tilde{\mathbf{t}} = \tilde{\mathbf{v}}_1$ that Alice uses for the information-bearing signal. He is then in turn able to calculate the optimal receive beamformer that maximizes SINR:

$$\mathbf{w}_{opt} = \mathbf{Q}_{int}^{-1} \mathbf{H}_{ba} \tilde{\mathbf{t}} . \quad (5.55)$$

The resulting SINR at Bob is given by

$$S = \rho P \tilde{\mathbf{t}}^H \mathbf{H}_{ba}^H \mathbf{Q}_{int}^{-1} \mathbf{H}_{ba} \tilde{\mathbf{t}} . \quad (5.56)$$

5.4.2 Robust Beamforming - TDD Case

In the TDD case, Bob is unaware of the exact values of $\tilde{\mathbf{Q}}'_z$ and $\tilde{\mathbf{v}}_1$ that Alice uses. However, assuming Bob knows the statistics of the CSI error, in particular $\mathbf{C}_{\Delta \mathbf{H}_{ba}}$, he can compute expected values for these quantities and use these as estimates to determine his receive beamformer. Using the second-order perturbation analysis of the previous section, the expected interference-plus-noise covariance matrix $\hat{\mathbf{Q}}_{int}$ can

be computed as

$$\begin{aligned}
\hat{\mathbf{Q}}_{int} &= E \left\{ \mathbf{H}_{ba} \mathbf{z}' \mathbf{z}'^H \mathbf{H}_{ba}^H + \mathbf{n}_b \mathbf{n}_b^H \right\} \\
&= \tilde{\beta} \left(\mathbf{H}_{ba} \mathbf{H}_{ba}^H - \sigma_1^2 \mathbf{u}_1 \mathbf{u}_1^H \right) - \beta \sigma_1^2 \mathbf{u}_1 E \{ \Delta \mathbf{v}_1 \} \mathbf{H}_{ba}^H \\
&\quad - \beta \sigma_1 \mathbf{H}_{ba} E \{ \Delta \mathbf{v}_1 \} \mathbf{u}_1^H + \sigma_b^2 \mathbf{I}.
\end{aligned} \tag{5.57}$$

Furthermore, Alice's transmit beamformer can be estimated as

$$\hat{\mathbf{t}} = E(\tilde{\mathbf{v}}_1) = \mathbf{v}_1 + E(\Delta \mathbf{v}_1). \tag{5.58}$$

Both of the above quantities require knowledge of $\Delta \mathbf{v}_1$. In the Appendix, we show that

$$E \{ \Delta \mathbf{v}_1 \} = E \left\{ [\Delta \mathbf{V}_s]_{:,1} \right\}, \tag{5.59}$$

where

$$E \{ \Delta \mathbf{V}_s \} = \mathbf{v}_F E \{ \bar{\mathbf{P}}_1 \} + \mathbf{V}_s E \{ \bar{\mathbf{P}}_2 \} \tag{5.60}$$

$$\begin{aligned}
E \{ \bar{\mathbf{P}}_1 \} &= (1 + \sigma_F^2) \mathbf{v}_F^H \mathbf{G} \mathbf{V}_s \mathbf{D}^H + \sigma_F^2 \mathbf{v}_F^H \mathbf{G}'' \mathbf{V}_s \mathbf{D}^H \\
&\quad - \sigma_F \mathbf{u}_F^H \mathbf{G}' \mathbf{U}_s (\mathbf{I} + \sigma_F^2 \mathbf{D}^H) \Sigma_s^{-1} \\
&\quad + \sigma_F \mathbf{u}_F^H \mathbf{G} \mathbf{U}_s \mathbf{D}^H (\sigma_F^2 \mathbf{D}^H + \mathbf{I}) \Sigma_s^{-1}
\end{aligned} \tag{5.61}$$

$$[\mathbf{G}]_{i,j} = \mathbf{v}_F^H \mathbf{C}_{ij} \mathbf{v}_F \tag{5.62}$$

$$[\mathbf{G}']_{i,j} = \text{Tr}(\mathbf{V}_s \mathbf{D}^H \mathbf{V}_s^H \mathbf{C}_{ij}) \tag{5.63}$$

$$[\mathbf{G}'']_{i,j} = \text{Tr}(\mathbf{U}_s \mathbf{D}^H \mathbf{U}_s^H \mathbf{C}_{ij}), \tag{5.64}$$

and where the expected value of $\bar{\mathbf{P}}_2 = \mathbf{V}_s^H \Delta \mathbf{V}_s$ is given in (5.46). The interference-plus-noise covariance matrix is obtained by substituting (5.59) into (5.58). Bob's receive beamformer is calculated as

$$\hat{\mathbf{w}}_{opt} = \hat{\mathbf{Q}}_{int}^{-1} \mathbf{H}_{ba} \hat{\mathbf{t}}. \quad (5.65)$$

Since $\hat{\mathbf{Q}}_{int} \neq \mathbf{Q}_{int}$, the resulting SINR for Bob must be determined as follows:

$$\text{SINR}_b = \frac{\rho P \left| \hat{\mathbf{t}}^H \mathbf{H}_{ba}^H \hat{\mathbf{Q}}_{int}^{-1} \mathbf{H}_{ba} \hat{\mathbf{t}} \right|^2}{\hat{\mathbf{t}}^H \mathbf{H}_{ba}^H \hat{\mathbf{Q}}_{int}^{-1} \mathbf{Q}_{int} \hat{\mathbf{Q}}_{int}^{-1} \mathbf{H}_{ba} \hat{\mathbf{t}}}. \quad (5.66)$$

5.5 Simulation Results

We present some examples that show the SINR and secrecy capacity performance of Bob and Eve for various array sizes, target performance levels, and array perturbations. In all simulations, the channel matrices were assumed to be composed of independent, zero-mean Gaussian random variables with unit variance ($\gamma_{ea}^2 = 1$). The channel perturbation covariance matrix is assumed to be $\mathbf{C}_{\Delta H_{ba}} = \sigma_H^2 \mathbf{I}$ which corresponds to the case where the CSI errors are independent and identically distributed. In the simulation plots, σ_H is specified in dB according to $20 \log_{10} \sigma_H$. For example, a value of $\sigma_H = -20\text{dB}$ corresponds to $\sigma_H = 0.1$, indicating channel perturbations on the order of 10% of the channel coefficients themselves. All displayed results are calculated based on an average of 3000 independent trials. The background noise power was assumed to be the same for both Bob and Eve: $\sigma_b^2 = \sigma_e^2 = 1$, and in all cases the available transmit power was assumed to be $P = 100$, or 20dB. In situations where the desired SINR for Bob cannot be achieved with the given P , rather than indicate an outage, we simply assign all power to Bob and zero to artificial interference and

average the resulting SINR with the others.

5.5.1 Effects of Eavesdropper CSI

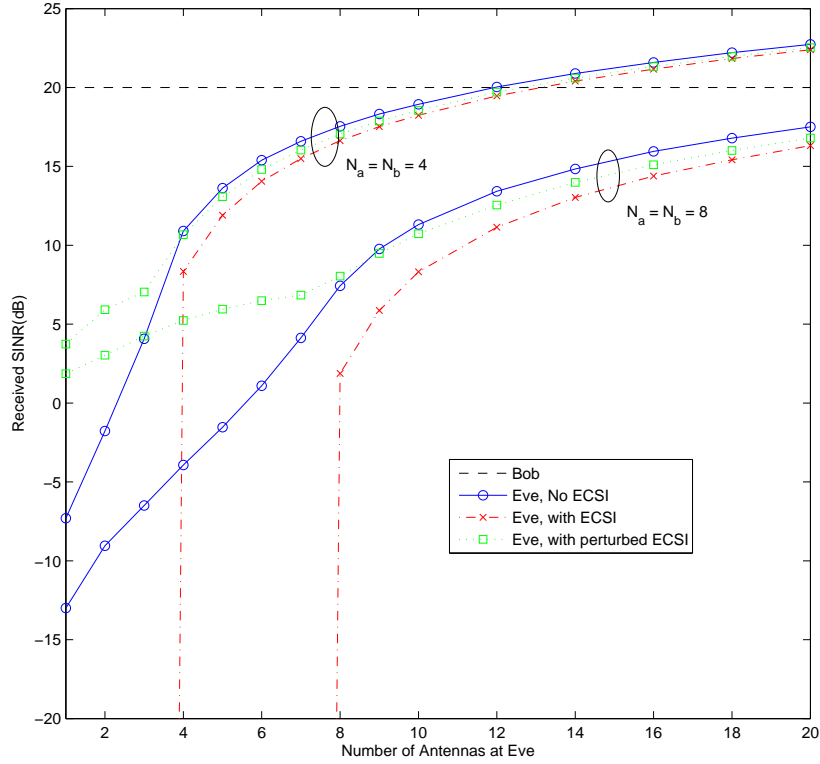


Figure 5.1: SINR versus number of antennas for Eve.

Figure 5.1 illustrates the performance of the algorithms when $S = 20\text{dB}$ and $N_e \in [1, 20]$. The number of antennas for Alice and Bob are assumed to be equal, and results are shown for $N_a = N_b = 4, 8$. The desired SINR for Bob was set to 20dB , and the available transmit power was sufficient in this simulation for the target to be met in all 3000 trials. Three curves are included for Eve, showing the performance of the algorithms for different assumptions about the eavesdropper's CSI (ECSI): (1) when it is unknown, in which case the artificial noise approach of Section 5.2.1 is used, (2) when it is perfectly known, in which case the generalized eigenvector approach of

Section 5.2.2 is used, and (3) when it is imperfectly known, where again the approach of Section 5.2.2 is used, but the ECSI perturbation is unaccounted for. The perturbed ECSI was generated by the following equation, assuming $\gamma = 0.05$ (which corresponds to a perturbation of about -13dB):

$$\tilde{\mathbf{H}}_{ea} = \sqrt{1 - \gamma} \mathbf{H}_{ea} + \sqrt{\gamma} \mathbf{W}_{ea} , \quad (5.67)$$

where \mathbf{H}_{ea} and \mathbf{W}_{ea} are independent, zero-mean Gaussian with unit-variance elements, and hence so is $\tilde{\mathbf{H}}_{ea}$. In the simulations, the actual channel is \mathbf{H}_{ea} , but Alice assumes it is $\tilde{\mathbf{H}}_{ea}$. The assumption of perfect ECSI provides a significant benefit when $N_e < \{N_a, N_b\}$; in fact, the eavesdropper's SINR can theoretically be driven to zero. The gain when $N_e \geq \{N_a, N_b\}$ is not as large, particularly for $N_a = N_b = 4$, when it is less than 2dB. Much of the benefit of ECSI is lost however if it is imprecisely known; even for this case when the perturbation is relatively small, we see that for small N_e it is often better to ignore the ECSI than to use a perturbed version of it.

5.5.2 SINR Degradation Analysis

In Figure 5.2, we compare the SINR expressions for the naive case based on second-order perturbation theory derived in Section 5.3 with measured SINR values from simulations for a range of channel perturbation powers. The set of channel matrices have dimensions of either $N_a = N_b = N_e = 2$ or $N_a = N_b = N_e = 5$, and the desired SINR for Bob is set to $S = 20$ dB. For both antenna configurations, the second-order approximations appear to be accurate up to about $\sigma_H = -10$ dB, which corresponds to $\sigma_H = 0.32$. This is a relatively large perturbation for channels with unit-variance elements. We see that inaccurate CSI substantially impacts Bob's SINR, even for relatively small values of σ_H . For example, when $N_a = 10$, Bob loses 6dB of SINR

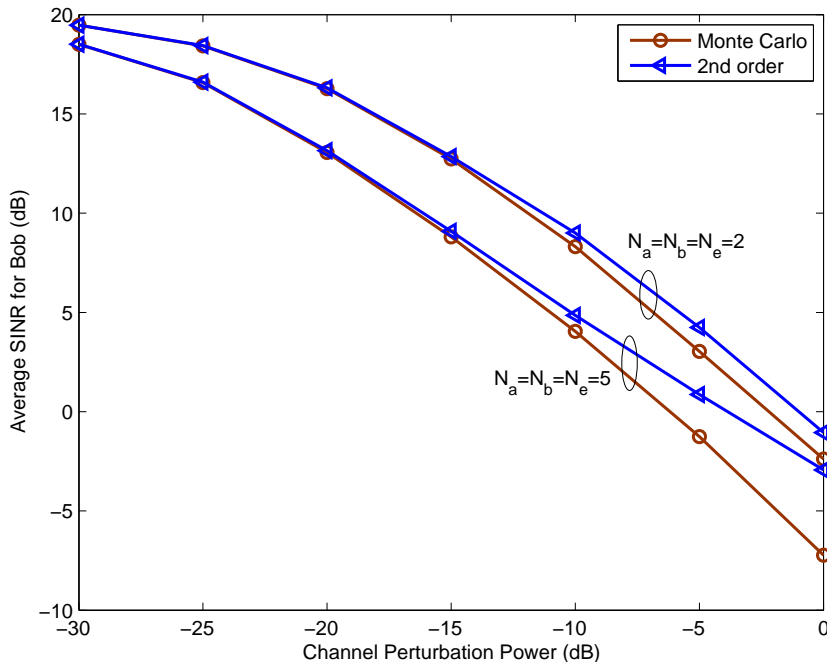


Figure 5.2: A comparison of the 2nd-order naive SINR approximations with Monte Carlo SINR results for $N_a = N_b = N_e = 2$ and $N_a = N_e = N_b = 5$.

for the relatively small value $\sigma_H = 0.1$.

5.5.3 Robust Beamforming Results

Figure 5.3 shows the SINR for Bob and Eve as a function of S for various approaches, including the robust beamforming schemes presented earlier. The channel perturbation power is fixed at $\sigma_H = -10$ dB, and we assume $N_a = N_b = N_e = 5$. It is evident that the naive schemes incur a significant SINR penalty for relatively small channel perturbations, with the achieved SINR at the intended receiver being 15-17dB below the target SINR and 6-7dB worse than the SINR for Eve. Note however that the robust receive beamforming schemes are able to restore Bob's SINR performance at or near the desired value. Obviously, the presence of uncanceled artificial interference due to imperfect CSI requires Alice to use additional power for the desired signal,

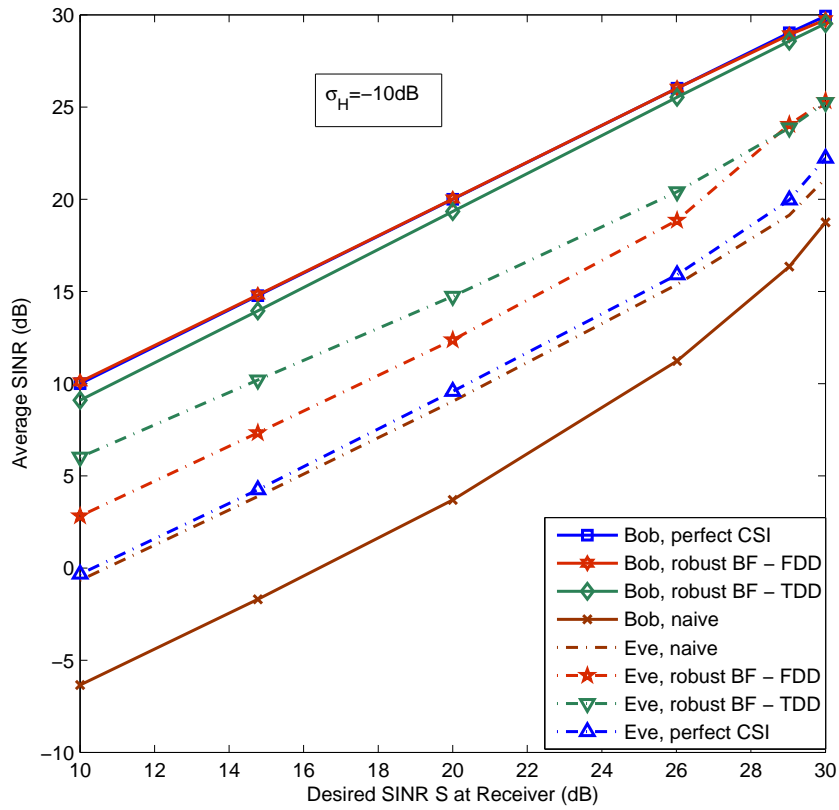


Figure 5.3: Measured SINR values versus desired SINR for Bob and Eve with perfect and imperfect CSI at Alice for $N_a = N_b = N_e = 5$ antennas, $\sigma_H = -10\text{dB}$.

thus reducing the amount of noise available to jam the eavesdropper. This is why Eve’s SINR increases with the robust beamforming methods. As expected, Eve’s performance is best degraded in the FDD case where Bob has exact knowledge of Alice’s transmission scheme¹. Note also that Eve’s SINR increases slightly for high values of S . This is due to the fact that as S increases, there will be an increasing number of cases where no power is available for jamming. This also inadvertently helps Bob in the naive case, since the lack of jamming eliminates interference for the desired signal.

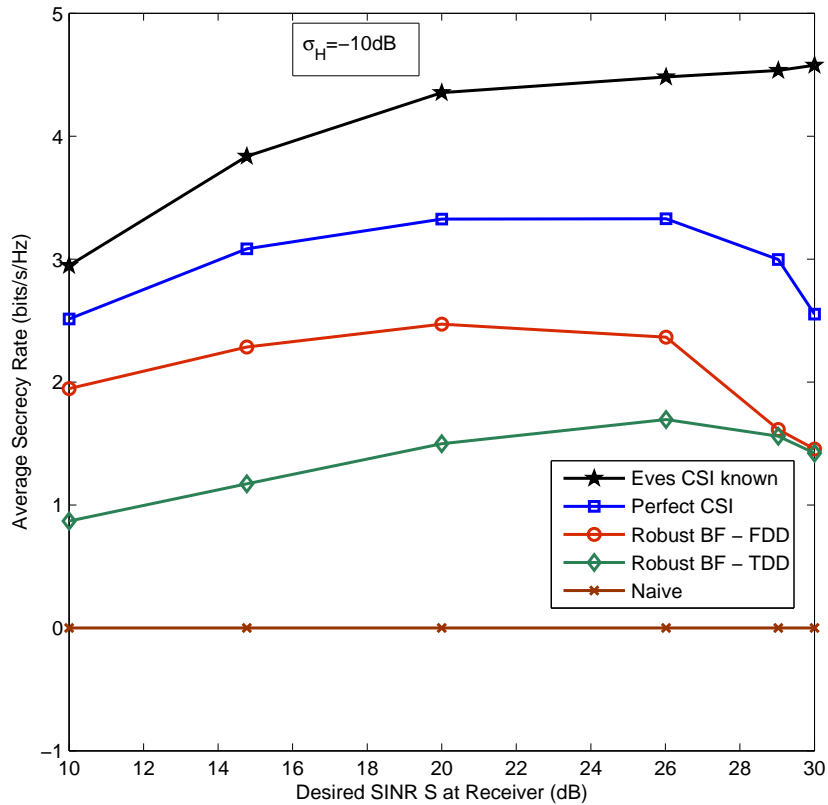


Figure 5.4: Secrecy rate versus desired SINR for Bob with perfect and imperfect CSI at Alice for $N_a = N_b = N_e = 5$ antennas, $\sigma_H = -10$ dB.

¹This does not imply that FDD systems are better than TDD systems for this application; one may expect that in practice the value for σ_H will be somewhat larger in the FDD case due to quantization and the added delay required for feedback.

Figure 5.4 plots the secrecy rate that results for the case considered here, for various CSI assumptions. The case where Eve’s CSI is perfectly known is shown for reference, and obviously for this case the best secrecy capacity is obtained. As expected, the benefit of knowing the eavesdropper’s CSI is largest when Bob demands a high QoS, and minimal for low values of S where more resources are available for jamming. The robust beamforming strategies provide non-zero secrecy capacity for all values of S , and recover a reasonable fraction of the performance available in the perfect CSI case. However, in the naive case, the secrecy capacity is reduced to zero since Eve’s SINR is always larger than Bob’s. This assumes of course that Bob does nothing to counteract the interference, while Eve uses an optimal beamformer that requires exact knowledge of the interference covariance.

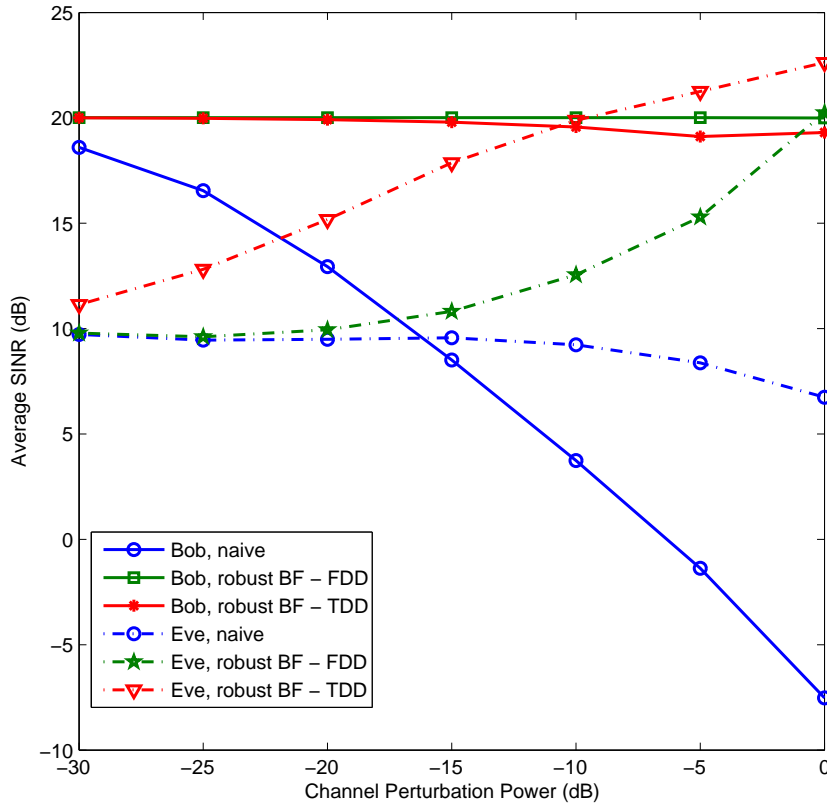


Figure 5.5: Average SINR for Bob and Eve as a function of σ_H for $N_a = N_b = N_e = 5$ antennas and $S = 20$ dB.

The effect of the magnitude of the channel perturbation on SINR performance is illustrated in Figure 5.5 for the case studied in the previous figures, assuming $S = 20\text{dB}$. Robust beamforming in the FDD case realizes little performance loss for values of σ_H up to -15dB , while the threshold for degradation in the TDD case is somewhat lower. Recall that Figure 5.4 showed a positive secrecy capacity for the TDD case at $\sigma_H = -10\text{dB}$, even though in Figure 5.5 both Bob and Eve appear to have approximately the same average SINR. This is because the secrecy capacity must be non-negative; a positive result is obtained when Bob's SINR exceeds Eve's, but the capacity is assumed to be zero otherwise.

5.6 Summary

We have presented beamforming-based approaches for improving the secrecy of the wireless communications between two multi-antenna nodes. The algorithms allocate transmit power in order to achieve a target SINR for a desired user, and then broadcast the remaining available power as artificial noise in order to disrupt the interception of the signal by a passive eavesdropper. The proposed approaches rely heavily on the availability of accurate CSI, and their performance can be quite sensitive to imprecise channel estimates. As a result, we conducted a detailed second-order perturbation analysis in order to precisely quantify the effects of inaccurate CSI. Simulations were used to demonstrate the validity of the analysis, and to illustrate the sensitivity of algorithms that depend on precise CSI. To reduce the impact of the CSI errors, we proposed two robust beamforming schemes that are able to recover a large fraction of the SINR lost due to the channel estimation errors. These techniques were shown to perform very well for moderate CSI errors, but ultimately a large enough channel mismatch can eliminate the secrecy advantage of using artificial noise.

Chapter 6

Jamming Games in the MIMO Wiretap Channel

6.1 Background

In this chapter, we consider a MIMO communication link in the presence of a more sophisticated adversary, one with the dual capability of either passively eavesdropping or actively jamming any ongoing transmission, with the objective of causing maximum disruption to the ability of the legitimate transmitter to share a secret message with its receiver. The legitimate transmitter now faces the dilemma of establishing a reliable communication link to the receiver that is robust to potential jamming, while also ensuring confidentiality from interception. Since it is not clear *a priori* what strategies should be adopted by the transmitter or adversary per channel use, a game-theoretic formulation of the problem is a natural solution due to the mutually opposite interests of the agents. Unlike the jamming scenarios mentioned above that do not consider link security, the game payoff function in our application is chosen

to be the achievable *MIMO secrecy rate* between the legitimate transmitter-receiver pair. Related concurrent work on the active eavesdropper scenario [84, 85] has focused on single-antenna nodes without the use of artificial noise, possibly operating together with additional ‘helping’ relays. As demonstrated later, the single-antenna assumption leads to a much more restrictive set of user strategies than the MIMO scenario we consider.

The chapter is organized as follows. In the next section, the assumed mathematical model is presented. An evaluation of the achievable secrecy rates and their relative magnitudes is carried out in Section 6.3. The strategic formulation of the wiretap game is described in Section 6.4 to establish the payoff table, and conditions for which Nash equilibria exist are derived. The extensive version of the wiretap game with perfect and imperfect information where the players move sequentially is detailed in Section 6.5. The resulting system performance is studied via simulation in Section 6.6, and we conclude in Section 6.7.

6.2 Signal and CSI Model

In the most general scenario where Alice jams Eve by transmitting artificial interference, we have

$$\mathbf{x}_a = \mathbf{T}\mathbf{z} + \mathbf{T}'\mathbf{z}', \tag{6.1}$$

where \mathbf{T} , \mathbf{T}' are the $N_a \times d$, $N_a \times (N_a - d)$ precoding matrices for the $d \times 1$ information vector \mathbf{z} and uncorrelated $(N_a - d) \times 1$ jamming signal \mathbf{z}' , respectively. To ensure that the artificial noise does not interfere with the information signal, a common approach taken in the literature [18, 19],[29]–[86] is to make these signals orthogonal

when received by Bob. If Alice knows \mathbf{H}_{ba} , this goal can be achieved by choosing \mathbf{T} and \mathbf{T}' as disjoint sets of the right singular vectors of \mathbf{H}_{ba} . Note that if the users have only a single antenna, the effect of the artificial noise cannot be eliminated at Bob, and it will degrade the SNR of both Bob and Eve. This makes it unlikely that Alice will employ a non-zero artificial noise signal when she has only a single transmit antenna, which significantly changes Alice's transmission strategy as we show later in the simulations. The matrix \mathbf{Q}_a may be expressed as

$$\mathbf{Q}_a = \mathbf{T}\mathbf{Q}_z\mathbf{T}^H + \mathbf{T}'\mathbf{Q}'_z\mathbf{T}'^H, \quad (6.2)$$

where $\mathbf{Q}_z, \mathbf{Q}'_z$ are the covariance matrices associated with \mathbf{z} and \mathbf{z}' , respectively. If we let ρ denote the fraction of the total power available at Alice that is devoted to the information signal, then $\text{Tr}(\mathbf{T}\mathbf{Q}_z\mathbf{T}^H) = \rho P_a$ and $\text{Tr}(\mathbf{T}'\mathbf{Q}'_z\mathbf{T}'^H) = (1 - \rho)P_a$. The covariance matrices of the received interference-plus-noise at Bob and Eve are

$$\mathbf{K}_b = g_2\mathbf{H}_{be}\mathbf{Q}_{be}\mathbf{H}_{be}^H + \sigma_b^2\mathbf{I} \quad (6.3)$$

$$\mathbf{K}_e = g_1\mathbf{H}_{ea}\mathbf{T}'\mathbf{Q}'_z\mathbf{T}'^H\mathbf{H}_{ea}^H + \sigma_e^2\mathbf{I}, \quad (6.4)$$

where \mathbf{Q}_{be} is the covariance of the jamming signal transmitted by Eve.

Note that we have assumed that Alice's jamming signal (if any) is orthogonal to the information signal received by Bob, and hence, from the point of view of mutual information, can be ignored in the expression for \mathbf{K}_b . For our purposes, we assume that Alice splits her transmit power between a stochastic encoding codebook and artificial noise for every channel use in *all* scenarios, while Bob employs a deterministic decoding function [14,15]. Firstly, this ensures that the general encoding and decoding architecture of the Alice-Bob link remains fixed irrespective of Eve's actions. Secondly,

for a point-to-point channel without an eavesdropper (*i.e.*, when the eavesdropper is jamming and not listening), using a stochastic codebook does not offer any advantage over a conventional codebook, but it does not hurt either, *i.e.*, the receiver still reliably decodes the transmitted codeword [15].

Given the signal framework introduced above, we are ready to discuss the important issue of CSI. We have already indicated that Alice knows \mathbf{H}_{ba} in order to appropriately precode the jamming and information signals via \mathbf{T} and \mathbf{T}' , conceivably obtained by public feedback from Bob after a training phase. At the receiver side, we will assume that Eve knows the channel from Alice \mathbf{H}_{ea} and the covariance \mathbf{K}_e of the interference and noise, and similarly we will assume that Bob knows \mathbf{H}_{ba} and \mathbf{K}_b . All other CSI at the various nodes is assumed to be non-informative; the only available information is that the channels are composed of independent $\mathcal{CN}(0, 1)$ random variables. This implies that when Eve jams Bob, her lack of information about \mathbf{H}_{be} and the half-duplex constraint prevents her from detecting the transmitted signal \mathbf{z} and applying correlated jamming [23]. Consequently, she will be led to uniformly distribute her available power over all N_e transmit dimensions, so that $\mathbf{Q}_{be} = \frac{P_e}{N_e} \mathbf{I}$. Similarly, when Alice transmits a jamming signal, it will also be uniformly distributed across the $N_a - d$ available dimensions: $\mathbf{Q}'_z = \frac{(1-\rho)P_a}{N_a-d} \mathbf{I}$. While in principle Alice could use her knowledge of \mathbf{H}_{ba} to perform power loading, for simplicity and robustness we will assume that the power of the information signal is also uniformly distributed, so that $\mathbf{Q}_z = \frac{\rho P_a}{d} \mathbf{I}$.

Given the above assumptions, equations (6.2)-(6.4) will simplify to

$$\mathbf{Q}_a = \frac{\rho P_a}{d} \mathbf{T} \mathbf{T}^H + \eta_a \mathbf{T}' \mathbf{T}'^H \quad (6.5)$$

$$\mathbf{K}_b = \frac{g_2 P_e}{N_e} \mathbf{H}_{be} \mathbf{H}_{be}^H + \sigma_b^2 \mathbf{I} \quad \mathbf{K}_e = g_1 \eta_a \mathbf{H}_{ea} \mathbf{T}' \mathbf{T}'^H \mathbf{H}_{ea}^H + \sigma_e^2 \mathbf{I}, \quad (6.6)$$

where we have defined $\eta_a = \frac{(1-\rho)P_a}{N_a-d}$.

The MIMO secrecy capacity between Alice and Bob is obtained by solving [17, 18, 87]

$$C_s = \max_{\mathbf{Q}_a \succeq 0} I(\mathbf{X}_a; \mathbf{Y}_b) - I(\mathbf{X}_a; \mathbf{Y}_e) , \quad (6.7)$$

where $\mathbf{X}_a, \mathbf{Y}_b, \mathbf{Y}_e$ are the random variable counterparts of the realizations $\mathbf{x}_a, \mathbf{y}_a, \mathbf{y}_e$. Given the CSI constraints discussed above, such an optimization cannot be performed since Alice is unaware of the instantaneous values of all channels and interference covariance matrices. Consequently, we choose to work with the the achievable lower bound on the MIMO ergodic secrecy capacity based on Gaussian inputs and uniform power allocation at all transmitters [88]:

$$C_s \geq \mathcal{E}_{\mathbf{H}} \left\{ \log_2 \left| \mathbf{I} + \frac{\rho P_a}{d} \mathbf{H}_{ba} \mathbf{T} \mathbf{T}^H \mathbf{H}_{ba}^H \mathbf{K}_b^{-1} \right| - \log_2 \left| \mathbf{I} + \frac{\rho P_a}{d} \mathbf{H}_{ea} \mathbf{T} \mathbf{T}^H \mathbf{H}_{ea}^H \mathbf{K}_e^{-1} \right| \right\} , \quad (6.8)$$

where we define $\mathbf{H} \triangleq \{\mathbf{H}_{ba}, \mathbf{H}_{be}, \mathbf{H}_{ea}\}$. Using ergodic secrecy as the utility function for the game between Alice and Eve implies that a large number of channel realizations will occur intermediate to any changes in their strategy. That is, the physical layer parameters are changing faster than higher (*e.g.*, application) layer functions that determine the user's strategy. Thus, the expectation is taken over all channel matrices, which in turn provides Alice and Eve with a common objective function, since neither possesses the complete knowledge of \mathbf{H} that is needed to compute the instantaneous MIMO secrecy rate.

Eve must decide whether to eavesdrop or jam with an arbitrary fraction of her transmit power. Alice's options include determining how many spatial dimensions are to be used for data and artificial noise (if any), and the appropriate fraction ρ that determines the transmit power allocated to them. As described in [19, 30, 86, 89], there are several options available to Alice for choosing ρ and d depending upon the accuracy

of her CSI, ranging from an exhaustive search for optimal values to lower-complexity approaches based on fixed-rate assumptions. Numerical results from this previous work have indicated that the achievable secrecy rate is not very sensitive to these parameters, and good performance can be obtained for a wide range of reasonable values. The general approach of this chapter is applicable to essentially any value for ρ and d , although the specific results we present assume that optimal values have been chosen by Alice under the assumption that the eavesdropper is in fact eavesdropping, and not jamming.

In Section 6.4 we show that it is sufficient to consider a set of two strategies for both players without any loss in optimality. In particular, we show that Alice need only consider the options of either transmitting the information signal with full power, or devoting an appropriate amount of power and signal dimensions to a jamming signal. On the other hand, Eve’s only reasonable strategies are to either eavesdrop passively or jam Bob with all her available transmit power.

6.3 Rate Thresholds

We will denote Eve’s set of possible actions as $\{E, J\}$ to indicate either “Eavesdropping” or “Jamming,” while Alice’s will be expressed as $\{F, A\}$ to indicate “Full-power” devoted to the information signal, or a non-zero fraction of the power allocated to “Artificial noise.” The secrecy rates that result from the resulting four possible scenarios will be denoted by R_{ik} , where $i \in \{F, A\}$ and $k \in \{E, J\}$. While (6.8) can be directly evaluated to determine the set of possible secrecy rates for a given scenario (which is the approach we take in the simulations), in this section we will investigate the problem of finding simpler approximate expressions that will facilitate comparisons between different scenarios. This will be useful for our game-theoretic

analysis in Sections 6.4 and 6.5. To this end, we first review some prior results from MIMO communication theory that assist our development of tractable secrecy rate expressions.

6.3.1 Asymptotic MIMO Rates

Let \mathbf{X} represent an $N \times L$ MIMO channel matrix composed of $\mathcal{CN}(0, 1)$ elements over which a source transmits to a receiver with signal-to-noise ratio (SNR) α . When interference is absent and thermal noise is the only impairment at the receiver, the MIMO information rate is given by $R = E \left\{ \log \left| \mathbf{I} + \frac{\alpha}{L} \mathbf{X} \mathbf{X}^H \right| \right\}$, assuming a uniform power allocation. A closed-form expression for this expectation in terms of generalized Laguerre polynomials is given in [40].

However, a more tractable expression for the ergodic MIMO capacity is available based on asymptotic results in the limit of a large number of antennas, as described next. Let $\beta = N/L$ denote the ratio of receive-to-transmit antennas. A useful closed-form expression for the ergodic MIMO capacity with uniform power allocation in the large-antenna regime is [90, 91]

$$R = N \cdot F(\beta, \alpha) \tag{6.9}$$

where

$$\begin{aligned} F(\beta, \alpha) = & \log \left(1 + \alpha \left(\sqrt{\beta} + 1 \right)^2 \right) + (\beta + 1) \log \left(\frac{1 + \sqrt{1 - a}}{2} \right) \\ & - \log(e) \sqrt{\beta} \frac{1 - \sqrt{1 - a}}{1 + \sqrt{1 - a}} + (\beta - 1) \log \left(\frac{1 + \gamma}{\gamma + \sqrt{1 - a}} \right) \end{aligned} \tag{6.10}$$

and

$$a = \frac{4\alpha\sqrt{\beta}}{1 + \alpha(\sqrt{\beta} + 1)^2} \quad \gamma = \frac{\sqrt{\beta} - 1}{\sqrt{\beta} + 1}. \quad (6.11)$$

Though originally derived under an asymptotic assumption, (6.9) has been shown to be very accurate even for small and medium-sized antenna array dimensions [90, 91].

Now, in addition to the desired signal over channel \mathbf{X} with SNR α , assume the presence of an interferer with interference-to-noise ratio (INR) η and an $N \times M$ channel \mathbf{Y} with $\mathcal{CN}(0, 1)$ elements. Assuming uniform power allocation at both the desired source and interferer, the ergodic MIMO information rate with interference and Gaussian background noise is given by

$$R_I = \mathcal{E}_{\mathbf{X}, \mathbf{Y}} \left\{ \log \left| \mathbf{I} + \frac{\alpha}{L} \mathbf{X} \mathbf{X}^H \left(\mathbf{I} + \frac{\eta}{M} \mathbf{Y} \mathbf{Y}^H \right)^{-1} \right| \right\}. \quad (6.12)$$

The asymptotic random matrix analysis technique referred to above has been extended in order to evaluate the MIMO capacity with interference in [48, 49], for example. In [48], a set of four simple closed-form expressions for the MIMO rate in the high-SNR regime is derived for different ratios of N/L when $N = M$. In [49], the replica approach is used to obtain a more involved expression for the first-order approximation of the mean value of the MIMO mutual information at any SNR. However, we propose to extend the result of (6.9) in a straightforward manner to obtain a more tractable upper bound for the ergodic MIMO rate when strong interference is present.

Lemma 1: In a MIMO channel where the legitimate transmitter, receiver, and interferer have L, N, M antennas respectively, the asymptotic MIMO information rate

with receive SNR α and INR η can be bounded as

$$R_I \leq (L + M) F\left(\frac{N}{L + M}, (\alpha + \eta)\right) - MF\left(\frac{N}{M}, \eta\right), \quad (6.13)$$

where $F(\beta, \alpha)$ is defined in (6.10).

Proof: Rewrite (6.12) as

$$R_I = E_{\mathbf{X}, \mathbf{Y}} \left\{ \log \left| \mathbf{I} + \frac{\alpha}{L} \mathbf{X} \mathbf{X}^H + \frac{\eta}{M} \mathbf{Y} \mathbf{Y}^H \right| \right\} - E_{\mathbf{Y}} \left\{ \log \left| \mathbf{I} + \frac{\eta}{M} \mathbf{Y} \mathbf{Y}^H \right| \right\}. \quad (6.14)$$

The first term is equivalent to the sum rate of a two-user MIMO multiple access channel (MIMO MAC) with uniform power allocation at each transmitter. The second term represents the MIMO rate between the interferer and the destination when treating the jamming signal as information. Since the transmitters cannot cooperate in the MIMO MAC, the sum rate of the MIMO MAC is upper-bounded by the rate of the equivalent point-to-point MIMO channel with composite channel $\mathbf{H} = \begin{bmatrix} \mathbf{X} & \mathbf{Y} \end{bmatrix}$, $(L + M)$ transmit antennas, and effective SNR $(\alpha + \eta)$. This leads to an upper bound on the MIMO interference rate as

$$R_I \leq E_{\mathbf{H}} \left\{ \log \left| \mathbf{I} + \left(\frac{\alpha + \eta}{L + M} \right) \mathbf{H} \mathbf{H}^H \right| \right\} - E_{\mathbf{Y}} \left\{ \log \left| \mathbf{I} + \frac{\eta}{M} \mathbf{Y} \mathbf{Y}^H \right| \right\}. \quad (6.15)$$

Applying the expression for the asymptotic MIMO rate without interference in (6.9) to each of the two terms on the right hand side of (6.15) leads to (6.13). ■

The rate loss between the MIMO MAC and the equivalent point-to-point MIMO channel is due to the inability to optimally allocate the global transmit power across all transmitting antennas. This rate loss was quantified in [92], and was shown to be bounded by a function of the global input and output dimensions at high SNR: $R_{loss} \leq \min \left[0.265 (L + M), 0.265 \frac{N}{2} \log \left(\frac{L+M}{N} \right) \right]$.

6.3.2 MIMO Secrecy Rate Analysis

We now return our attention to the rate outcomes of the MIMO wiretap game. Define the effective channels conveying information \mathbf{z} from Alice to Bob and Eve as $\tilde{\mathbf{H}}_{ba} \triangleq \mathbf{H}_{ba}\mathbf{T}$ and $\tilde{\mathbf{H}}_{ea} \triangleq \mathbf{H}_{ea}\mathbf{T}$, respectively. Since \mathbf{T} is a submatrix of an isotropically-random unitary matrix, $\tilde{\mathbf{H}}_{ba}$ and $\tilde{\mathbf{H}}_{ea}$ are also zero-mean complex Gaussian matrices with i.i.d elements. However, the elements of $\tilde{\mathbf{H}}_{ba}$ will in general have a variance greater than unity due to the fact that the data is concentrated in a subset of the spatial subchannels corresponding to the stronger singular values. In order to apply the random matrix results stated previously, it is necessary to normalize the effective channel $\tilde{\mathbf{H}}_{ba}$ to obtain unit variance elements. The exact normalization constant is difficult to obtain analytically, and since we are dealing with an upper bound on the achievable rate, our results will be based on scaling $\tilde{\mathbf{H}}_{ba}$ by an approximate factor $\sqrt{d/N_a}$. The inverse of this factor, which represents an upper bound on the increase in the variance of the elements of $\tilde{\mathbf{H}}_{ba}$, will be absorbed into the transmit power constraint.

Assuming Gaussian inputs \mathbf{z} and \mathbf{z}' , the MIMO secrecy rate between Alice and Bob when Eve is in eavesdropping mode is

$$R_{iE} = \mathcal{E}_{\mathbf{H}} \left\{ \log \left| \mathbf{I} + \frac{\rho P_a}{d\sigma_b^2} \mathbf{H}_{ba} \mathbf{T} \mathbf{T}^H \mathbf{H}_{ba}^H \right| - \log \left| \mathbf{I} + \frac{g_1 \rho P_a}{d} \mathbf{H}_{ea} \mathbf{T} \mathbf{T}^H \mathbf{H}_{ea}^H \mathbf{K}_e^{-1} \right| \right\}, \quad (6.16)$$

whereas the secrecy rate when Eve is jamming reduces to

$$R_{iJ} = \mathcal{E}_{\mathbf{H}} \left\{ \log \left| \mathbf{I} + \frac{\rho P_a}{d} \mathbf{H}_{ba} \mathbf{T} \mathbf{T}^H \mathbf{H}_{ba}^H \mathbf{K}_b^{-1} \right| \right\}, \quad (6.17)$$

where $i = F, A$ denotes the transmission strategies available to Alice. We refer to (6.17) as a secrecy rate even though there is technically no eavesdropper, since

Eve's mutual information is identically zero and Alice still uses a stochastic encoder (cf. Sec. 6.2). Therefore, when evaluating the secrecy rate definition (11) for the case where Eve chooses to jam, the second term is zero which yields R_{FJ} and R_{AJ} in (6.17) as the effective secrecy rate. Recall that the definition of the secrecy rate is the maximum transmission rate which can be reliably decoded by Bob while remaining perfectly secret from Eve, which is still satisfied by the rates in (6.17). Note also that when Alice employs artificial noise, a choice for ρ and d must be made that holds regardless of Eve's strategy. Therefore, the values of ρ and d that are numerically computed to maximize R_{AE} in (6.16) [19] remain unchanged for R_{AJ} in (6.17). When Alice transmits with full power, then $d = r$, where $r = \min(N_a, N_b)$, and the precoder \mathbf{T} consists of the right singular vectors of \mathbf{H}_{ba} corresponding to the r largest singular values.

While Alice uses the same type of encoder regardless of Eve's strategy, achieving the rates in (6.16)-(6.17) requires adjustments to the code rate that *will* depend on Eve's actions. For example, if Alice is transmitting with full power (strategy F), the code rate needed to achieve either R_{FE} or R_{AE} in (6.16) or (6.17) will be different. Thus, we assume that Alice can be made aware of Eve's strategy choice, for example through feedback from Bob, in order to make such adjustments¹. Such behavior is not limited to just Alice and Bob; Eve also makes adjustments based on Alice's choice of strategy. In particular, when Eve is eavesdropping, her method of decoding Alice's signal will depend on whether or not Alice is transmitting artificial noise. We do not consider adjustments such as these as part of Alice or Eve's strategy *per se*, which in our game theory framework is restricted to the decision of whether or not to use artificial noise/jamming. We assume that minor adaptations to the coding or decoding algorithm for Alice and Eve occur relatively quickly, and that any resulting

¹Based on such feedback, Alice could also in principle switch from a stochastic encoder to a more standard non-secure code if she discovers that Eve is jamming and not eavesdropping. In either case, the rate expressions in (6.16)-(6.17) will be valid.

transients are negligible due to our use of ergodic secrecy rate as the utility function. The more interesting question is whether or not Alice and Eve decide to change strategies based on the actions of the other is addressed in Section 6.5.

In view of (6.9), (6.13), (6.16) and (6.17), the asymptotic MIMO secrecy rate outcomes therefore are

$$R_{AE} \leq dF\left(\frac{N_b}{d}, \frac{\rho P_a N_a}{d\sigma_b^2}\right) - \left[N_a F\left(\frac{N_e}{N_a}, \frac{g_1 P_a}{\sigma_e^2}\right) - (N_a - d) F\left(\frac{N_e}{N_a - d}, \frac{g_1(1 - \rho)P_a}{\sigma_e^2}\right) \right] \quad (6.18)$$

$$R_{AJ} \leq (N_e + d) F\left(\frac{N_b}{N_e + d}, \frac{\rho N_a P_a}{d\sigma_b^2} + \frac{g_2 P_e}{\sigma_b^2}\right) - N_e F\left(\frac{N_b}{N_e}, \frac{g_2 P_e}{\sigma_b^2}\right) \quad (6.19)$$

$$R_{FE} \leq N_a F\left(\frac{N_b}{N_a}, \frac{P_a}{\sigma_b^2}\right) - N_a F\left(\frac{N_e}{N_a}, \frac{g_1 P_a}{\sigma_e^2}\right) \quad (6.20)$$

$$R_{FJ} \leq (N_e + N_a) F\left(\frac{N_b}{N_e + N_a}, \frac{P_a + g_2 P_e}{\sigma_b^2}\right) - N_e F\left(\frac{N_b}{N_e}, \frac{g_2 P_e}{\sigma_b^2}\right). \quad (6.21)$$

The asymptotic rates above are compared with the exact rate expressions obtained through Monte Carlo trials in Fig. 6.1, which demonstrates reasonable accuracy even for small antenna arrays.

In [18], the instantaneous MIMO secrecy rate with artificial interference at high SNR is characterized in terms of the generalized singular values of $(\mathbf{H}_{ba}, \mathbf{H}_{ea})$. A closed-form lower bound for the ergodic MISO ($N_b = 1$) secrecy rate with artificial interference is derived using the Gauss hypergeometric function in [30]. In contrast, the upper bounds derived in (6.18)-(6.21) explicitly display the various system parameters, and are also amenable to analysis. It is apparent that any comparison of the relative magnitudes of a pair of rates taken from those defined in (6.18)-(6.21) would

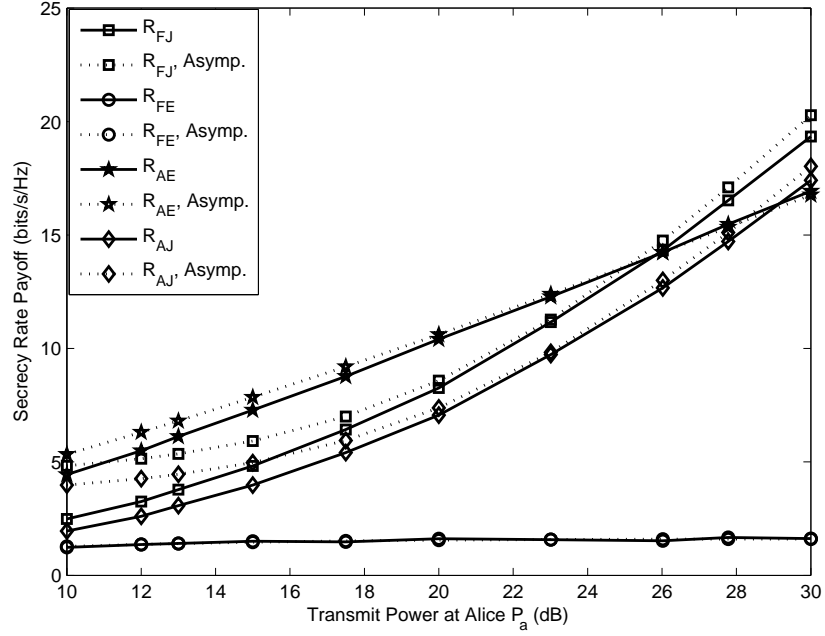


Figure 6.1: Comparison of exact and asymptotic MIMO secrecy rate outcomes, $P_e = 10dB$, $N_a = 7$, $N_b = N_e = 5$, $d = 4$ and $g_1 = 0.8$, $g_2 = 1.2$.

involve a large number of parameters. It is therefore convenient to vary a subset of the parameters while holding the others constant when comparing the different rate outcomes. This exercise is conducted in the numerical results of Section 6.6 for several cases.

In the game theoretic analysis of the next two sections, we will utilize the following general properties of the MIMO wiretap channel:

$$(P1) \quad R_{FE} \leq R_{AE}$$

$$(P2) \quad R_{AJ} \leq R_{FJ}$$

The validity of (P2) is obvious; if Alice employs artificial interference, it reduces the power allocated to the information signal, which in turn can only decrease the mutual information at Bob. Since Eve is jamming, her mutual information is zero regardless

of Alice's strategy, so R_{AJ} can never be larger than R_{FJ} . The validity of (P1) can be established by recalling that Alice chooses a value for ρ that maximizes R_{AE} , assuming Eve is eavesdropping. Since $\rho = 0$ is an available option and corresponds to R_{FE} , Alice can do no worse than R_{FE} in choosing the optimal ρ for strategy R_{AE} .

6.4 Strategic Wiretap Game

In this section we construct the zero-sum model of the proposed wiretap game. We define the payoff to Alice as the achievable MIMO secrecy rate between her and Bob. Modeling the strategic interactions between Alice and Eve as a strictly competitive game leads to a zero-sum formulation, where Alice tries to maximize her payoff and Eve attempts to minimize it.

Formally, we can define a compact strategy space $A_i, i = 1, 2$, for both Alice and Eve: Alice has to optimize the pair $(d, \rho) \in A_1$, where ρ is chosen from the unit interval $[0, 1]$ and $d \in \{1, \dots, r = \min(N_a, N_b)\}$; and Eve can choose her jamming power $P_j \in A_2$ from the interval $[0, P_e]$, where zero jamming power corresponds to the special case of passive eavesdropping. In other words, each player theoretically has a continuum of (pure) strategies to choose from, where the payoff for each combination of strategies is the corresponding MIMO secrecy rate. In the following discussion, let (d_s^*, ρ_s^*) represent the choice of Alice's parameters that maximizes the ergodic secrecy rate R_{AE} .

The complete set of mixed strategies for player i is the set of Borel probability measures on A_i . Let Δ_i be the set of all probability measures that assign strictly positive mass to every nonempty open subset of A_i . The optimal mixed strategy for player i must belong to Δ_i , since any pure strategies that are assigned zero probability in

equilibrium can be pruned without changing the game outcome. Furthermore, as in the case of finite games, the subset of pure strategies included in the optimal mixed strategy must be *best responses* to particular actions of the opponent [93]. Consider Alice: when Eve chooses the action of eavesdropping, (d_s^*, ρ_s^*) is Alice's corresponding best response pure strategy since by definition it offers a payoff at least as great as *any* other possible choice of (d, ρ) [cf. (P1)]. Similarly, when Eve chooses to jam with any arbitrary power, Alice's best response pure strategy is $(d = r, \rho = 1)$ [cf. (P2)]. Therefore, these two pure strategies are Alice's best responses for any possible action by Eve, and it is sufficient to consider them alone in the computation of the optimal mixed strategy since all other pure strategies are assigned zero probability. A similar argument holds for Eve with her corresponding best responses of $P_j = 0$ and $P_j = P_e$.

Therefore, it is sufficient to consider the following strategy sets \mathcal{X}, \mathcal{Y} for the players: Alice chooses between transmitting with full power for data (F) or devoting an appropriate fraction of power to jam Eve (A), described as $\mathcal{X} = \{F, A\}$. Eve must decide between eavesdropping (E) or jamming Bob with full power P_e (J) at every channel use, represented by $\mathcal{Y} = \{E, J\}$.

6.4.1 Pure-strategy Equilibria

PAYOFF MATRIX \mathbf{R} OF THE STRATEGIC FORM OF THE MIMO WIRETAP GAME.

		Eve	
		<i>Eavesdrop (E)</i>	<i>Jam Bob (J)</i>
Alice	<i>Full Power (F)</i>	R_{FE}	R_{FJ}
	<i>Artificial Noise (A)</i>	R_{AE}	R_{AJ}

Figure 6.2: Payoff matrix \mathbf{R} of the strategic MIMO wiretap game.

The strategic form of the game can be represented by the 2×2 payoff matrix \mathbf{R} in Fig. 6.2. Our first result establishes the existence of Nash equilibria for the strategic

game.

Proposition 1: For an arbitrary set of antenna array sizes, transmit powers and channel gain parameters, the following unique pure-strategy saddle-points or Nash Equilibria (NE) (x^*, y^*) exist in the proposed MIMO wiretap game:

$$\mathbf{R}(x^*, y^*) = \begin{cases} R_{AE} & \text{if } R_{AE} \leq R_{AJ} \\ R_{FJ} & \text{if } R_{FJ} \leq R_{FE}. \end{cases} \quad (6.22a)$$

$$(6.22b)$$

Proof: Of the 24 possible orderings of the four rate outcomes, only six satisfy both conditions (P1)-(P2) of the previous section. Furthermore, it is easy to check that only two of these six mutually exclusive outcomes results in a pure NE. If $R_{AE} \leq R_{AJ}$, then assumptions (P1) and (P2) imply the following rate ordering

$$R_{FJ} \geq R_{AJ} \geq \underbrace{R_{AE}}_{NE} \geq R_{FE}. \quad (6.23)$$

In this case, R_{AE} represents an NE since neither Alice nor Eve can improve their respective payoffs by switching strategies; *i.e.*, the secrecy rate will decrease if Alice chooses to transmit the information signal with full power, and the secrecy rate will increase if Eve decides to jam. Similarly, when $R_{FJ} \leq R_{FE}$, then (P1)-(P2) result in the rate ordering

$$R_{AE} \geq R_{FE} \geq \underbrace{R_{FJ}}_{NE} \geq R_{AJ}, \quad (6.24)$$

and R_{FJ} will be the mutual best response for both players. Evidently only one such ordering can be true for a given wiretap game scenario. ■

6.4.2 Mixed-strategy Equilibria

Proposition 1 establishes that there is no single pure strategy choice that is always optimal for either player if the inequalities in (6.23)-(6.24) are not satisfied. This occurs in four of the six valid rate orderings of the entries of \mathbf{R} that satisfy conditions (P1)-(P2). Therefore, since the minimax theorem guarantees that any finite zero-sum game has a saddle-point in randomized strategies [94], in such scenarios Alice and Eve should randomize over $\mathcal{X} \times \mathcal{Y}$; that is, they should adopt mixed strategies.

Let $\mathbf{p} = (p, 1 - p)$ and $\mathbf{q} = (q, 1 - q)$, $0 \leq p, q \leq 1$, represent the probabilities with which Alice and Eve randomize over their strategy sets $\mathcal{X} = \{F, A\}$ and $\mathcal{Y} = \{E, J\}$, respectively. In other words, Alice plays $x = F$ with probability p , while Eve plays $y = E$ with probability q . Alice obtains her optimal strategy by solving

$$\max_p \min_q \mathbf{p}^T \mathbf{R} \mathbf{q}, \quad (6.25)$$

while Eve optimizes the corresponding minimax problem. For the payoff matrix \mathbf{R} in Fig. 6.2, the optimal mixed strategies and expected value v of the game can be easily derived as [94, 95]

$$\begin{aligned} (p^*, 1 - p^*) &= (R_{AJ} - R_{AE}, R_{FE} - R_{FJ})/D \\ (q^*, 1 - q^*) &= (R_{AJ} - R_{FJ}, R_{FE} - R_{AE})/D \\ v(p^*, q^*) &= (R_{FE}R_{AJ} - R_{FJ}R_{AE})/D, \end{aligned} \quad (6.26)$$

where $D = R_{FE} + R_{AJ} - R_{FJ} - R_{AE}$. A graphical illustration of the saddle-point in mixed strategies as p and q are varied for a specific wiretap channel is shown in Fig. 6.3. For the specified parameters $N_a = 5, N_b = 3, N_e = 4, d = 2, P_a = P_e = 20\text{dB}, g_1 = 1.1, g_2 = 0.9$, the rate ordering turns out to be $R_{AE} = 5.04 > R_{FJ} = 5.02 > R_{AJ} = 2.85 > R_{FE} = 0$, which results in a mixed NE with optimal mixing

probabilities ($p^* = 0.3, q^* = 0.3$) and value $v = 3.45$. Alice’s bias towards playing $x = A$ more frequently is expected since that guarantees a secrecy rate of at least 2.85, whereas playing $x = F$ risks a worst-case payoff of zero. Eve is privy to Alice’s reasoning and is therefore biased towards playing $y = J$ more frequently since she prefers a game value close to R_{AJ} .

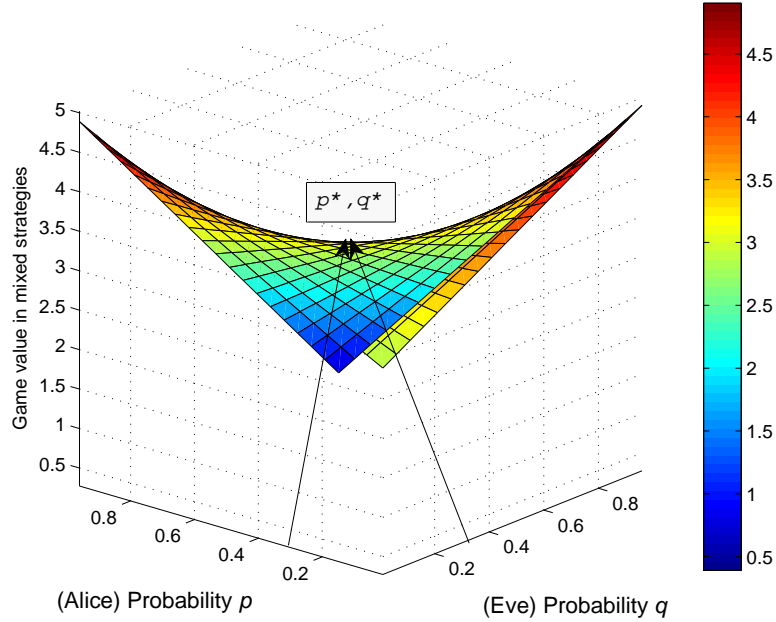


Figure 6.3: Game value in mixed strategies as the mixing probabilities at Alice and Eve are varied, $N_a = 5, N_b = 3, N_e = 4, d = 2, P_a = P_e = 20\text{dB}$, and $g_1 = 1.1, g_2 = 0.9$.

The *repeated* wiretap game is a more sophisticated game model in which Alice and Eve play against each other repeatedly over multiple stages in time. At each stage in time, the set of player strategies and payoff function representation is identical to the single-stage zero-sum game \mathbf{R} in Fig. 6.2. If the game is played over a finite number of stages, then in each stage the players will continue to play their single-stage game NE strategies. On the other hand, if the game is repeated over an infinite time horizon, then with the introduction of a discounting factor the players may be able to improve upon their max-min payoffs [94, Ch. 7].

6.4.3 Wiretap Channel Parameters

We are now in a position to examine a number of wiretap channel configurations and determine what the equilibrium outcomes of the corresponding game would be. In particular, we isolate either N_e or P_e relative to Alice and Bob's parameters, while assuming other variables are of comparable magnitude.

Case 1: All users have the same number of antennas, $N_a = N_b = N_e$ and comparable power $P_a \approx P_e$:

- If Eve is proximate to Alice ($g_1 \gg 1, g_2 \rightarrow 0$), then applying $F(\beta, 0) \approx 0$, $F(\beta, \infty) \approx \log(\alpha)$ in (6.18)-(6.21), the resultant rate ordering is given by (6.23) with a pure NE in R_{AE} . This outcome is in accordance with Eve being very near to Alice, and therefore being much more capable of driving the secrecy rate to zero by eavesdropping as compared to jamming Bob from a distance.
- If Eve is proximate to Bob ($g_2 \gg 1, g_1 \rightarrow 0$), the resultant rate ordering is given by (6.24), and we have a pure NE in R_{FJ} . Eve can exploit her proximity to Bob to completely drown the signal received at Bob's antenna array from Alice via jamming.

Case 2: Eve has more antennas than Alice and Bob ($N_e > N_a = N_b$) and comparable power $P_a \approx P_e$:

- If $N_e \geq 3(N_a + N_b)$ in the large-antenna regime, then [18] showed that the MIMO secrecy capacity with complete eavesdropper CSI is zero almost surely, which implies that the secrecy rate with artificial noise is also zero. Therefore, we have the rate ordering of (6.23), and a pure NE in R_{AE} .
- If $N_a < N_e < 3(N_a + N_b)$, as N_e approaches N_a , i.e., as R_{AE} and R_{FE} increase

from zero, the game outcome changes to a mixed NE for the value of N_e at which the rate ordering changes to $R_{FJ} \geq R_{AE} \geq R_{AJ} \geq R_{FE}$.

Case 3: Eve has fewer antennas than Alice and Bob ($N_e < N_a, N_e < N_b, N_a \geq N_b$) and comparable power $P_a \approx P_e$:

- If $N_e \leq (N_a - d)$, then Eve cannot suppress the artificial interference and therefore she chooses $y = J$ and the NE is R_{FJ} .
- If $(N_b - d) \geq N_e$, then Bob can suppress Eve if she jams and also recover the secret message from Alice, therefore Eve should eavesdrop and the NE is R_{AE} .

Case 4: Highly advantaged eavesdropper:

- $N_e \gg N_a = N_b, P_e = P_a$: If Eve has an insuperable advantage in the size of her antenna array, then for standard values of (g_1, g_2) all four rate outcomes are zero almost surely; both players are indifferent to the choice of strategies.
- $P_e \gg P_a, N_e \approx N_a = N_b$: As $P_e \rightarrow \infty$, we have the rate ordering of (6.24), and a pure NE in R_{FJ} .

For general scenarios not covered above, a mixed-strategy NE as defined in (6.26) is the most probable outcome. Although most of the above outcomes are intuitive, the true utility of the analysis in this section stems from the ability to plug in an arbitrary set of system parameters for the MIMO wiretap game and predict the ensuing (pure or mixed) Nash Equilibrium outcome.

6.5 Extensive Form Wiretap Game

Given the strategic game analysis of the previous section, we can now proceed to analyze the actions of a given player in response to the opponent's strategy. Here, one player is assumed to move first, followed by the opponent's response, which can then lead to a strategy (and code rate) change for the first player, and so on. Accordingly, in this section we examine the sequential or *extensive form* of the MIMO wiretap game, which is also known as a Stackelberg game. We begin with the worst-case scenario where Alice moves first by either playing F or A , which is observed by Eve who responds accordingly. It is convenient to represent the sequential nature of an extensive-form game with a rooted tree or directed graph, as shown in Fig. 6.4. The payoffs for Alice are shown at each terminal node, while the corresponding payoffs for Eve are omitted for clarity due to the zero-sum assumption. In this section, we explore extensive-form games with and without perfect information, and the variety of equilibrium solution concepts available for them.

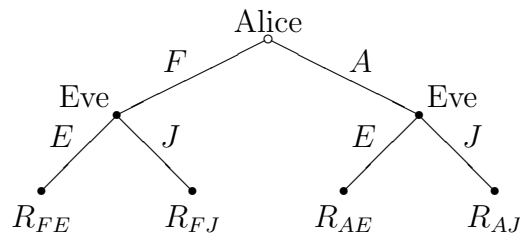


Figure 6.4: Extensive form game tree with perfect information $\Gamma^{e,1}$ where Alice moves first and Eve moves second.

6.5.1 Perfect Information

Assuming that Eve can distinguish which move was adopted by Alice, and furthermore determine the exact jamming power $(1-\rho)P_a$ if she is being jammed by Alice, then the

extensive game is classified as one of *perfect information*. In the sequel, we will make use of the notions of an *information state* and a *subgame*. A player's information state represents the node(s) on the decision tree at which she must make a move conditioned on her knowledge of the previous move of the opponent. For the case of perfect information in Fig. 6.4, Alice has a single information state, while Eve has two information states (each with a single node) based on Alice's choice, since she has perfect knowledge of Alice's move. A subgame is a subset (subgraph) of a game that starts from an information state with a single node, contains all of that node's successors in the tree, and contains all or none of the nodes in each information state [94].

Next, we analyze *subgame-perfect equilibria* (SPE) of the extensive game, which are a more refined form of NE that eliminate irrational choices within subgames [94,95]. It is well known that in extensive games with perfect information, a sequential equilibrium in pure strategies is guaranteed to exist [94, Theorem 4.7]. The equilibrium strategies can be obtained by a process of backward induction on the extensive game tree, as shown below.

Proposition 2: In the extensive form wiretap game $\Gamma^{e,1}$ with perfect information where Alice moves first, the unique subgame-perfect equilibrium in pure strategies is determined by the following:

$$\text{SPE}(\Gamma^{e,1}) = \begin{cases} R_{AE} & \text{if } R_{AE} \leq R_{AJ} & (6.27a) \\ R_{FJ} & \text{if } R_{FJ} \leq R_{FE} & (6.27b) \\ \max[R_{FE}, R_{AJ}] & \text{if } R_{FE} \leq R_{FJ} \text{ and } R_{AJ} \leq R_{AE} & (6.27c) \end{cases}$$

Proof: The extensive game tree for this problem, depicted in Fig. 6.4, is comprised of three subgames: the two subgames at Eve's decision nodes, and the game itself with Alice's decision node as the root. Consider the scenario $R_{FE} \leq R_{FJ}$ and $R_{AJ} \leq R_{AE}$.

Under this assumption, Eve always plays E in the lower-left subgame of Fig. 6.4, whereas Eve picks J in the lower-right subgame. By backward induction, Alice then chooses the larger of $[R_{FE}, R_{AJ}]$ at her decision node. The other two SPE outcomes can be established in a similar manner. ■

Proposition 3: The extensive form game $\Gamma^{e,2}$ with perfect information where Eve moves first and Alice moves second has the following subgame-perfect equilibrium:

$$\text{SPE}(\Gamma^{e,2}) = \min[R_{FJ}, R_{AE}] . \quad (6.28)$$

Proof: The extensive game tree for this scenario is depicted in Fig. 6.5, and is comprised of three subgames: the two subgames at Alice's decision nodes, and the game itself with Eve's decision node as the root. Based on properties (P1)-(P2), Alice always plays A in the lower-left subgame and F in the lower-right subgame. By backward induction, Eve then chooses the action corresponding to the smaller payoff between $[R_{AE}, R_{AJ}]$ at her decision node. ■

We see from both propositions that, when conditions for one of the pure-strategy NEs hold, the outcome of both $\Gamma^{e,1}$ and $\Gamma^{e,2}$ will be the corresponding NE. This is also true of an extensive game with more than 2 stages; if an NE exists, the overall SPE outcome will be composed of repetitions of this constant result. However, for the case of (6.27c) where no NE exists, a multi-stage extensive game will lead to the players continually alternating through each of the four possible outcomes, depending on which is the most advantageous to a given user at his turn.

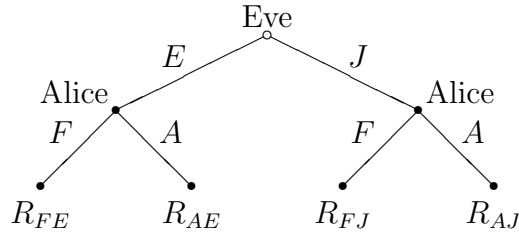


Figure 6.5: Extensive form game tree with perfect information $\Gamma^{e,2}$ where Eve moves first and Alice moves second.

6.5.2 Imperfect Information

A full treatment of the case with imperfect information is beyond the scope of this chapter; here, we will briefly consider the extensive game Γ_f^e between Alice and Eve, where Alice moves first, but Eve is uncertain of the exact strategy adopted by Alice. The game tree representation of $\Gamma_f^{e,1}$ can be drawn by connecting the decision nodes of Eve in Fig. 6.4 to indicate her inability to correctly determine Alice's move in the initial phase of the game. Thus, in this case, Eve effectively only possesses a single information state. While no player has an incentive to randomize in the game with perfect information in Section 6.5.1, mixed strategies enter the discussion when the game is changed to one of imperfect information. The subgame perfect equilibrium solution is generally unsatisfactory for such games, since the only valid subgame in this case is the entire game $\Gamma_f^{e,1}$ itself. Therefore, *sequential equilibrium* is a stronger solution concept better suited for extensive games of imperfect information.

Consider the special case where it is common knowledge at all nodes that Eve is completely unable to determine what move was made by Alice in the first stage of the game. Let Eve assign the *a priori* probabilities $(\alpha, 1 - \alpha)$ to Alice's moves over $\{F, A\}$ for some ρ and d , while Eve herself randomizes over $\{E, J\}$ with probabilities $(\gamma, 1 - \gamma)$. Therefore, Eve's left and right decision nodes are reached with probability α and $(1 - \alpha)$, respectively. There are three possible supports for Eve's moves at

her information state: pure strategies $\{E\}$ or $\{J\}$ exclusively, or randomizing over $\{E, J\}$. In the general scenario where Eve randomizes over $\{E, J\}$ with probabilities $(\gamma, 1 - \gamma)$, her expected payoff can be expressed as

$$-\alpha [\gamma R_{FE} + (1 - \gamma) R_{FJ}] + (\alpha - 1) [\gamma R_{AE} + (1 - \gamma) R_{AJ}].$$

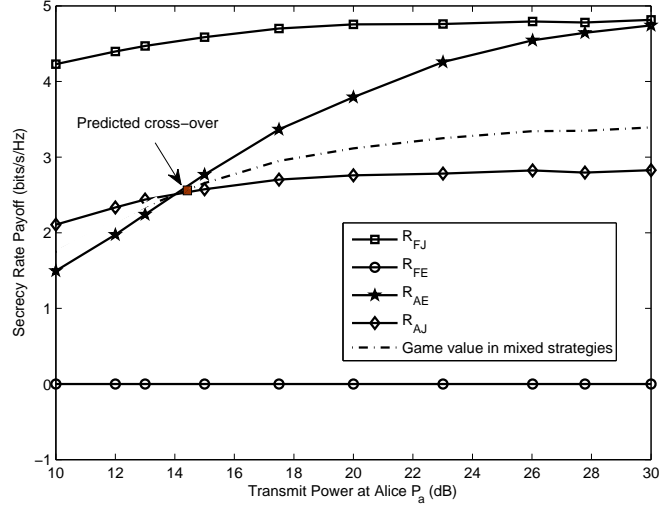
Using a probabilistic version of backward induction, it is straightforward to compute the sequential equilibrium of $\Gamma_f^{e,1}$, which in fact turns out to be identical to the mixed-strategy NE in (6.26).

In a more realistic setting, Eve would have to form her beliefs about Alice's move (F or A) from a binary hypothesis test based on her received signal \mathbf{y}_e . Since Alice has no means of estimating the beliefs possessed by Eve, Alice can stick to playing her maximin strategy to protect herself, although the optimality of such a decision, and whether Eve should assume Alice is playing pure or mixed strategies has not been completely resolved [96]. For the dual game $\Gamma_f^{e,2}$ where Eve moves first, Bob must carry out a hypothesis test to discern Eve's move, and then report back to Alice to help her form a belief vector.

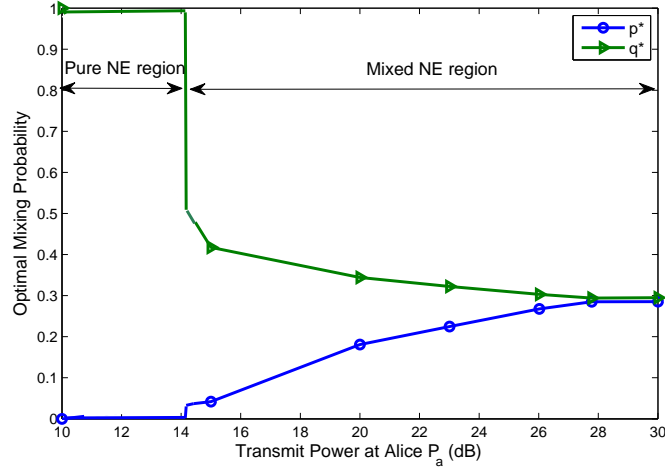
6.6 Simulation Results

In this section, we present several examples that show the equilibrium secrecy rate payoffs for various channel and user configurations. All displayed results are based on the *actual* numerically computed secrecy rates with 5000 independent trials per point, and not on the bounds in (6.18)-(6.21). The bounds were used to determine thresholds on the system parameters where changes in strategy for Alice and Eve occur, and it will be seen that these are in good agreement with the actual computed

secrecy rate transition points. In all of the simulations, the noise power was assumed to be the same for both Bob and Eve: $\sigma_b^2 = \sigma_e^2 = 1$.



(a) Resulting secrecy rates.



(b) Optimal mixing probabilities.

Figure 6.6: Strategic MIMO wiretap game for $P_e = 4P_a$, $N_a = N_e = 8$, $N_b = 6$, $d = 4$, $g_1 = 1.2$, $g_2 = 0.75$ as a function of the transmit power at Alice.

For the strategic game in Fig. 6.6 we set $N_a = N_e = 8$, $N_b = 6$, and Eve's power is larger than Alice's: $P_e = 4P_a$. The optimal choice for the signal dimension in this scenario is $d = 4$. In Fig. 6.6(a), the predicted cross-over point for rates R_{AE} and R_{AJ} is computed numerically from (6.18)-(6.19). Prior to the cross-over, a pure strategy

NE in R_{AE} is the game outcome since the rate ordering is that of (6.23), whereas after the cross-over it is optimal for both players to play mixed strategies according to (6.26). In this case, randomizing strategies clearly leads to better payoffs for the players as Eve's jamming power increases, compared to adopting a pure strategy. The optimal mixing probabilities are shown in Fig. 6.6(b) with a clear division between pure and mixed strategy NE regions.

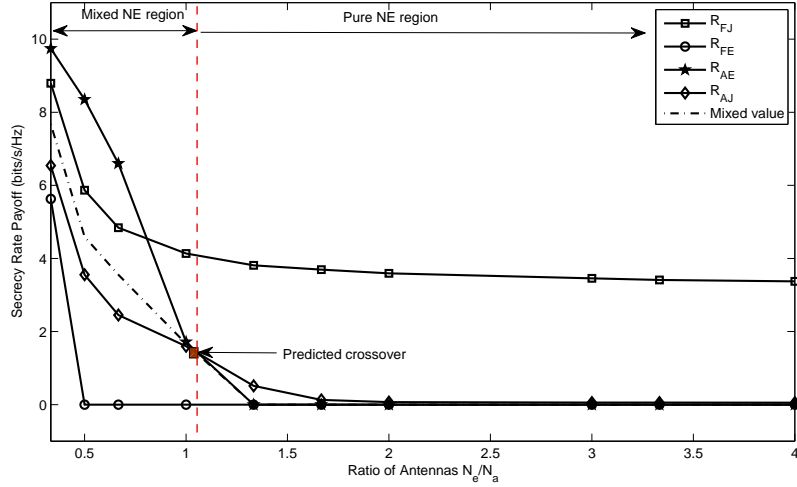


Figure 6.7: Payoff versus antenna ratio N_e/N_a for fixed transmit powers $P_e = P_a = 100$ and $N_a = 6, N_b = 3, d = 2, g_1 = 1.1, g_2 = 0.9$.

For the case of equal transmit powers $P_e = P_a = 100$ and parameters $N_a = 6, N_b = 3, d = 2$, the outcomes of the strategic game as the ratio of eavesdropper to transmitter antennas varies is shown in Fig. 6.7. We observe that a similar dichotomy exists between a pure-strategy saddle-point region and a mixed-strategy equilibrium in terms of N_e/N_a (with the transition roughly at $(N_e/N_a) = 1$ marked by the dashed red line). The theoretical crossover point for rates R_{AE} and R_{FJ} , which marks the transition from a pure strategy NE to a mixed strategy NE, is obtained by numerically comparing (20) and (6.21).

Next, the subgame-perfect outcomes of the two extensive-form games $\Gamma^{e,1}$ and $\Gamma^{e,2}$ over a range of transmit power ratios P_e/P_a are shown in Fig. 6.8. The red and

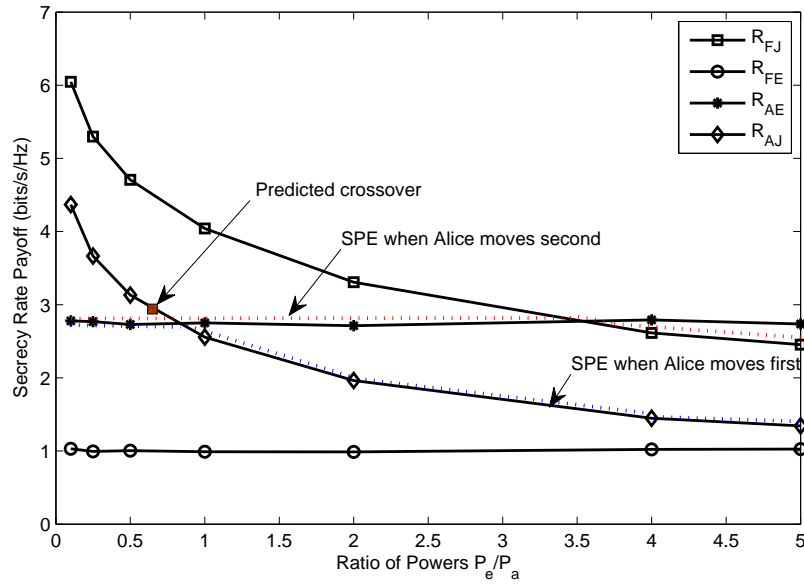


Figure 6.8: Extensive-form games with perfect information, $N_a = N_b = N_e = 3$, $P_a = 20dB$, $d = 1$, $g_1 = 0.8$, $g_2 = 1.1$.

blue dotted lines represent the subgame-perfect outcomes of the game where Alice moves first or second, respectively, as defined in Proposition 2 and Corollary 1. In the extensive form game, Alice could adjust her transmission parameters (ρ , d , \mathbf{T} , etc.) in addition to her overall strategy (A or F) in response to Eve's move. For simplicity, and to allow us to present the main result in a single figure, we have assumed instead that the transmission parameters are chosen independently of Eve's actions, as described for the strategic game. Observe that prior to the crossover point of R_{AE} and R_{AJ} , both equilibria are equal as determined by Proposition 2, since a pure-strategy NE results. We see that it is always beneficial for Alice to move second especially as Eve's jamming power increases, which agrees with intuition.

Finally, in Fig. 6.9 we examine the special case of the single-antenna wiretap channel with the same transmit powers and channel scale factors as the MIMO case of Fig. 6.8. We observe that there is no longer any benefit in using artificial noise since R_{AE} and R_{FE} coincide. This indicates that in the SISO case with the above parameters,

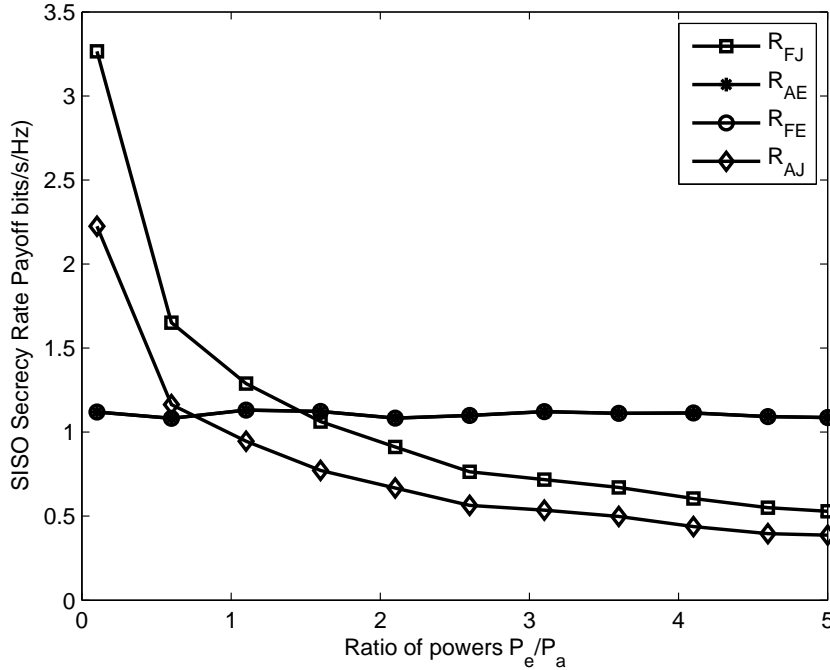


Figure 6.9: Single-antenna wiretap channel with $N_a = N_b = N_e = 1$, $P_a = 20dB$, $d = 1$, $g_1 = 0.8$, $g_2 = 1.1$

Alice has only one strategy to play and the nominal two-person game is reduced to a single-person optimization problem for Eve. Thus, the SISO counterpart of the MIMO wiretap game is generally lacking in strategic possibilities, and it is much more instructive to examine the transmitter-eavesdropper interactions in a multi-antenna setting.

6.7 Summary

We have formulated the interactions between a multi-antenna transmitter and a dual-mode eavesdropper/jammer as a zero-sum game with the MIMO secrecy rate as the payoff function. We began by developing simple yet accurate closed-form expressions for the various secrecy rate outcomes of the game, and then examined the conditions under which Nash equilibria existed in pure and mixed strategies for the strategic

version of the game. We also investigated subgame-perfect and sequential equilibria in the extensive forms of the game with and without perfect information. Our numerical results demonstrated the accuracy of the approximate secrecy rate expressions, and showed that a change in a single parameter set while others remain constant can shift the equilibrium from a pure to a mixed NE outcome or vice versa.

Chapter 7

Robust MIMO CR Transmissions for Primary Secrecy

7.1 Background

We have seen thus far that one mechanism to increase the security of wireless communications links when the channel state of the eavesdropper is unknown is to transmit ‘artificial interference’ simultaneously with the confidential data. The idea is to selectively increase the interference seen by the eavesdropper in such a way that her channel is degraded while the channel of the legitimate receiver is not. The artificial interference can be generated by the transmitter itself [19],[20], or by ‘helpers’ that are deployed for the sole purpose of jamming the eavesdropper [97]. The cooperative jamming signals from helpers generally comprise either white Gaussian noise, or dummy codewords that are independent of the actual confidential message.

This concept was further extended by [98–100] in the context of underlay cognitive radio (CR) networks, where it was suggested that the CR transmit signals could also

serve as cooperative jamming signals to shield the primary link. The idea is that the CR transmissions would serve a dual purpose of jamming the eavesdropper while simultaneously communicating meaningful information to the underlay receivers. The primary network would then have an incentive to allow concurrent co-channel transmissions by the CRs, as long as the CR interference to the primary receiver (PR) is limited to be below a prescribed threshold. The analysis in [98,99] is restricted to single-antenna networks, while [100] considers a multi-antenna UCT with a single UCR. Furthermore, [98–100] all assume perfect CSI at all nodes. It is clear that when the CRs have only imperfect CSI available to them, the security of the primary link can be severely degraded since the CR interference to the PR cannot be effectively controlled, and the jamming signals cannot accurately target the eavesdropper. With this as motivation, we focus on devising robust CR transmission schemes that reduce the degradation in primary secrecy rate due to imperfect CSI for more general settings where the primary and secondary users potentially have multiple antennas. Our simulations indicate that the proposed robust schemes yield a significant improvement in performance compared to methods that do not take the imperfect CSI into account.

7.2 Mathematical Model

7.2.1 Network Model

The general network is as described in Chapter 2 with a multiple-access channel configuration for the underlay system, and an additional passive eavesdropper Eve. Each UCT is equipped with N_a antennas while the common UCR has N_s antennas, and Eve is assumed to have N_e antennas.

The PT wishes to transmit a confidential signal $\mathbf{x}_p \in \mathbb{C}^{N_p \times 1}$ to the PR, while each

underlay UCT sends a unique signal $\mathbf{x}_s \in \mathbb{C}^{N_a \times 1}$, $s = 1, \dots, K_s$, to the UCR. The PT and UCTs are assumed to employ Gaussian signaling such that $\mathbf{x}_p \sim \mathcal{CN}(\mathbf{0}, \mathbf{Q}_p)$ and $\mathbf{x}_s \sim \mathcal{CN}(\mathbf{0}, \mathbf{Q}_s)$, where $\mathbf{Q}_p = \mathcal{E}\{\mathbf{x}_p \mathbf{x}_p^H\}$, $\mathbf{Q}_s = \mathcal{E}\{\mathbf{x}_s \mathbf{x}_s^H\}$, with corresponding average transmit power constraints $\text{Tr}(\mathbf{Q}_p) \leq P_t$ and $\text{Tr}(\mathbf{Q}_s) \leq P_s$ for all s . Eve is interested in decoding *only the primary signal*, which implies that the UCT signals potentially degrade her interception capability; however they also add to the interference at the PR.

The received signal at the PR is

$$\mathbf{y}_p = \mathbf{H}_p \mathbf{x}_p + \sum_{s=1}^{K_s} \mathbf{G}_s \mathbf{x}_s + \mathbf{n}_p, \quad (7.1)$$

where $\mathbf{H}_p \in \mathbb{C}^{r_p \times N_p}$ is the primary channel and $\mathbf{G}_s \in \mathbb{C}^{r_p \times N_a}$ is the interfering channel from UCT s , and $\mathbf{n}_p \sim \mathcal{CN}(\mathbf{0}, \sigma_p^2 \mathbf{I})$ is zero-mean complex additive Gaussian noise.

The received signal at the UCR is

$$\mathbf{y}_s = \sum_{s=1}^{K_s} \mathbf{H}_s \mathbf{x}_s + \mathbf{F}_p \mathbf{x}_p + \mathbf{n}_s, \quad (7.2)$$

where $\mathbf{H}_s \in \mathbb{C}^{N_s \times N_a}$ is the channel from UCT s , $\mathbf{F}_p \in \mathbb{C}^{N_s \times N_p}$ is the interfering channel from the PT, and $\mathbf{n}_s \sim \mathcal{CN}(\mathbf{0}, \sigma_s^2 \mathbf{I})$ is additive complex Gaussian noise. According to the underlay CR paradigm [5], the PR declares an upper limit Γ_p on the instantaneous aggregate interference I_p from all UCTs:

$$I_p \triangleq \sum_{s=1}^{K_s} \text{Tr}(\mathbf{G}_s \mathbf{Q}_s \mathbf{G}_s) \leq \Gamma_p. \quad (7.3)$$

Finally, the received signal at Eve is

$$\mathbf{y}_e = \mathbf{H}_e \mathbf{x}_p + \sum_{s=1}^{K_s} \mathbf{F}_s \mathbf{x}_s + \mathbf{n}_e, \quad (7.4)$$

where $\mathbf{H}_e \in \mathbb{C}^{N_e \times N_p}$ is the channel from the PT, $\mathbf{F}_s \in \mathbb{C}^{N_e \times N_a}$ is the interfering channel from UCT s , and $\mathbf{n}_e \sim \mathcal{CN}(\mathbf{0}, \sigma_e^2 \mathbf{I})$ is complex additive Gaussian noise.

In [98] it is assumed that the PR and UCR exchange codebooks and attempt to decode each other's signals, but this may be infeasible since, (1) the PR may be a legacy user incapable of multi-user detection, and (2) allowing the UCR to decode the confidential primary message may defeat the purpose of using UCTs for secrecy. Therefore, in this work the PR and UCR treat each other's signals as noise while decoding their desired signals. Given the above assumptions, the primary secrecy rate is [19],[18]

$$R_{sec} = \log_2 |\mathbf{I} + \mathbf{H}_p \mathbf{Q}_p \mathbf{H}_p^H \mathbf{K}_p^{-1}| - \log_2 |\mathbf{I} + \mathbf{H}_e \mathbf{Q}_p \mathbf{H}_e^H \mathbf{K}_e^{-1}|, \quad (7.5)$$

where the first term is the rate from the PT to the PR which perceives interference-plus-noise covariance matrix $\mathbf{K}_p = \sigma_p^2 \mathbf{I} + \sum_{s=1}^{K_s} \mathbf{G}_s \mathbf{Q}_s \mathbf{G}_s^H$. The second term is the leakage rate to Eve, whose effective interference-plus-noise covariance matrix \mathbf{K}_e depends on the capabilities of the eavesdropper. If Eve is another primary user, it is assumed that she does not know the UCT codebooks and always treats their signals as noise [99], such that

$$\mathbf{K}_e = \sigma_e^2 \mathbf{I} + \sum_{s=1}^{K_s} \mathbf{F}_s \mathbf{Q}_s \mathbf{F}_s^H. \quad (7.6)$$

Alternately, a worst-case assumption could be made that she can jointly decode the PT and UCT signals [98], in which case $\mathbf{K}_e = \sigma_e^2 \mathbf{I}$ if the transmission rates from the PT and UCTs lie within the capacity region of their multiple access channel to Eve, otherwise (7.6) holds. Both eavesdropper scenarios are accommodated in our analysis, as described next.

We assume that the UCTs have neither instantaneous nor statistical CSI of the PT

channels $\{\mathbf{H}_p, \mathbf{H}_e\}$, and thus they cannot directly optimize the primary secrecy rate. Instead, in this chapter we follow the approach of [20, 97], where the UCTs devote unused power and spatial resources for jamming Eve once a desired quality of service has been achieved for their own data. To facilitate the robust designs we consider later, we assume that the PR interference constraint is evenly distributed among UCTs; *i.e.*, each UCT must limit its interference level at the PR to within Γ_p/K_s . Since the secrecy rate is not directly optimized and the artificial interference is “best effort,” the UCT transmit strategies are independent of the eavesdropper capabilities.

7.2.2 CR Transmission with Perfect CSI

To begin, we first consider two CR transmission schemes based on the assumption of perfect CSI; this assumption will be relaxed in the discussion that follows. In the first approach, referred to as *max-rate* transmission, the UCTs attempt to optimize their sum rate to the UCR, while agreeing to jam Eve with a certain minimum interference level I_t :

$$\max_{\mathbf{Q}_s} \log_2 \left| \mathbf{I} + \sum_{s=1}^{K_s} \mathbf{H}_s \mathbf{Q}_s \mathbf{H}_s^H \mathbf{Z}^{-1} \right| \quad (7.7a)$$

$$\text{s.t. } \forall s \quad \text{Tr}(\mathbf{G}_s \mathbf{Q}_s \mathbf{G}_s) \leq \Gamma_p / K_s \quad (7.7b)$$

$$\text{Tr}(\mathbf{F}_s \mathbf{Q}_s \mathbf{F}_s^H) \geq I_t \quad (7.7c)$$

$$\text{Tr}(\mathbf{Q}_s) \leq P_s \quad (7.7d)$$

where $\mathbf{Z} = \sigma_s^2 \mathbf{I} + \mathbf{F}_p \mathbf{Q}_p \mathbf{F}_p^H$ is the UCR interference-plus-noise covariance matrix. The objective function is concave and all constraints are convex in $\{\mathbf{Q}_s\}$, and therefore can be solved efficiently via standard interior-point methods. The feasibility of the problem is dependent on the channel realizations and the stringency of the various interference constraints. If the UCTs acquire the right to share the spectrum based

on monetary payments or leasing, then they may conceivably relax I_t and prioritize their own traffic. However, note that the PR interference cap Γ_p is immutable and must strictly be adhered to by the CR network.

Alternately, the UCTs can attempt to maximize the aggregate jamming power at Eve subject to individual signal-to-noise ratio constraints Γ_s at the UCR, which we denote as *max-jamming* transmission. The corresponding convex (linear) program is

$$\max_{\mathbf{Q}_1, \dots, \mathbf{Q}_{K_s}} \sum_{s=1}^{K_s} \text{Tr}(\mathbf{F}_s \mathbf{Q}_s \mathbf{F}_s^H) \quad (7.8a)$$

$$\text{s.t. } \forall s \quad \text{Tr}(\mathbf{H}_s \mathbf{Q}_s \mathbf{H}_s^H) \geq \Gamma_s \quad (7.8b)$$

$$\text{Tr}(\mathbf{G}_s \mathbf{Q}_s \mathbf{G}_s^H) \leq \Gamma_p / K_s \quad (7.8c)$$

$$\text{Tr}(\mathbf{Q}_s) \leq P_s. \quad (7.8d)$$

In this case, the UCTs give higher priority to the primary secrecy as compared to their own traffic. For example, the primary network may allow the UCTs to share a fraction of the licensed spectrum in exchange for their jamming support. Note that the UCT SNR constraints at the UCR are more tractable compared to individual UCT rate constraints, since the individual rates are coupled by the intra-UCT uplink interference.

7.3 Robust CR Transmission

We now relax the assumption that the UCTs have perfect CSI regarding their channels to the PR and Eve; in particular, we will assume that only imprecise estimates $\tilde{\mathbf{G}}_s$

and $\tilde{\mathbf{F}}_s$ are available. We define the channel errors as

$$\mathbf{E}_s = \mathbf{G}_s - \tilde{\mathbf{G}}_s; \quad \mathbf{L}_s = \mathbf{F}_s - \tilde{\mathbf{F}}_s, \quad (7.9)$$

and we assume they lie in norm bounded uncertainty regions [101–103]:

$$\mathbf{E}_s \in \mathcal{G}_s = \{\mathbf{E}_s : \|\mathbf{E}_s\|_{\mathcal{F}}^2 \leq \Delta_s^2\}; \quad \mathbf{L}_s \in \mathcal{L}_s = \{\mathbf{L}_s : \|\mathbf{L}_s\|_{\mathcal{F}}^2 \leq \delta_s^2\}, \quad (7.10)$$

where Δ_s and δ_s are known constants.

With the above definitions, we focus on developing robust versions of the UCT transmission strategies in (7.7) and (7.8) of the previous section. Beginning with (7.7), we aim to optimize the worst-case performance given the imperfect CSI scenario, so the constraint (7.7b) is rewritten as

$$\max_{\mathbf{E}_s \in \mathcal{G}_s} \text{Tr} \left[(\tilde{\mathbf{G}}_s + \mathbf{E}_s) \mathbf{Q}_s (\tilde{\mathbf{G}}_s + \mathbf{E}_s)^H \right] \leq \Gamma_p / K_s. \quad (7.11)$$

We next convert constraint (7.11) to a set of Linear Matrix Inequalities (LMIs). In particular, note that (7.11) is equivalent to

$$\text{Tr} \left[(\tilde{\mathbf{G}}_s + \mathbf{E}_s) \mathbf{Q}_s (\tilde{\mathbf{G}}_s + \mathbf{E}_s)^H \right] \leq \Gamma_p / K_s, \quad \forall \mathbf{E}_s : \|\mathbf{E}_s\|_{\mathcal{F}}^2 \leq \Delta_s^2, \quad (7.12)$$

which can be expressed in the vector form

$$\begin{aligned} & - \text{vec}(\mathbf{E})^H (\mathbf{Q}_s^T \otimes \mathbf{I}_{N_s}) \text{vec}(\mathbf{E}) - 2\text{Re} \left[\text{vec}(\tilde{\mathbf{G}}_s)^H (\mathbf{Q}_s^T \otimes \mathbf{I}_{N_s}) \text{vec}(\mathbf{E}) \right] \\ & - \text{vec}(\tilde{\mathbf{G}}_s)^H (\mathbf{Q}_s^T \otimes \mathbf{I}_{N_s}) \text{vec}(\tilde{\mathbf{G}}_s) + \frac{\Gamma_p}{K_s} \geq 0, \quad \forall \mathbf{E}_s : -\text{vec}(\mathbf{E}_s)^H \text{vec}(\mathbf{E}) + \Delta_s^2 \geq 0. \end{aligned} \quad (7.13)$$

According to the \mathcal{S} -procedure [104], (7.13) holds if and only if there exists a $\mu_s \geq 0$

such that

$$\begin{bmatrix} (\mu_s \mathbf{I}_{N_a} - \mathbf{Q}_s)^T \otimes \mathbf{I}_{N_s} & -(\mathbf{Q}_s^T \otimes \mathbf{I}_{N_s}) \text{vec}(\tilde{\mathbf{G}}_s) \\ -\text{vec}(\tilde{\mathbf{G}}_s)^H (\mathbf{Q}_s^T \otimes \mathbf{I}_{N_s}) & \frac{\Gamma_p}{K_s} - \text{vec}(\tilde{\mathbf{G}}_s)^H (\mathbf{Q}_s^T \otimes \mathbf{I}_{N_s}) \text{vec}(\tilde{\mathbf{G}}_s) - \mu_s \Delta_s^2 \end{bmatrix} \succeq \mathbf{0}. \quad (7.14)$$

Using the property of generalized Schur complements [104] for (7.14), we have

$$\begin{aligned} & \frac{\Gamma_p}{K_s} - \text{vec}(\tilde{\mathbf{G}}_s)^H (\mathbf{Q}_s^T \otimes \mathbf{I}_{N_s}) \text{vec}(\tilde{\mathbf{G}}_s) - \mu_s \Delta_s^2 \\ & - \text{vec}(\tilde{\mathbf{G}}_s)^H (\mathbf{Q}_s^T \otimes \mathbf{I}_{N_s}) [(\mu_s \mathbf{I}_{N_a} - \mathbf{Q}_s)^T \otimes \mathbf{I}_{N_s}]^\dagger (\mathbf{Q}_s^T \otimes \mathbf{I}_{N_s}) \text{vec}(\tilde{\mathbf{G}}_s) \geq 0, \end{aligned} \quad (7.15)$$

which is equivalent to the following LMIs:

$$\text{Tr}[\tilde{\mathbf{G}}_s (\mathbf{Q}_s + \Phi_s) \tilde{\mathbf{G}}_s^H] + \mu_s \Delta_s^2 \leq \Gamma_p / K_s \quad (7.16)$$

$$\begin{bmatrix} \mu_s \mathbf{I}_{N_a} - \mathbf{Q}_s & \mathbf{Q}_s \\ \mathbf{Q}_s^H & \Phi_s \end{bmatrix} \succeq \mathbf{0}. \quad (7.17)$$

Similarly, for optimizing the worst-case performance of the artificial interference, constraint (7.7c) is rewritten as

$$\min_{\mathbf{L}_s \in \mathcal{L}_s} \text{Tr}(\tilde{\mathbf{F}}_s + \mathbf{L}_s) \mathbf{Q}_s (\tilde{\mathbf{F}}_s + \mathbf{L}_s)^H \geq I_t. \quad (7.18)$$

Using the same procedure as (7.11)-(7.17), assuming a non-negative scalar $\nu \geq 0$ and a Hermitian matrix $\Psi_s \succeq 0$, (7.18) can be converted to the following LMIs:

$$\text{Tr} \left(\tilde{\mathbf{F}}_s (\mathbf{Q}_s - \Psi_s) \tilde{\mathbf{F}}_s^H \right) - \nu_s \delta_s^2 \geq I_t \quad (7.19)$$

$$\begin{bmatrix} \nu_s \mathbf{I}_{N_a} + \mathbf{Q}_s & \mathbf{Q}_s \\ \mathbf{Q}_s^H & \Psi_s \end{bmatrix} \succeq \mathbf{0}. \quad (7.20)$$

Therefore, the robust counterpart of the max-rate strategy in (7.7) under imperfect CSI becomes

$$\max_{\mathbf{Q}_s, \Phi_s, \Psi_s, \mu_s, \nu_s} \log_2 \left| \mathbf{I} + \sum_{s=1}^{K_s} \mathbf{H}_s \mathbf{Q}_s \mathbf{H}_s^H \mathbf{Z}^{-1} \right| \quad (7.21a)$$

$$\text{s.t. } \forall s \quad \begin{bmatrix} \mu_s \mathbf{I}_{N_a} - \mathbf{Q}_s & \mathbf{Q}_s \\ \mathbf{Q}_s^H & \Phi_s \end{bmatrix} \succeq \mathbf{0} \quad (7.21b)$$

$$\begin{bmatrix} \nu_s \mathbf{I}_{N_a} + \mathbf{Q}_s & \mathbf{Q}_s \\ \mathbf{Q}_s^H & \Psi_s \end{bmatrix} \succeq \mathbf{0} \quad (7.21c)$$

$$\text{Tr}[\tilde{\mathbf{G}}_s (\mathbf{Q}_s + \Phi_s) \tilde{\mathbf{G}}_s^H] + \mu_s \Delta_s^2 \leq \Gamma_p / K_s \quad (7.21d)$$

$$\text{Tr}(\tilde{\mathbf{F}}_s (\mathbf{Q}_s - \Psi_s) \tilde{\mathbf{F}}_s^H) - \nu_s \delta_s^2 \geq I_t \quad (7.21e)$$

$$\text{Tr}(\mathbf{Q}_s) \leq P_s, \mu_s \geq 0, \nu_s \geq 0 \quad (7.21f)$$

$$\mathbf{Q}_s \succeq \mathbf{0}, \Phi_s \succeq \mathbf{0}, \Psi_s \succeq \mathbf{0}. \quad (7.21g)$$

This is a convex problem involving the maximization of a concave objective function over a set of convex LMI and linear constraints, and can be solved using standard convex optimization procedures.

Proceeding to the max-jamming strategy, we first give an equivalent form of the perfect CSI case in (7.8) as

$$\max_{\mathbf{Q}_s, \dots, \mathbf{Q}_{K_s} \succeq \mathbf{0}, \mathbf{m} \succeq \mathbf{0}} \mathbf{m}^T \mathbf{1} \quad (7.22a)$$

$$\text{s.t. } \forall s \quad \text{Tr}(\mathbf{F}_s \mathbf{Q}_s \mathbf{F}_s^H) \geq m_s \quad (7.22b)$$

$$\text{Tr}(\mathbf{H}_s \mathbf{Q}_s \mathbf{H}_s^H) \geq \Gamma_s \quad (7.22c)$$

$$\text{Tr}(\mathbf{G}_s \mathbf{Q}_s \mathbf{G}_s^H) \leq \Gamma_p / K_s \quad (7.22d)$$

$$\text{Tr}(\mathbf{Q}_s) \leq P_s, \quad (7.22e)$$

where $\mathbf{m} = [m_1, \dots, m_s, \dots, m_{K_s}]^T$. Using an approach similar to the solution of (7.7) with imperfect CSI, the corresponding robust counterpart of (7.8) can be shown to be

$$\max_{\mathbf{Q}_s, \Phi_s, \Psi_s, \mu_s, \nu_s, \mathbf{m}} \mathbf{m}^T \mathbf{1} \quad (7.23a)$$

$$\text{s.t. } \forall s \quad \begin{bmatrix} \mu_s \mathbf{I}_{N_a} - \mathbf{Q}_s & \mathbf{Q}_s \\ \mathbf{Q}_s^H & \Phi_s \end{bmatrix} \succeq \mathbf{0} \quad (7.23b)$$

$$\begin{bmatrix} \nu_s \mathbf{I}_{N_a} + \mathbf{Q}_s & \mathbf{Q}_s \\ \mathbf{Q}_s^H & \Psi_s \end{bmatrix} \succeq \mathbf{0} \quad (7.23c)$$

$$\text{Tr}[\tilde{\mathbf{G}}_s(\mathbf{Q}_s + \Phi_s)\tilde{\mathbf{G}}_s^H] + \mu_s \Delta_s^2 \leq \Gamma_p / K_s \quad (7.23d)$$

$$\text{Tr}(\tilde{\mathbf{F}}_s(\mathbf{Q}_s - \Psi_s)\tilde{\mathbf{F}}_s^H) - \nu_s \delta_s^2 \geq m_s \quad (7.23e)$$

$$\text{Tr}(\mathbf{H}_s \mathbf{Q}_s \mathbf{H}_s^H) \geq \Gamma_s \quad (7.23f)$$

$$\text{Tr}(\mathbf{Q}_s) \leq P_s, \mu_s \geq 0, \nu_s \geq 0 \quad (7.23g)$$

$$\mathbf{Q}_s \succeq \mathbf{0}, \Phi_s \succeq \mathbf{0}, \Psi_s \succeq \mathbf{0}, \mathbf{m} \succeq \mathbf{0}. \quad (7.23h)$$

The robust max-jamming algorithm above is a semi-definite program with a linear objective function and a set of LMI and linear constraints, and like (7.21) can be solved using standard convex optimization procedures.

7.4 Numerical Results

We present some examples that compare the performance of the proposed robust UCT strategies with non-robust methods that ignore the imperfect CSI. In all simulations, the channels and background noise samples are assumed to be composed of independent, zero-mean Gaussian random variables with unit variance. The convex

optimization programs are solved using the `cvx` MATLAB toolbox [73]. We focus on the case where the eavesdropper is another primary user and always treats the UCT signals as noise. In all cases, we set the number of secondary users to be 2 ($K_s = 2$), all nodes are assumed to have two antennas ($N_p = r_p = N_s = N_e = 2$), except the UCT whose number of antennas will vary, $I_t = 8$ for max-rate transmission, and $\Gamma_s = 5$ for max-jamming. Without loss of generality, the PT adopts uniform power allocation such that $\mathbf{Q}_p = (P_t/N_p) \mathbf{I}$.

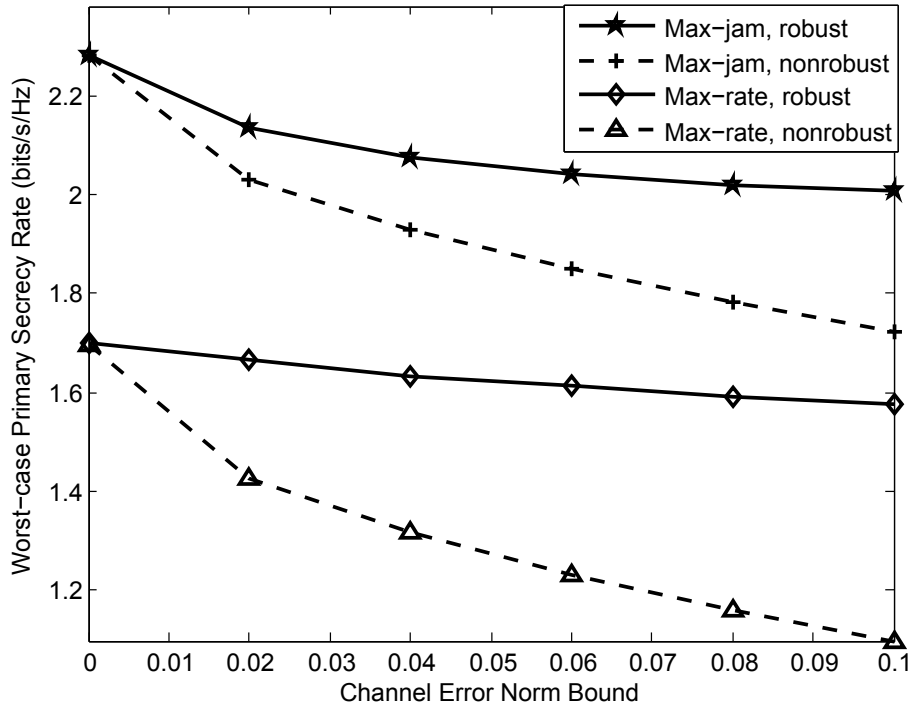


Figure 7.1: Primary secrecy rate versus UCT CSI error, $K_s = N_p = N_a = N_r = N_s = 2$.

Fig. 7.1 illustrates the performance of the algorithms as the size of the worst-case channel errors ($\Delta_s^2 = \delta_s^2$) are varied from zero to 0.1, with fixed powers $P_t = 10\text{dB}$, $P_s = 5\text{dB}$, PR interference threshold $\Gamma_p = 8$, and $N_a = 2$. The robust max-rate and max-jamming schemes provide a significantly enhanced worst-case secrecy rate for the primary link as the severity of the CSI imperfection increases. At the same time, the robust schemes are guaranteed to conform to the PR interference cap, which is a

critical aspect of the underlay CR paradigm. While the max-jam approach is better than the max-rate approach in terms of PR secrecy for this example, the relative performance of the two methods will depend on the choices for I_t and Γ_s .

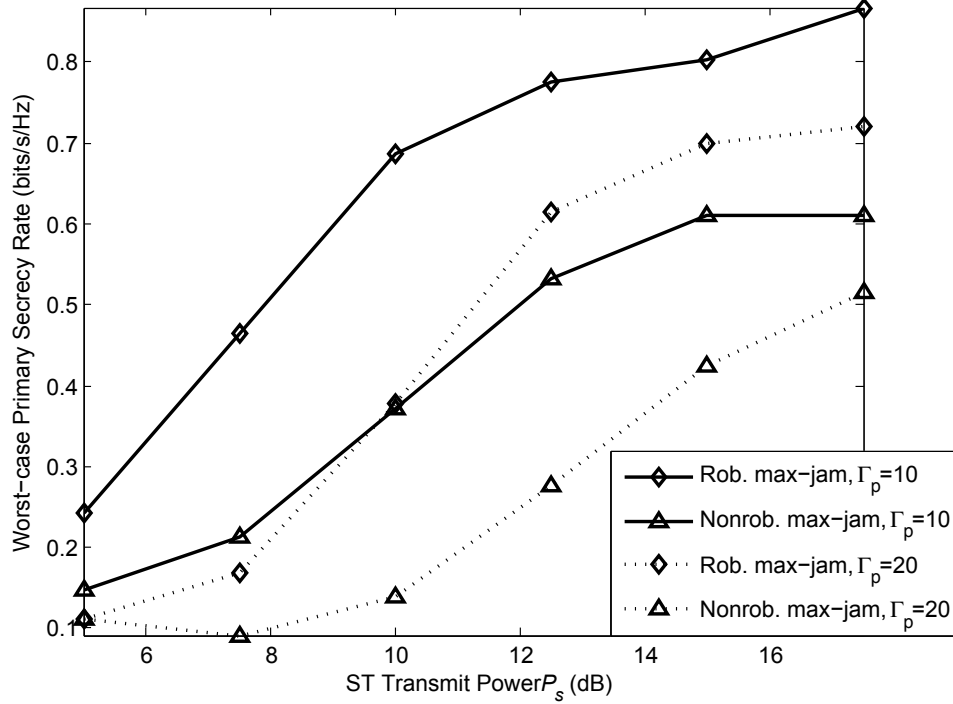


Figure 7.2: Primary secrecy rate versus UCT transmit power, $N_a = 5$, $\Delta_s^2 = \delta_s^2 = 0.075$.

Fig. 7.2 depicts the robust and naïve max-jamming PT worst-case secrecy performance with thresholds $\Gamma_p = 10$ and $\Gamma_p = 20$ as the UCT transmit power increases, for $P_t = 1.5$ dB, $N_a = 5$, and fixed channel error bounds $\Delta_s^2 = \delta_s^2 = 0.075$. Since the UCTs are endowed with significantly larger antenna arrays and transmit powers than the primary link, the inadvertent interference to the PR and the less selective eavesdropper jamming can severely degrade the PR performance if the imperfect CSI is not accounted for. Interestingly, a smaller choice of Γ_p improves the secrecy rate since the PR is especially susceptible to UCT interference given the low PT transmit power, even though the larger Γ_p offers more leeway in jamming the eavesdropper.

7.5 Summary

Underlay CR transmissions can serve the dual purpose of jamming passive eavesdroppers while communicating meaningful information to the underlay receivers, as long as the CR interference to the primary receiver is limited to be below a prescribed threshold. However, it is demonstrated that when the CRs have only imperfect CSI available to them, the security of the primary link can be severely degraded since the CR interference to the PR cannot be controlled effectively, and the jamming signals cannot accurately target the eavesdropper. In this chapter we have presented two categories of robust multi-antenna CR transmission schemes that reduce the degradation in primary secrecy rate under imperfect CSI. Numerical results verify the significant improvement in performance of the proposed robust schemes compared to methods that do not take the imperfect CSI into account.

Chapter 8

Remarks

8.1 Recapitulation

The underlying theme of this dissertation has been the development of multi-antenna transmission techniques for interference mitigation and/or secure communication in multi-user wireless networks, with emphasis on robust designs for scenarios with imperfect channel state information.

In Chapter 2, as an example of the coexistence issue, we examined a novel underlay MIMO cognitive radio network where the CR has a complete lack of knowledge of its interfering channels to primary receivers. We then proposed a rank minimization precoding strategy for such uninformed underlay MIMO CR systems, assuming a minimum information rate must be guaranteed on the CR main channel. We presented a simple frugal waterfilling approach that can be used to find the minimum rank transmit covariance that achieves the desired CR rate with minimum power. We also presented two alternatives to FWF that are based on convex approximations to the min-rank criterion, one that leads to conventional waterfilling for our CR problem,

and another based on a log-determinant heuristic. The CWF approach turns out to be a poor approximation to the min-rank objective, while the log-det approach provides performance similar to FWF, although FWF consistently leads to the highest throughput for the primary link. We also observed that reducing the interference temperature metric is surprisingly not consistent with improving the PR throughput; in particular, FWF has the highest interference temperature of the algorithms studied, but also leads to the highest PR rate. As an alternative, we proposed an interference leakage metric that is a better indicator of the impact of the CR on the primary link.

We then presented a novel heterogeneous dynamic spectrum access network in Chapter 3 where the primary users coexist with both underlay (UCRs) and interweave cognitive radios (ICRs); all terminals being potentially equipped with multiple antennas. We investigated the design of MIMO precoding algorithms for the UCRs so as to increase the detection probability at the ICRs, while simultaneously meeting a desired Quality-of-Service target to its own receivers and constraining interference leaked to PUs. The objective of such a proactive approach, referred to as *prescient* precoding, is to minimize the probability of interference from ICRs to the UCR and PU receivers due to imperfect spectrum sensing. We began with three different downlink prescient precoding algorithms for a plurality of single-antenna UCR and multi-antenna PUs/ICRs. We then presented prescient block-diagonalization algorithms for the MIMO underlay downlink where spatial multiplexing is performed for multiple multi-antenna UCR receivers. Numerical experiments demonstrated that prescient precoding by the UCT preemptively mitigates missed detections at the ICRs, and provides a significantly pronounced performance gain in underlay sum rate compared to conventional precoding strategies.

Turning to the secure MIMO transmission problem, in Chapter 4 we examined the impact of imperfect knowledge of the legitimate channel on the achievable secrecy

rate of the MIMO wiretap channel. Under such unfavorable conditions, the naïve employment of artificial interference to jam passive eavesdroppers is seen to significantly degrade the SINR of the legitimate receiver. We first analytically characterized this performance degradation based on a second-order perturbation analysis of the singular value decomposition. To reduce the impact of the CSI errors, we proposed two robust beamforming schemes that are able to recover a large fraction of the SINR lost due to the channel estimation errors. These techniques were shown to perform very well for moderate CSI errors, but ultimately a large enough channel mismatch can eliminate the secrecy advantage of using artificial noise.

In Chapter 5, we considered a more formidable adversary capable of either eavesdropping or jamming in the MIMO wiretap channel. We formulated the interactions between the multi-antenna transmitter and the dual-mode eavesdropper/jammer as a zero-sum game with the MIMO ergodic secrecy rate as the payoff function. We began by developing simple yet accurate closed-form expressions for the various secrecy rate outcomes of the game, and then examined the conditions under which Nash equilibria existed in pure and mixed strategies for the strategic version of the game. We also investigated subgame-perfect and sequential equilibria in the extensive forms of the game with and without perfect information. Our numerical results demonstrated the accuracy of the approximate secrecy rate expressions, and showed that a change in a single parameter set while others remain constant can shift the equilibrium from a pure to a mixed Nash Equilibrium outcome or vice versa.

The culmination of this work was to bring together the coexistence and confidentiality aspects in Chapter 6, where we considered a MIMO cognitive radio network where the CR transmissions serve a dual purpose of jamming the eavesdropper while communicating meaningful information to the underlay receivers, but the CR interference to the primary receiver (PR) must also be limited to a prescribed threshold.

When only imperfect CSI is available to the CRs, the primary link security is severely degraded since the CR interference to the PR cannot be effectively controlled, and the jamming signals cannot accurately target the eavesdropper. Therefore, we devised robust CR transmission schemes for more general multi-antenna networks that reduce the degradation in primary secrecy rate under imperfect CSI. The proposed robust methods provided significantly better secrecy performance than methods that did not take imperfect CSI into account.

8.2 Future Directions

A number of avenues for further research can be discerned for the aspect of coexistence and interference mitigation. It would be useful to develop information-theoretic upper bounds on the maximal achievable rate or sum rate in the considered networks in order to gauge the optimality (or lack thereof) of the proposed approaches based on linear MIMO precoding. The extension of the MIMO cognitive radio downlink network in Chapters 2 and 3 to a general interference channel scenario with multiple CR transmit-receive pairs is expected to be challenging, and opens the door to incorporation of interference alignment techniques. Finally, cross-layer algorithms that take physical-layer considerations into account for cognitive radio scheduling are of interest, and preliminary progress has been made in this regard.

From the perspective of secure MIMO communications, it would be of significant interest to consider the development of robust methods for MIMO secret key establishment, as opposed to the artificial interference paradigm espoused in this work. In the case of MIMO secret key establishment, the secret key rate is the performance metric instead of the secrecy rate, and determines the number of key bits that can be generated reliably and securely at both Alice and Bob by exploiting a public

communication and feedback channel. Due to the similarity in the mathematical expressions for these metrics, the MIMO transmission schemes presented in this thesis are expected to offer insight into the design of secret key establishment methods as well.

Bibliography

- [1] E. Hossain, D. Niyato, and Z. Han, *Dynamic Spectrum Access and Management in Cognitive Radio Networks*. Cambridge University Press, 2009.
- [2] A. Goldsmith, S. A. Jafar, I. Maric, and S. Srinivasa, “Breaking spectrum gridlock with cognitive radios: An information theoretic perspective,” *Proc. IEEE*, vol. 97, no. 5, pp. 894–914, May 2009.
- [3] J. F.-Segura and X. Wang, “GLRT-based spectrum sensing for cognitive radio with prior information,” *IEEE Trans. Commun.*, vol. 58, no. 7, pp. 2137–2146, Jul. 2010.
- [4] L. B. Le and E. Hossain, “Resource allocation for spectrum underlay in cognitive wireless networks,” *IEEE Trans. Wireless Commun.*, vol. 7, no. 12, pp. 5306–5315, Dec. 2008.
- [5] R. Zhang and Y.-C. Liang, “Exploiting multi-antennas for opportunistic spectrum sharing in cognitive radio networks,” *IEEE J. Sel. Topics Signal Process.*, vol. 2, no. 1, pp. 88–102, Feb. 2008.
- [6] A. Tajer, N. Prasad, and X. Wang, “Beamforming and rate allocation in MISO cognitive radio networks,” *IEEE Trans. Signal Process.*, vol. 58, no. 1, pp. 362–377, Jan. 2010.
- [7] L. Zhang, Y.-C. Liang, Y. Xin, and H. V. Poor, “Robust cognitive beamforming with partial channel state information,” *IEEE Trans. Wireless Commun.*, vol. 8, no. 8, pp. 4143–4153, Aug. 2009.
- [8] E. A. Gharavol, Y.-C. Liang, and K. Moutaah, “Robust downlink beamforming in multiuser MISO cognitive radio networks with imperfect channel-state information,” *IEEE Trans. Veh. Technol.*, vol. 59, no. 6, pp. 2852–2867, Jul. 2010.
- [9] K. T. Phan, S. A. Vorobyov, N. D. Sidiropoulos, and C. Tellambura, “Spectrum sharing in wireless networks via QoS-aware secondary multicast beamforming,” *IEEE Trans. Signal Process.*, vol. 57, no. 6, pp. 2323–2335, Jun. 2009.

- [10] Y. Zhang and A. So, “Optimal spectrum sharing in mimo cognitive radio networks via semidefinite programming,” *IEEE J. Sel. Areas Commun.*, vol. 29, no. 2, pp. 362–373, Feb. 2011.
- [11] O. Besson, S. Kraut, and L. L. Scharf, “Detection of an unknown rank-one component in white noise,” *IEEE Trans. Signal Process.*, vol. 54, no. 7, pp. 2835–2839, Jul. 2006.
- [12] D. Ramirez, G. V.-Vilar, R. L.-Valcarce, J. Va, and I. Santamara, “Detection of rank- p signals in cognitive radio networks with uncalibrated multiple antennas,” *IEEE Trans. Signal Process.*, vol. 59, no. 8, pp. 3764–3774, Aug. 2011.
- [13] B. Schneir, “Cryptographic design vulnerabilities,” *IEEE Computer*, vol. 31, no. 9, pp. 29–33, Sep. 1998.
- [14] A. D. Wyner, “The wire-tap channel,” *The Bell System Technical Journal*, vol. 54, pp. 1355–1387, 1975.
- [15] I. Csiszar and J. Körner, “Broadcast channels with confidential messages,” *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.
- [16] S. Leung-Yan-Cheong and M. Hellman, “The Gaussian wire-tap channel,” *IEEE Trans. Inf. Theory*, vol. 24, no. 4, pp. 451–456, Jul. 1978.
- [17] F. Oggier and B. Hassibi, “The secrecy capacity of the MIMO wiretap channel,” in *Proc. IEEE ISIT*, 2008, pp. 524–528.
- [18] A. Khisti and G. W. Wornell, “Secure transmission with multiple antennas-ii: The MIMOME wiretap channel,” *IEEE Trans. Inf. Theory*, vol. 56, no. 11, pp. 5515–5532, nov. 2010.
- [19] S. Goel and R. Negi, “Guaranteeing secrecy using artificial noise,” *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, Jun. 2008.
- [20] © 2011 IEEE. Reprinted, with permission, from A. Mukherjee and A. L. Swindlehurst, “Robust beamforming for secrecy in MIMO wiretap channels with imperfect CSI,” *IEEE Trans. Signal Process.*, vol. 59, no. 1, pp. 351–361, Jan. 2011.
- [21] W. E. Stark and R. J. McEliece, “On the capacity of channels with block memory,” *IEEE Trans. Inf. Theory*, vol. 34, no. 3, pp. 322–324, Mar. 1988.
- [22] S. N. Diggavi and T. M. Cover, “The worst additive noise under a covariance constraint,” *IEEE Trans. Inf. Theory*, vol. 47, no. 11, pp. 3072–3081, Nov. 2001.
- [23] A. Kashyap, T. Başar, and R. Srikant, “Correlated jamming on MIMO Gaussian fading channels,” *IEEE Trans. Inf. Theory*, vol. 50, no. 9, pp. 2119–2223, Sep. 2004.

- [24] T. Wang and G. B. Giannakis, “Mutual information jammer-relay games,” *IEEE Trans. Inf. Forensics Security*, vol. 3, no. 2, pp. 290–303, Jun. 2008.
- [25] A. Mukherjee and A. L. Swindlehurst, “Detecting passive eavesdroppers in the MIMO wiretap channel,” in *Proc. IEEE ICASSP*.
- [26] —, “Utility of beamforming strategies for secrecy in multiuser MIMO wiretap channels,” in *Proc. 47th Allerton Conf.*, pp. 1134–1141.
- [27] —, “User selection in multiuser MIMO systems with secrecy considerations,” in *Proc. Asilomar Conf.*, Pacific Grove, CA, 2009, pp. 1479–1482.
- [28] —, “Poisoned feedback: The impact of malicious users in closed-loop multiuser MIMO systems,” in *Proc. IEEE ICASSP*, Dallas, TX, 2010, pp. 2558–2561.
- [29] A. L. Swindlehurst, “Fixed SINR solutions for the MIMO wiretap channel,” in *Proc. IEEE ICASSP*, pp. 2437–2440.
- [30] X. Zhou and M. R. McKay, “Secure transmission with artificial noise over fading channels: Achievable rate and optimal power allocation,” *IEEE Trans. Veh. Technol.*, vol. 59, no. 8, pp. 3831–3842, Oct. 2010.
- [31] A. Mukherjee and A. L. Swindlehurst, “A full-duplex active eavesdropper in MIMO wiretap channels: Construction and countermeasures,” in *Proc. Asilomar Conf.*
- [32] K. Hamdi, W. Zhang, and K. B. Letaief, “Opportunistic spectrum sharing in cognitive MIMO wireless networks,” *IEEE Trans. Wireless Commun.*, vol. 8, no. 8, pp. 4098–4111, Aug. 2009.
- [33] H. Yi, H. Hu, Y. Rui, K. Guo, and J. Zhang, “Null space-based precoding scheme for secondary transmission in a cognitive radio MIMO system using second-order statistics,” in *Proc. IEEE ICC*, 2009.
- [34] Z. Chen, C.-X. Wang, X. Hong, J. S. Thompson, S. A. Vorobyov, F. Zhao, H. Xiao, and X. Ge, “Interference mitigation for cognitive radio MIMO systems based on practical precoding,” <http://arxiv.org/abs/1104.4155>.
- [35] D. S. Papailiopoulos and A. G. Dimakis, “Interference alignment as a rank constrained rank minimization,” in *Proc. IEEE GLOBECOM*, 2010.
- [36] M. Fazel, H. Hindi, and S. P. Boyd, “A rank minimization heuristic with application to minimum order system approximation,” in *Proc. Amer. Control Conf.*, 2001, pp. 4734–4739.
- [37] —, “Log-det heuristic for matrix rank minimization with applications to Hankel and Euclidean distance matrices,” in *Proc. Amer. Control Conf.*, 2003, pp. 2156–2162.

- [38] Y. Noam and A. Goldsmith, “Blind null-space learning for MIMO underlay cognitive radio networks.”
- [39] S. A. Jafar, “Blind interference alignment,” *IEEE J. Sel. Topics Signal Process.*, 2012.
- [40] I. E. Telatar, “Capacity of multi-antenna Gaussian channels,” *Eur. Trans. Telecomm.*, vol. 10, no. 6, pp. 585–595, Nov. 1999.
- [41] W. Mao, X. Su, and X. Xu, “Comments on ‘correlated jamming on MIMO Gaussian fading channels’,” *IEEE Trans. Inf. Theory*, vol. 52, no. 11, pp. 5163–5165, Nov. 2006.
- [42] R. S. Blum, “MIMO capacity with interference,” *IEEE J. Sel. Areas Commun.*, vol. 21, no. 5, pp. 793–801, Jun. 2003.
- [43] J. G. Andrews, W. Choi, and R. W. Heath, “Overcoming interference in spatial multiplexing MIMO wireless networks,” *IEEE Wireless Commun. Mag.*, vol. 14, no. 6, pp. 95–104, Dec. 2007.
- [44] G. Arslan, M. F. Demirkol, and Y. Song, “Equilibrium efficiency improvement in MIMO interference systems: A decentralized stream control approach,” *IEEE Trans. Wireless Commun.*, vol. 6, no. 8, pp. 2984–2993, Jun. 2007.
- [45] H. Yu and V. K. N. Lau, “Rank-constrained Schur-convex optimization with multiple trace/log-det constraints,” *IEEE Trans. Signal Process.*, vol. 59, no. 1, pp. 304–314, Jan. 2011.
- [46] A. Mukherjee and A. L. Swindlehurst, “Modified waterfilling algorithms for MIMO spatial multiplexing with asymmetric CSI,” *IEEE Wireless Commun. Lett.*, vol. 1, 2012.
- [47] Q. Spencer, A. L. Swindlehurst, and M. Haardt, “Zero-forcing methods for downlink spatial multiplexing in multi-user mimo channels,” *IEEE Trans. Signal Process.*, vol. 52, no. 2, pp. 461–471, Feb. 2004.
- [48] A. Lozano and A. M. Tulino, “Capacity of multiple-transmit multiple-receive antenna architectures,” *IEEE Trans. Inf. Theory*, vol. 48, no. 12, pp. 3117–3128, Dec. 2002.
- [49] A. L. Moustakas, S. H. Simon, and A. M. Sengupta, “MIMO capacity through correlated channels in the presence of correlated interferers and noise: A (not so) large n analysis,” *IEEE Trans. Inf. Theory*, vol. 49, no. 10, pp. 2545–2561, Oct. 2003.
- [50] G. Alfano, A. Lozano, A. M. Tulino, and S. Verdú, “Eigenvalue statistics of finite-dimensional random matrices for MIMO wireless communications,” in *Proc. IEEE ICC*, pp. 4125–4129.

- [51] T. Clancy, “Achievable capacity under the interference temperature model,” in *Proc. IEEE INFOCOM*, May 2007.
- [52] Y.-C. Liang, R. Zhang, and J. M. Cioffi, “Subchannel grouping and statistical water-filling for vector block fading channels,” *IEEE Trans. Commun.*, vol. 54, no. 6, pp. 1131–1142, Jun. 2006.
- [53] A. Zanella and M. Chiani, “Analytical comparison of power allocation methods in MIMO systems with singular value decomposition,” in *Proc. IEEE GLOBECOM*, 2009.
- [54] F. Zhang and Q. Zhang, “Eigenvalue inequalities for matrix product,” *IEEE Trans. Autom. Control*, vol. 51, no. 9, pp. 1506–1509, Sep. 2006.
- [55] H. Kang, J. S. Kwak, T. G. Pratt, and G. L. Stüber, “Analytical framework for optimal combining with arbitrary-power co-channel interferers and thermal noise,” *IEEE Trans. Veh. Technol.*, vol. 57, no. 5, pp. 1564–1575, May 2008.
- [56] M. Chiani, M. Z. Win, and A. Zanella, “On the capacity of spatially correlated MIMO channels,” *IEEE Trans. Inf. Theory*, vol. 49, no. 10, pp. 2363–2371, Oct. 2003.
- [57] H. Shin, M. Z. Win, J. Lee, and M. Chiani, “On the capacity of doubly correlated MIMO channels,” *IEEE Trans. Wireless Commun.*, vol. 5, no. 8, pp. 2253–2265, Aug. 2006.
- [58] A. Zanella, M. Chiani, and M. Z. Win, “On the marginal distribution of the eigenvalues of Wishart matrices,” *IEEE Trans. Commun.*, vol. 57, no. 4, pp. 1050–1060, Apr. 2009.
- [59] M. G. Khoshkholgh, K. Navaie, and H. Yanikomeroglu, “Access strategies for spectrum sharing in fading environment: Overlay, underlay and mixed,” *IEEE Trans. Mobile Comput.*, vol. 9, no. 12, pp. 1780–1793, Dec. 2010.
- [60] V. Chakravarthy, L. Xue, Z. Ruolin, W. Zhiqiang, and M. Temple, “A novel hybrid overlay-underlay cognitive radio waveform in frequency selective fading channels,” in *Proc. CROWNCOM Conf.*, 2009.
- [61] J. Ma, G. Zhao, and Y. Li, “Soft combination and detection for cooperative spectrum sensing in cognitive radio networks,” *IEEE Trans. Wireless Commun.*, vol. 7, no. 11, pp. 4502–4507, Nov. 2008.
- [62] S. Kim, J. Lee, H. Wang, and D. Hong, “Sensing performance of energy detector with correlated multiple antennas,” *IEEE Signal Process. Lett.*, vol. 16, no. 8, pp. 671–674, Aug. 2009.
- [63] S. M. Kay, *Fundamentals of Statistical Signal Processing Vol. II: Detection Theory*. Prentice Hall, 1998.

- [64] —, “Optimal signal design for detection of Gaussian point targets in stationary Gaussian clutter/reverberation,” *IEEE J. Sel. Topics Signal Process.*, vol. 1, no. 1, pp. 31–41, Jun. 2007.
- [65] H. Weingarten, Y. Steinberg, and S. Shamai, “The capacity region of the Gaussian multiple-input multiple-output broadcast channel,” *IEEE Trans. Inf. Theory*, vol. 52, no. 9, pp. 3936–3964, Sep. 2006.
- [66] C. Peel, B. Hochwald, and A. L. Swindlehurst, “A vector-perturbation technique for near-capacity multi-antenna multi-user communication-part i: Channel inversion and regularization,” *IEEE Trans. Commun.*, vol. 53, no. 1, pp. 195–202, Jan. 2005.
- [67] C. Guthy, W. Utschick, R. Hunger, and M. Joham, “Efficient weighted sum rate maximization with linear precoding,” *IEEE Trans. Signal Process.*, vol. 58, no. 4, pp. 2284–2297, Apr. 2010.
- [68] L. Venturino, N. Prasad, and X. Wang, “Coordinated linear beamforming in downlink multi-cell wireless networks,” *IEEE Trans. Wireless Commun.*, vol. 9, no. 4, pp. 1451–1461, Apr. 2010.
- [69] D. C. Y. S. U. Pillai, H. S. Oh and J. R. Guerci, “Optimum transmit-receiver design in the presence of signal-dependent interference and channel noise,” *IEEE Trans. Inf. Theory*, vol. 46, no. 2, pp. 577–584, Mar. 2000.
- [70] D. P. Bertsekas, *Nonlinear Programming*. Belmont, MA: Athena Scientific, 1995.
- [71] E. Karipidis, N. D. Sidiropoulos, and Z.-Q. Luo, “Quality of service and max-min-fair transmit beamforming to multiple co-channel multicast groups,” *IEEE Trans. Signal Process.*, vol. 56, no. 3, pp. 1268–1279, Mar. 2008.
- [72] R. Zhang, “Cooperative multi-cell block diagonalization with per-base-station power constraints,” *IEEE J. Sel. Areas Commun.*, vol. 28, no. 12, pp. 1435–1445, Dec. 2010.
- [73] M. Grant and S. Boyd, “CVX: Matlab software for disciplined convex programming, version 1.21,” `././cvx`, Apr. 2011.
- [74] A. Mukherjee and A. L. Swindlehurst, “Fixed-rate power allocation strategies for enhanced secrecy in mimo wiretap channels,” in *Proc. 10th IEEE SPAWC*, Jun. 2009, pp. 344–348.
- [75] A. Khisti and G. W. Wornell, “Secure transmission with multiple antennas-i: The MISOME wiretap channel,” *IEEE Trans. Inf. Theory*, vol. 56, no. 7, pp. 3088–3104, Jul. 2010.

- [76] M. Bloch, J. Barros, M. Rodrigues, and S. W. McLaughlin, “Wireless information-theoretic security,” *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, Jun. 2008.
- [77] M. Bloch and J. Laneman, “Information-spectrum methods for information-theoretic security,” in *Proc. Inf. Theory and Appl. Work.*, 2009.
- [78] S. A. Jafar and A. Goldsmith, “Transmitter optimization and optimality of beamforming for multiple antenna systems,” *IEEE Trans. Wireless Commun.*, vol. 3, no. 4, pp. 1165–1175, Jul. 2004.
- [79] M. Larsen and A. L. Swindlehurst, “Mimo svd-based multiplexing with imperfect channel knowledge,” in *Proc. IEEE ICASSP*, 2010.
- [80] M. Jorgensen, B. Yanakiev, G. Kirkelund, P. Popovski, H. Yomo, and T. Larsen, “Shout to secure: physical-layer wireless security with known interference,” in *Proc. IEEE GLOBECOM*, 2007, pp. 33–38.
- [81] E. Tekin and A. Yener, “The general Gaussian multiple-access and two-way wiretap channels: Achievable rates and cooperative jamming,” *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2735–2751, Jun. 2008.
- [82] O. Koyluoglu, H. E. Gamal, L. Lai, and H. V. Poor, “On the secure degrees of freedom in the k -user Gaussian interference channel,” in *Proc. IEEE ISIT*, 2008, pp. 384–388.
- [83] Z. Xu, “Perturbation analysis for subspace decomposition with applications in subspace-based algorithms,” *IEEE Trans. Signal Process.*, vol. 50, no. 11, pp. 2820–2830, Nov. 2002.
- [84] G. Amariuca and S. Wei, “Half-duplex active eavesdropping in fast fading channels: A block-Markov Wyner secrecy encoding scheme.”
- [85] M. Yuksel, X. Liu, and E. Erkip, “A secure communication game with a relay helping the eavesdropper,” *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 818–830, Sep. 2011.
- [86] S.-C. Lin, T.-H. Chang, Y.-L. Liang, Y.-W. P. Hong, and C.-Y. Chi, “On the impact of quantized channel feedback in guaranteeing secrecy with artificial noise - the noise leakage problem,” *IEEE Trans. Wireless Commun.*, vol. 10, no. 3, pp. 901–915, Mar. 2011.
- [87] T. Liu and S. Shamai, “A note on the secrecy capacity of the multiple-antenna wiretap channel,” *IEEE Trans. Inf. Theory*, vol. 55, no. 6, pp. 2547–2553, Jun. 2009.
- [88] A. Mukherjee and A. L. Swindlehurst, “Optimal strategies for countering dual-threat jamming/eavesdropping-capable adversaries in MIMO channels,” in *Proc. IEEE MILCOM*.

- [89] —, “Fixed-rate power allocation strategies for enhanced secrecy in MIMO wiretap channels,” in *Proc. IEEE SPAWC*, Perugia, Italy, 2009, pp. 344–348.
- [90] B. Hochwald, T. Marzetta, and B. Hassibi, “Space-time autocoding,” *IEEE Trans. Inf. Theory*, vol. 47, no. 7, pp. 2761–2781, Nov. 2001.
- [91] B. Hochwald, T. Marzetta, and V. Tarokh, “Multiple-antenna channel hardening and its implications for rate feedback and scheduling,” *IEEE Trans. Inf. Theory*, vol. 50, no. 9, pp. 1893–1909, Sep. 2004.
- [92] T. Philosf and R. Zamir, “The cost of uncorrelation and noncooperation in MIMO channels,” *IEEE Trans. Inf. Theory*, vol. 53, no. 11, pp. 3904–3920, Nov. 2007.
- [93] L. A. Petrosjan and N. A. Zenkevich, *Game Theory*. World Scientific, 1996.
- [94] R. Myerson, *Game Theory: Analysis of Conflict*. Harvard University Press, 1997.
- [95] D. Fudenberg and J. Tirole, *Game Theory*. MIT Press, 1991.
- [96] Z. Yin, D. Korzhyk, C. Kiekintveld, V. Conitzer, and M. Tambe, “Stackelberg vs. Nash in security games: Interchangeability, equivalence, and uniqueness,” in *Proc. AAMAS*, 2010.
- [97] J. Huang and A. L. Swindlehurst, “Robust secure transmission in MISO channels based on worst-case optimization,” *IEEE Trans. Signal Process.*, vol. 60, no. 4, pp. 1696–1707, Apr. 2012.
- [98] Y. Wu and K. J. R. Liu, “An information secrecy game in cognitive radio networks,” *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 831–842, Sep. 2011.
- [99] I. Stanojev and A. Yener, “Cooperative jamming via spectrum leasing,” in *Proc. WiOpt.*, 2011.
- [100] K. Lee, O. Simeone, C.-B. Chae, and J. Kang, “Spectrum leasing via cooperation for enhanced physical-layer secrecy,” in *Proc. IEEE ICC*, 2011.
- [101] L. Zhang, Y.-C. Liang, Y. Pei, and R. Zhang, “Robust beamforming design: From cognitive radio MISO channels to secrecy MISO channels,” in *Proc. IEEE GLOBECOM*, 2009.
- [102] S. A. Vorobyov, A. B. Gershman, and Z.-Q. Luo, “Robust secure transmission in MISO channels based on worst-case optimization,” *IEEE Trans. Signal Process.*, vol. 51, no. 2, pp. 313–324, Feb. 2003.
- [103] J. Wang and D. P. Palomar, “Worst-case robust MIMO transmission with imperfect channel knowledge,” *IEEE Trans. Signal Process.*, vol. 57, no. 8, pp. 3086–3100, Aug. 2009.

- [104] F. Zhang, *The Schur Complement and Its Applications*. New York: Springer, 2005.