Analysis and Design of Multi-antenna Systems for Physical-layer Security and Interference Characterization

Wei Shi

A dissertation
submitted in partial fulfillment of the
requirements for the degree of

Doctor of Philosophy

University of Washington

2012

Reading Committee:

James A. Ritcey, Chair

James A. Ritcey

Radha Poovendran

John E. Ehrenberg

Program Authorized to Offer Degree:
Electrical Engineering

University of Washington

Abstract

Analysis and Design of Multi-antenna Systems for Physical-layer Security and Interference Characterization

Wei Shi

Chair of the Supervisory Committee:
Professor James A. Ritcey
Electrical Engineering

It has become crucial to provide effective solutions to the security issues associated in a wireless transmission medium. The essential goal of physical-layer security is to enable the transmission of confidential messages over a wireless medium in the presence of unauthorized eavesdroppers. We begin with an overview of the foundations dating back to the pioneering work on physical-layer security, and the evolution of secure transmission strategies from point-to-point channels to multiple-antenna systems. The explosion of interest in multi-antenna systems led to the realization that exploiting the available spatial dimensions could also enhance the secrecy capabilities of wireless channels. Our work analyzes and optimizes multi-antenna systems under various assumptions on system model and channel information: transmission only versus joint transmission/jamming, perfect channel state information (CSI), imperfect CSI, and completely unknown CSI.

With perfect CSI: We first study the problem of joint transmit and cooperative jamming to maximize the secrecy rate of MISOSE wiretap channels. We reduce the problem of maximizing the secrecy rate to the problem of finding the optimal jamming levels, and solve it by a one-dimensional search that is computationally affordable. We then study MIMOME wiretap channel with transmit beamforming (the rank-1 constraint on the transmit covariance matrix) and cooperative jamming. We propose an iterative algorithm by relating the MIMOME channel to the effective MISOSE channel.

With imperfect CSI: assuming the CSI of the receiver and the eavesdropper channel belong to given uncertainty sets, we optimize the worst-case secrecy rate of the MISOSE wiretap channel. By proving the saddle-point solution, we transformed the worst-case optimization problem into a quasi-convex optimization problem. Moreover, for jamming-aided MISOSE channel with imperfect CSI, we propose to approximate the worst-case secrecy rate as the worst-case SINR-ratio problem. A minimax solution is shown to exist for the problem, based on which some insightful results of the optimal transmit and jamming covariances are obtained. A quasi-convex optimization algorithm that is tractable and efficient is provided for solving the worst-case SINR-ratio problem.

With no CSI: We study how cooperative jamming helps improve the secure throughput of large decentralized networks where both the locations and CSI of eavesdroppers are unknown. The spatial distributions are modeled as Poisson point processes. The helping jammers broadcast artificial noise that confuses eavesdropper but zero-forcing to the legitimate receiver. A jamming protocol based on IEEE 802.11 RTS/CTS is proposed. Closed-form results analyze the benefits of jamming on secure communications.

This thesis continues on analyzing large distributed networks using stochastic geometry. The geometry of the locations of the nodes plays a key role since it determines the signal-to-interference-plus-noise-ratio (SINR) at each receiver. The advantages of using stochastic geometry are: 1) performance metric can be exactly derived in some important cases, and tightly bounded in many others; 2) performance depends on fundamental network parameters, such as the densities of the underlying point processes. Design insights are obtainable from these performance expressions. Specifically, we study the performance of minimum-mean-square-error (MMSE) receivers under supposition of multiple Poisson point processes, non-homogeneous Poisson process and cluster Poisson point process of interferers. We discover that the SINR outage exhibits a superposition property for multiple homogeneous (or non-homogeneous) Poisson fields of interferers. Using this property, we extend the outage analysis to Poisson clustered processes which is formed by Poisson clusters consisting of Poisson distributed children points.

TABLE OF CONTENTS

Page

LIST OF FIGURES

ACKNOWLEDGMENTS

I wish to express heartfelt gratitude to everyone who has ever helped and supported me during my Ph.D. study.

First of all, I would like to thank my academic advisor Prof. James A. Ritcey for his guidance and encouragement on my creative days as well as on difficult ones. He has been a constant source of inspiration on how to be a serious researcher and a better person.

Let me also thank my committee members, Prof. Radha Poovendran, Dr. John E. Ehrenberg and Prof. Archis Vijay Ghate for their interest and valuable suggestions for my Ph.D. work.

I would like to acknowledge the support from U.S. Army Research Office under the Multi-University Research Initiative (ARO-MURI) on my research.

During my Ph.D. study, I have received generous help from many people. My lab-mates and other friends in UW, such as Xiang Zou, Hui Ma, Ling Luo, Xiaoyue Zheng, Fei Ye, Nathan Parrish, Linda Bai, Bin Zhang, Wei Wu, Xiaolan Xu, Yanping Huang, Ruizhu Huang, and Ruihua Ding, has supported my study in various ways. I would like to thank them all.

Finally, I would like to thank my dear parents Danchun Shi and Jine Yuan for their love, support and encouragement over the years. I would like to thank my dear wife Mei for her long-term support. I am afraid I cannot acknowledge her enough.

DEDICATION

to my wife Mei and my parents

Chapter 1

INTRODUCTION

1.1 Information-theoretic Security

The advances of today's communication networks, both wired and wireless, have dramatically improved its accessibility and affordability. People have become increasingly dependent on the ability to stay connected, both in their personal and professional lives. However, the pervasive access to online services often comes at the expense of security. For instance, the broadcast nature of wireless communications makes them particularly sensitive to eavesdropping. Therefore secure communications has been receiving more and more attention recently because of high demand for privacy and data protection.

Existing mechanisms to ensure the communication network security largely rely on the symmetric key and public/private key infrastructures that were developed since 1970s with the advent of computer networks. While they have been fairly successful in providing robust security performance against some common security threats, its vulnerability has also been exploited through various deliberate attacks [30]. For example, RSA-129 Factoring Challenge Project is successfully attacked in 1994; DES system with a shorter key length was cracked in 1997; Netscape SSL RC4 was successfully attacked within months of its release.

These examples are not entirely surprising; these existing security schemes are based primarily on some unproven hypotheses on the difficulty of certain problems. Even without taking into account potential advances of cryptanalysis, the exponentially increasing computing power as predicted by Moore's law kept raising the bar for data security. More importantly, the emergence of potentially new computing paradigms may completely change the entire landscape. For example, under the quantum computing regime, factoring prime numbers requires only polynomial time (i.e., Shor's algorithm [8]). This will render the current RSA-based [48] public-key cryptographic primitives obsolete.

Therefore, it is imperative for us to give more attention to the notion of information-theoretic security, where we can assume that adversaries have infinite computing power. Such notion of unconditional security was pioneered by Claude E. Shannon in 1948 [51] from an information theoretic perspective. Contrary to existing key primitive based approaches, security is assured even if the adversary is assumed to have infinite computing power. In the following, we review related work about the information-theoretic security.

The notion of information theoretic security was first developed by Shannon and first appeared as a technical paper in [51]. The information-theoretic secrecy [51] model assumes that a non-reusable private key K is used to encrypt the confidential message M to generate the cryptogram C, which is then transmitted over a noiseless channel. The eavesdropper has unbounded computational power, has knowledge of the transmit coding scheme, and has access to an copy of the signal. The notion of perfect secrecy was introduced, which requires that the *a posteriori* probability of the secret message computed by the eavesdropper based on her received signal be equal to the *a priori* probability of the message. In other words,

$$I(M;C) = 0, \tag{1.1}$$

where $I(\cdot;\cdot)$ denotes mutual information. Shannon showed that if an eavesdropper had perfect knowledge of the signals sent by a transmitter and had unbounded computational power, then to achieve perfect secrecy, the transmitter and the receiver would have to share a key whose rate equals that of the data to be sent, $H(K) \geq H(M)$. Because the required length of the key increases with the length of the data, which is difficult to implement in practice, the result in [51] shows that achieving perfect secrecy is impractical in this setting. This is the reason that research shifted its focus to computation-power-bounded adversaries, and lead to the birth of the field "cryptography".

Recently, there is a revival of interest in information theoretic secrecy proposed by Shannon in [51]. This should largely be credited to Wyner's work [67]. Wyner, in [67], found that Shannon's result showing the necessity of one time-pad for secrecy was overly pessimistic, if the eavesdropper only had a noisy observation of the signals sent by the transmitter.

In the wiretap channel, the information signal X is transmitted to the intended receiver

over the "main channel" which is modeled as a discrete memoryless channel. The receiver observes Y, which subsequently passes through an additional "wiretap channel" before being received by the eavesdropper as Z. Under the assumption that the source-wiretapper channel is a probabilistically degraded version of the main channel [67], Wyner sought to maximize the transmission rate R in the main channel while making negligible the amount of information leaked to the wiretapper channel. He showed that a positive rate could be achieved for transmitting confidential messages without requiring the communicating parties to share keys beforehand. The essential result for the secrecy capacity C_S was the following:

$$C_S = C_M - C_W, \tag{1.2}$$

where C_S and C_W are the Shannon capacities of the main and wiretap channels, respectively. It was established that a non-zero secrecy capacity can be obtained if the eavesdropper's channel is of lower quality than that of the intended recipient. Note that, different from cryptography, which is based on computation complexity, information theoretic secrecy is achieved by assuming the fundamental receiving capability of the eavesdropper is limited. In Wyner's case, this is due to the added uncertainty in the channel model the eavesdropper observes.

The wiretap channel model considered by Wyner [67] [6] [29] has inspired a myriad of works studying the information theoretic limits of different kinds of wiretap channels. A set of models follows the classical model of Wyner's wiretap channel [67], where there is one external eavesdropper is present in addition to legitimate parties and its channel model is known to the legitimate parties. This line of work includes the multiple input multiple output (MIMO) wiretap channel [25] [42] [49], the MIMO broadcast wiretap channel [9], the multiple access wiretap channel [10, 57, 59, 58], the two-way wiretap channel [59], the relay channel with an external eavesdropper [28]. In these models, where information leaked to the eavesdropper is a loss to the legitimate communication system, it was observed that legitimate parties could aid in enhancing secrecy by introducing intentional interference to the eavesdropper via cooperative jamming [60, 59]. Another set of models deals with a more symmetric scenario, where each receiver of an intended message is also modeled as

an eavesdropper for the remaining unintended messages in the system. This setting has been considered for the discrete memoryless multiple access channel [36], Gaussian MIMO broadcast channel [37], and discrete memoryless interference channels [38, 68]. In these models, one communication pair, in the interest of protecting its own information, may end up helping the other pair [68].

1.2 Multi-antenna Systems for Secure Communications

The explosion of interest in multiple-input multiple-output (MIMO) systems soon led to the realization that exploiting the available spatial dimensions could also enhance the secrecy capabilities of wireless channels.

In a fading MIMO channel where the transmitter, receiver and eavesdropper are equipped with N_T, N_R, N_E antennas respectively, a general representation for the signal received by the legitimate receiver is

$$\mathbf{y}_b = \mathbf{H}_b \mathbf{x}_a + \mathbf{n}_b, \tag{1.3}$$

while the received signal at the eavesdropper is

$$\mathbf{y}_e = \mathbf{H}_e \mathbf{x}_a + \mathbf{n}_e, \tag{1.4}$$

where $\mathbf{x}_a \in C^{N_T \times 1}$ is the transmit signal with covariance $E\{\mathbf{x}_a \mathbf{x}_a^H\} = \mathbf{Q}_x$, $\mathrm{Tr}(\mathbf{Q}_x) \leq P$, $\mathbf{H}_b \in C^{N_R \times N_T}$, $\mathbf{H}_e \in C^{N_E \times N_T}$ are the MIMO complex Gaussian channel matrices, $\mathbf{n}_b$ and $\mathbf{n}_e$ are the respective zero-mean complex Gaussian additive noise vectors.

Parada and Blahut analyzed a degraded single-input multiple-output ($N_T = 1, N_R, N_E > 1$) wiretap channel in [43], and obtained a single-letter characterization of its secrecy capacity via transformation into a scalar Gaussian wiretap channel, and then re-applying (1.2). The authors also proposed a secrecy rate outage metric for the SIMO wiretap channel with slow fading, and observed a secrecy diversity gain of order proportional to the number of receiver antennas. The corresponding MISO case was studied in [32], [50], who noted that the MIMO wiretap channel is not degraded in general. For the special case of $N_T = 2, N_R = 2, N_E = 1$ analyzed by Shafiee and coworkers in [49], a beamforming transmission strategy was shown to be optimal.

Understanding the MIMO wiretap channel were given in [42, 25, 18], which considered the case of multiple antennas at all nodes and termed it the MIMOME (multiple-input multiple-output multiple-eavesdropper) channel. Khisti et al. [25] developed a genie-aided upper bound for the MIMO secrecy capacity for which Gaussian inputs are optimal. When the eavesdropper's instantaneous channel state is known at the transmitter, it was shown that an asymptotically optimal (high SNR) scheme is to apply a transmit precoder based upon the generalized singular value decomposition (GSVD) of the pencil ($\mathbf{H}_b$,$\mathbf{H}_e$), which decomposes the system into parallel channels and leads to a closed-form secrecy rate expression. For the so-called MISOME special case where $N_R = 1, N_T, N_E > 1$, the optimal transmit beamformer is obtained as the generalized eigenvector $\mathbf{w}$ corresponding to the largest generalized eigenvalue λ of

$$\mathbf{h}_b^H \mathbf{h}_b \mathbf{w} = \lambda \mathbf{H}_e^H \mathbf{H}_e \mathbf{w}. \tag{1.5}$$

The MIMO wiretap channel was studied independently by Oggier and Hassibi [42], who computed a similar upper bound on the MIMO secrecy capacity, and showed after a matrix optimization analysis that

$$C_S = \max_{\mathbf{Q}_x \succeq 0} \log\det(\mathbf{I} + \mathbf{H}_b \mathbf{Q}_x \mathbf{H}_b^H) - \log\det(\mathbf{I} + \mathbf{H}_e \mathbf{Q}_x \mathbf{H}_e^H). \tag{1.6}$$

In [38], Liu and Shamai reexamined the MIMO wiretap channel with a more general matrix input power-covariance constraint $\mathbf{Q}_x \preceq \mathbf{S}$, and showed that the conjecture of a Gaussian input $U = X$ without prefix coding is indeed an optimal secrecy capacity-achieving choice.

Negi and Goel described secret communication using artificially added noise in systems in which the number of transmit antennas exceeds the number of receive antennas [18]. Based on channel information provided by the legitimate receiver, the transmitter places artificial noise in the null space of the channel matrix associated with the legitimate receiver. Depending on the eavesdropper's channel matrix, some component of this noise will be projected onto its range space, thereby degrading the performance of the eavesdropper.

Subsequently, numerous research contributions emerged that considered a number of practical issues regarding the MISO/MIMO wiretap channel, of which we enumerate a few below: Optimal power allocation methods for the artificial noise strategy were presented

in [72]. If even statistical information regarding the eavesdropper's channel is unavailable, then Swindlehurst et al. [40] suggested an approach where just enough power is allocated to meet a target performance criterion (SNR or rate) at the receiver, and any remaining power is used for broadcasting artificial noise, since the secrecy rate cannot be computed at the transmitter. The effects of imperfect channel states information at the transmitter upon the secrecy rate were examined in [35]. MIMO secrecy capacity has also been studied for frequency-selective [26] and ergodic [46] channel fading processes.

1.3 Interference Characterization for Large Distributed Networks

A wireless network can be viewed as a collection of nodes, located in some domain, and can be transmitters or receivers. As wireless networks become more pervasive with denser deployments, interference management has been becoming a defining issue of wireless network design. At a given time, several nodes transmit simultaneously, each toward its own receiver. The signal received from the transmitter may be jammed by the signals received from the other transmitters. The geometry of the locations of the nodes plays a key role since it determines the signal to interference and noise ratio (SINR) at each receiver.

Stochastic geometry provides a natural way of defining and computing macroscopic properties of such networks, by averaging over all potential geometrical patterns for the nodes. The advantages of using stochastic geometry are: 1) performance metric can be exactly derived in some important cases, and tightly bounded in many others; 2) performance depends on fundamental network parameters, such as the densities of the underlying point processes. Design insights are obtainable from these performance expressions. It is relatively new to use stochastic geometry to model communication networks. The first papers appeared in the engineering literature shortly before 2000. Gilberts paper [16] may be considered as the first paper on continuum and Boolean percolation and as the first paper on the analysis of the connectivity of large wireless networks using stochastic geometry. Similar observations can be made on [17] concerning PoissonVoronoi tessellations. But the number of papers using some form of stochastic geometry is increasing fast, e.g. models of specific mechanisms of wireless communications.

Antenna arrays is a promising technique to improve the performance of wireless net-

works by increasing robustness through diversity, and data rates through spatial multiplexing, beam-forming and interference mitigation. Multi-antenna systems employed in these networks depend heavily on propagation characteristics and spatial distribution of the interferers scattered in the network. Hence performance analysis of multi-antenna systems in spatially distributed networks has received significant attention in recent years. Previous results in the literature that explicitly model the spatial distribution of multi-antenna nodes mainly focus on homogenous Poisson point process, i.e. systems where node positions are independent of one another and are distributed uniformly randomly on a plane. For instance, [19], [23], [1], [39] have analyzed multi-antenna systems in homogenous Poisson networks under different assumptions. While simpler and (somewhat) analytically tractable, homogeneous spatial node distributions may not apply in many scenarios. For instance, in networks with hotspots or clusters of users, which are often encountered in practice, the assumption of homogenous Poisson distribution becomes invalid. There are also other scenarios where a non-homogenous spatial node distribution is appropriate such as in networks with physical limitations on user locations.

A number of works such as [65], [13], [12], and [56] have considered single antenna systems and interference modeling for non-homogeneous Poisson and clustered networks. Relatively fewer works have analyzed multi-antenna systems in non-homogeneous or clustered networks. [61] considered interference-alignment in clustered wireless networks where a partial interference-alignment protocol is used. While interference-alignment can provide enormous data rates, it requires significant overhead for the exchange of transmit (Tx) Channel-State Information (CSI). [22] approximates networks of multiple-input-multiple-output (MIMO) links with Carrier-Sensing-Multiple-Access (CSMA) using a Poisson approximation for the spatial node distribution. However, the multiple antennas are not used for interference mitigation compared to our work. [73] considers non-homogenous Poisson networks.

Our work extends the performance analysis of multi-antenna minimum-mean-square-error (MMSE) receivers under Poisson point process (PPP) of interferers to that under more sophisticated Poisson spatial distributions, such as non-homogeneous PPP and Poisson clustered processes. Our work reveal an important fact that the effective interference caused by superposition of PPPs is the sum of the responses which would have been caused by each

PPP individually.

The superposition property is used to analyze the secure performance of how cooperative jamming helps improve the secrecy throughput of large decentralized networks where the locations and channel state information (CSI) of eavesdroppers are both unknown. The spatial distribution of legitimate nodes including transmitter, receiver and helping jammers, and eavesdroppers are modeled as Poisson point processes. A jamming protocol based on the RTS/CTS handshake of IEEE 802.11 standard is proposed for decentralized implementation. Our results show that multi-antenna jammers can significantly increase the secrecy of the network, compared to single-antenna jammers.

1.4 Dissertation Organization

We first consider perfect CSI and optimize transmit/jamming design for MISOSE and MIMOME wiretap channels in Chapter 2. In Chapter 3 and Chapter 4, we consider imperfect CSI where the channels are assumed to be chosen from given uncertainty sets. Chapter 3 solves the worst-case optimization problem for MISOSE wiretap channel and Chapter 4 solves the problem for jamming-aided MISOSE wiretap channel. Further we consider in Chapter 5 a large network where both locations and CSI of the eavesdroppers are unknown. Chapter 6 extends the performance analysis of MMSE multi-antenna receiver under Poisson field of interferers to that under more sophisticated spatial distribution such as superposition of Poisson fields, non-homogeneous Poisson fields and cluster Poisson processes. Finally we conclude this thesis in Chapter 7.

Chapter 2

JAMMING-AIDED MISOSE AND MIMOME WIRETAP CHANNEL WITH PERFECT CSI

2.1 Background and Related Work

Recently the physical layer security (or information theoretic security) of wireless communications emerges as an active research area. It has been shown in the pioneering work [67, 29] that the transmitter can broadcast signals with a nonzero coding rate to the legitimate receiver without any information being eavesdropped, if the mutual information between the transmitter and the receiver is higher than that between the transmitter and the eavesdropper.

The role of multiple antennas in wiretap channels is studied recently in [50, 49, 24, 5, 11, 18, 55, 53]. With multi-antenna systems, assuming the channel state information is available at the transmitter, the available degree of freedom can be utilized to substantially degrade the eavesdropper's effective channel. The secrecy capacity of MISOSE wiretap channels is derived in [50]. For a MIMO channel wiretaped by a multi-antenna eavesdropper, the secrecy capacity is considered and derived in [49, 24, 5]. The optimization of transmit covariance under average power constraint is in general a non-convex optimization problem, and alternative approaches are given by [5, 11]. A closed-form expression under power-covariance constraint is derived in [5]. A generalized singular value decomposition (GSVD) based solution is given in [11].

Another idea of utilizing multiple antennas is to interfere the eavesdropper through artificial spatial noise, [18, 55, 53, 66], to list a few. The artificial noise can substantially degrade the eavesdropper's channel quality with little or no harm to the receiver's channel. The idea of using artificial noise at the transmitter to ensure the secrecy of the communication was proposed in [18] and extended in [55, 53] etc. Many work constrains the jamming noise to be orthogonal to the message signal seen at the receiver. Although this disable any harm

to the signal quality at the receiver, the orthogonal design is not optimal to maximization of the secrecy rate.

This chapter provides optimal solution to cooperative jamming for MISOSE (multiple input single output single-antenna eavesdropper) wiretap channels and cooperative jamming for MIMOME (multiple input multiple output multi-antenna eavesdropper) wiretap channels with beamforming contraint.

- Cooperative jamming for MISOSE: Previous works design the artificial noise to be orthogonal (zero-forcing) to the receiver's channel. It is pointed out in [25] that the zero-forcing (ZF) artificial noise is nearly optimal for the secrecy rate at asymptotical high SNR. However, at arbitrary SNR, the optimal design to the maximization of the secrecy rate is unavailable. Considering a MISOSE wiretap channel with a multi-antenna friendly jammer, our contribution is providing a solution that maximizes the secrecy rate of the MISOME wiretap channels. Specifically, we reduce the problem of maximizing the secrecy rate to the problem of finding the optimal jamming levels at the receiver and the eavesdropper. The achievable region of jamming levels and the region's boundary where the optimal jamming point is located is obtained. Finding the optimal jamming levels in the whole region is reduced to finding those on a segment of the boundary, which is a one-dimensional search problem.

- Cooperative jamming for MIMOME: we consider the model that the transmitter, legitimate receiver, eavesdropper and helping jammer are all equipped with multiple antennas. The transmitter sends messages to the receiver, while the helping jammer assists the transmitter by broadcasting artificial noise independent of the messages to confuse the eavesdropper. The problem of joint optimization of the transmit and jamming covariances to maximize the secrecy rate is a difficult non-convex optimization problem. We propose an iterative algorithm to solving the problem under an additional constraint that the data stream of the transmitter is only one, i.e. transmit beamforming. Under the constraint of transmit beamforming, we notice that the MIMOME channel can be related to an effective MISOSE channel, where the effective MISO channels are the production of the MIMO channels and the beamformers

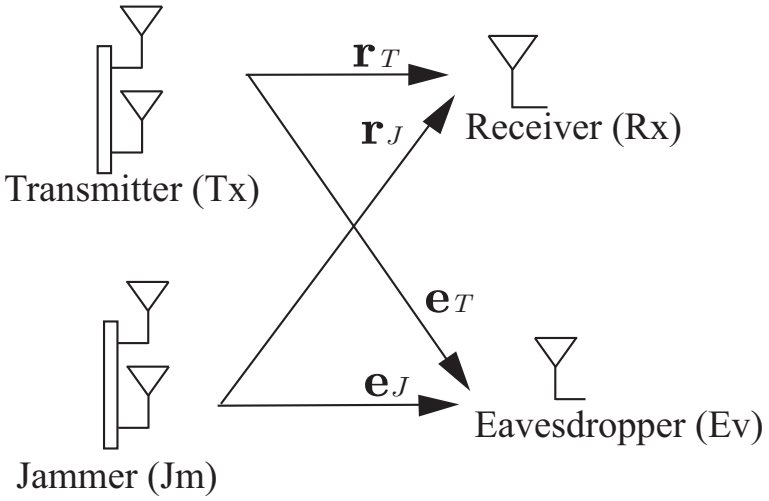


Figure 2.1: The system model for the MISOSE wiretap channel consisting of a multi-antenna transmitter and jammer and a single-antenna receiver and eavesdropper.

used at the receiving side. The idea of our proposed algorithm is to use the effective MISOSE channel to guide the search of the jamming covariance.

2.2 MISOSE: Problem Formulation of Cooperative Jamming

Consider a wireless network model consisting of one transmitter (Tx), one jamming helper (Jm), one legitimate receiver (Rx) and one eavesdropper (Ev), as shown in Fig. 2.1. The Tx and the Jm are equipped with multiple antennas, and the Rx and the Ev have single antenna each. A real-world example corresponding to this model is a scenario that a multi-antenna commanding unit with the help of a multi-antenna jammer wants to transmit to a mobile unit equipped with a single antenna while an opponent unit attempts to eavesdrop.

The Tx transmits a narrowband signal $\mathbf{s}b$ where b is the information bit, $\mathbf{s}$ is the beamforming vector, and the transmit covariance is $\mathbf{Q}_T = E\left\{\mathbf{s}\mathbf{s}^H\right\}$. At the same time, the Jm broadcasts an artificial noise $\mathbf{n}$ with covariance $\mathbf{Q}_J = E\left\{\mathbf{n}\mathbf{n}^H\right\}$. Suppose the maximum transmit powers at the Tx and the Jm are P_T and P_J, respectively. The channel from the Tx and the Jm to the Rx are denoted by $\mathbf{r}_T$ and $\mathbf{r}_J$, and those to the Ev are denoted by $\mathbf{e}_T$ and $\mathbf{e}_J$. We assume the Rx and the Ev are not co-located, and thus $\mathbf{r}_T \not\parallel \mathbf{r}_J$ (not in the

same one-dimensional space) and $\mathbf{e}_T \not\perp \mathbf{e}_J$.

The received signal at the Rx is given by

$$y_r = \mathbf{r}_T^H \mathbf{s} b + \mathbf{r}_J^H \mathbf{n} + n_r, \tag{2.1}$$

and that at the Ev is given by

$$y_e = \mathbf{e}_T^H \mathbf{s} b + \mathbf{e}_J^H \mathbf{n} + n_e, \tag{2.2}$$

where n_r and n_e are additive Gaussian noise with variance N_0.

Suppose all the channels are perfectly known at both the Tx and the Jm. The secrecy rate is equal to the difference between the rates of the receiver and the eavesdropper channels [67], and is maximized by jointly optimizing $\mathbf{Q}_T$ and $\mathbf{Q}_J$,

$$\begin{aligned} C_{\text{sec}}^* &= \max C_{\text{sec}} = \max_{\substack{\mathbf{Q}_T \succeq 0, \text{Tr}(\mathbf{Q}_T) \leq P_T \\ \mathbf{Q}_J \succeq 0, \text{Tr}(\mathbf{Q}_J) \leq P_J}} \left\{ \begin{array}{c} \log\left(1 + \text{SINR}_R\right) \\ -\log\left(1 + \text{SINR}_E\right) \end{array} \right\} \\ &= \max_{\substack{\mathbf{Q}_T \succeq 0, \text{Tr}(\mathbf{Q}_T) \leq P_T \\ \mathbf{Q}_J \succeq 0, \text{Tr}(\mathbf{Q}_J) \leq P_J}} \left\{ \begin{array}{c} \log\left(1 + \frac{\mathbf{r}_T^H \mathbf{Q}_T \mathbf{r}_T}{\mathbf{r}_J^H \mathbf{Q}_J \mathbf{r}_J + N_0}\right) \\ -\log\left(1 + \frac{\mathbf{e}_T^H \mathbf{Q}_T \mathbf{e}_T}{\mathbf{e}_J^H \mathbf{Q}_J \mathbf{e}_J + N_0}\right) \end{array} \right\}, \end{aligned} \tag{2.3}$$

where $\mathbf{Q} \succeq 0$ denotes $\mathbf{Q}$ is a positive semidefinite matrix. Problem (2.3) can be written in terms of trace functions to simplify the expression

$$2^{C_{\text{sec}}^*} = \max_{\substack{\mathbf{Q}_T \succeq 0, \text{Tr}(\mathbf{Q}_T) \leq P_T \\ \mathbf{Q}_J \succeq 0, \text{Tr}(\mathbf{Q}_J) \leq P_J}} \frac{1 + \frac{\text{Tr}(\mathbf{R}_T \mathbf{Q}_T)}{\text{Tr}(\mathbf{R}_J \mathbf{Q}_J) + N_0}}{1 + \frac{\text{Tr}(\mathbf{E}_T \mathbf{Q}_T)}{\text{Tr}(\mathbf{E}_J \mathbf{Q}_J) + N_0}} \tag{2.4}$$

where $\text{Tr}(\cdot)$ denotes the trace and the channel covariances are

$$\begin{aligned} \mathbf{R}_T &= \mathbf{r}_T \mathbf{r}_T^H, \mathbf{R}_J = \mathbf{r}_J \mathbf{r}_J^H, \\ \mathbf{E}_T &= \mathbf{e}_T \mathbf{e}_T^H, \mathbf{E}_J = \mathbf{e}_J \mathbf{e}_J^H. \end{aligned} \tag{2.5}$$

Previous work such as [18] [55] designs the artificial noise to be orthogonal (zero-forcing) to the receiver's channel. The ZF $\mathbf{Q}_J$ is given by $\mathbf{Q}_J = P_J \mathbf{q}_J \mathbf{q}_J^H$ and

$$\mathbf{q}_J = \frac{\Pi_{\mathbf{r}_J}^{\perp} \mathbf{e}_J}{\left|\left|\Pi_{\mathbf{r}_J}^{\perp} \mathbf{e}_J\right|\right|}, \tag{2.6}$$

where $\Pi^{\perp}_{\mathbf{r}_J} = (\mathbf{I} - \frac{\mathbf{r}_J \mathbf{r}_J^H}{||\mathbf{r}_J||^2})$ is the projection onto the null space of $\mathbf{r}_J$. It is pointed out in [25] [66] that the zero-forcing (ZF) artificial noise is nearly optimal for the secrecy rate at asymptotical high SNR. However, at arbitrary SNR, the optimal design to the maximization of the secrecy rate is unavailable.

Our work is to provide an optimal solution that maximizes (2.4). Specifically, we reduce the problem of maximizing the secrecy rate to the problem of finding the optimal jamming levels at the receiver and the eavesdropper. The achievable region of jamming levels and the region's boundary where the optimal jamming point is located are obtained. Finding the optimal jamming levels in the whole region is reduced to finding those on a segment of the boundary, which is a one-dimensional search problem.

2.3 MISOSE: Optimal Transmit and Jamming Design

2.3.1 Reduction of Problem (2.4)

Under the assumption that $\mathbf{h}_T \not\perp \mathbf{h}_J$, we can first show that $C^*_{\text{sec}} > 0$. Then we prove $\mathbf{Q}^*_T$ must have the maximum power, i.e. $\text{Tr}(\mathbf{Q}^*_T) = P_T$. The proofs are omitted here due to brevity.

Let

$$\alpha = \text{Tr}\left(\mathbf{R}_J \mathbf{Q}_J\right), \beta = \text{Tr}\left(\mathbf{E}_J \mathbf{Q}_J\right), \tag{2.7}$$

denote the jamming interference levels at the Rx and the Ev, respectively. Since we already know $\text{Tr}(\mathbf{Q}^*_T) = P_T$, problem (2.4) can be equivalently written as

$$\begin{aligned}
2^{C^*_{\text{sec}}} &= \max_{\substack{\mathbf{Q}_J \succeq 0, \text{Tr}(\mathbf{Q}_J) \le P_J \\ \alpha, \beta}} \max_{\substack{\mathbf{Q}_T \succeq 0, \\ \text{Tr}(\mathbf{Q}_T) \le P_T}} \frac{\text{Tr}\left(\frac{\mathbf{I}}{P_T}\mathbf{Q}_T\right) + \text{Tr}\left(\frac{\mathbf{R}_T}{\alpha + N_0}\mathbf{Q}_T\right)}{\text{Tr}\left(\frac{\mathbf{I}}{P_T}\mathbf{Q}_T\right) + \text{Tr}\left(\frac{\mathbf{E}_T}{\beta + N_0}\mathbf{Q}_T\right)} \\
&= \max_{\substack{\mathbf{Q}_J \succeq 0, \text{Tr}(\mathbf{Q}_J) \le P_J \\ \alpha, \beta}} \max_{\substack{\mathbf{Q}_T \succeq 0, \\ \text{Tr}(\mathbf{Q}_T) \le P_T}} \frac{\text{Tr}\left(\left(\frac{\mathbf{I}}{P_T} + \frac{\mathbf{R}_T}{\alpha + N_0}\right)\mathbf{Q}_T\right)}{\text{Tr}\left(\left(\frac{\mathbf{I}}{P_T} + \frac{\mathbf{E}_T}{\beta + N_0}\right)\mathbf{Q}_T\right)} \qquad (2.8) \\
&= \max_{\substack{\mathbf{Q}_J \succeq 0, \text{Tr}(\mathbf{Q}_J) \le P_J \\ \alpha, \beta}} \lambda_{\max}\left(\mathbf{I} + \frac{P_T}{\alpha + N_0}\mathbf{R}_T, \mathbf{I} + \frac{P_T}{\beta + N_0}\mathbf{E}_T\right), \qquad (2.9)
\end{aligned}$$

where the optimal $\mathbf{Q}_T$ that maximizes the Rayleigh quotient problem (2.8) is $\mathbf{Q}^*_T = P_T \mathbf{q}^*_T \mathbf{q}^{*H}_T$, $\mathbf{q}^*_T = \mathcal{P}\left\{\mathbf{I} + \frac{P_T}{\alpha + N_0}\mathbf{R}_T, \mathbf{I} + \frac{P_T}{\beta + N_0}\mathbf{E}_T\right\}$ and $\mathcal{P}\{\mathbf{A}, \mathbf{B}\}$ denotes the eigenvector corresponding

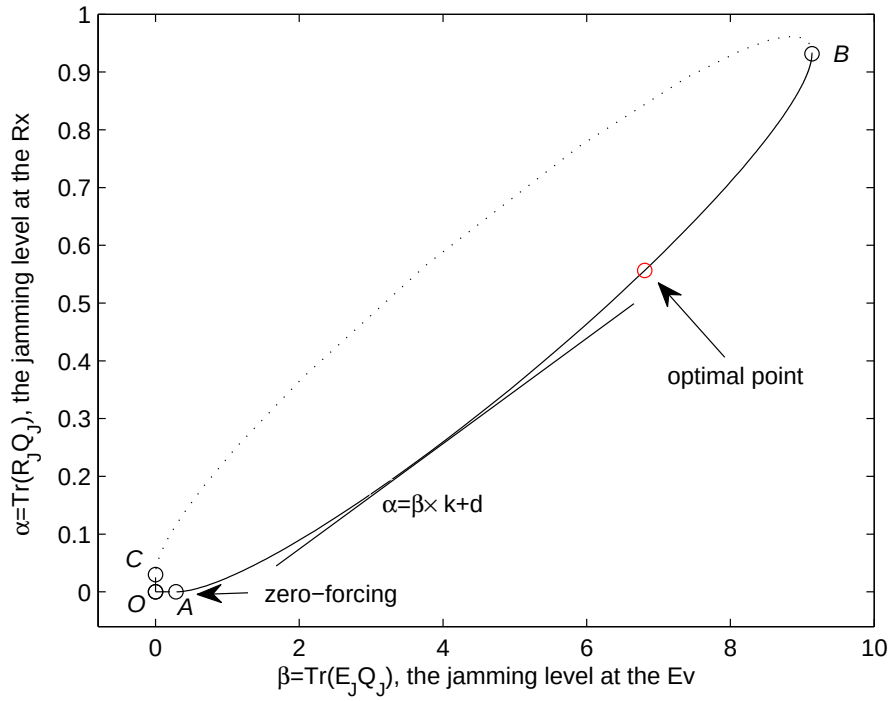


Figure 2.2: The achievable region of (α, β). The boundary consists of three segments: OA, OC and AC. OA and OC are two lines radiating from the origin, corresponding to $\mathbf{Q}_J$ zero-forcing to the Rx and the Ev respectively. AC is a curve on which $\mathrm{Tr}(\mathbf{Q}_J) = P_J$. The optimal point must be on AB, the "southeastern" boundary. Points on AB can be computed by finding a line $\alpha = k\beta + d$ tangent to the boundary.

to the largest generalized eigenvalue[1] of $\{\mathbf{A}, \mathbf{B}\}$.

What remains is to find the optimal (α^*, β^*) and the corresponding $\mathbf{Q}_J^*$ that maximize (2.9).

2.3.2 Optimal Jamming levels (α^*, β^*)

Denote the region of all possible (α, β) as

$$\mathcal{R} = \{(\alpha, \beta) \,|\alpha = \mathrm{Tr}\left(\mathbf{R}_J \mathbf{Q}_J\right), \beta = \mathrm{Tr}\left(\mathbf{E}_J \mathbf{Q}_J\right), \mathbf{Q}_J \succeq 0, \mathrm{Tr}\left(\mathbf{Q}_J\right) \leq P_J\}\,. \tag{2.10}$$

[1]The generalized eigenvalue-eigenvector pair $(\lambda, \mathbf{u})$ of $(\mathbf{A}, \mathbf{B})$ is the pair satisfying $\mathbf{A}\mathbf{u} = \lambda\mathbf{B}\mathbf{u}$.

The region $\mathcal{R}$ has the following properties. Fig. 2.2 provides an example for helping understand the properties:

1. $\mathcal{R}$ is in the first quadrant since $\alpha \geq 0, \beta \geq 0$,

2. $\mathcal{R}$ is a convex set,

3. For every $(\alpha, \beta) \in \mathcal{R}$ and $0 \leq \rho \leq 1$, we have that $(\rho\alpha, \rho\beta) \in \mathcal{R}$. The geometric interpretation for this statement is that $\mathcal{R}$ radiates from the origin. The reason is that for any $(\alpha, \beta) \in \mathcal{R}$ with the corresponding $\mathbf{Q}_J$, then $(\rho\alpha, \rho\beta), 0 \leq \rho \leq 1$ with $\rho\mathbf{Q}_J$ is also an element of (2.10).

Based on these properties, it can be concluded that the boundary of $\mathcal{R}$ will consist of three segments, two lines and a curve. The "southern" and the "western" boundaries are two lines radiating from the origin, illustrated by OA and OC in Fig. 2.2. Line OA corresponds to $\mathbf{Q}_J$ that is ZF to the Rx; line OC is where $\mathbf{Q}_J$ is ZF to the Ev.

By property (3), the outer boundary (the curve AC) at the "northeast" must be a curve on which $\mathrm{Tr}(\mathbf{Q}_J) = P_J$. We prove (the proof is omitted here) the optimal point must be on the curve AB, where A is the ZF point and B is the most "eastern" point.

Next, all the points on AB can be computed by finding lines $\{\alpha = k\beta + d\}$ that touch AB, where k is the slope of the line and d is the intercept on the vertical axis. Given a fixed slope $k > 0$, the tangent line is the one with the minimum possible d among all the lines $\{\alpha = k\beta + d, d \in R\}$ that intersect $\mathcal{R}$. The minimum d and the corresponding $\mathbf{Q}_n$ can be found by solving

$$\begin{aligned} &\min_{\mathbf{Q}_n} \quad d \\ \text{s.t.} \quad &\mathrm{Tr}\left(\mathbf{R}_J\mathbf{Q}_J\right) = k\mathrm{Tr}\left(\mathbf{E}_J\mathbf{Q}_J\right) + d, \\ &\mathbf{Q}_J \succeq 0, \mathrm{Tr}\left(\mathbf{Q}_J\right) = P_J, \end{aligned} \tag{2.11}$$

where the constraints of (2.11) ensures that the line intersects $\mathcal{R}$. The solution to (2.11) is given by $\mathbf{Q}_J = P_J\mathbf{q}_J\mathbf{q}_J^H$, where $\mathbf{q}_J$ is the eigenvector corresponding to $\lambda_{\min}\left(\mathbf{R}_J - k\mathbf{E}_J\right)$.

Subsequently the tangent point is calculated by substituting the resulting $\mathbf{Q}_J$ into (2.10). Varying k from 0 to ∞, we can find $\mathbf{Q}_J$ corresponding to all the points on AB.

To sum up, the optimal (α^*, β^*) maximizing (2.9) must be on AB, and all points on AB can be found by solving the tangent line problem (2.11) with different k. The overall algorithm for the optimal (α^*, β^*) is essentially a one-dimensional search for the optimal k^*, and summarized in the following table.

Finding the optimal (α^*, β^*) by a one-dimensional search on AB,
or equivalently, finding the optimal $k^* \in [0, \infty)$.

1: Given k, compute $\mathbf{Q}_J = P_J \mathbf{q}_J \mathbf{q}_J^H$, where $\mathbf{q}_J$ is the eigenvector corresponding to $\lambda_{\min}(\mathbf{R}_J - k\mathbf{E}_J)$. The tangent point is given by $\alpha = \mathrm{Tr}(\mathbf{R}_J \mathbf{Q}_J), \beta = \mathrm{Tr}(\mathbf{E}_J \mathbf{Q}_J)$.

2: Evaluate $\lambda_{\max}\left(\mathbf{I} + \frac{P_T}{\alpha+N_0}\mathbf{R}_T, \mathbf{I} + \frac{P_T}{\beta+N_0}\mathbf{E}_T\right)$.

After obtaining the optimal k^*, together with the resulting $\mathbf{Q}_J^*$ and (α^*, β^*), the optimal $\mathbf{Q}_T^*$ is $\mathbf{Q}_T^* = P_T \mathbf{q}_T^* \mathbf{q}_T^{*H}$ where $\mathbf{q}_T$ is the eigenvector corresponding to $\lambda_{\max}\left(\mathbf{I} + \frac{P_T}{\alpha+N_0}\mathbf{R}_T, \mathbf{I} + \frac{P_T}{\beta+N_0}\mathbf{E}_T\right)$.

Since the outer loop is a one-dimensional search of k^* while inside the loop is only two eigenvalue computations, the total computational load is affordable.

2.4 MISOSE: Numerical Examples

This section presents a numerical example for the optimal cooperative jamming. After investigating many channel realizations, we find that a non-ZF $\mathbf{Q}_J$ shows little improvement over the ZF $\mathbf{Q}_J$ when $\mathbf{r}_T$ and $\mathbf{e}_T$ are nearly orthogonal. However, when $\mathbf{r}_T$ and $\mathbf{e}_T$ are correlated, a non-ZF $\mathbf{Q}_J$ shows significant improvement. Take two extreme cases as examples. In an extreme case when $\mathbf{r}_T$ and $\mathbf{e}_T$ are orthogonal, transmit beamforming $\mathbf{q}_T = \frac{\mathbf{r}_T}{||\mathbf{r}_T||}$ will maximize the signal level at Rx and null the signal level at the Ev simultaneously, making collaborative jamming useless. At the other extreme case when $\mathbf{r}_T$ and $\mathbf{e}_T$ are equal, the signal level at Rx and that at the Ev will be equal, so the secrecy relies highly on jamming the Ev. The following example shows that a non-ZF $\mathbf{Q}_J$ can improve C_{sec} significantly.

Suppose the Tx and the Jm are equipped with 2 antennas. Let $P_T = 2N_0$ and $P_J = 2N_0$.

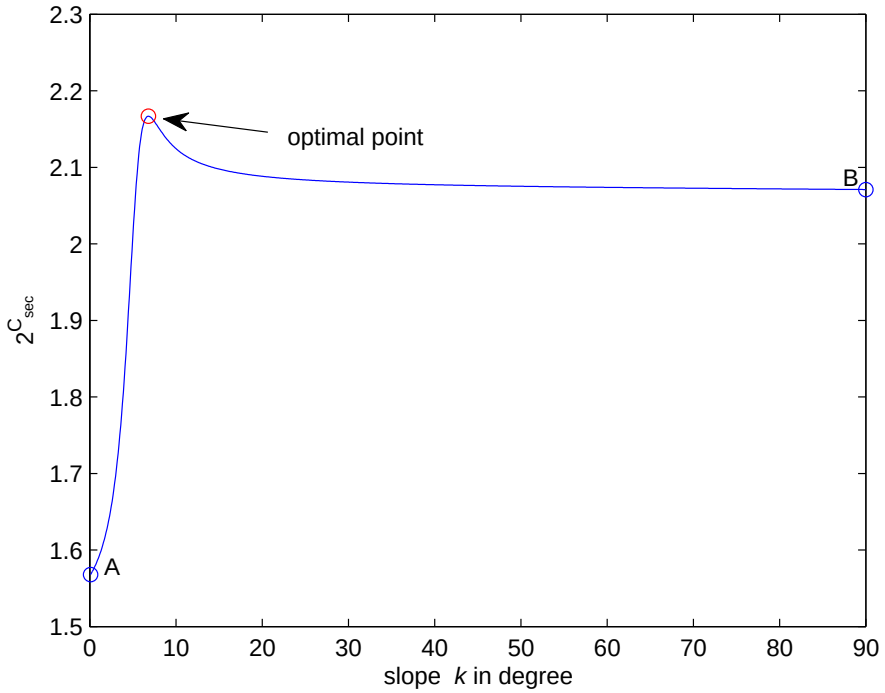


Figure 2.3: The secrecy rate (2.9) versus the jamming levels (α, β) on the curve AB in Fig. 2.2. The point on AB in Fig. 2.2 is represented by the tangent point where the tangent line of slope k ($k \in [\tan(0°), \tan(90°))$) touches the boundary.

Let the channels be

$$\mathbf{r}_T = \begin{bmatrix} 1.5139 - 0.5026i \\ 0.0856 + 0.7058i \end{bmatrix}, \mathbf{r}_J = \begin{bmatrix} 0.1197 + 0.4821i \\ -0.0857 - 0.4760i \end{bmatrix}, \tag{2.12}$$

$$\mathbf{e}_T = \begin{bmatrix} 2.1170 + 0.8067i \\ 0.0990 + 1.0169i \end{bmatrix}, \mathbf{e}_J = \begin{bmatrix} -0.9334 + 0.9850i \\ 1.4725 - 0.7467i \end{bmatrix}. \tag{2.13}$$

The achievable region of (α, β) is given in Fig. 2.2. Point A is the ZF jamming point, yielding jamming levels $(\alpha_A, \beta_A) = (0, 0.2833)$. The jamming covariance $\mathbf{Q}_J$ at A is $\mathbf{Q}_J = P_J \mathbf{q}_J \mathbf{q}_J^H$, where

$$\mathbf{q}_J = \frac{\Pi_{\mathbf{r}_J}^{\perp} \mathbf{e}_J}{||\Pi_{\mathbf{r}_J}^{\perp} \mathbf{e}_J||} = \begin{bmatrix} 0.2558 + 0.0590i \\ 0.2583 + 0.0776i \end{bmatrix}. \tag{2.14}$$

The secrecy rate (2.9) given the jamming levels (α_A, β_A) is $\log_2(1.5659)$.

Varying the slope k of the tangent line, all the points on the curve AB and the corresponding $\mathbf{Q}_J$ can be found. The secrecy rate (2.9) for each point on the curve AB is evaluated and plotted in Fig. 2.3, where the horizontal axis is slope k and corresponds to the tangent point on AB where a tangent line of slope k touches the boundary. The optimal slope is $k^* = \tan(6.8^\circ) = 0.1192$, and the resulting secrecy rate is $C^*_{\text{sec}} = \log_2(2.1667)$. By solving (2.11), the optimal $\mathbf{Q}^*_J$ at this optimal point is $\mathbf{Q}^*_J = P_J \mathbf{q}^*_J \mathbf{q}^{*H}_J$, where

$$\mathbf{q}^*_J = \begin{bmatrix} -0.0689 + 0.4312i \\ 0.8996 \end{bmatrix}. \tag{2.15}$$

The optimal point in Fig. 2.2, where the line $\alpha = k^*\beta + d$ touches the boundary, is $(\alpha^*, \beta^*) = (0.5565, 6.8068)$. Comparing the optimal point with the ZF point A in Fig. 2.2, it can be seen that at the optimal point the jamming level at Ev increases from $\beta_A = 0.2833$ to $\beta_* = 6.8068$ only with a small cost of increasing the jamming at Rx by $\alpha^* = 0.5565$. The optimal $\mathbf{Q}^*_T$, at the given (α^*, β^*), is given by $\mathbf{Q}^*_T = P_T \mathbf{q}^*_T \mathbf{q}^{*H}_T$ where

$$\mathbf{q}^*_T = \mathcal{P}\left\{\mathbf{I} + \frac{P_T}{\alpha^* + N_0}\mathbf{R}_T, \mathbf{I} + \frac{P_T}{\beta^* + N_0}\mathbf{E}_T\right\} = \begin{bmatrix} 0.7342 + 0.2367i \\ -0.6363 \end{bmatrix}. \tag{2.16}$$

2.5 MIMOME: Problem Formulation of Cooperative Jamming

As shown in Fig. 2.4 (a), we consider a wiretap system model consisting of one transmitter (Tx), one cooperative jammer (Jm), one legitimate receiver (Rx) and one eavesdropper (Ev), with M_T, M_J, M_r, M_e antennas, respectively. The Tx wants to send a message to the Rx and does not want the message leaked to the Ev. The cooperative Jm broadcasts an artificial noise which aims to significantly increase the noise level at the Ev while harm the received signal at the Rx as little as possible.

The Tx transmits a narrowband signal $\mathbf{x} \in \mathbb{C}^{M_T \times 1}$ and the transmit covariance is $\mathbf{Q}_T = E\left\{\mathbf{x}\mathbf{x}^H\right\}$. At the same time, the Jm broadcasts an artificial Gaussian noise $\mathbf{z} \in \mathbb{C}^{M_J \times 1}$ with covariance $\mathbf{Q}_J = E\left\{\mathbf{z}\mathbf{z}^H\right\}$. The transmitted signal and the jamming noise satisfies Tx's and Jm's power constraints: $\text{Tr}(\mathbf{Q}_T) \le P_T$ and $\text{Tr}(\mathbf{Q}_J) \le P_J$, respectively. The channels from the Tx and the Jm to the Rx are denoted by $\mathbf{R}_T \in \mathbb{C}^{M_r \times M_T}$ and $\mathbf{R}_J \in \mathbb{C}^{M_r \times M_J}$, respectively, and those to the Ev are denoted by $\mathbf{E}_T \in \mathbb{C}^{M_e \times M_T}$ and $\mathbf{E}_J \in \mathbb{C}^{M_e \times M_J}$, respectively.

The received signals at the Rx and the Ev are given by, respectively

$$\begin{aligned} \mathbf{y}_r &= \mathbf{R}_T\mathbf{x} + \mathbf{R}_J\mathbf{z} + \mathbf{n}_r, \\ \mathbf{y}_e &= \mathbf{E}_T\mathbf{x} + \mathbf{E}_J\mathbf{z} + \mathbf{n}_e, \end{aligned} \tag{2.17}$$

where $\mathbf{n}_r$ and $\mathbf{n}_e$ are additive Gaussian noise with covariance matrix $\sigma^2\mathbf{I}$. Without loss of generality, we assume $\sigma^2 = 1$ for simplicity of the expression of secrecy rate.

Assume all the channels are perfectly known at both the Tx and the Jm. The Rx also knows the covariance matrix of the Jm. At the receiving side, the Rx knows its channel matrices, and the Ev is aware of all the channel matrices and both the Tx's and the Jm's covariance matrices. The secrecy rate is equal to the difference between the rates of the Rx and the Ev channels [67], and is maximized by jointly optimizing $\mathbf{Q}_T$ and $\mathbf{Q}_J$,

$$\begin{aligned} C_{\text{sec}} = \max_{\substack{\mathbf{Q}_T \succeq 0, \text{Tr}(\mathbf{Q}_T) \le P_T \\ \mathbf{Q}_J \succeq 0, \text{Tr}(\mathbf{Q}_J) \le P_J}} & \left\{ \begin{array}{c} \log\det\left(\mathbf{I} + \left(\mathbf{I} + \mathbf{R}_J\mathbf{Q}_J\mathbf{R}_J^H\right)^{-1}\mathbf{R}_T\mathbf{Q}_T\mathbf{R}_T^H\right) \\ -\log\det\left(\mathbf{I} + \left(\mathbf{I} + \mathbf{E}_J\mathbf{Q}_J\mathbf{E}_J^H\right)^{-1}\mathbf{E}_T\mathbf{Q}_T\mathbf{E}_T^H\right) \end{array} \right\} \end{aligned} \tag{2.18}$$

where $\mathbf{Q} \succeq 0$ denotes $\mathbf{Q}$ is a positive semidefinite matrix.

2.5.1 Previous work: no jamming

For no jamming, i.e. $\mathbf{Q}_J = \mathbf{0}$, the maximization of the secrecy rate (2.18) is reduced to

$$C_{\text{sec}} = \max_{\mathbf{Q}_T \succeq 0, \text{Tr}(\mathbf{Q}_T) \le P_T} \left\{ \begin{array}{c} \log\det\left(\mathbf{I} + \mathbf{R}_T\mathbf{Q}_T\mathbf{R}_T^H\right) \\ -\log\det\left(\mathbf{I} + \mathbf{E}_T\mathbf{Q}_T\mathbf{E}_T^H\right) \end{array} \right\}. \tag{2.19}$$

Under the average power constraint $\text{Tr}(\mathbf{Q}_T) \le P_T$, the solution to this problem is unknown, to the best knowledge of the authors.

But under a different matrix constraint $\mathbf{Q}_T \preceq \mathbf{S}$, where $\mathbf{S}$ is a given positive semi-definite matrix, the problem is solvable [5]. It is shown that the solution to

$$C_{\text{sec}}(\mathbf{S}) = \max_{0 \preceq \mathbf{Q}_T \preceq \mathbf{S}} \left\{ \begin{array}{c} \log\det\left(\mathbf{I} + \mathbf{R}_T\mathbf{Q}_T\mathbf{R}_T^H\right) \\ -\log\det\left(\mathbf{I} + \mathbf{E}_T\mathbf{Q}_T\mathbf{E}_T^H\right) \end{array} \right\} \tag{2.20}$$

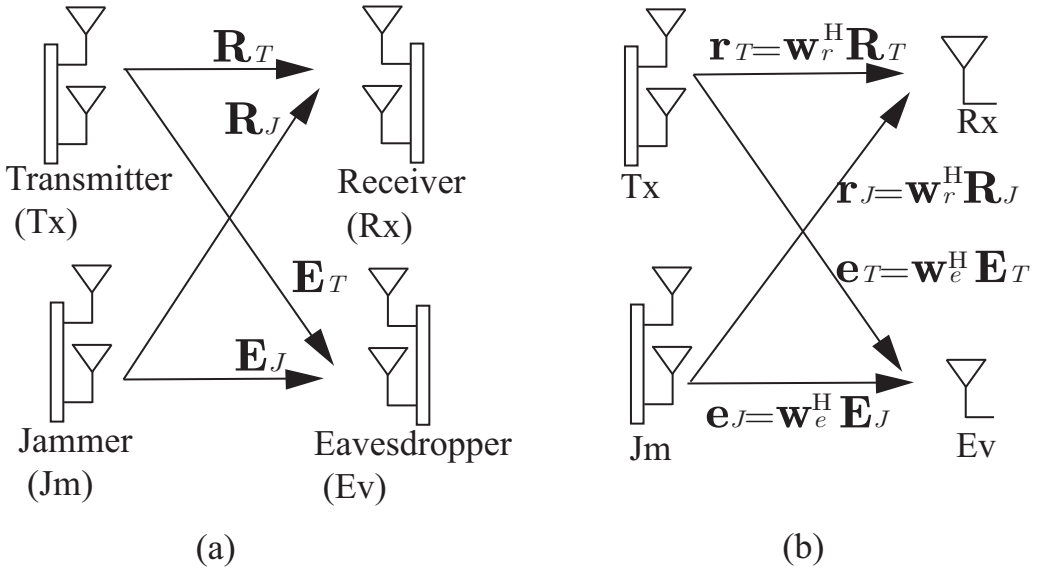


Figure 2.4: (a) The system model for the MIMOME wiretap channel with a transmitter, a jammer, a receiver and an eavesdropper, each with multiple antennas. (b) The equivalent MISOSE channel of the original MIMOME channel, assuming the Rx and Ev adopt receiving beamformers $\mathbf{w}_r^*$ and $\mathbf{w}_e^*$, respectively.

is given by

$$C_{\text{sec}}(\mathbf{S}) = \sum \log\left(\lambda_i\right) \tag{2.21}$$

where λ_i's are the larger-than-unity generalized eigenvalues of the matrix pair

$$\left(\begin{array}{c} \mathbf{I} + \mathbf{S}^{\frac{1}{2}} \mathbf{R}_T^H \mathbf{R}_T \mathbf{S}^{\frac{1}{2}}, \\ \mathbf{I} + \mathbf{S}^{\frac{1}{2}} \mathbf{E}_T^H \mathbf{E}_T \mathbf{S}^{\frac{1}{2}} \end{array} \right). \tag{2.22}$$

2.5.2 Problem transformation when $\mathbf{Q}_J$ is fixed

For a given $\mathbf{Q}_J$, the artificial noise plus the background noise in (2.17) is non-white Gaussian noise with variance $\mathbf{R}_J \mathbf{Q}_J \mathbf{R}_J^H + \mathbf{I}$ at the Rx and $\mathbf{E}_J \mathbf{Q}_J \mathbf{E}_J^H + \mathbf{I}$ at the Ev. Without changing the secrecy rate, the system model (2.17) can be rewritten equivalently as, after passing $\mathbf{y}_r$ and $\mathbf{y}_e$ into whitening filters,

$$\begin{aligned} \tilde{\mathbf{y}}_r &= \tilde{\mathbf{R}}_T \mathbf{x} + \tilde{\mathbf{n}}_r = \left(\mathbf{R}_J \mathbf{Q}_J \mathbf{R}_J^H + \mathbf{I}\right)^{-\frac{1}{2}} \mathbf{R}_T \mathbf{x} + \tilde{\mathbf{n}}_r, \\ \tilde{\mathbf{y}}_e &= \tilde{\mathbf{E}}_T \mathbf{x} + \tilde{\mathbf{n}}_e = \left(\mathbf{E}_J \mathbf{Q}_J \mathbf{E}_J^H + \mathbf{I}\right)^{-\frac{1}{2}} \mathbf{E}_T \mathbf{x} + \tilde{\mathbf{n}}_e, \end{aligned} \tag{2.23}$$

where $\tilde{\mathbf{n}}_r$ and $\tilde{\mathbf{n}}_e$ are white Gaussian noise with variance $\mathbf{I}$. This equivalent system model (2.23) can be viewed the same as the case of no jamming, except that the channel matrices $\mathbf{R}_T$ and $\mathbf{E}_T$ have been "transformed" by the jamming noise. The secrecy rate of the effective channels $\tilde{\mathbf{R}}_T$ and $\tilde{\mathbf{E}}_T$ in (2.23) yields (2.18).

Therefore the key to the joint optimization of (2.18) is to find $\mathbf{Q}_J$: once $\mathbf{Q}_J$ is given, a good solution of $\mathbf{Q}_T$ at the given $\mathbf{Q}_J$ can be computed accordingly by substituting $\tilde{\mathbf{R}}_T$ and $\tilde{\mathbf{E}}_T$ into (2.22).

2.5.3 Single data stream: rank($\mathbf{Q}_T$) = 1

In general, the optimal transmit covariance $\mathbf{Q}_T$ for the MIMO wiretap channel is a multi-rank matrix, meaning multiple data streams are transmitted. A special case is that only single data stream is sent, that is, $\text{rank}(\mathbf{Q}_T) = 1$. Although the rank-one $\mathbf{Q}_T$ is generally not optimal for MIMO channels, it is still of significant interest to solve problem (2.18) under the additional constraint $\text{rank}(\mathbf{Q}_T) = 1$. The reasons for the rank-one constraint are as follows. First, for $M_T = 2$, M_J =arbitrary number, $M_r = 2$, $M_e = 1$, $\text{rank}(\mathbf{Q}_T)$ must be 1. For this setting, the equivalent $\tilde{\mathbf{R}}_T$ and $\tilde{\mathbf{E}}_T$ is a 2-2-1 wiretap channel, i.e. $M_T = 2$, $M_r = 2$, $M_e = 1$. It is shown in [49] that the optimal $\mathbf{Q}_T$ for the 2-2-1 wiretap channel must be a rank-one matrix. Second, $\text{rank}(\mathbf{Q}_T)$ will be 1 at low SNR region. It is well-known that beamforming is optimal for MIMO systems in the low SNR region, explained by the waterfilling property. Like MIMO channels, beamforming is optimal for MIMOME wiretap channels at low SNR. Finally, beamforming enables low-complexity design at both the Tx and the Rx side. Because of these reasons, we study problem (2.18) under the additional constraint $\text{rank}(\mathbf{Q}_T) = 1$.

Under the rank-one constraint, problem (2.18) can be simplified to an optimization problem that contains only $\mathbf{Q}_J$. First, it can be proved that $\text{Tr}(\mathbf{Q}_T) = P_T$, as long as $C_{\text{sec}} > 0$. The proof is omitted here due to page limit. Then problem (2.18) under the rank-1 constraint can be reformulated so that the part of optimizing $\mathbf{Q}_T$ at any fixed $\mathbf{Q}_J$ is a Rayleigh quotient problem, shown as below. The optimal $\mathbf{q}_T$ is the principle generalized eigenvector of the matrix pair of (2.24).

$$
\begin{aligned}
C_{\text{sec ,rank-1}} &= \max_{\substack{\mathbf{Q}_T=P_T\mathbf{q}_T\mathbf{q}_T^H,\|\mathbf{q}_T\|=1\\ \mathbf{Q}_J\succeq 0,\mathrm{Tr}(\mathbf{Q}_J)\le P_J}} \\
&\log\frac{\det\left(\mathbf{I}+\left(\mathbf{I}+\mathbf{R}_J\mathbf{Q}_J\mathbf{R}_J^H\right)^{-1}\mathbf{R}_T\mathbf{Q}_T\mathbf{R}_T^H\right)}{\det\left(\mathbf{I}+\left(\mathbf{I}+\mathbf{E}_J\mathbf{Q}_J\mathbf{E}_J^H\right)^{-1}\mathbf{E}_T\mathbf{Q}_T\mathbf{E}_T^H\right)} \\
= &\max_{\substack{\|\mathbf{q}_T\|=1\\ \mathbf{Q}_J\succeq 0,\\ \mathrm{Tr}(\mathbf{Q}_J)\le P_J}} \log\frac{\mathbf{q}_T^H\left(\mathbf{I}+P_T\mathbf{R}_T^H\left(\mathbf{I}+\mathbf{R}_J\mathbf{Q}_J\mathbf{R}_J^H\right)^{-1}\mathbf{R}_T\right)\mathbf{q}_T}{\mathbf{q}_T^H\left(\mathbf{I}+P_T\mathbf{E}_T^H\left(\mathbf{I}+\mathbf{E}_J\mathbf{Q}_J\mathbf{E}_J^H\right)^{-1}\mathbf{E}_T\right)\mathbf{q}_T} \\
= &\max_{\substack{\mathbf{Q}_J\succeq 0,\\ \mathrm{Tr}(\mathbf{Q}_J)\le P_J}} \log\lambda_{\max}\left(\begin{array}{c}\mathbf{I}+P_T\mathbf{R}_T^H\left(\mathbf{I}+\mathbf{R}_J\mathbf{Q}_J\mathbf{R}_J^H\right)^{-1}\mathbf{R}_T,\\ \mathbf{I}+P_T\mathbf{E}_T^H\left(\mathbf{I}+\mathbf{E}_J\mathbf{Q}_J\mathbf{E}_J^H\right)^{-1}\mathbf{E}_T\end{array}\right). \qquad (2.24)
\end{aligned}
$$

The remaining problem (2.24) only need to search $\mathbf{Q}_J$. Blindly searching cannot guaranteer a good solution. Indeed, it will be shown in Section IV that using matlab built-in function fmincon to blindly search will stagnate at many local optimums. Our contribution is that we propose a method of iterative 1-dim search guided by the search boundary of MISOSE wiretap channels.

2.6 MIMOME: Iterative Algorithm

In this section, we first present the result of MISOSE channel that reduces the search region of $\mathbf{Q}_J$ to a boundary and yields a 1-dim search algorithm. Then we relate the MIMOME channel to the MISOSE channel, and propose an iterative algorithm that utilize the search boundary of MISOSE channel to guide the search of $\mathbf{Q}_J$ of the MIMOME channel.

2.6.1 1-dim search for MISOSE wiretap channels

Consider a MISOSE wiretap channel shown in Fig. 2.4 (b). The channels from the Tx and the Jm to the Rx are denoted by $\mathbf{r}_T \in \mathbb{C}^{1\times M_T}$ and $\mathbf{r}_J \in \mathbb{C}^{1\times M_J}$, respectively, and those to the Ev are denoted by $\mathbf{e}_T \in \mathbb{C}^{1\times M_T}$ and $\mathbf{e}_J \in \mathbb{C}^{1\times M_J}$, respectively. The received signals at the Rx and the Ev are given by, respectively

$$
\begin{aligned}
y_r &= \mathbf{r}_T\mathbf{x}+\mathbf{r}_J\mathbf{z}+n_r, \\
y_e &= \mathbf{e}_T\mathbf{x}+\mathbf{e}_J\mathbf{z}+n_e. \qquad (2.25)
\end{aligned}
$$

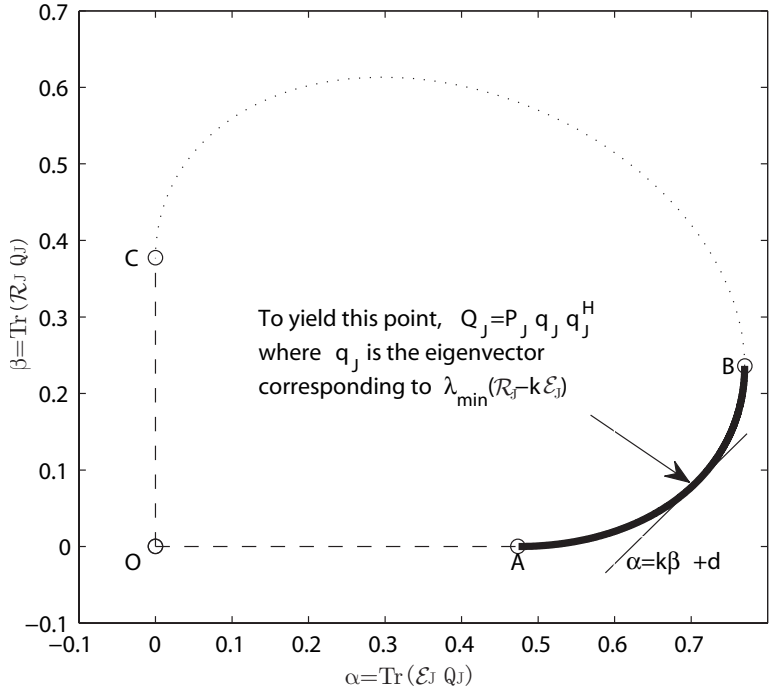


Figure 2.5: The achievable region of $(\mathrm{Tr}\left(\mathcal{R}_J\mathbf{Q}_J\right), \mathrm{Tr}\left(\mathcal{E}_J\mathbf{Q}_J\right))$. The optimal point must be on AB, the "southeastern" boundary. Points on AB can be computed by finding a line $\alpha = k\beta + d$ tangent to the boundary.

The secrecy rate for this wiretap channel is given by

$$\begin{aligned} & \max_{\substack{\mathbf{Q}_T\succeq 0, \mathrm{Tr}(\mathbf{Q}_T)\le P_T \\ \mathbf{Q}_J\succeq 0, \mathrm{Tr}(\mathbf{Q}_J)\le P_J}} \left\{ \begin{array}{c} \log\left(1+\frac{\mathbf{r}_T\mathbf{Q}_T\mathbf{r}_T^H}{r_J\mathbf{Q}_J\mathbf{r}_J^H+1}\right) - \\ \log\left(1+\frac{\mathbf{e}_T\mathbf{Q}_T\mathbf{e}_T^H}{\mathbf{e}_J\mathbf{Q}_J\mathbf{e}_J^H+1}\right) \end{array} \right\} \\ = & \max_{\substack{\mathbf{Q}_T\succeq 0, \mathrm{Tr}(\mathbf{Q}_T)\le P_T \\ \mathbf{Q}_J\succeq 0, \mathrm{Tr}(\mathbf{Q}_J)\le P_J}} \log \frac{1+\frac{\mathrm{Tr}(\mathcal{R}_T\mathbf{Q}_T)}{\mathrm{Tr}(\mathcal{R}_J\mathbf{Q}_J)+1}}{1+\frac{\mathrm{Tr}(\mathcal{E}_T\mathbf{Q}_T)}{\mathrm{Tr}(\mathcal{E}_J\mathbf{Q}_J)+1}}, \end{aligned} \tag{2.26}$$

where $\mathcal{R}_T = \mathbf{r}_T^H\mathbf{r}_T$ etc.

Fig. 2.5 shows an example of the achievable region of (α, β) where $\alpha = \mathrm{Tr}(\mathcal{R}_J\mathbf{Q}_J)$ and $\beta = \mathrm{Tr}(\mathcal{E}_J\mathbf{Q}_J)$. The point yielded by the optimal $\mathbf{Q}_J^*$ must be on the "southeast" boundary, the bold curve in the figure. This is because that decreasing $\mathrm{Tr}(\mathcal{R}_J\mathbf{Q}_J)$ and increasing $\mathrm{Tr}(\mathcal{E}_J\mathbf{Q}_J)$ simultaneously will increase the objective in (2.26). In Fig. 2.5, this corresponds to moving towards the "southeast". Therefore the search space of $\mathbf{Q}_J$ can be reduced to

the boundary, i.e. a 1-dim search.

Any point on AB can be computed by finding a line $\{\alpha = k\beta + d\}$ that touches AB, where k is the slope and d is the intercept on the vertical axis. Given a fixed slope $k > 0$, the tangent line is the one with the minimum possible d. The minimum d and the corresponding $\mathbf{Q}_J$ can be found by solving

$$\begin{aligned} &\min_{\mathbf{Q}_J} \quad d \\ \text{s.t.} \quad &\mathrm{Tr}\left(\mathcal{R}_J \mathbf{Q}_J\right) = k\mathrm{Tr}\left(\mathcal{E}_J \mathbf{Q}_J\right) + d, \\ &\mathbf{Q}_J \succeq 0, \mathrm{Tr}\left(\mathbf{Q}_J\right) = P_J, \end{aligned} \tag{2.27}$$

in which the constraints of the above optimization ensures that the line intersects $\mathcal{R}$. The solution to (2.27) is given by $\mathbf{Q}_J = P_J \mathbf{q}_J \mathbf{q}_J^H$, where $\mathbf{q}_J$ is the eigenvector corresponding to $\lambda_{\min}\left(\mathcal{R}_J - k\mathcal{E}_J\right)$. Therefore, the search space of $\mathbf{Q}_J$ for the MISOSE channel is reduced to a 1-dim search of k that

$$\left\{ (k, \mathbf{Q}_J) \,\middle|\, \begin{array}{l} \mathbf{Q}_J = P_J \mathbf{q}_J \mathbf{q}_J^H, \\ \mathbf{q}_J = \text{eigenvector of } \lambda_{\min}\left(\mathcal{R}_J - k\mathcal{E}_J\right), \\ k \in [0, \infty) \end{array} \right\}. \tag{2.28}$$

2.6.2 Reducing MIMOME to MISOSE channel

Under the rank-1 constraint, the transmitted vector signal is a beamforming vector $\mathbf{x} = \sqrt{P_T}\mathbf{q}_T b$ where b is a information bit. Given $\mathbf{Q}_T$ and $\mathbf{Q}_J$, the receiving beamformers at the Rx and the Ev are given by maximizing the received SINR's of the information bit, respectively,

$$\begin{aligned} \mathbf{w}_r &= \arg\max_{\|\mathbf{w}\|=1} \frac{\mathbf{w}^H \left(\mathbf{R}_T \mathbf{Q}_T \mathbf{R}_T^H\right) \mathbf{w}}{\mathbf{w}^H \left(\mathbf{R}_J \mathbf{Q}_J \mathbf{R}_J^H + \mathbf{I}\right) \mathbf{w}} \\ &= \mathcal{P}\left(\mathbf{R}_T \mathbf{Q}_T \mathbf{R}_T^H, \mathbf{R}_J \mathbf{Q}_J \mathbf{R}_J^H + \mathbf{I}\right), \\ \mathbf{w}_e &= \mathcal{P}\left(\mathbf{E}_T \mathbf{Q}_T \mathbf{E}_T^H, \mathbf{E}_J \mathbf{Q}_J \mathbf{E}_J^H + \mathbf{I}\right), \end{aligned} \tag{2.29}$$

where $\mathcal{P}(\cdot)$ denotes the principle generalized eigenvector. When $\mathbf{w}_r$ and $\mathbf{w}_e$ are used at the Rx and the Ev respectively, the MIMOME channel is effectively a MISOSE channel shown in Fig. 2.4 (b), where the effective channel vector from the multi-antenna Tx to the

equivalent single-antenna Rx is $\mathbf{w}_r^H \mathbf{R}_T \in \mathbb{C}^{1\times M_T}$ and so on. The secrecy rate in terms of $\mathbf{Q}_T$ and $\mathbf{Q}_J$

$$\log \frac{\det\left(\mathbf{I}+\left(\mathbf{I}+\mathbf{R}_J\mathbf{Q}_J\mathbf{R}_J^H\right)^{-1}\mathbf{R}_T\mathbf{Q}_T\mathbf{R}_T^H\right)}{\det\left(\mathbf{I}+\left(\mathbf{I}+\mathbf{E}_J\mathbf{Q}_J\mathbf{E}_J^H\right)^{-1}\mathbf{E}_T\mathbf{Q}_T\mathbf{E}_T^H\right)}, \mathrm{rank}\left(\mathbf{Q}_T\right)=1$$

can also be equivalently expressed as

$$\begin{aligned} & \log\left(1+\mathrm{SINR}_r\right)-\log\left(1+\mathrm{SINR}_e\right) \\ = & \log\frac{1+\frac{\mathbf{w}_r^H\left(\mathbf{R}_T\mathbf{Q}_T\mathbf{R}_T^H\right)\mathbf{w}_r}{\mathbf{w}_r^H\left(\mathbf{R}_J\mathbf{Q}_J\mathbf{R}_J^H+\mathbf{I}\right)\mathbf{w}_r}}{1+\frac{\mathbf{w}_e^H\left(\mathbf{R}_T\mathbf{Q}_T\mathbf{R}_T^H\right)\mathbf{w}_e}{\mathbf{w}_e^H\left(\mathbf{R}_J\mathbf{Q}_J\mathbf{R}_J^H+\mathbf{I}\right)\mathbf{w}_e}} \\ = & \log\frac{1+\frac{\mathrm{Tr}\left(\mathbf{R}_T^H\mathbf{W}_r\mathbf{R}_T\mathbf{Q}_T\right)}{\mathrm{Tr}\left(\mathbf{R}_J^H\mathbf{W}_r\mathbf{R}_J\mathbf{Q}_J\right)+1}}{1+\frac{\mathrm{Tr}\left(\mathbf{E}_T^H\mathbf{W}_e\mathbf{E}_T\mathbf{Q}_T\right)}{\mathrm{Tr}\left(\mathbf{E}_J^H\mathbf{W}_e\mathbf{E}_J\mathbf{Q}_J\right)+1}}, \end{aligned} \tag{2.30}$$

where SINR_r and SINR_e are the received SINR's, $\mathbf{w}_r$ and $\mathbf{w}_e$ are the beamformers for $\mathbf{Q}_T$ and $\mathbf{Q}_J$, and $\mathbf{W}_r = \mathbf{w}_r\mathbf{w}_r^H$ and $\mathbf{W}_e = \mathbf{w}_e\mathbf{w}_e^H$ are the receiving covariances.

Let $\mathbf{Q}_T^*$ and $\mathbf{Q}_J^*$ denote the optimal solution to (2.24). Let $\mathbf{W}_r^*$ and $\mathbf{W}_e^*$ denote the receiving covariances for $\mathbf{Q}_T^*$ and $\mathbf{Q}_J^*$. Assuming $\mathbf{W}_r^*$ and $\mathbf{W}_e^*$ are known, then $\mathbf{Q}_T^*$ and $\mathbf{Q}_J^*$ can be solved by searching on the 1-dim space (2.28) where $\mathcal{R}_J = \mathbf{R}_J^H\mathbf{W}_r^*\mathbf{R}_J$ and $\mathcal{E}_J = \mathbf{E}_J^H\mathbf{W}_e^*\mathbf{E}_J$. Since $\mathbf{W}_r^*$ and $\mathbf{W}_e^*$ are unknown, a practical method is to alternatively 1) search $\mathbf{Q}_T$ on the 1-dim space defined by the inaccurate $\mathbf{W}_r$ and $\mathbf{W}_e$, and 2) update $\mathbf{W}_r$ and $\mathbf{W}_e$ given $\mathbf{Q}_T$ and $\mathbf{Q}_J$, and so on, as shown in Fig. 2.6. As $\mathbf{W}_r$ and $\mathbf{W}_e$ approach to $\mathbf{W}_r^*$ and $\mathbf{W}_e^*$, the optimal $\mathbf{Q}_T^*$ and $\mathbf{Q}_J^*$ are obtained.

The detailed algorithm is given in the following table.

2.7 MIMOME: Numerical Results

In the follwing examples, channels are assumed to be independent Rayleigh fading, and the entries of the channel matrices are i.i.d. distributed as $\mathcal{CN}(0,2)$.

Fig. 2.7 shows the convergence of the proposed algorithm on a $M_T = M_J = M_r = M_e = 3$ channel. The secrecy rate monotonically increases and converges within a few iterations. And all the transmit beamformer $\mathbf{q}_T$, the jamming beamformer $\mathbf{q}_J$ etc. approach to their final beamforming vectors.

Algorithm 1 Iterative algorithm for solving (2.24)

1: INPUT: Channel matrices $\mathbf{R}_T$, $\mathbf{R}_J$, $\mathbf{E}_T$, $\mathbf{E}_J$, and maximum power P_T, P_J.

2: OUTPUT: Jamming covariance $\mathbf{Q}_J$ and the corresponding $\mathbf{Q}_T$.

3: **Initialization:**

Let the iteration index to be $n = 0$.

Randomly initialize $\mathbf{Q}_J(0)$ to be a $M_J \times M_J$ positive semidefinite matrix.

Given $\mathbf{Q}_J(0)$, compute $\mathbf{Q}_T(0)$ to be the beamforming matrix for (2.24).

Given $\mathbf{Q}_J(0)$ and $\mathbf{Q}_T(0)$, calculate $\mathbf{w}_r(0)$ and $\mathbf{w}_e(0)$ using (2.29). The receiving covariances are then given by $\mathbf{W}_r(0) = \mathbf{w}_r(0)\mathbf{w}_r^H(0)$ and $\mathbf{W}_e(0) = \mathbf{w}_e(0)\mathbf{w}_e^H(0)$.

4: **repeat**

5: **Step 1. Optimize $\mathbf{Q}_J(n)$ on the 1-dim boundary defined by the given $\mathbf{W}_r(n)$ and $\mathbf{W}_e(n)$:**

One-dim search on the slope k to maximize the secrecy rate

$$(k^*, \mathbf{Q}_J(n)) = \arg\max \lambda_{\max}\left(\begin{array}{c} \mathbf{I} + P_T\left(\mathbf{I} + \mathbf{R}_J\mathbf{Q}_J\mathbf{R}_J^H\right)^{-1}\mathbf{R}_T\mathbf{Q}_T\mathbf{R}_T^H, \\ \mathbf{I} + P_T\left(\mathbf{I} + \mathbf{E}_J\mathbf{Q}_J\mathbf{E}_J^H\right)^{-1}\mathbf{E}_T\mathbf{Q}_T\mathbf{E}_T^H \end{array}\right),$$

where the 1-dim search space is

$$\left\{(k, \mathbf{Q}_J) \,\middle|\, \begin{array}{l} \mathbf{Q}_J = P_J\mathbf{q}_J\mathbf{q}_J^H, \mathbf{q}_J = \text{eigenvector of} \\ \lambda_{\min}\left(\mathbf{R}_J\mathbf{W}_r(n)\mathbf{R}_J^H - k\mathbf{E}_J\mathbf{W}_e(n)\mathbf{E}_J\right), \\ k \in [0, \infty) \end{array}\right\}$$

After $\mathbf{Q}_J(n)$ is optimized, calculate the corresponding $\mathbf{Q}_T(n)$ to be $\mathbf{Q}_T(n) = P_T\mathbf{q}_T\mathbf{q}_T^H$ where

$$\mathbf{q}_T = \mathcal{P}\left(\begin{array}{c} \mathbf{I} + P_T\left(\mathbf{I} + \mathbf{R}_J\mathbf{Q}_J(n)\mathbf{R}_J^H\right)^{-1}\mathbf{R}_T\mathbf{Q}_T\mathbf{R}_T^H, \\ \mathbf{I} + P_T\left(\mathbf{I} + \mathbf{E}_J\mathbf{Q}_J(n)\mathbf{E}_J^H\right)^{-1}\mathbf{E}_T\mathbf{Q}_T\mathbf{E}_T^H \end{array}\right).$$

6: **Step 2. Update $\mathbf{W}_r(n+1)$ and $\mathbf{W}_e(n+1)$:**

Calculate the receiving beamformers at the given $\mathbf{Q}_J(n)$ and $\mathbf{Q}_T(n)$,

$$\begin{aligned} \mathbf{w}_r(n) &= \mathcal{P}\left(\mathbf{R}_T\mathbf{Q}_T(n)\mathbf{R}_T^H, \mathbf{R}_J\mathbf{Q}_J(n)\mathbf{R}_J^H + \mathbf{I}\right), \\ \mathbf{w}_e(n) &= \mathcal{P}\left(\mathbf{E}_T\mathbf{Q}_T(n)\mathbf{E}_T^H, \mathbf{E}_J\mathbf{Q}_J(n)\mathbf{E}_J^H + \mathbf{I}\right). \end{aligned}$$

Update the new receiving covariances as

$$\begin{aligned} \mathbf{W}_r(n+1) &= \rho\mathbf{W}_r(n) + (1-\rho)\mathbf{w}_r(n)\mathbf{w}_r^H(n), \\ \mathbf{W}_e(n+1) &= \rho\mathbf{W}_e(n) + (1-\rho)\mathbf{w}_e(n)\mathbf{w}_e^H(n), \end{aligned}$$

where $\rho = 0.9$ is a moving average factor.

7: **until** the secrecy rate converges at an adequate precision. Otherwise, $n \leftarrow (n+1)$ and repeat Step 1 and Step 2.

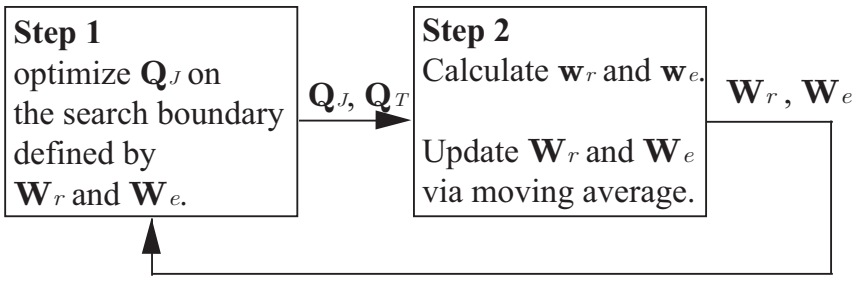


Figure 2.6: The iteration procedure of alternatively 1-dim searching $\mathbf{Q}_J$ and updating $\mathbf{W}_r$ and $\mathbf{W}_e$.

Fig. 2.8 compares the secrecy rate obtained by searching (2.24) using the matlab function fmincon and the proposed algorithm on 20 independently generated channels. The figure shows that at each trial the proposed algorithm achieves higher secrecy rate than the function fmincon. We also observe that when starting with different initial points, the function fmincon arrives at different local optimums. But for the proposed algorithm, the final result is irrelevant to the initial point.

Finally, we compare the proposed algorithm with the existing artificial noise scheme [18]. The scheme in [18] can only deal with a system model consisting of a Tx, a Rx and a Ev. The Rx takes the roles of both transmitting and jamming. This is equivalent to say $\mathbf{R}_T = \mathbf{R}_J$ and $\mathbf{E}_T = \mathbf{E}_J$ in our system model in Fig. 2.4. For simplicity, we assume the transmit power is equally distributed between the signal and the artificial noise. It is assumed in [18] that the Tx does not know the Ev channel, so the joint transmit beamforming and artificial noise scheme only makes use of the channel information on $\mathbf{R}_T$. Specifically, the signal is transmitted along the principal direction of $\mathbf{R}_T$ and the noise is equally broadcast on the remaining dimension of $\mathbf{R}_T$. The transmitted signal is $\mathbf{x} = \sqrt{P_T}\mathbf{q}_T b + \mathbf{z}$, where $\mathbf{q}_T$ is the right singular vector of $\mathbf{R}_T$ with the largest singular value, b is an information bit, and $\mathbf{z}$ is an artificial noise equally distributed in the null space of $\mathbf{q}_T$.

The histogram of the achieved secrecy rate of $M_T = M_r = M_e = 3$ channels by both the proposed algorithm and the existing artificial noise scheme [18] is compared in Fig. 2.9. Our algorithm achieves higher secrecy rate than [18]. The first reason is that our

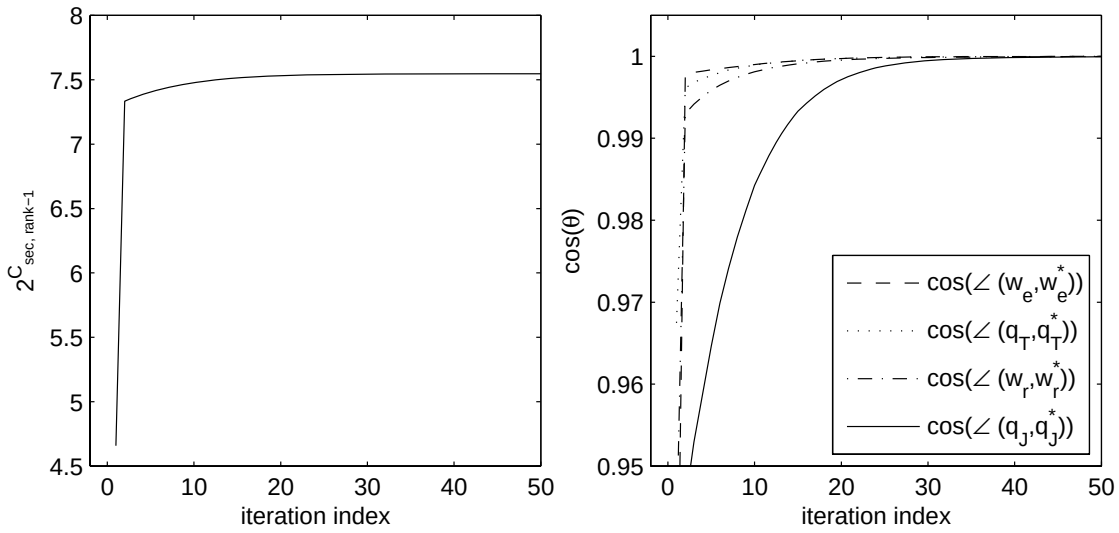


Figure 2.7: A typical iteration of the proposed algorithm on a $M_T = M_J = M_r = M_e = 3$ channel shows that $C_{\text{sec},\text{rank-1}}$ converges and $\mathbf{w}_e$ etc. approach to $\mathbf{w}_e^*$ etc. The maximum power constraint is $P_T = P_J = 10$dB.

algorithm considers the channel information on $\mathbf{E}_T$ (or $\mathbf{E}_J$), whereas in [18] choosing the principal singular vector of $\mathbf{R}_T$ to transmit the signal may not be the optimal transmit beamforming direction. The second reason is that in [18] the jamming noise is constrained to be orthogonal to the signal, which may not be optimal. It is explained in [53] that using a jamming noise that is not orthogonal to the signal may be beneficial to the secrecy rate, because the non-orthogonal jamming noise may greatly raise the noise level at the Ev with little noise level increased at the Rx.

2.8 Conclusion

We have studied the problem of joint transmit and collaborative jamming design to maximize the secrecy rate of MISOSE wiretap channels. The optimal conditions of the transmit and jamming covariances are shown to be that both the covariance are of full power. We reduce the problem of maximizing the secrecy rate to the problem of find the optimal jamming levels. Moreover, finding the optimal jamming levels can be solved by a one-dimensional

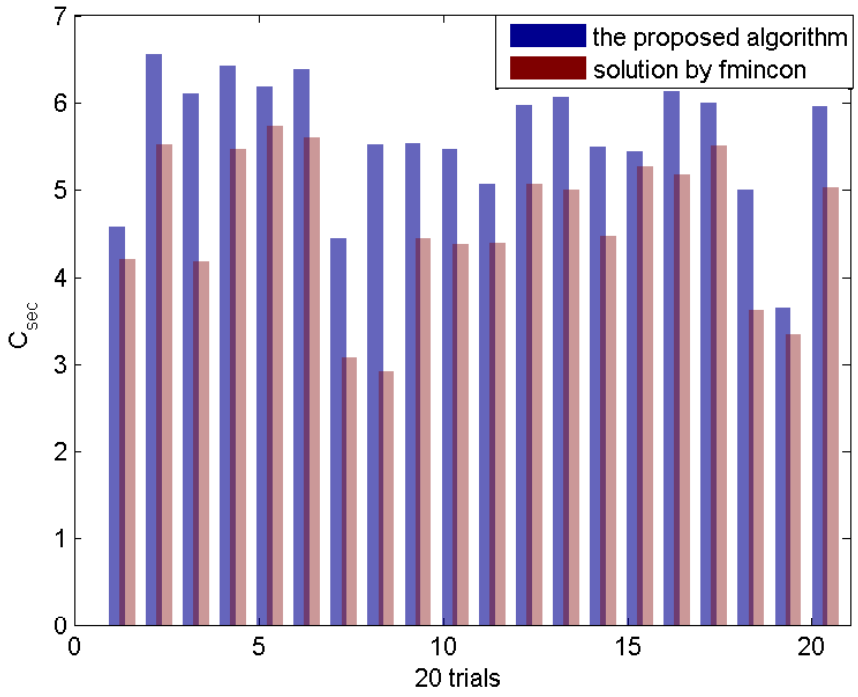


Figure 2.8: For 20 trials of independently generated $M_T = M_J = M_r = M_e = 3$ channels, the secrecy rate solved by the matlab function fmincon and our proposed algorithm. The power constraint is $P_T = P_J = 10$dB.

search that is computationally affordable. A numerical example illustrates our proposed solution, and shows that the optimized jamming significantly improves C_{sec}.

We also have studied the MIMOME wiretap channel with transmit beamforming (the rank-1 constraint on the transmit covariance matrix) and cooperative jamming. By relating the MIMOME channel to the effective MISOSE channel, we propose an iterative algorithm that in each iteration searches the jamming covariance on the 1-dim space defined by the effective MISOSE channel. Numerical results show that our proposed algorithm converges within a few iterations. The algorithm achieves higher secrecy rate than the existing artificial noise scheme.

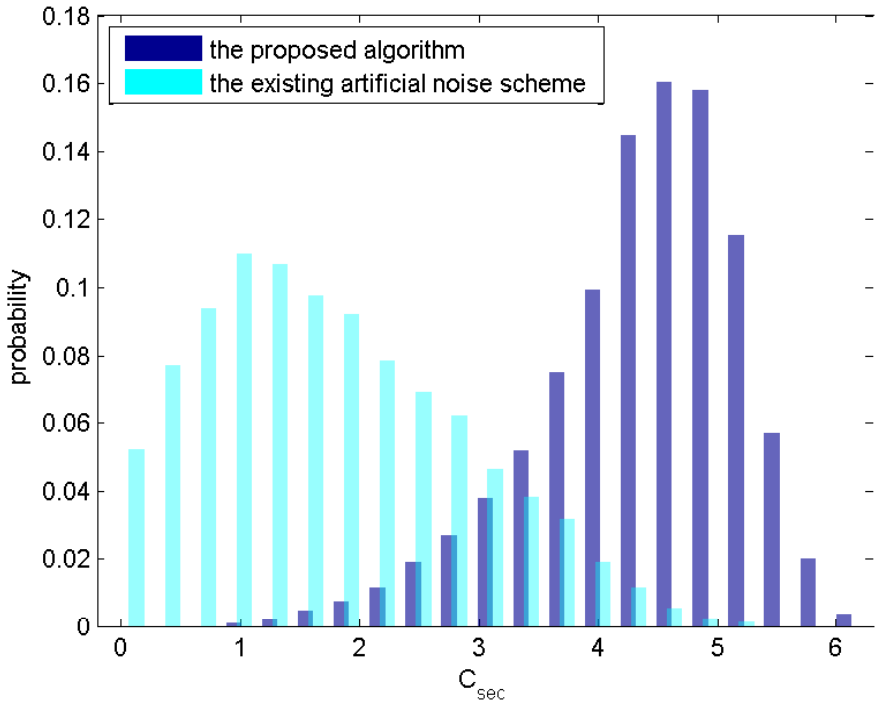


Figure 2.9: The comparison between the histograms of the secrecy rates of a $M_T = M_r = M_e = 3$ channels achieved by the existing artificial noise scheme [18] and our proposed algorithm. The Tx transmits a signal and an jamming noise, whose power is $P_T = P_J =$ 10dB.

Chapter 3

MISOSE WIRETAP CHANNEL WITH IMPERFECT CSI

3.1 Introduction and Motivation

The information theoretic secrecy is first introduced by Wyner in his seminal work [67]. Wyner showed that when the eavesdropper (Ev) channel is a degraded version of the legitimate receiver (Rx) channel, a positive information rate between the transmitter (Tx) and the Rx can be achieved. The Gaussian wiretap channel was studied in [29], where the optimality of Gaussian codebooks is established. The security limits for other wireless channel models have been studied, such as broadcast channels [6] [33], multiple access channels [36] and interference channels [37] [34]. The role of multiple antennas in wiretap channel is studied recently in [50], [25], [24] and [38].

In the above works, the channel state information (CSI) is usually assumed to be perfectly known. However, this assumption does not hold in practice, because the non-cooperative Ev will try to passively listen without being detected and will not feedback its CSI to the Tx. Even if the Ev is willing to cooperatively feedback its CSI, there always exists CSI uncertainty due to the mismatch between reciprocal uplink and downlink channels, estimation mismatch, feedback quantization error, and etc. To this end, designing the transmit strategy under partial CSI is important in practice.

The channel uncertainty is usually assumed to be stochastic and deterministic uncertainties.

- *Stochastic uncertainties.* Assuming the Gaussian distribution of the channels, the ergodic secrecy rate and the optimal transmit covariance for MISOSE wiretap channels has been studied in [31]. Assuming the small channel perturbations and the perturbations' distribution, the robust beamformer with artificial noise for MIMO wiretap channels has been designed using perturbation analysis in [41].

- *Deterministic uncertainties.* The assumption of deterministic uncertainty is adopted by [35], where the wiretap channel under the deterministic uncertainty is named compound wiretap channel. The deterministic uncertainty assumes that the channel state belongs to a given uncertainty set. During the current transmission duration, the channel takes a certain fixed state from the uncertainty set and takes another state during the next duration. The Tx does not have any knowledge about the channel state realizations but only the set which the channel state belongs to. To ensure the perfect secrecy of the message irrespective of the channel state realizations, the optimal transmit strategy is to optimize the worst-case secrecy rate of all channel states.

In this chapter, assuming arbitrary uncertainty of both the Rx and Ev channel, we propose a minimax method to solve the problem. Using a minimax theorem, we prove that the max-min problem is equivalent to its min-max counterpart, and the two problems share a saddle point solution. This enables us to circumvent the max-min problem by solving the min-max problem instead. The min-max problem, by solving the inner maximization, is then reduced to a single minimization problem, which is a convex or quasi-convex problem. It is shown that the optimal transmit covariance may be multi-rank, in contrast to the rank-one conclusion in [69] where only spherical uncertainty of the Ev channel is assumed. Not only does our minimax method solves the problem, but also it enables us to obtain some interesting insights. The worst-case secrecy rate is in the same eigenvalue form as the conventional case [50], except that the channel covariances in the conventional case [50] is replaced by those at the worst case. A relation between the worst-case design and the average design is also discussed.

3.2 System Model and Problem Formulation

We investigate a MISOSE wiretap channel as shown in Fig. 3.1, where the transmitter (Tx) is equipped with multiple antennas and the desired receiver (Rx) and the eavesdropper (E) has single antenna each. The channel response of the intended link from Tx to Rx is denoted by $\mathbf{h}_R$, and the eavesdropper link from Tx to E by $\mathbf{h}_E$.

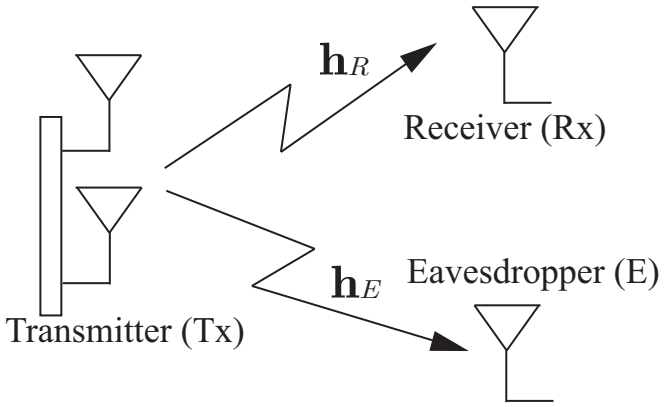


Figure 3.1: The system model for the MISOSE wiretap channel with a multi-antenna transmitter and a single-antenna receiver and eavesdropper.

The secrecy capacity is defined as the maximum rate at which the eavesdropper is unable to decode any information. Given perfect CSI on $\mathbf{h}_R$ and $\mathbf{h}_E$, the secrecy capacity C_{sec} is equal to the maximum difference between the capacities of the intended and the eavesdropper channels [50],

$$\begin{aligned} C_{\text{sec}} &= \max_{\substack{\mathbf{Q}\succeq 0,\\ \text{Tr}(\mathbf{Q})\leq P}} \left\{\log\left(1+\mathbf{h}_R^H\mathbf{Q}\mathbf{h}_R\right) - \log\left(1+\mathbf{h}_E^H\mathbf{Q}\mathbf{h}_E\right)\right\} \\ &= \max_{\substack{\mathbf{Q}\succeq 0,\\ \text{Tr}(\mathbf{Q})\leq P}} \log\left(\frac{1+\mathbf{h}_R^H\mathbf{Q}\mathbf{h}_R}{1+\mathbf{h}_E^H\mathbf{Q}\mathbf{h}_E}\right), \end{aligned} \tag{3.1}$$

where $\mathbf{Q} = E\{\mathbf{x}\mathbf{x}^H\}$ denotes the input covariance matrix and $\mathbf{Q} \succeq 0$ denotes $\mathbf{Q}$ is a positive semidefinite matrix. Without loss of generality, assuming the noise variances at both the Rx and Ev to be 1, and let P denote the maximum transmit power.

If $\lambda_{\max}\left(\mathbf{h}_R\mathbf{h}_R^H,\mathbf{h}_E\mathbf{h}_E^H\right) \leq 1$,where $\lambda_{\max}\left(\mathbf{A},\mathbf{B}\right)$ denotes the largest generalized eigenvalue[1] of the matrix pair $(\mathbf{A},\mathbf{B})$, then $\mathbf{h}_R^H\mathbf{Q}\mathbf{h}_R \leq \mathbf{h}_E^H\mathbf{Q}\mathbf{h}_E$ for any $\mathbf{Q} \succeq 0$. The reason is that $\mathbf{h}_R\mathbf{h}_R^H - \mathbf{h}_E\mathbf{h}_E^H$ is a negative semidefinite matrix and thus $\mathbf{h}_R^H\mathbf{Q}\mathbf{h}_R - \mathbf{h}_E^H\mathbf{Q}\mathbf{h}_E$
$= \text{Tr}\left(\left(\mathbf{h}_R^H\mathbf{h}_R - \mathbf{h}_E^H\mathbf{h}_E\right)\mathbf{Q}\right) \leq 0$. This means under any $\mathbf{Q}$ the equivalent Ev channel $\mathbf{Q}^{\frac{1}{2}}\mathbf{h}_E$

[1]The generalized eigenvalue-eigenvector pair $(\lambda,\mathbf{u})$ of $(\mathbf{A},\mathbf{B})$ is the pair satisfying $\mathbf{A}\mathbf{u} = \lambda\mathbf{B}\mathbf{u}$.

will be better than the equivalent Rx channel $\mathbf{Q}^{\frac{1}{2}}\mathbf{h}_R$, and thus it is impossible to transmit any information with secrecy. The optimal objective and solution in this case are

$$C_{\text{sec}} = \log(1) = 0,\ \mathbf{Q}^* = \mathbf{0}. \tag{3.2}$$

If $\lambda_{\max}\left(\mathbf{h}_R\mathbf{h}_R^H,\mathbf{h}_E\mathbf{h}_E^H\right) > 1$, then the optimal C_{sec} is given by [50]

$$C_{\text{sec}} = \log\left\{\lambda_{\max}\left(\mathbf{I} + P\mathbf{h}_R\mathbf{h}_R^H, \mathbf{I} + P\mathbf{h}_E\mathbf{h}_E^H\right)\right\}. \tag{3.3}$$

The optimal $\mathbf{Q}^*$ is rank-one, of full transmit power and is given by [50]

$$\begin{aligned} \mathbf{Q}^* &= P\mathbf{q}\mathbf{q}^H, \\ \mathbf{q} &= \mathcal{P}\left\{\mathbf{I} + P\mathbf{h}_R\mathbf{h}_R^H, \mathbf{I} + P\mathbf{h}_E\mathbf{h}_E^H\right\}\ . \end{aligned} \tag{3.4}$$

Formulation (3.2)-(3.4) characterizes the secrecy capacity under the perfect CSI on $\mathbf{h}_R$ and $\mathbf{h}_E$. However, this assumption is unrealistic, as in general it is difficult to obtain accurate $\mathbf{h}_E$ from a non-cooperative eavesdropper. The same for $\mathbf{h}_R$ due to mismatch between uplink and downlink channels, estimation error, feedback delay and Rx's mobility. Thus it is of significant interest to study the secrecy capacity under the imperfect CSI's. Recent works [31][41] investigate the ergodic (or average) secrecy capacity by assuming that statistical information of the channels is available at the Tx. However, these works do not guarantee the perfect secrecy which requires that the eavesdropper is unable to decode under all possible channel realizations. Thus our work focuses on the worst-case secrecy capacity which ensures the perfect secrecy.

Our assumption is that $\mathbf{h}_R$ and $\mathbf{h}_E$ belong to given uncertainty sets Δ_R and Δ_E, respectively. Only the uncertainty sets are available at the Tx. The uncertainty sets can be ellipsoids (or spheres) that models a bounded mismatch between the actual and the estimated channel, or discrete sets. The discrete uncertainty sets, $\Delta_R = \{\mathbf{h}_{R_1}, \cdots, \mathbf{h}_{R_N}\}$ and $\Delta_E = \{\mathbf{h}_{E_1}, \cdots, \mathbf{h}_{E_M}\}$, can model the scenario of multicast with multiple eavesdroppers as shown in Fig. 3.2, where the Tx wants to send a same message to all the Rx's and does not want the message to be leaked to any Ev. At this point we do not assume a particular shape of Δ_R and Δ_E. Our minimax method in the next section applies to any shape of uncertainties. Under the assumption that $\mathbf{h}_R \in \Delta_R$ and $\mathbf{h}_E \in \Delta_E$, the *worst-case secrecy*

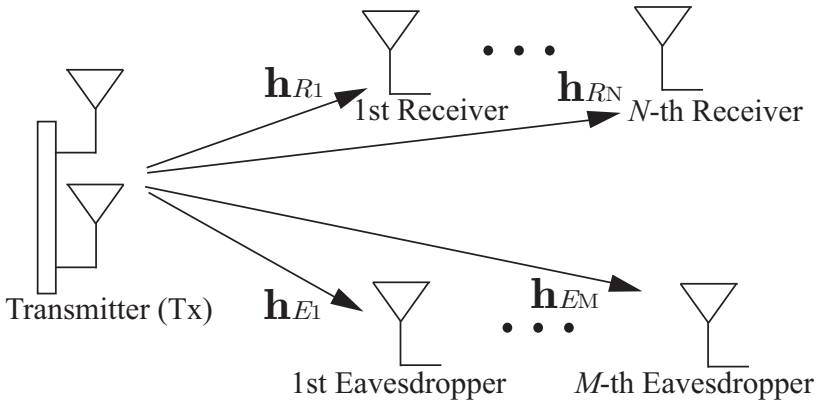


Figure 3.2: The system model for the MISOSE multicast secrecy channel with a transmitter and multiple receivers and multiple eavesdroppers.

rate is defined as the secrecy rate that guarantees the eavesdropper is unable to decode under any channel realization,

$$\begin{aligned} & \underline{C_{\text{sec}}} \\ = & \max_{\substack{\mathbf{Q}\succeq 0,\\ \text{Tr}(\mathbf{Q})\le P}} \min_{\substack{\mathbf{h}_R\in\Delta_R\\ \mathbf{h}_E\in\Delta_E}} \left\{\log\left(1+\mathbf{h}_R^H\mathbf{Q}\mathbf{h}_R\right)-\log\left(1+\mathbf{h}_E^H\mathbf{Q}\mathbf{h}_E\right)\right\} \\ = & \log\left(\max_{\substack{\mathbf{Q}\succeq 0,\\ \text{Tr}(\mathbf{Q})\le P}} \min_{\substack{\mathbf{h}_R\in\Delta_R\\ \mathbf{h}_E\in\Delta_E}} \frac{1+\mathbf{h}_R^H\mathbf{Q}\mathbf{h}_R}{1+\mathbf{h}_E^H\mathbf{Q}\mathbf{h}_E}\right). \end{aligned} \tag{3.5}$$

Our objective is to determine the optimal transmit covariance $\mathbf{Q}$ to maximize (3.5).

Follwing from that $\mathbf{h}^H\mathbf{Q}\mathbf{h}$ can be rewritten in a linear form of $\mathbf{Q}$, i.e. $\mathbf{h}^H\mathbf{Q}\mathbf{h}=\text{Tr}\{\mathbf{h}^H\mathbf{h}\mathbf{Q}\}$, problem (3.5) is rewritten into,

$$\max_{\substack{\mathbf{Q}\succeq 0,\\ \text{Tr}(\mathbf{Q})\le P}} \min_{\substack{\mathbf{R}\in\Omega_R\\ \mathbf{E}\in\Omega_E}} \frac{1+\text{Tr}\{\mathbf{R}\mathbf{Q}\}}{1+\text{Tr}\{\mathbf{E}\mathbf{Q}\}}, \tag{3.6}$$

where the channel covariances and the corresponding uncertainties are

$$\begin{aligned} \mathbf{R} &= \mathbf{h}_R\mathbf{h}_R^H, \\ \mathbf{E} &= \mathbf{h}_E\mathbf{h}_E^H, \\ \Omega_R &= \left\{\mathbf{R}|\mathbf{R}=\mathbf{h}_R\mathbf{h}_R^H, \mathbf{h}_R\in\Delta_R\right\}, \\ \Omega_E &= \left\{\mathbf{E}|\mathbf{E}=\mathbf{h}_E\mathbf{h}_E^H, \mathbf{h}_E\in\Delta_E\right\}. \end{aligned} \tag{3.7}$$

The optimization problem (3.6) is non-concave in $\mathbf{Q}$ and thus cannot be solved by standard convex algorithms. In the next section, we will prove that the max-min problem (3.6) is equivalent to its min-max counterpart and the two problems share a saddle point solution. Therefore the solution to the min-max problem also solves the max-min problem (3.6).

3.3 Minimax Solution

3.3.1 Equivalence between (3.6) and its Min-max Counterpart

Problem (3.6) is equivalent to its min-max counterpart by using a minimax theorem with the aid of two lemmas.

The first lemma proves that problem (3.6) under any Ω_R and Ω_E is the same as that under the convex hull $\text{conv}(\Omega_R)$ and $\text{conv}(\Omega_E)$. That is to say,

$$\begin{aligned} & \max_{\substack{\mathbf{Q}\succeq 0,\\ \text{Tr}(\mathbf{Q})\leq P}} \min_{\substack{\mathbf{R}\in\Omega_R\\ \mathbf{E}\in\Omega_E}} \frac{1+\text{Tr}\{\mathbf{RQ}\}}{1+\text{Tr}\{\mathbf{EQ}\}} \\ = & \max_{\substack{\mathbf{Q}\succeq 0,\\ \text{Tr}(\mathbf{Q})\leq P}} \min_{\substack{\mathbf{R}\in\text{conv}(\Omega_R)\\ \mathbf{E}\in\text{conv}(\Omega_E)}} \frac{1+\text{Tr}\{\mathbf{RQ}\}}{1+\text{Tr}\{\mathbf{EQ}\}}. \end{aligned} \tag{3.8}$$

This equivalence follows from Lemma 3.1.

Lemma 3.1:

$$\min_{\substack{\mathbf{R}\in\Omega_R\\ \mathbf{E}\in\Omega_E}} \frac{1+\text{Tr}\{\mathbf{RQ}\}}{1+\text{Tr}\{\mathbf{EQ}\}} = \min_{\substack{\mathbf{R}\in\text{conv}(\Omega_R)\\ \mathbf{E}\in\text{conv}(\Omega_E)}} \frac{1+\text{Tr}\{\mathbf{RQ}\}}{1+\text{Tr}\{\mathbf{EQ}\}}, \forall \mathbf{Q}. \tag{3.9}$$

Proof:

On the one hand, since $\Omega_R \subseteq \text{conv}(\Omega_R)$ and $\Omega_E \subseteq \text{conv}(\Omega_E)$,

$$\min_{\substack{\mathbf{R}\in\Omega_R\\ \mathbf{E}\in\Omega_E}} \frac{1+\text{Tr}\{\mathbf{RQ}\}}{1+\text{Tr}\{\mathbf{EQ}\}} \geq \min_{\substack{\mathbf{R}\in\text{conv}(\Omega_R)\\ \mathbf{E}\in\text{conv}(\Omega_E)}} \frac{1+\text{Tr}\{\mathbf{RQ}\}}{1+\text{Tr}\{\mathbf{EQ}\}}, \forall \mathbf{Q}. \tag{3.10}$$

On the other hand, $\forall \mathbf{R}_0 \in \text{conv}(\Omega_R)$ and $\forall \mathbf{E}_0 \in \text{conv}(\Omega_E)$, there must exist a $\mathbf{R} \in \Omega_R$ such that $\text{Tr}\{\mathbf{RQ}\} \leq \text{Tr}\{\mathbf{R}_0\mathbf{Q}\}$ and a $\mathbf{E} \in \Omega_E$ such that $\text{Tr}\{\mathbf{EQ}\} \geq \text{Tr}\{\mathbf{E}_0\mathbf{Q}\}$. The reason

is as follows. For any $\mathbf{R}_0 \in$conv(Ω_R), $\mathbf{R}_0$ can be expressed as a convex combination of $\mathbf{R}_i \in \Omega_R$, namely,

$$\begin{aligned} \mathbf{R}_0 &= \nu_1\mathbf{R}_1 + \nu_2\mathbf{R}_2 + \cdots + \nu_N\mathbf{R}_N, \\ \sum_i \nu &= 1,\ \nu_i \geq 0, \\ \mathbf{R}_i &\in \Omega_R,\ i = 1, \cdots, N. \end{aligned}$$

By this, Tr$\{\mathbf{R}_0\mathbf{Q}\}$ can be decomposed as

$$\begin{aligned} & \mathrm{Tr}\left\{\mathbf{R}_0\mathbf{Q}\right\} \\ = \ & \mathrm{Tr}\left\{\left(\nu_1\mathbf{R}_1 + \nu_2\mathbf{R}_2 + \cdots + \nu_N\mathbf{R}_N\right)\mathbf{Q}\right\} \\ = \ & \nu_1\mathrm{Tr}\left\{\mathbf{R}_1\mathbf{Q}\right\} + \cdots + \nu_N\mathrm{Tr}\left\{\mathbf{R}_N\mathbf{Q}\right\}. \end{aligned} \tag{3.11}$$

Among $\mathbf{R}_1, \cdots, \mathbf{R}_N$, there is at least one $\mathbf{R}_i$ such that Tr$\{\mathbf{R}_i\mathbf{Q}\} \leq$Tr$\{\mathbf{R}_0\mathbf{Q}\}$; otherwise the right-hand-side of (3.11) will be strictly greater than Tr$\{\mathbf{R}_0\mathbf{Q}\}$. For the similar reason, to guarantee Tr$\{\mathbf{E}_0\mathbf{Q}\} = \mu_1Tr\{\mathbf{E}_1\mathbf{Q}\} + \cdots + \mu_MTr\{\mathbf{E}_M\mathbf{Q}\}$, where μ_j's are the coefficients and $\mathbf{E}_j \in \Omega_E$, there must exist one $\mathbf{E}_j$ among $\mathbf{E}_1, \cdots, \mathbf{E}_M$ such that Tr$\{\mathbf{E}_j\mathbf{Q}\} \geq$Tr$\{\mathbf{E}_0\mathbf{Q}\}$. Therefore,

$$\begin{aligned} & \left.\begin{array}{l} \forall \mathbf{R}_0 \in \mathrm{conv}\left(\Omega_R\right) \\ \forall \mathbf{E}_0 \in \mathrm{conv}\left(\Omega_E\right) \end{array}\right., \text{and } \forall \mathbf{Q} \\ & \exists \mathbf{R}_i \in \Omega_R \text{ and } \exists \mathbf{E}_j \in \Omega_E \text{ such that} \\ & \frac{1 + \mathrm{Tr}\left\{\mathbf{R}_i\mathbf{Q}\right\}}{1 + \mathrm{Tr}\left\{\mathbf{E}_j\mathbf{Q}\right\}} \leq \frac{1 + \mathrm{Tr}\left\{\mathbf{R}_0\mathbf{Q}\right\}}{1 + \mathrm{Tr}\left\{\mathbf{E}_0\mathbf{Q}\right\}}, \end{aligned}$$

and from which we have

$$\min_{\substack{\mathbf{R}\in\Omega_R \\ \mathbf{E}\in\Omega_E}} \frac{1 + \mathrm{Tr}\left\{\mathbf{R}\mathbf{Q}\right\}}{1 + \mathrm{Tr}\left\{\mathbf{E}\mathbf{Q}\right\}} \leq \min_{\substack{\mathbf{R}\in\mathrm{conv}(\Omega_R) \\ \mathbf{E}\in\mathrm{conv}(\Omega_E)}} \frac{1 + \mathrm{Tr}\left\{\mathbf{R}\mathbf{Q}\right\}}{1 + \mathrm{Tr}\left\{\mathbf{E}\mathbf{Q}\right\}}, \forall \mathbf{Q}. \tag{3.12}$$

From (3.10) and (3.12), the lemma is proved. ■

Lemma 3.2:

The objective function in (3.6) is quasi-concave in $\mathbf{Q}$ and quasi-convex in $(\mathbf{R}, \mathbf{E})$.

Proof:

The linear-fractional function

$$f(\mathbf{x}) = \frac{\mathbf{a}^T\mathbf{x} + b}{\mathbf{c}^T\mathbf{x} + d} \tag{3.13}$$

with domain $\mathrm{dom}_f = \{\mathbf{x}|\mathbf{c}^T\mathbf{x} + d > 0\}$ is both quasi-convex and quasi-concave [4, Chap. 3].

The objective function can be expressed as a linear-fractional function of $\mathbf{Q}$ for any fixed $(\mathbf{R}_0, \mathbf{E}_0)$, i.e.

$$f(\mathrm{vec}\,(\mathbf{Q})) = \frac{1 + \mathrm{Tr}\,\{\mathbf{R}_0\mathbf{Q}\}}{1 + \mathrm{Tr}\,\{\mathbf{E}_0\mathbf{Q}\}} = \frac{\left(\mathrm{vec}\left(\mathbf{R}_0^T\right)\right)^T \mathrm{vec}\,(\mathbf{Q}) + 1}{\left(\mathrm{vec}\left(\mathbf{E}_0^T\right)\right)^T \mathrm{vec}\,(\mathbf{Q}) + 1}, \tag{3.14}$$

and a linear-fractional function of $(\mathbf{R}, \mathbf{E})$ for any fixed $\mathbf{Q}_0$, i.e.

$$f\left(\begin{pmatrix}\mathrm{vec}\,(\mathbf{R})\\ \mathrm{vec}\,(\mathbf{E})\end{pmatrix}\right) = \frac{1 + \mathrm{Tr}\,\{\mathbf{R}\mathbf{Q}_0\}}{1 + \mathrm{Tr}\,\{\mathbf{E}\mathbf{Q}_0\}} = \frac{\begin{pmatrix}\mathrm{vec}\left(\mathbf{Q}_0^T\right)\\ \mathbf{0}\end{pmatrix}^T \begin{pmatrix}\mathrm{vec}(\mathbf{R})\\ \mathrm{vec}(\mathbf{E})\end{pmatrix} + 1}{\begin{pmatrix}\mathbf{0}\\ \mathrm{vec}\left(\mathbf{Q}_0^T\right)\end{pmatrix}^T \begin{pmatrix}\mathrm{vec}(\mathbf{R})\\ \mathrm{vec}(\mathbf{E})\end{pmatrix} + 1} \tag{3.15}$$

where vec$(\cdot)$ denotes the vectorization of a matrix into a column vector. Therefore the lemma is proved. ■

Theorem 3.1 by von Neumann [7, Chap. 1]:

Let $\mathcal{X}$ and $\mathcal{Y}$ be nonempty compact, convex subsets of Euclidean space, and f be jointly continuous. Suppose that f is quasi-concave on $\mathcal{X}$ and quasi-conex on $\mathcal{Y}$, that is to say,

$$f\,(x, y_0) \text{ is quasi-convex in } x \text{ for any } y_0 \in \mathcal{Y}, \tag{3.16}$$

$$f\,(x_0, y) \text{ is quasi-convex in } y \text{ for any } x_0 \in \mathcal{X}. \tag{3.17}$$

Then

$$\max_{x\in\mathcal{X}} \min_{y\in\mathcal{Y}} f\,(x, y) = \min_{y\in\mathcal{Y}} \max_{x\in\mathcal{X}} f\,(x, y)\,. \tag{3.18}$$

A saddle point (x^*, y^*) such that

$$f(x, y^*) \le f(x^*, y^*) \le f\,(x^*, y)\,, \forall x \in \mathcal{X}, \forall y \in \mathcal{Y} \tag{3.19}$$

will be the solution for both problems:

$$\begin{aligned} f(x^*, y^*) &= \max_{x\in\mathcal{X}} \min_{y\in\mathcal{Y}} f(x, y) \\ &= \min_{y\in\mathcal{Y}} \max_{x\in\mathcal{X}} f(x, y). \end{aligned} \tag{3.20}$$

That is to say, the max-min and the min-max problems share the same optimal solution at the saddle point (x^*, y^*).

The above minimax theorem indicates the equivalence between the max-min problem (3.6) and its min-max counterpart. By the two lemmas, the conditions in the minimax theorem are satisfied and thus problem (3.6) is equivalent to the min-max problem (3.22), and the two problem share a saddle point solution. That is,

$$\max_{\substack{\mathbf{Q}\succeq 0,\\ \mathrm{Tr}(\mathbf{Q})\le P}} \min_{\substack{\mathbf{R}\in\Omega_R\\ \mathbf{E}\in\Omega_E}} \frac{1+\mathrm{Tr}\{\mathbf{RQ}\}}{1+\mathrm{Tr}\{\mathbf{EQ}\}} = \max_{\substack{\mathbf{Q}\succeq 0,\\ \mathrm{Tr}(\mathbf{Q})\le P}} \min_{\substack{\mathbf{R}\in\mathrm{conv}(\Omega_R)\\ \mathbf{E}\in\mathrm{conv}(\Omega_E)}} \frac{1+\mathrm{Tr}\{\mathbf{RQ}\}}{1+\mathrm{Tr}\{\mathbf{EQ}\}} \tag{3.21}$$

$$= \min_{\substack{\mathbf{R}\in\mathrm{conv}(\Omega_R)\\ \mathbf{E}\in\mathrm{conv}(\Omega_E)}} \max_{\substack{\mathbf{Q}\succeq 0,\\ \mathrm{Tr}(\mathbf{Q})\le P}} \frac{1+\mathrm{Tr}\{\mathbf{RQ}\}}{1+\mathrm{Tr}\{\mathbf{EQ}\}}, \tag{3.22}$$

where the first equality follows from Lemma 3.1 and the second equality follows from the minimax theorem.

3.3.2 The Worst-case Channel Covariances $(\mathbf{R}^*, \mathbf{E}^*)$ *and the Worst-case Secrecy Rate*

The inner maximization problem of (3.22) is to find the optimal transmit covariance given channel covariances. From (3.2) to (3.4), the solution to the inner maximization problem is given by

$$\begin{aligned} &\max_{\substack{\mathbf{Q}\succeq 0,\\ \mathrm{Tr}(\mathbf{Q})\le P}} \frac{1+\mathrm{Tr}\{\mathbf{RQ}\}}{1+\mathrm{Tr}\{\mathbf{EQ}\}} \\ = &\begin{cases} 1 & ,\text{if } \lambda_{\max}(\mathbf{R}, \mathbf{E}) \le 1 \\ \lambda_{\max}(\mathbf{I}+P\mathbf{R}, \mathbf{I}+P\mathbf{E}) & ,\text{if } \lambda_{\max}(\mathbf{R}, \mathbf{E}) > 1 \end{cases} \\ = &\max\{\lambda_{\max}(\mathbf{I}+P\mathbf{R}, \mathbf{I}+P\mathbf{E}), 1\}. \end{aligned} \tag{3.23}$$

The above equation is the secrecy capacity at the perfectly known $(\mathbf{R}, \mathbf{E})$. Therefore, problem (3.6) is now reduced to a problem finding $(\mathbf{R}^*, \mathbf{E}^*)$ that has the worst-case secrecy rate

$$(\mathbf{R}^*, \mathbf{E}^*) = \arg \min_{\substack{\mathbf{R}\in\text{conv}(\Omega_R) \\ \mathbf{E}\in\text{conv}(\Omega_E)}} \max\left\{\lambda_{\max}\left(\mathbf{I}+P\mathbf{R}, \mathbf{I}+P\mathbf{E}\right), 1\right\}. \tag{3.24}$$

We only need to solve

$$J^* = \min_{\substack{\mathbf{R}\in\text{conv}(\Omega_R) \\ \mathbf{E}\in\text{conv}(\Omega_E)}} \lambda_{\max}\left(\mathbf{I}+P\mathbf{R}, \mathbf{I}+P\mathbf{E}\right). \tag{3.25}$$

If $J^* > 1$ then (3.24) is the same as (3.25). Otherwise (3.24) has the optimal objective 1 and the optimal Tx covariance is $\mathbf{Q}^* = \mathbf{0}$.

For only receiver uncertainty or only eavesdropper uncertainty, the problem

$$\min_{\mathbf{R}\in\text{conv}(\Omega_R)} \lambda_{\max}\left(\mathbf{I}+P\mathbf{R}, \mathbf{I}+P\mathbf{E}\right) \tag{3.26}$$

or the problem

$$\min_{\mathbf{E}\in\text{conv}(\Omega_E)} \lambda_{\max}\left(\mathbf{I}+P\mathbf{R}, \mathbf{I}+P\mathbf{E}\right) \tag{3.27}$$

is a convex optimization problem and thus can be solved efficiently by convex minimization algorithms. See Appendix 3.A for the convexities of the objective function. For both uncertainties, problem (3.25) is a quasi-convex but not a convex optimization problem, because $\lambda_{\max}\left(\mathbf{I}+P\mathbf{R}, \mathbf{I}+P\mathbf{E}\right)$ is quasi-convex but not convex in $(\mathbf{R}, \mathbf{E})$. Also see Appendix 3.A for the quasi-convexity. Based on the equivalence between

$$\lambda_{\max}\left(\mathbf{I}+P\mathbf{R}, \mathbf{I}+P\mathbf{E}\right) \leq t \tag{3.28}$$

and

$$t\left(\mathbf{I}+P\mathbf{E}\right) - \left(\mathbf{I}+P\mathbf{R}\right) \succeq 0, \tag{3.29}$$

problem (3.25) can be solved by solving a sequence of feasibility problems as the following bisection method shows.

Bisection method for solving (3.25)

1: Given a lower bound l and an upper bound u, such that the interval $[l, u]$ is guaranteed to contain the optimal objective J^*.

2: Let $t = \frac{l+u}{2}$. Solve the feasibility problem:

$$\begin{aligned} \text{find} \quad & (\mathbf{R}, \mathbf{E}) \\ \text{s.t.} \quad & t(\mathbf{I} + P\mathbf{E}) - (\mathbf{I} + P\mathbf{R}) \succeq 0 \\ & \mathbf{R} \in \text{conv}\,(\Omega_R)\,, \\ & \mathbf{E} \in \text{conv}\,(\Omega_E)\,. \qquad (3.30) \end{aligned}$$

If (3.30) is feasible then $u \leftarrow t$, else $l \leftarrow t$.

3: Repeat step 2 until the bounding interval $[l, u]$ is small enough.

Until here we have not made any assumption on the uncertainty sets. Next we will discuss the problem under discrete uncertainties. The first reason is that the discrete uncertainty is the most general case of uncertainty,

$$\begin{aligned} \Delta_R &= \{\mathbf{h}_{R_1}, \cdots, \mathbf{h}_{R_N}\}\,, \\ \Delta_E &= \{\mathbf{h}_{E_1}, \cdots, \mathbf{h}_{E_M}\}\,, \end{aligned} \qquad (3.31)$$

since all kinds of uncertainty can be viewed as a set containing either finite or infinite numbers of discrete elements. The second reason is that by solving (3.25) we obtain $(\mathbf{R}^*, \mathbf{E}^*)$ and the associated $\mathbf{R}_i$'s and $\mathbf{E}_j$'s whose convex combinations yield $\mathbf{R}^*$ and $\mathbf{E}^*$. We only need to consider the worst-case problems (3.6) and (3.25) under reduced sets $\hat{\Omega}_R, \hat{\Omega}_E$ that contain only the associated $\mathbf{R}_i$'s and $\mathbf{E}_j$'s. In other words, the problems (3.6) and (3.25) remain unchanged if the original sets Ω_R, Ω are reduced to $\hat{\Omega}_R, \hat{\Omega}_E$.

It is worth noting that the worst-case optimization (3.5) under the discrete uncertainty (3.31) can also be interpreted by a scenario of *secure multicast against multiple eavesdroppers*, as shown in Fig. 3.2, where a transmitter tries to send a common message to multiple receivers in the presence of multiple eavesdroppers, where the receiver channels $\{\mathbf{h}_{R_i}\}_{i=1}^N$ and the eavesdropper channels $\left\{\mathbf{h}_{E_j}\right\}_{j=1}^M$ are perfectly known.

By the relation (3.7), the covariance uncertainties are given by

$$\Omega_R = \left\{\mathbf{h}_{R_1}\mathbf{h}_{R_1}^H, \cdots, \mathbf{h}_{R_N}\mathbf{h}_{R_N}^H\right\}, \tag{3.32}$$

$$\Omega_E = \left\{\mathbf{h}_{E_1}\mathbf{h}_{E_1}^H, \cdots, \mathbf{h}_{E_M}\mathbf{h}_{E_M}^H\right\} \tag{3.33}$$

And $\text{conv}(\Omega_R)$ and $\text{conv}(\Omega_E)$ can be expressed as, respectively

$$\begin{aligned}\text{conv}\left(\Omega_R\right) &= \left\{\nu_1\mathbf{h}_{R_1}\mathbf{h}_{R_1}^H + \cdots + \nu_N\mathbf{h}_{R_N}\mathbf{h}_{R_N}^H\right\} \\ \text{conv}\left(\Omega_E\right) &= \left\{\mu_1\mathbf{h}_{E_1}\mathbf{h}_{E_1}^H + \cdots + \mu_M\mathbf{h}_{E_M}\mathbf{h}_{E_M}^H\right\},\end{aligned} \tag{3.34}$$

where the convex combination coefficients are

$$\begin{aligned}&\left\{\nu_1, \cdots, \nu_N | 0 \le \nu_i \le 1, \ \sum \nu_i = 1\right\}, \\ &\left\{\mu_1, \cdots, \mu_N | 0 \le \mu_j \le 1, \ \sum \mu_j = 1\right\}.\end{aligned} \tag{3.35}$$

Substituting (3.34)-(3.35) into (3.25), the optimal objective is then given by

$$\min_{\substack{0\le\nu_i\le 1,\ \sum\nu_i=1,\\ 0\le\mu_j\le 1,\ \sum\mu_j=1}} \lambda_{\max}\begin{pmatrix}\mathbf{I} + P\sum\nu_i\mathbf{h}_{R_i}\mathbf{h}_{R_i}^H, \\ \mathbf{I} + P\sum\mu_j\mathbf{h}_{E_j}\mathbf{h}_{E_j}^H\end{pmatrix} \tag{3.36}$$

Comparing (3.36) with (3.3), it can be concluded that the worst-case design is a generalization of the conventional case. When the uncertainties only contain one element, i.e. $\Delta_R = \{\mathbf{h}_R\}$, $\Delta_E = \{\mathbf{h}_E\}$, the worst-case design degrades into the conventional case.

3.3.3 The Optimal $\mathbf{Q}^*$

The optimal $\mathbf{Q}^*$ maximizes $\lambda_{\max}\left(\mathbf{I} + P\mathbf{R}^*, \mathbf{I} + P\mathbf{E}^*\right)$, where $(\mathbf{R}^*, \mathbf{E}^*)$ is the solution to (3.25). It is worth noting that the optimal $\mathbf{Q}^*$ may be rank-one or multi-rank, depending on the uniqueness of the largest eigenvalue of $(\mathbf{I} + P\mathbf{R}^*, \mathbf{I} + P\mathbf{E}^*)$. If the largest eigenvalue is unique, then the optimal $\mathbf{Q}^*$ is rank-one and in the form of $\mathbf{Q}^*{=}P\mathbf{q}^*\mathbf{q}^{*H}$, where $\mathbf{q}^* = \mathcal{P}\left\{\mathbf{I} + P\mathbf{R}, \mathbf{I} + P\mathbf{E}\right\}$, the eigenvector corresponding to the largest eigenvalue. If there are multiple largest eigenvalues, say two largest eigenvalues, then $\mathbf{Q}^*$ must be in the form of $\mathbf{Q}^*{=}\left[\mathbf{q}_1^*, \mathbf{q}_2^*\right]\tilde{\mathbf{Q}}\left[\mathbf{q}_1^*, \mathbf{q}_2^*\right]^H$, where $\mathbf{q}_1^*$ and $\mathbf{q}_2^*$ are the corresponding eigenvectors and $\tilde{\mathbf{Q}}$ is a 2×2 positive semi-definite matrix. We will show how to determine $\tilde{\mathbf{Q}}$ for the multi-rank case.

Let J^* denote the optimal objective of (3.36), let $\{\nu_1^*, \cdots, \nu_N^*\}$ and $\{\mu_1^*, \cdots, \mu_M^*\}$ denote the optimal solution to (3.36), and let $\mathbf{Q}^*$ denote the optimal covariance. Those $\mathbf{h}_{R_i}$ and $\mathbf{h}_{E_j}$ such that $\nu_i^* > 0$ and $\mu_j^* > 0$ are the worst-case elements for $\mathbf{Q}^*$. That is to say,

$$\frac{1+\mathrm{Tr}\left\{\mathbf{h}_{R_i}\mathbf{h}_{R_i}^H\mathbf{Q}^*\right\}}{1+\mathrm{Tr}\left\{\mathbf{h}_{E_j}\mathbf{h}_{E_j}^H\mathbf{Q}^*\right\}} = J^*, \quad \begin{array}{l}\text{for every } i,j \text{ such that}\\ \text{both } \nu_i^*, \mu_j^* > 0,\end{array} \tag{3.37}$$

$$\frac{1+\mathrm{Tr}\left\{\mathbf{h}_{R_i}\mathbf{h}_{R_i}^H\mathbf{Q}^*\right\}}{1+\mathrm{Tr}\left\{\mathbf{h}_{E_j}\mathbf{h}_{E_j}^H\mathbf{Q}^*\right\}} > J^*, \quad \begin{array}{l}\text{for other combinations}\\ \text{of } i,j.\end{array} \tag{3.38}$$

The reason of the worst-case conditions (3.37) is given in Appendix 3.B.

The optimal covariance $\mathbf{Q}^*$ may be rank-one or multi-rank, depending on whether the largest eigenvalue of $\left(\mathbf{I}+P\sum\nu_i^*\mathbf{h}_{R_i}\mathbf{h}_{R_i}^H, \mathbf{I}+P\sum\mu_j^*\mathbf{h}_{E_j}\mathbf{h}_{E_j}^H\right)$ is unique or not.

If the largest eigenvalue is unique, then $\mathbf{Q}^*$ must be rank-one and is given by

$$\begin{aligned}\mathbf{Q}^* &= P\mathbf{q}^*\mathbf{q}^{*H},\\ \mathbf{q}^* &= \mathcal{P}\left\{\mathbf{I}+P\sum\nu_i^*\mathbf{h}_{R_i}\mathbf{h}_{R_i}^H, \mathbf{I}+P\sum\mu_j^*\mathbf{h}_{E_j}\mathbf{h}_{E_j}^H\right\}.\end{aligned} \tag{3.39}$$

Note that the above beamforming vector $\mathbf{q}^*$ is in the same generalized eigenvector form as (3.4), except that the receiver channel covariance $\mathbf{h}_R\mathbf{h}_R^H$ and the eavesdropper channel covariance $\mathbf{h}_E\mathbf{h}_E^H$ in (3.4) is replaced by $\sum\nu_i^*\mathbf{h}_{R_i}\mathbf{h}_{R_i}^H$ and $\sum\mu_j^*\mathbf{h}_{E_j}\mathbf{h}_{E_j}^H$, respectively.

If there are multiple largest eigenvalues, then $\mathbf{Q}^*$ may be multi-rank. Let $\mathbf{U}=[\mathbf{q}_1^*, \cdots, \mathbf{q}_n^*]$, where $\mathbf{q}_1^*, \cdots, \mathbf{q}_n^*$ denote the multiple eigenvectors corresponding to the multiple largest eigenvalues. The optimal $\mathbf{Q}^*$ must in the eigen-space $\mathbf{U}$ and can be written in the form of

$$\mathbf{Q}^* = \mathbf{U}\tilde{\mathbf{Q}}\mathbf{U}^H, \tag{3.40}$$

where $\tilde{\mathbf{Q}}$ is a $n\times n$ positive semi-definite matrix. To determine $\tilde{\mathbf{Q}}$, notice that $\mathbf{Q}^*$ has to satisfy the worst-case condition (3.37), which can be expressed as linear equations of $\tilde{\mathbf{Q}}$,

$$\begin{aligned}1+\mathrm{Tr}\left\{\mathbf{h}_{R_i}\mathbf{h}_{R_i}^H\mathbf{U}\tilde{\mathbf{Q}}\mathbf{U}^H\right\} &= J^*\left(1+\mathrm{Tr}\left\{\mathbf{h}_{E_j}\mathbf{h}_{E_j}^H\mathbf{U}\tilde{\mathbf{Q}}\mathbf{U}^H\right\}\right),\\ &\text{for every } i,j \text{ such that both } \nu_i^*, \mu_j^* > 0.\end{aligned} \tag{3.41}$$

By solving the set of linear equations including (3.41) and

$$\begin{aligned} \tilde{\mathbf{Q}}^H &= \tilde{\mathbf{Q}}, \\ \mathrm{Tr}\left\{\tilde{\mathbf{Q}}\right\} &= P, \end{aligned} \tag{3.42}$$

the elements of $\tilde{\mathbf{Q}}$ can be determined.

3.3.4 Relation between the Worst-case and Average Design

We first rewrite the worst-case formulation into

$$\begin{aligned} & \max_{\substack{\mathbf{Q}\succeq 0,\\ \mathrm{Tr}(\mathbf{Q})\leq P}} \min_{\substack{\mathbf{h}_R\in\Delta_R\\ \mathbf{h}_E\in\Delta_E}} \frac{1+\mathbf{h}_R^H\mathbf{Q}\mathbf{h}_R}{1+\mathbf{h}_E^H\mathbf{Q}\mathbf{h}_E} \\ = & \max_{\substack{\mathbf{Q}\succeq 0,\\ \mathrm{Tr}(\mathbf{Q})\leq P}} \frac{1+\min\limits_{\mathbf{h}_R\in\Delta_R}\mathbf{h}_R^H\mathbf{Q}\mathbf{h}_R}{1+\max\limits_{\mathbf{h}_E\in\Delta_E}\mathbf{h}_E^H\mathbf{Q}\mathbf{h}_E} \\ = & \max_{\substack{\mathbf{Q}\succeq 0,\\ \mathrm{Tr}(\mathbf{Q})\leq P}} \frac{1+\underline{\mathrm{SNR}_R}}{1+\overline{\mathrm{SNR}_E}}, \end{aligned} \tag{3.43}$$

which $\underline{\mathrm{SNR}_R}$ and $\overline{\mathrm{SNR}_E}$ denote the worst-case SNR at the Rx and the best-case SNR at the Ev, respectively. In the following we will relate the worst-case design to a weighted average design.

Assuming weights $\{\nu_1,\cdots,\nu_N|0\leq\nu_i\leq 1,\sum\nu_i=1\}$ is given for channel states $\{\mathbf{h}_{R_i}\}_{i=1}^N$, the average SNR_R weighted at different channel states can be written as

$$\widehat{\mathrm{SNR}_R} = \sum \nu_i \mathrm{SNR}_{R_i} = \sum \nu_i \mathbf{h}_{R_i}\mathbf{Q}\mathbf{h}_{R_i}^H. \tag{3.44}$$

Similarly, given weights $\{\mu_1,\cdots,\mu_M|0\leq\mu_j\leq 1,\sum\mu_j=1\}$,

$$\widehat{\mathrm{SNR}_E} = \sum \mu_j \mathrm{SNR}_{E_j} = \sum \mu_j \mathbf{h}_{E_j}\mathbf{Q}\mathbf{h}_{E_j}^H. \tag{3.45}$$

We define the average design as a problem by replacing the SNRs in (3.1) with the average SNRs,

$$\max_{\substack{\mathbf{Q}\succeq 0,\\ \mathrm{Tr}(\mathbf{Q})\leq P}} \frac{1+\widehat{\mathrm{SNR}_R}}{1+\widehat{\mathrm{SNR}_E}}. \tag{3.46}$$

The optimal objective to the above is given by,

$$\begin{cases} \lambda_{\max}\left(\begin{array}{c}\mathbf{I}+P\sum\nu_i\mathbf{h}_{R_i}\mathbf{h}_{R_i}^H,\\ \mathbf{I}+P\sum\mu_j\mathbf{h}_{E_j}\mathbf{h}_{E_j}^H\end{array}\right) & ,\text{if } \widehat{\mathrm{SNR}_R} > \widehat{\mathrm{SNR}_E} \\ 1 & ,\text{otherwise} \end{cases} . \tag{3.47}$$

The relation between the worst-case design and the average design is that the average one serves as an upper bound for the worst-case one. Because

$$\underline{\mathrm{SNR}_R} \leq \widehat{\mathrm{SNR}_R}, \forall\left\{\nu_i|0\leq\nu_i\leq 1, \sum\nu_i = 1\right\}, \tag{3.48}$$

$$\overline{\mathrm{SNR}_E} \geq \widehat{\mathrm{SNR}_E}, \forall\left\{\mu_j|0\leq\mu_j\leq 1, \sum\mu_j = 1\right\}, \tag{3.49}$$

we have

$$\frac{1+\underline{\mathrm{SNR}_R}}{1+\overline{\mathrm{SNR}_E}} \leq \frac{1+\widehat{\mathrm{SNR}_R}}{1+\widehat{\mathrm{SNR}_E}}, \forall\left\{\nu_i\right\},\left\{\mu_j\right\}. \tag{3.50}$$

Since the above inequality holds true for any $\{\nu_i\}_{i=1}^N$ and $\{\mu_j\}_{j=1}^M$, the tightest upper bound can be yield by finding $\{\nu_i\}_{i=1}^N$ and $\{\mu_j\}_{j=1}^M$ for the minimum $\frac{1+\widehat{\mathrm{SNR}_R}}{1+\widehat{\mathrm{SNR}_E}}$. Thus

$$\begin{aligned} & \frac{1+\underline{\mathrm{SNR}_R}}{1+\overline{\mathrm{SNR}_E}} \\ \leq & \min_{\substack{0\leq\nu_i\leq 1,\ \sum\nu_i=1,\\ 0\leq\mu_j\leq 1,\ \sum\mu_j=1}} \frac{1+\widehat{\mathrm{SNR}_R}}{1+\widehat{\mathrm{SNR}_E}} \\ = & \min_{\substack{0\leq\nu_i\leq 1,\ \sum\nu_i=1,\\ 0\leq\mu_j\leq 1,\ \sum\mu_j=1}} \lambda_{\max}\left(\begin{array}{c}\mathbf{I}+P\sum\nu_i\mathbf{h}_{R_i}\mathbf{h}_{R_i}^H,\\ \mathbf{I}+P\sum\mu_j\mathbf{h}_{E_j}\mathbf{h}_{E_j}^H\end{array}\right). \end{aligned} \tag{3.51}$$

The result in the previous subsection shows that our solution (3.36) meets the tightest upper bound (3.51).

In conclusion, both the worst-case and the average design can be viewed as a generalization of the conventional case, in that the channel covariances are replaced by combinations of the channel covariances at different states. Any average design serves as an upper bound for the worst-case one. And the worst-case design achieves the tightest bound obtained by the minimum of the average design.

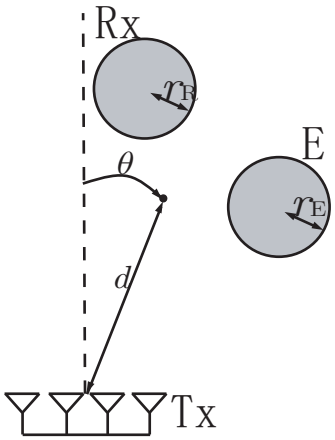


Figure 3.3: The simulation setting illustrates the uncertainty of the locations of the receiver and the eavesdropper. The receiver (Rx) and the eavesdropper (E) are assumed to be located within the shaded circles, but their precise locations are unknown.

3.4 Numerical Results

We provide numerical examples to show the impact of imperfect CSI on the secrecy capacity and demonstrate the effectiveness of the proposed design in combating uncertainty. In our examples, a multiple-antenna transmitter wants to send messages to a single-antenna receiver but does not want to leak the message to the eavesdropper. The transmitter knows roughly the position of the receiver and the eavesdropper, as illustrated by Fig. 3.3. To achieve secrecy, the approach of the transmitter is to steer its beam along the direction of the receiver and simultaneously nulls the direction of the eavesdropper.

The transmitter is equipped with $N = 4$ linear antenna elements spaced half wavelength apart. The antenna elements are assumed to be omni-isotropic and have unit gains. The signals arrived at the receiver and the eavesdropper are modeled as far-field signals, so that the channel at location (d, θ) is expressed as

$$\mathbf{h}\left(d,\theta\right) = \frac{1}{d^{\alpha}}\left[1, e^{-j\pi\sin(\theta)}, e^{-j2\pi\sin(\theta)}, e^{-j3\pi\sin(\theta)}\right]^{T}, \tag{3.52}$$

where d is the distance, $\alpha = 3$ is the path loss exponent, and angle θ is the direction.

In the first example in Fig. 3.4 showing location uncertainties of a single receiver and

a single eavesdropper, the receiver is assumed to be located within the blue circle and the eavesdropper the yellow circle. Notice that the worst-case locations will only happen at the boundary of the circles. The reason is that for any interior location (d, θ), there exist boundary locations (d_1, θ) and (d_2, θ) at the same direction θ such that

$$d_1 < d < d_2 \tag{3.53}$$

and hence

$$\begin{aligned} & \mathbf{h}^H (d_1, \theta) \mathbf{Q} \mathbf{h} (d_1, \theta) \\ > \; & \mathbf{h}^H (d, \theta) \mathbf{Q} \mathbf{h} (d, \theta) \\ > \; & \mathbf{h}^H (d_2, \theta) \mathbf{Q} \mathbf{h} (d_2, \theta) . \end{aligned} \tag{3.54}$$

Thus the channel at the interior location cannot be the worst-case solution of $\arg\min_{\mathbf{h}_R \in \Delta_R} \mathbf{h}_R^H \mathbf{Q} \mathbf{h}_R$ nor $\arg\max_{\mathbf{h}_E \in \Delta_E} \mathbf{h}_E^H \mathbf{Q} \mathbf{h}_E$. For this reason, the uncertainty sets Δ_R and Δ_E containing all the channels within the circles can be reduced to the sets containing only the channels at the boundary. The reduced sets are further discretized into the channels at discrete location samples on the circles, in order to apply the solution in Section III.B designed for discrete uncertainty.

Fig. 3.4 plots the SNR distributions under our proposed design and the conventional design. As shown in Fig. 3.4(b), assuming that the receiver and the eavesdropper are perfectly located at the centers of the circles, the conventional design has a main beam pointing to the receiver and a narrow null pointing to the eavesdropper. Whereas in Fig. 3.4(a), our proposed design places two nulls towards the directions of the eavesdropper and each null has a wider nulling range.

Fig. 3.5 plots the secrecy capacity versus $r = r_R = r_E$ that is the radius of the circular location uncertainty. As the uncertainty radius increases, both the worst-case secrecy capacities of the proposed and the conventional design decreases, but that of the conventional design decreases at a deeper slope than that of the proposed one. The degradation of the conventional design is more phenomenal at high transmit power. Fig. 3.5 also plots the average secrecy capacities when the locations are uniformly distributed within the circles. The

average secrecy capacity of the proposed design is also higher than that of the conventional one.

The second example in Fig. 3.6 shows the proposed design in the scenario of multicast with multiple eavesdroppers. The transmitter wants to broadcast a common message to everyone of the multiple receivers but none of the multiple eavesdroppers. In Fig. 3.6, three receivers with location uncertainties are located within the blue circles, and two eavesdroppers within yellow circles. The conventional design is intended for single receiver and single eavesdropper, and cannot provide a solution to this scenario. The proposed design places three beams pointing to the receivers and two nulls to the eavesdroppers. Unlike in the first example that the optimal transmit covariance $\mathbf{Q}^*$ is rank-one, in this case $\mathbf{Q}^*$ is rank-two. The achievable worst-case secrecy capacity under the proposed design is 1.89bps/Hz.

3.5 Conclusion

We have studied the problem of optimizing the transmit covariance for the worst-case secrecy rate of the MISOSE wiretap channel, when the CSI of the receiver and the eavesdropper channel belong to given uncertainty sets. By proving the saddle-point solution, we transformed the worst-case optimization problem into a quasi-convex optimization problem. The result of the worst-case optimization problem can be expressed in the form of generalized eigenvalue, which is the same form as that of the conventional case. We also have shown that the average design serves as an upper bound on the worst-case design, and the worst-case design meets the lowest of the average design. Two numerical examples of the receiver's and the eavesdropper's location uncertainties demonstrated the effectiveness of our proposed design.

3.6 Appendix 3.A: Proof of Quasi-convexity

The properties that $\lambda_{\max}(\mathbf{I}+P\mathbf{R}, \mathbf{I}+P\mathbf{E})$ is quasiconvex in $(\mathbf{R}, \mathbf{E})$, convex in $\mathbf{R}$ for any fixed $\mathbf{E}_0$ and convex in $\mathbf{E}$ for any fixed $\mathbf{R}_0$ are resulted from those of $\lambda_{\max}(\mathbf{R}, \mathbf{E})$, as given in the following.

The function $f(\mathbf{R}, \mathbf{E}) = \lambda_{\max}(\mathbf{R}, \mathbf{E})$ is quasiconvex in $(\mathbf{R}, \mathbf{E}) \in \mathbf{S} \times \mathbf{S}_{++}$, but is not convex in $(\mathbf{R}, \mathbf{E})$, where $\mathbf{S}$ and $\mathbf{S}_{++}$ denote positive-semidefinite and positive-definite matrices

respectively. For any fixed $\mathbf{E}_0 \in \mathbf{S}_{++}$, $f_R(\mathbf{R}) = \lambda_{\max}(\mathbf{R}, \mathbf{E}_0)$ is convex in $\mathbf{R} \in \mathbf{S}$, and for any fixed $\mathbf{R}_0 \in \mathbf{S}$, $f_E(\mathbf{E}) = \lambda_{\max}(\mathbf{R_0}, \mathbf{E})$ is convex in $\mathbf{E} \in \mathbf{S}_{++}$.

Proof:

Refer to [4, Chap. 3] for that $\lambda_{\max}(\mathbf{X}, \mathbf{Y})$ is quasi-convex, $\lambda_{\max}(\mathbf{X})$ is convex and $\lambda_{\min}(\mathbf{X})$ is concave.

That $f_R(\mathbf{R}) = \lambda_{\max}(\mathbf{R}, \mathbf{E}_0) = \lambda_{\max}\left(\mathbf{E}_0^{-1}\mathbf{R}\right)$ is convex follows from the convexity of $\lambda_{\max}(\mathbf{X})$.

To prove the convexity of $f_E(\mathbf{E})$, we will prove for any $\mathbf{E}_1$ and $\mathbf{E}_2$ such that $f_E(\mathbf{E}_1) = f_1$ and $f_E(\mathbf{E}_2) = f_2$,

$$f_E(\mu\mathbf{E}_1 + (1-\mu)\mathbf{E}_2) \leq \mu f_1 + (1-\mu) f_2, \mu \in [0,1]. \tag{3.55}$$

We can rewrite $f_E(\mathbf{E})$ into

$$f_E(\mathbf{E}) = \lambda_{\max}\left(\mathbf{E}^{-1}\mathbf{R_0}\right) = \frac{1}{\lambda_{\min}\left(\mathbf{R}_0^{-1}\mathbf{E}\right)}. \tag{3.56}$$

Since $\lambda_{\min}(\mathbf{X})$ is a concave function [4, Chap. 3], we have

$$\begin{aligned} & \lambda_{\min}\left(\mathbf{R}_0^{-1}\left(\mu\mathbf{E}_1 + (1-\mu)\mathbf{E}_2\right)\right) \\ \geq\ & \mu\lambda_{\min}\left(\mathbf{R}_0^{-1}\mathbf{E}_1\right) + (1-\mu)\lambda_{\min}\left(\mathbf{R}_0^{-1}\mathbf{E}_2\right) && (3.57) \\ =\ & \frac{\mu}{f_1} + \frac{1-\mu}{f_2}. && (3.58) \end{aligned}$$

Therefore,

$$\begin{aligned} f_E(\mu\mathbf{E}_1 + (1-\mu)\mathbf{E}_2) &= \frac{1}{\lambda_{\min}\left(\mathbf{R}_0^{-1}\left(\mu\mathbf{E}_1 + (1-\mu)\mathbf{E}_2\right)\right)} \\ &\leq \frac{1}{\frac{\mu}{f_1} + \frac{1-\mu}{f_2}} \\ &\leq \mu f_1 + (1-\mu) f_2. && (3.59) \end{aligned}$$

In the above derivation, the last inequality follows from that

$$\begin{aligned} & (\mu f_1 + (1-\mu) f_2)\left(\frac{\mu}{f_1} + \frac{1-\mu}{f_2}\right) \\ =\ & \mu^2 + (1-\mu)^2 + \mu(1-\mu)\left(\frac{f_1}{f_2} + \frac{f_2}{f_1}\right) \\ \geq\ & \mu^2 + (1-\mu)^2 + 2\mu(1-\mu) = 1. && (3.60) \end{aligned}$$

■

3.7 Appendix 3.B: Worst-case Conditions

Suppose $(\mathbf{Q}^*; \mathbf{R}^*, \mathbf{E}^*)$ is the saddle point solution under the discrete uncertainty (3.31), where

$$\begin{aligned} \mathbf{R}^* &= \sum \nu_i^* \mathbf{h}_{R_i} \mathbf{h}_{R_i}^H, \\ \mathbf{E}^* &= \sum \mu_j^* \mathbf{h}_{E_j} \mathbf{h}_{E_j}^H. \end{aligned}$$

Then the worst-case conditions (3.37) holds for every i, j such that both $\nu_i^*, \mu_j^* > 0$.

Proof:

Let $\{\alpha_i\}$ denote the indexes of the non-zero elements of $\{\nu_i^*\}$, and let $\{\beta_j\}$ denote the non-zero elements of $\left\{\mu_j^*\right\}$. Let f_{α_i,β_j} denote

$$f_{\alpha_i,\beta_j} = \frac{1 + \mathrm{Tr}\left\{\mathbf{h}_{R_{\alpha_i}} \mathbf{h}_{R_{\alpha_i}}^H \mathbf{Q}^*\right\}}{1 + \mathrm{Tr}\left\{\mathbf{h}_{E_{\beta_j}} \mathbf{h}_{E_{\beta_j}}^H \mathbf{Q}^*\right\}}. \tag{3.61}$$

First, the problem

$$\max_{\substack{\mathbf{Q}\succeq 0, \\ \mathrm{Tr}(\mathbf{Q})\le P}} \min_{\substack{\mathbf{h}_R \in \left\{\mathbf{h}_{R_i}\right\} \\ \mathbf{h}_E \in \left\{\mathbf{h}_{E_j}\right\}}} \frac{1 + \mathrm{Tr}\left\{\mathbf{h}_R \mathbf{h}_R^H \mathbf{Q}^*\right\}}{1 + \mathrm{Tr}\left\{\mathbf{h}_E \mathbf{h}_E^H \mathbf{Q}^*\right\}} \tag{3.62}$$

has the optimal objective J^* and the optimal solution $\mathbf{Q}^*$. Consider the inner minimization problem of (3.62), we have for any i, j,

$$f_{i,j} = \frac{1 + \mathrm{Tr}\left\{\mathbf{h}_{R_i} \mathbf{h}_{R_i}^H \mathbf{Q}^*\right\}}{1 + \mathrm{Tr}\left\{\mathbf{h}_{E_j} \mathbf{h}_{E_j}^H \mathbf{Q}^*\right\}} \ge J^*. \tag{3.63}$$

Second, for (α_i, β_j) we will narrow down (3.63) into $f_{\alpha_i,\beta_j} = J^*$. Rewrite (3.61) into a linear form

$$\begin{aligned} & 1 + \mathrm{Tr}\left\{\mathbf{h}_{R_{\alpha_i}} \mathbf{h}_{R_{\alpha_i}}^H \mathbf{Q}^*\right\} \\ = \;& f_{\alpha_i,\beta_j} \left(1 + \mathrm{Tr}\left\{\mathbf{h}_{E_{\beta_j}} \mathbf{h}_{E_{\beta_j}}^H \mathbf{Q}^*\right\}\right). \end{aligned} \tag{3.64}$$

Also rewrite $f\left(\mathbf{Q}^*; \mathbf{R}^*, \mathbf{E}^*\right) = J^*$ into the linear form

$$\begin{aligned} & 1 + \mathrm{Tr}\left\{\sum_{\alpha_i} \nu_{\alpha_i}^* \mathbf{h}_{R_{\alpha_i}} \mathbf{h}_{R_{\alpha_i}}^H \mathbf{Q}^*\right\} \\ = \;& J^* \left(1 + \mathrm{Tr}\left\{\sum_{\beta_j} \mu_{\beta_j}^* \mathbf{h}_{E_{\beta_j}} \mathbf{h}_{E_{\beta_j}}^H \mathbf{Q}^*\right\}\right). \end{aligned} \tag{3.65}$$

For each pair of (α_i, β_j) multiplying (3.64) by $\nu^*_{\alpha_i}\mu^*_{\beta_j}$, and then adding up all the multiplied (3.64), we have

$$\sum_{\alpha_i}\sum_{\beta_j}\left\{\nu^*_{\alpha_i}\mu^*_{\beta_j}\left(1+\mathrm{Tr}\left\{\mathbf{h}_{R_{\alpha_i}}\mathbf{h}^H_{R_{\alpha_i}}\mathbf{Q}^*\right\}\right)\right\} \tag{3.66}$$

$$= \sum_{\alpha_i}\sum_{\beta_j}\left\{\nu^*_{\alpha_i}\mu^*_{\beta_j}f_{\alpha_i,\beta_j}\left(1+\mathrm{Tr}\left\{\mathbf{h}_{E_{\beta_j}}\mathbf{h}^H_{E_{\beta_j}}\mathbf{Q}^*\right\}\right)\right\}$$

$$= \sum_{\alpha_i}\sum_{\beta_j}\left\{\nu^*_{\alpha_i}\mu^*_{\beta_j}J^*\left(1+\mathrm{Tr}\left\{\mathbf{h}_{E_{\beta_j}}\mathbf{h}^H_{E_{\beta_j}}\mathbf{Q}^*\right\}\right)\right\} \tag{3.67}$$

$$+\sum_{\alpha_i}\sum_{\beta_j}\left\{\nu^*_{\alpha_i}\mu^*_{\beta_j}\left(f_{\alpha_i,\beta_j}-J^*\right)\left(1+\mathrm{Tr}\left\{\mathbf{h}_{E_{\beta_j}}\mathbf{h}^H_{E_{\beta_j}}\mathbf{Q}^*\right\}\right)\right\}. \tag{3.68}$$

By $\sum_{\alpha_i}\sum_{\beta_j}\nu^*_{\alpha_i}\mu^*_{\beta_j}=1$, $\sum_{\alpha_i}\nu^*_{\alpha_i}=1$ and $\sum_{\beta_j}\mu^*_{\beta_j}=1$, (3.66), (3.67)-(3.68) are simplified into

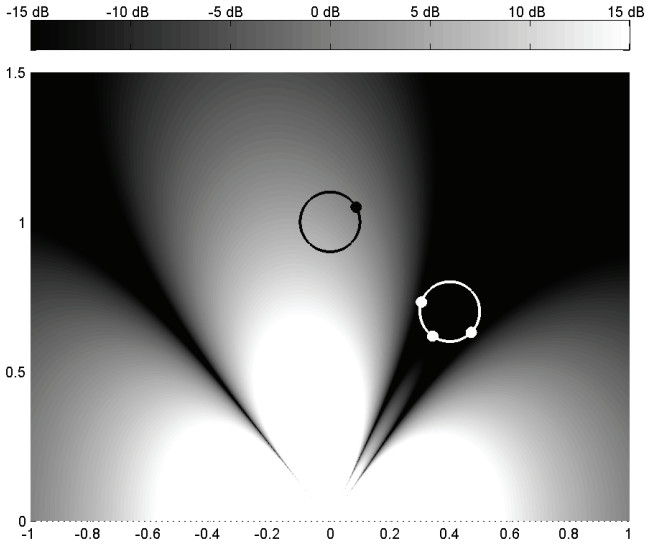
$$1+\mathrm{Tr}\left\{\left(\sum_{\alpha_i}\nu^*_{\alpha_i}\mathbf{h}_{R_{\alpha_i}}\mathbf{h}^H_{R_{\alpha_i}}\right)\mathbf{Q}^*\right\}$$

$$= J^*\left(1+\mathrm{Tr}\left\{\left(\sum_{\beta_j}\mu^*_{\beta_j}\mathbf{h}_{E_{\beta_j}}\mathbf{h}^H_{E_{\beta_j}}\right)\mathbf{Q}^*\right\}\right)$$

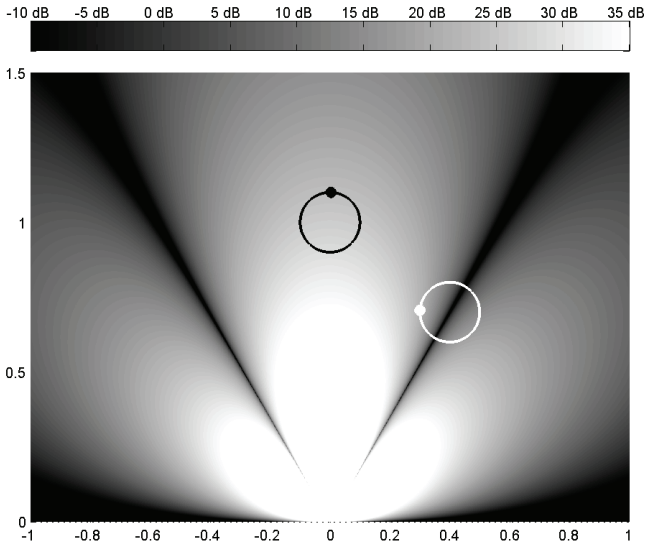
$$+\sum_{\alpha_i}\sum_{\beta_j}\left\{\nu^*_{\alpha_i}\mu^*_{\beta_j}\left(f_{\alpha_i,\beta_j}-J^*\right)\left(1+\mathrm{Tr}\left\{\mathbf{h}_{E_{\beta_j}}\mathbf{h}^H_{E_{\beta_j}}\mathbf{Q}^*\right\}\right)\right\}. \tag{3.69}$$

Comparing (3.69) with (3.65), $f_{\alpha_i,\beta_j}=J^*$ is proved.

■



(a) the proposed design



(b) the conventional design

Figure 3.4: Gray-scale image shows the SNR versus location. The transmit power is $P = 20$dB. (a) Our proposed transmit design. The receiver is assumed to be within the blue circle of radius $r_R = 0.1$ and center $[1, 0]$ in Cartesian coordinates. The eavesdropper is assumed to be within the yellow circle of radius $r_E = 0.1$ and center $[0.4, 0.7]$ in Cartesian coordinates. The worst-case points are shown as the blue point and the yellow points. (b) The conventional design assumes that the receiver and the eavesdropper to be precisely located at the centers of the circles respectively.

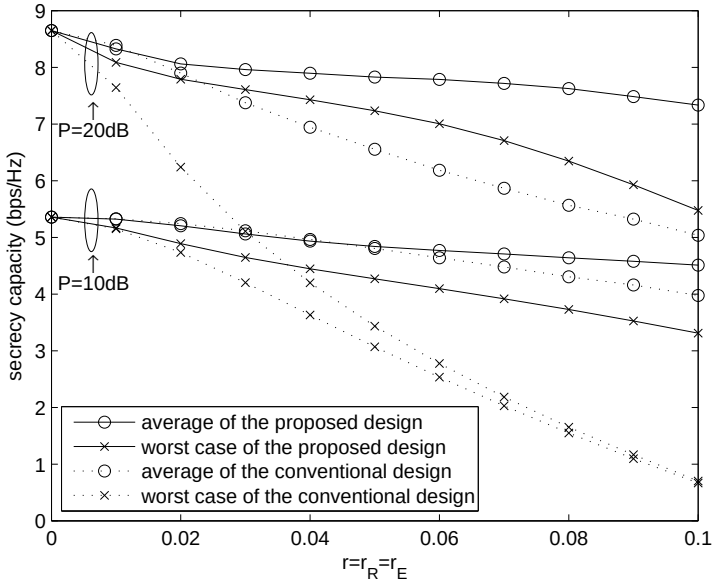


Figure 3.5: The secrecy capacity of the MISOSE secrecy channels versus the location uncertainty radius r, when the transmit power is $P = 20$dB and $P = 10$dB. The locations of the receiver and the eavesdropper are known imprecisely and are assumed to be within the circles of radius $r = r_R = r_E$ and centers $[1, 0]$ and $[0.4, 0.7]$.

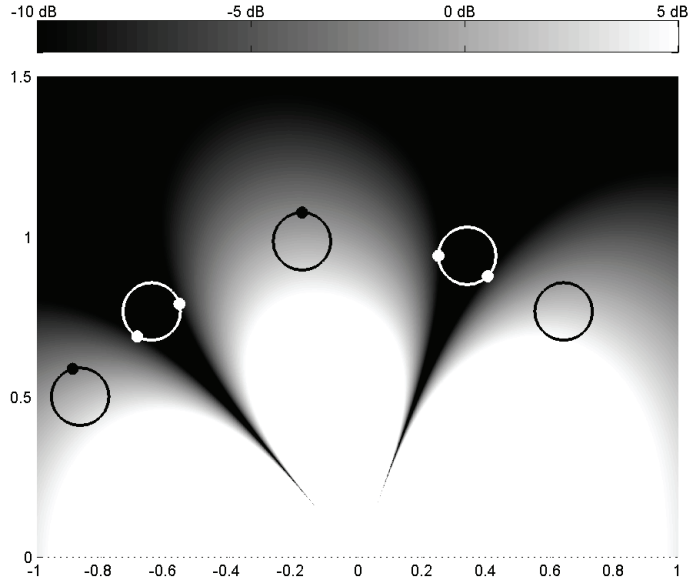


Figure 3.6: Gray-scale image shows the SNR versus location under our proposed transmit design. The transmit power is $P = 20$dB. The multiple receivers are located in the blue circles of radius $r_R = 1$ and centered respectively at $(d = 1, \theta = -60^\circ)$, $(1, -10^\circ)$ and $(1, 40^\circ)$ in polar coordinates. The multiple eavesdroppers are located in the yellow circles of radius $r_E = 1$ and centered respectively at $(1, -40^\circ)$ and $(1, 20^\circ)$. The worst-case points are shown as the blue and the yellow points respectively.

Chapter 4

JAMMING-AIDED MISOSE WIRETAP CHANNEL WITH IMPERFECT CSI

In most existing works, the channel state information (CSI) is usually assumed to be perfectly known or completely unknown. On the one hand, this assumption of perfectly known channels does not hold in practice, because the non-cooperative eavesdropper will try to passively listen. On the other hand, the assumption of completely unknown channel will result in isotropic artificial noise design that is inefficient in jamming a targeted eavesdroppers. For these reasons, designing the transmit/jamming strategy under partial CSI is important in practice. There are two types of assumptions of the channel uncertainty: stochastic and deterministic uncertainties. Assuming the Guassian distribution of the channels, the ergodic secrecy rate and the optimal transmit covariance for MISOSE wiretap channels has been studied in [31]. Assuming the small channel pertubations and the pertubations' distribution, the robust beamformer with artificial noise for MIMO wiretap channels has been designed using perturbation analysis in [41]. A beamforming design for fading wiretap channels is studxied in [15]. The assumption of deterministic uncertainty is adopted by [35], where the wiretap channel under the deterministic uncertainty is named compound wiretap channel. The deterministic uncertainty assumes that the channel state belongs to a given uncertainty set that is known at the transmitter. The secrecy rate of the compound wiretap channel is a worst-case secrecy rate that guarantees secure communication under any possible channel state in the uncertainty set.

We study the joint transmit/jamming design of a MISOSE channel with a friendly multi-antenna jammer and a single-antenna eavesdropper. Assuming arbitrary uncertainty of both the Rx and Ev channel states, we characterize the worst-case secrecy rate and propose to solve the approximate SINR-ratio problem. The worst-case SINR-ratio problem, which is a max-min optimization problem, is non-convex and generally difficult to solve. Two

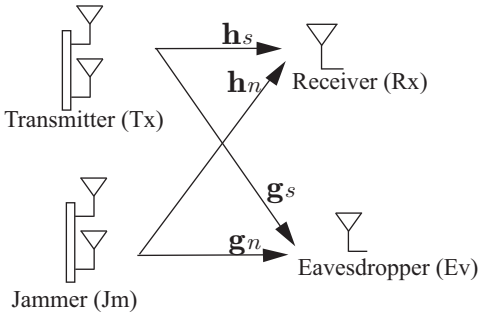


Figure 4.1: The system model for the MISOSE secrecy channel with a multi-antenna transmitter and a single-antenna receiver and eavesdropper.

solutions, a minimax solution and quasiconvex solution, are proposed. 1) Using a minimax theorem, we show that the max-min problem is equivalent to a min-max problem, and the two problem shares a saddle point solution. The min-max problem can be simplified further to a single minimization problem, which seeks to find the worst-case performance under all possible convex combination of the channel states. The minimax solution enables to ease our analysis and provide some insights. 2) A quasiconvex solution that is easy to implement but less insightful is provided.

4.1 System Model and Problem Formulation

Consider a wireless network model consisting of one transmitter (Tx), one jammer (Jm), one legitimate receiver (Rx) and one eavesdropper (Ev), as shown in Fig. 4.1. The Tx and the Jm are equipped with multiple antennas, while the Rx and the Ev have single antenna each. While the Tx transmits a narrowband signal $\mathbf{x}$ with covariance $\mathbf{Q}_T = E\left\{\mathbf{x}\mathbf{x}^H\right\}$, the Jm broadcasts an artificial noise $\mathbf{n}$ with covariance $\mathbf{Q}_J = E\left\{\mathbf{n}\mathbf{n}^H\right\}$. The maximum transmit powers at the Tx and the Jm are respectively P_T and P_J, i.e. $\mathrm{Tr}(\mathbf{Q}_T) \leq P_T$ and $\mathrm{Tr}(\mathbf{Q}_J) \leq P_J$. The channel from the Tx and the Jm to the Rx are denoted by $\mathbf{r}_T$ and $\mathbf{r}_J$, and those to the Ev are denoted by $\mathbf{e}_T$ and $\mathbf{e}_J$.

The received signal at the Rx is given by

$$r_R = \mathbf{r}_T^H \mathbf{x} + \mathbf{r}_J^H \mathbf{n} + n_R, \tag{4.1}$$

and that at the Ev is given by

$$r_E = \mathbf{e}_T^H \mathbf{s} + \mathbf{e}_J^H \mathbf{n} + n_E, \tag{4.2}$$

where n_R and n_E are additive Gaussian noises with variance N_0.

The secrecy rate C_{sec} is equal to the maximum difference between the rates of the receiver and the eavesdropper channels [67],

$$\begin{aligned} C_{\text{sec}} &= \max_{\substack{\mathbf{Q}_T \succeq 0, \text{Tr}(\mathbf{Q}_T) \leq P_T \\ \mathbf{Q}_J \succeq 0, \text{Tr}(\mathbf{Q}_J) \leq P_J}} \left\{ \begin{array}{c} \log\left(1 + \text{SINR}_R\right) \\ -\log\left(1 + \text{SINR}_E\right) \end{array} \right\} \\ &= \max_{\substack{\mathbf{Q}_T \succeq 0, \text{Tr}(\mathbf{Q}_T) \leq P_T \\ \mathbf{Q}_J \succeq 0, \text{Tr}(\mathbf{Q}_J) \leq P_J}} \left\{ \begin{array}{c} \log\left(1 + \frac{\mathbf{r}_T^H \mathbf{Q}_T \mathbf{r}_T}{\mathbf{r}_J^H \mathbf{Q}_J \mathbf{r}_J + N_0}\right) \\ -\log\left(1 + \frac{\mathbf{e}_T^H \mathbf{Q}_T \mathbf{e}_T}{\mathbf{e}_J^H \mathbf{Q}_J \mathbf{e}_J + N_0}\right) \end{array} \right\}. \end{aligned} \tag{4.3}$$

Equation (4.3) characterizes the secrecy rate under the perfect CSI on $(\mathbf{r}_T, \mathbf{r}_J)$ and $(\mathbf{e}_T, \mathbf{e}_J)$. However, the assumption of the perfect CSI is unrealistic. On the one hand, the imperfect CSI of $(\mathbf{r}_T, \mathbf{r}_J)$ is due to estimation error at the Rx, the mobility of the Rx, and quantization error and feedback delay when the Rx feedbacks to the Tx and the Jm. On the other hand, in general it is difficult to obtain accurate $(\mathbf{e}_T, \mathbf{e}_J)$ from a non-cooperative eavesdropper. Thus it is of significant interest to study the secrecy capacity under the imperfect CSI's.

The *worst-case secrecy rate* is defined as the secrecy rate that guarantees the eavesdropper is unable to decode under any channel realization,

$$\begin{aligned} \underline{C_{\text{sec}}} &= \max_{\substack{\mathbf{Q}_T \succeq 0, \text{Tr}(\mathbf{Q}_T) \leq P_T \\ \mathbf{Q}_J \succeq 0, \text{Tr}(\mathbf{Q}_J) \leq P_J}} \min_{\substack{(\mathbf{r}_T, \mathbf{r}_J) \in \Delta_r \\ (\mathbf{e}_T, \mathbf{e}_J) \in \Delta_e}} \log\left(\frac{1 + \text{SINR}_R}{1 + \text{SINR}_E}\right) \\ &= \max_{\substack{\mathbf{Q}_T \succeq 0, \text{Tr}(\mathbf{Q}_T) \leq P_T \\ \mathbf{Q}_J \succeq 0, \text{Tr}(\mathbf{Q}_J) \leq P_J}} \min_{\substack{(\mathbf{r}_T, \mathbf{r}_J) \in \Delta_r \\ (\mathbf{e}_T, \mathbf{e}_J) \in \Delta_e}} \log\left(\frac{1 + \frac{\mathbf{r}_T^H \mathbf{Q}_T \mathbf{r}_T}{\mathbf{r}_J^H \mathbf{Q}_J \mathbf{r}_J + N_0}}{1 + \frac{\mathbf{e}_T^H \mathbf{Q}_T \mathbf{e}_T}{\mathbf{e}_J^H \mathbf{Q}_J \mathbf{e}_J + N_0}}\right). \end{aligned} \tag{4.4}$$

In the sequel, we will consider problem (4.9) with discrete uncertainties,

$$\begin{aligned} \Delta_r &= \left\{(\mathbf{r}_{i,T}, \mathbf{r}_{i,J})\right\}_{i=1}^N, \\ \Delta_e &= \left\{(\mathbf{e}_{j,T}, \mathbf{e}_{j,J})\right\}_{j=1}^M. \end{aligned} \tag{4.5}$$

The discrete uncertainty is the most general case of uncertainty, since all kinds of uncertainty can be viewed as a set containing either finite or infinite numbers of discrete elements.

Problem (4.4) can be rewritten in terms of channel covariances

$$\underline{C_{\text{sec}}} = \max_{\substack{\mathbf{Q}_T \succeq 0, \text{Tr}(\mathbf{Q}_T) \leq P_T \\ \mathbf{Q}_J \succeq 0, \text{Tr}(\mathbf{Q}_J) \leq P_J}} \min_{\substack{(\mathbf{R}_T, \mathbf{R}_J) \in \Omega_r \\ (\mathbf{E}_T, \mathbf{E}_J) \in \Omega_e}} \log \left(\frac{1 + \frac{\text{Tr}(\mathbf{R}_T \mathbf{Q}_T)}{\text{Tr}(\mathbf{R}_J \mathbf{Q}_J) + N_0}}{1 + \frac{\text{Tr}(\mathbf{E}_T \mathbf{Q}_T)}{\text{Tr}(\mathbf{E}_J \mathbf{Q}_J) + N_0}} \right). \tag{4.6}$$

where the channel covariances are

$$\begin{aligned} \mathbf{R}_T &= \mathbf{r}_T \mathbf{r}_T^H, \mathbf{R}_J = \mathbf{r}_J \mathbf{r}_J^H, \\ \mathbf{E}_T &= \mathbf{e}_T \mathbf{e}_T^H, \mathbf{E}_J = \mathbf{e}_J \mathbf{e}_J^H, \end{aligned} \tag{4.7}$$

and Ω_r and Ω_e denote the uncertainty sets of the channel covariances corresponding to Δ_r and Δ_e.

Problem (4.6) is discussed on the following two cases that either $\underline{C_{\text{sec}}} = 0$ or $\underline{C_{\text{sec}}} > 0$.

(**Case 1**) The condition for $\underline{C_{\text{sec}}} = 0$ is that it is impossible to find $\mathbf{Q}_T$ and $\mathbf{Q}_J$ such that $\text{SINR}_R > \text{SINR}_E$. Under this condition, problem (4.6) has a trival optimal solution that $\mathbf{Q}_T^* = \mathbf{0}$ and $\mathbf{Q}_J^* = \mathbf{0}$ and an optimal objective $\underline{C_{\text{sec}}} = 0$. This solution and objective means that none secrecey can be guaranteed, and the best strategy is simply not to transmit anything.

(**Case 2**) We are interested in the case that $\underline{C_{\text{sec}}} > 0$, or in other words, there exists $\mathbf{Q}_T$ and $\mathbf{Q}_J$ such that $\text{SINR}_R > \text{SINR}_E$. In this case, the optimal $\mathbf{Q}_T^*$ to (4.6) must have the maximum power, i.e. $\text{Tr}(\mathbf{Q}_T^*) = P_T$. This is because

$$f(\alpha) = \frac{1 + \text{SINR}_R}{1 + \text{SINR}_E} = \frac{1 + \frac{\text{Tr}(\mathbf{R}_T(\alpha \mathbf{Q}_T))}{\text{Tr}(\mathbf{R}_J \mathbf{Q}_J) + N_0}}{1 + \frac{\text{Tr}(\mathbf{E}_T(\alpha \mathbf{Q}_T))}{\text{Tr}(\mathbf{E}_J \mathbf{Q}_J) + N_0}} \tag{4.8}$$

is a increasing function when $\text{SINR}_R > \text{SINR}_E$.

A good approximate of (4.6) is to approximate $\frac{1+\text{SINR}_R}{1+\text{SINR}_E}$ by $\frac{\text{SINR}_R}{\text{SINR}_E}$. The resulting approximated SINR-ratio problem is

$$\begin{aligned} \widehat{\underline{C_{\text{sec}}}} &= \max_{\substack{\mathbf{Q}_T \succeq 0, \text{Tr}(\mathbf{Q}_T) \leq P_T \\ \mathbf{Q}_J \succeq 0, \text{Tr}(\mathbf{Q}_J) \leq P_J}} \min_{\substack{(\mathbf{r}_T, \mathbf{r}_J) \in \Delta_r \\ (\mathbf{e}_T, \mathbf{e}_J) \in \Delta_e}} \frac{\text{SINR}_R}{\text{SINR}_E} \\ &= \max_{\substack{\mathbf{Q}_T, \mathbf{Q}_J \succeq 0, \\ \text{Tr}(\mathbf{Q}_T) \leq P_T \\ \text{Tr}(\mathbf{Q}_J) \leq P_J}} \min_{\substack{(\mathbf{R}_T, \mathbf{R}_J) \in \Omega_r \\ (\mathbf{E}_T, \mathbf{E}_J) \in \Omega_e}} \frac{\text{Tr}(\mathbf{R}_T \mathbf{Q}_T)}{\text{Tr}(\mathbf{E}_T \mathbf{Q}_T)} \frac{\text{Tr}(\mathbf{E}_J \mathbf{Q}_J) + N_0}{\text{Tr}(\mathbf{R}_J \mathbf{Q}_J) + N_0}. \end{aligned} \tag{4.9}$$

Since $\frac{\text{SINR}_R}{\text{SINR}_E} \geq \frac{1+\text{SINR}_R}{1+\text{SINR}_E}$ when $\text{SINR}_R \geq \text{SINR}_E \geq 0$, $\widehat{\underline{C_{\text{sec}}}}$ (4.9) is an upper bound for $\underline{C_{\text{sec}}}$ (4.4).

In the case of perfectly known channels, a jamming scheme commonly used is an artificial noise orthogonal to the Rx channel $\mathbf{r}_J$, or in other words zero-forcing to $\mathbf{r}_J$, such as [18] and [55]. The idea behind is to increase the jamming level seen by the Ev while the channel of the Rx is not interfered. However, the zero-forcing beamforming methods may be infeasible in the case of uncertain channels. Especially when the number of Rx's channel states is greater than that of the number of Jm's antennas, it is impossible to find a nullspace that is orthogonal to all the possible $\mathbf{r}_J$. It should be noted that the worst-case secrecy rate (4.6) and the approximate SINR ratio (4.9) problems do not constrain that the jamming noise must be interference free to the Rx.

In the next section, we will analyze problem (4.9) under the minimax framework, which helps to understand the problem and obtain some insights. After that, we will reformulate problem (4.9) into a quasiconvex optimization problem.

4.2 Minimax Solution

This section is based on the following minimax theorem, which proves that the min-max problem is equivalent to the max-min problem. We are going to use the theorem to transfer the difficult problem (4.9) into its max-min counterpart, and by solving the max-min counterpart we can solve problem (4.9).

4.2.1 Equivalence between the Max-min and the Min-max Problems

In order to apply Theorem 3.1 onto problem (4.9), we provide two lemmas to satisfy the two conditions of Theorem 3.1.

Lemma 4.1:

The problem (4.9) under any Ω_r and Ω_e is the same as that under the convex hull $\text{conv}(\Omega_r)$ and $\text{conv}(\Omega_e)$. That is to say,

$$\begin{aligned} & \max_{\substack{\mathbf{Q}_T,\mathbf{Q}_J\succeq 0,\\ \text{Tr}(\mathbf{Q}_T)\le P_T\\ \text{Tr}(\mathbf{Q}_J)\le P_J}} \min_{\substack{(\mathbf{R}_T,\mathbf{R}_J)\in\Omega_r\\ (\mathbf{E}_T,\mathbf{E}_J)\in\Omega_e}} \frac{\text{Tr}\left(\mathbf{R}_T\mathbf{Q}_T\right)}{\text{Tr}\left(\mathbf{E}_T\mathbf{Q}_T\right)} \frac{\text{Tr}\left(\mathbf{E}_J\mathbf{Q}_J\right)+N_0}{\text{Tr}\left(\mathbf{R}_J\mathbf{Q}_J\right)+N_0} \\ = & \max_{\substack{\mathbf{Q}_T,\mathbf{Q}_J\succeq 0,\\ \text{Tr}(\mathbf{Q}_T)\le P_T\\ \text{Tr}(\mathbf{Q}_J)\le P_J}} \min_{\substack{(\mathbf{R}_T,\mathbf{R}_J)\in\text{conv}(\Omega_r)\\ (\mathbf{E}_T,\mathbf{E}_J)\in\text{conv}(\Omega_e)}} \frac{\text{Tr}\left(\mathbf{R}_T\mathbf{Q}_T\right)}{\text{Tr}\left(\mathbf{E}_T\mathbf{Q}_T\right)} \frac{\text{Tr}\left(\mathbf{E}_J\mathbf{Q}_J\right)+N_0}{\text{Tr}\left(\mathbf{R}_J\mathbf{Q}_J\right)+N_0}. \end{aligned} \tag{4.10}$$

This equivalence is proved in Appendix 4.A.

Lemma 4.2:

The objective function in (4.9) is quasiconcave in either $\mathbf{Q}_T$ or $\mathbf{Q}_J$, and quasiconvex in either $(\mathbf{R}_T, \mathbf{R}_J)$ or $(\mathbf{E}_T, \mathbf{E}_J)$.

Proof: The linear-fractional function

$$f(\mathbf{x}) = \frac{\mathbf{a}^T\mathbf{x} + b}{\mathbf{c}^T\mathbf{x} + d} \tag{4.11}$$

with domain $\text{dom}_f = \{\mathbf{x}|\mathbf{c}^T\mathbf{x} + d > 0\}$ is both quasiconvex and quasiconcave [4, Chap. 3].

The objective function in (4.9) can be expressed as a linear-fractional function of either $(\mathbf{R}_T, \mathbf{R}_J)$ or $(\mathbf{E}_T, \mathbf{E}_J)$, thus the function is quasi-convex in either $(\mathbf{R}_T, \mathbf{R}_J)$ or $(\mathbf{E}_T, \mathbf{E}_J)$. The function can be expressed as a linear-fractional function of either $\mathbf{Q}_T$ or $\mathbf{Q}_J$, thus the function is quasi-concave in either $\mathbf{Q}_T$ or $\mathbf{Q}_J$. ■

Using Lemma 4.1, problem (4.9) is first equivalent to problem (4.10). Then using Lemma 4.2 and Theorem 3.1, problem (4.10) is equivalent to the following max-min problem

$$\min_{\substack{(\mathbf{R}_T,\mathbf{R}_J)\in\text{conv}(\Omega_r)\\(\mathbf{E}_T,\mathbf{E}_J)\in\text{conv}(\Omega_e)}} \max_{\substack{\mathbf{Q}_T,\mathbf{Q}_J\succeq 0,\\ \text{Tr}(\mathbf{Q}_T)\le P_T\\ \text{Tr}(\mathbf{Q}_J)\le P_J}} \frac{\text{Tr}\left(\mathbf{R}_T\mathbf{Q}_T\right)}{\text{Tr}\left(\mathbf{E}_T\mathbf{Q}_T\right)} \frac{\text{Tr}\left(\mathbf{E}_J\mathbf{Q}_J\right) + N_0}{\text{Tr}\left(\mathbf{R}_J\mathbf{Q}_J\right) + N_0}. \tag{4.12}$$

The min-max problem (4.9) and the max-min problem (4.12) shares the same solution which is the saddle point of the objective function.

4.2.2 SINR-ratio Problem for Perfectly Known Channels

The inner maximization of (4.12) is the problem of maximizing the SINR ratio at given perfectly known channels. The inner maximization is two indepedent maximization problems, that is to say,

$$\begin{aligned} &\max_{\substack{\mathbf{Q}_T,\mathbf{Q}_J\succeq 0,\\ \text{Tr}(\mathbf{Q}_T)\le P_T\\ \text{Tr}(\mathbf{Q}_J)\le P_J}} \frac{\text{Tr}\left(\mathbf{R}_T\mathbf{Q}_T\right)}{\text{Tr}\left(\mathbf{E}_T\mathbf{Q}_T\right)} \frac{\text{Tr}\left(\mathbf{E}_J\mathbf{Q}_J\right) + N_0}{\text{Tr}\left(\mathbf{R}_J\mathbf{Q}_J\right) + N_0} \\ = &\left(\max_{\substack{\mathbf{Q}_T\succeq 0,\\ \text{Tr}(\mathbf{Q}_T)\le P_T}} \frac{\text{Tr}\left(\mathbf{R}_T\mathbf{Q}_T\right)}{\text{Tr}\left(\mathbf{E}_T\mathbf{Q}_T\right)}\right)\left(\max_{\substack{\mathbf{Q}_J\succeq 0,\\ \text{Tr}(\mathbf{Q}_J)\le P_J}} \frac{\text{Tr}\left(\mathbf{E}_J\mathbf{Q}_J\right) + N_0}{\text{Tr}\left(\mathbf{R}_J\mathbf{Q}_J\right) + N_0}\right). \end{aligned} \tag{4.13}$$

The goal of $\mathbf{Q}_T$ is to maximize the ratio of the signal power at the Rx to that at the Ev, and that of $\mathbf{Q}_J$ is to maximize the ratio of the jamming-plus-noise level at the Ev to that at the Rx. This is consistent with our intuition that the Tx will transmit along the Rx channel while avoid leakage to the Ev channel, and the Jm will jam the Ev channel and avoid interference onto the Rx channel.

Both problems of (4.13) are Rayleigh quotient problems and can be easily solved. The first problem, the maximization of $\mathbf{Q}_T$, has optimal objective $\lambda_{\max}(\mathbf{R}_T, \mathbf{E}_T)$. The reason is that assuming $\mathbf{Q}_T$ has decomposition that $\mathbf{Q}_T = \mathbf{q}_{T1}\mathbf{q}_{T1}^H + \cdots + \mathbf{q}_{TK}\mathbf{q}_{TK}^H$,

$$\begin{aligned} & \frac{\mathrm{Tr}(\mathbf{R}_T\mathbf{Q}_T)}{\mathrm{Tr}(\mathbf{E}_T\mathbf{Q}_T)} \\ = & \frac{\mathbf{q}_{T1}\mathbf{R}_T\mathbf{q}_{T1}^H + \cdots + \mathbf{q}_{TK}\mathbf{R}_T\mathbf{q}_{TK}^H}{\mathbf{q}_{T1}\mathbf{E}_T\mathbf{q}_{T1}^H + \cdots + \mathbf{q}_{TK}\mathbf{E}_T\mathbf{q}_{TK}^H} \\ \leq & \max_{\mathbf{q}_{Ti}} \frac{\mathbf{q}_{Ti}^H\mathbf{R}_T\mathbf{q}_{Ti}}{\mathbf{q}_{Ti}^H\mathbf{E}_T\mathbf{q}_{Ti}} \leq \lambda_{\max}(\mathbf{R}_T, \mathbf{E}_T). \end{aligned} \tag{4.14}$$

The second problem, the maximization of $\mathbf{Q}_J$ has optimal objective that

$$\max_{\substack{\mathbf{Q}_J \succeq 0, \\ \mathrm{Tr}(\mathbf{Q}_J) \leq P_J}} \frac{\mathrm{Tr}(\mathbf{E}_J\mathbf{Q}_J) + N_0}{\mathrm{Tr}(\mathbf{R}_J\mathbf{Q}_J) + N_0} \tag{4.15}$$

$$= \begin{cases} 1 & , \text{if } \lambda_{\max}(\mathbf{E}_J, \mathbf{R}_J) < 1 \\ \lambda_{\max}\left(\mathbf{I} + \frac{P_J}{N_0}\mathbf{E}_J, \mathbf{I} + \frac{P_J}{N_0}\mathbf{R}_J\right) & , \text{if } \lambda_{\max}(\mathbf{E}_J, \mathbf{R}_J) \geq 1 \end{cases}. \tag{4.16}$$

If $\lambda_{\max}(\mathbf{E}_J, \mathbf{R}_J) < 1$, the optimal objective to (4.15) is 1 with $\mathbf{Q}_J^* = \mathbf{0}$, because $\mathrm{Tr}(\mathbf{E}_J\mathbf{Q}_J) \leq \mathrm{Tr}(\mathbf{R}_J\mathbf{Q}_J)$, $\forall \mathbf{Q}_J$. If $\lambda_{\max}(\mathbf{E}_J, \mathbf{R}_J) \geq 1$, the optimal $\mathbf{Q}_J^*$ must have the maximum power P_J since

$$g(\alpha) = \frac{\mathrm{Tr}(\mathbf{E}_J(\alpha\mathbf{Q}_J^*)) + N_0}{\mathrm{Tr}\left(\mathbf{R}_J\left(\alpha\mathbf{Q}_J^*\right)\right) + N_0} \tag{4.17}$$

is an increasing function when $\mathrm{Tr}(\mathbf{E}_J\mathbf{Q}_J^*) \geq \mathrm{Tr}(\mathbf{R}_J\mathbf{Q}_J^*)$. Given that $\mathrm{Tr}(\mathbf{Q}_J^*) = P_J$, problem (4.15) can be reformulated into

$$\max_{\substack{\mathbf{Q}_J \succeq 0, \\ \mathrm{Tr}(\mathbf{Q}_J) \leq P_J}} \frac{\mathrm{Tr}(\mathbf{E}_J\mathbf{Q}_J) + N_0}{\mathrm{Tr}(\mathbf{R}_J\mathbf{Q}_J) + N_0} = \max_{\substack{\mathbf{Q}_J \succeq 0, \\ \mathrm{Tr}(\mathbf{Q}_J) \leq P_J}} \frac{\mathrm{Tr}\left(\left(\mathbf{I} + \frac{P_n}{N_0}\mathbf{E}_J\right)\mathbf{Q}_J\right)}{\mathrm{Tr}\left(\left(\mathbf{I} + \frac{P_n}{N_0}\mathbf{R}_J\right)\mathbf{Q}_J\right)} \tag{4.18}$$

which is a Rayleigh quotient problem and has optimal objective $\lambda_{\max}\left(\mathbf{I} + \frac{P_J}{N_0}\mathbf{E}_J, \mathbf{I} + \frac{P_J}{N_0}\mathbf{R}_J\right)$.

4.2.3 Reduction to a Single Minimization Problem

Problem (4.12) is reduced to, by solving the inner maximization,

$$\min_{\substack{(\mathbf{R}_T,\mathbf{R}_J)\in\mathrm{conv}(\Omega_r)\\(\mathbf{E}_T,\mathbf{E}_J)\in\mathrm{conv}(\Omega_e)}} \frac{\lambda_{\max}\left(\mathbf{R}_T,\mathbf{E}_T\right)\times}{\max\left\{1,\lambda_{\max}\left(\mathbf{I}+\frac{P_J}{N_0}\mathbf{E}_J,\mathbf{I}+\frac{P_J}{N_0}\mathbf{R}_J\right)\right\}}. \tag{4.19}$$

Let $(\mathbf{R}_T^*,\mathbf{R}_J^*)$ and $(\mathbf{E}_T^*,\mathbf{E}_J^*)$ denote the optimal solution to (4.19). Depending on whether $\lambda_{\max}\left(\mathbf{E}_T^*,\mathbf{E}_J^*\right)$ is greater or smaller than 1, (**Case 2**) in Section II can be divided into two cases:

(**Case 2-1**) If $\lambda_{\max}\left(\mathbf{E}_T^*,\mathbf{E}_J^*\right)<1$, then the optimal $\mathbf{Q}_J^*=\mathbf{0}$. It means under any non-zero $\mathbf{Q}_J$ the Jm will put less noise onto the worst-case Ev channel than to the worst-case Rx channel, thus the best strategy for the Jm is merely not to transmit. The problem in this case is degraded to transmit design without jamming for uncertain MISO channels which is studied in our previous work [52].

(**Case 2-2**) If $\lambda_{\max}\left(\mathbf{E}_T^*,\mathbf{E}_J^*\right)\geq 1$, the Jm will transmit in full power to maximize the SINR ratio. Problem (4.19) becomes

$$\min_{\substack{(\mathbf{R}_T,\mathbf{R}_J)\in\mathrm{conv}(\Omega_r)\\(\mathbf{E}_T,\mathbf{E}_J)\in\mathrm{conv}(\Omega_e)}} \lambda_{\max}\left(\mathbf{R}_T,\mathbf{E}_T\right)\times\lambda_{\max}\left(\mathbf{I}+\frac{P_J}{N_0}\mathbf{E}_J,\mathbf{I}+\frac{P_J}{N_0}\mathbf{R}_J\right). \tag{4.20}$$

Jm is beneficial to increasing the SINR ratio, if Jm can exert more jamming noise onto the worst-case Ev channel than onto the worst-case Rx channel.

4.2.4 Relation between the Worst-case and Average Design

Assuming the discrete uncertainty (4.5), averaging weights $\{\nu_1,\cdots,\nu_N|0\leq\nu_i\leq 1,\sum\nu_i=1\}$ associated with Rx's states, and weights $\{\mu_1,\cdots,\mu_M|0\leq\mu_j\leq 1,\sum\mu_j=1\}$ associated with Ev's states. These weights can also be viewed as probabilities at the random states.

The weighted average of the signal level at the Rx is given by

$$\widehat{\mathrm{S}_R}=\sum\nu_i\left(\mathbf{r}_{i,T}^H\mathbf{Q}_T\mathbf{r}_{i,T}\right)=\mathrm{Tr}\left(\left(\sum\nu_i\mathbf{R}_{i,T}\right)\mathbf{Q}_T\right), \tag{4.21}$$

and the weighted average of the jamming noise level at the Rx is

$$\widehat{\mathrm{N}_R}=\sum\nu_i\left(\mathbf{r}_{i,J}^H\mathbf{Q}_J\mathbf{r}_{i,J}\right)=\mathrm{Tr}\left(\left(\sum\nu_i\mathbf{R}_{i,J}\right)\mathbf{Q}_J\right), \tag{4.22}$$

where $\mathbf{R}_{iT}, \mathbf{R}_{iJ}$ are the corresponding channel covariances at different states. Those at the Ev is given by

$$\widehat{\mathrm{S}_E} = \sum \mu_j \left(\mathbf{e}_{j,T}^H \mathbf{Q}_T \mathbf{e}_{j,T}\right) = \mathrm{Tr}\left(\left(\sum \mu_j \mathbf{E}_{j,T}\right)\mathbf{Q}_T\right), \tag{4.23}$$

and

$$\widehat{\mathrm{N}_E} = \sum \mu_j \left(\mathbf{e}_{j,J}^H \mathbf{Q}_J \mathbf{e}_{j,J}\right) = \mathrm{Tr}\left(\left(\sum \mu_j \mathbf{E}_{j,J}\right)\mathbf{Q}_J\right). \tag{4.24}$$

The average design aims to solve the problem of maximizing the average SINR ratio,

$$\begin{aligned}
& \max_{\substack{\mathbf{Q}_T,\mathbf{Q}_J\succeq 0,\\ \mathrm{Tr}(\mathbf{Q}_T)\le P_T\\ \mathrm{Tr}(\mathbf{Q}_J)\le P_J}} \frac{\widehat{\mathrm{S}_R}/\left(\widehat{\mathrm{N}_R}+N_0\right)}{\widehat{\mathrm{S}_E}/\left(\widehat{\mathrm{N}_E}+N_0\right)} \\
= & \max_{\substack{\mathbf{Q}_T,\mathbf{Q}_J\succeq 0,\\ \mathrm{Tr}(\mathbf{Q}_T)\le P_T\\ \mathrm{Tr}(\mathbf{Q}_J)\le P_J}} \frac{\mathrm{Tr}\left(\left(\sum \nu_i \mathbf{R}_{i,T}\right)\mathbf{Q}_T\right)}{\mathrm{Tr}\left(\left(\sum \mu_j \mathbf{E}_{j,T}\right)\mathbf{Q}_T\right)} \frac{\mathrm{Tr}\left(\left(\sum \mu_j \mathbf{E}_{j,J}\right)\mathbf{Q}_J\right)+N_0}{\mathrm{Tr}\left(\left(\sum \nu_i \mathbf{R}_{i,J}\right)\mathbf{Q}_J\right)+N_0} \\
= & \lambda_{\max}\left(\widehat{\mathbf{R}_T}, \widehat{\mathbf{E}_T}\right) \times \lambda_{\max}\left(\mathbf{I}+\frac{P_J}{N_0}\widehat{\mathbf{E}_J}, \mathbf{I}+\frac{P_J}{N_0}\widehat{\mathbf{R}_J}\right),
\end{aligned} \tag{4.25}$$

where the average channel covariances are

$$\widehat{\mathbf{R}_T} = \sum \nu_i \mathbf{R}_{iT}, \widehat{\mathbf{R}_J} = \sum \nu_i \mathbf{R}_{i,J}, \tag{4.26}$$

$$\widehat{\mathbf{E}_T} = \sum \mu_j \mathbf{E}_{jT}, \widehat{\mathbf{E}_J} = \sum \mu_j \mathbf{E}_{j,J}. \tag{4.27}$$

Given the discrete uncertainty (4.5), the worst-case design (4.20) can be written into

$$\min_{\substack{0\le\nu_i\le 1,\ \sum \nu_i=1,\\ 0\le\mu_j\le 1,\ \sum \mu_j=1}} \lambda_{\max}\left(\widehat{\mathbf{R}_T}, \widehat{\mathbf{E}_T}\right) \times \lambda_{\max}\left(\mathbf{I}+\frac{P_J}{N_0}\widehat{\mathbf{E}_J}, \mathbf{I}+\frac{P_J}{N_0}\widehat{\mathbf{R}_J}\right). \tag{4.28}$$

Comparing (4.28) with (4.25), it can be concluded that the worst-case design (4.28) is a special case of the average design (4.25). Moreover, the worst-case design has the lowest objective among all average designs.

4.3 Quasiconvex Optimization Formulation

Although problem (4.9) has been reduced to a simple minimization problem (4.20) (or (4.28) given discrete uncertainties), it is not straightforward that whether problem (4.20)

can be written into a convex optimization form. Alternatively, we propose a quasiconvex optimization formulation for

$$\max_{\mathbf{Q}_T,\mathbf{Q}_J\succeq 0,}\ \min_{\substack{(\mathbf{R}_T,\mathbf{R}_J)\in\Omega_r\\(\mathbf{E}_T,\mathbf{E}_J)\in\Omega_e}} \frac{\mathrm{Tr}\left(\mathbf{R}_T\mathbf{Q}_T\right)}{\mathrm{Tr}\left(\mathbf{E}_T\mathbf{Q}_T\right)}\frac{\mathrm{Tr}\left(\left(\mathbf{I}+\frac{P_J}{N_0}\mathbf{E}_J\right)\mathbf{Q}_J\right)}{\mathrm{Tr}\left(\left(\mathbf{I}+\frac{P_J}{N_0}\mathbf{R}_J\right)\mathbf{Q}_J\right)}. \tag{4.29}$$

Problem (4.29) is a simplified form of (4.9) under (**Case 2-2**).

First, problem (4.29) can be rewritten into a constrained maximization problem:

$$\begin{aligned}
&\max_{t,\mathbf{Q}_T,\mathbf{Q}_J} \quad t\\
\text{s.t.}\quad &\mathbf{Q}_T\succeq 0,\quad \mathbf{Q}_J\succeq 0,\\
&\left(\min_{(\mathbf{R}_T,\mathbf{R}_J)\in\Omega_r}\frac{\mathrm{Tr}\left(\mathbf{R}_T\mathbf{Q}_T\right)}{\mathrm{Tr}\left(\left(\mathbf{I}+\frac{P_J}{N_0}\mathbf{R}_J\right)\mathbf{Q}_J\right)}\right)\times\\
&\left(\min_{(\mathbf{E}_T,\mathbf{E}_J)\in\Omega_e}\frac{\mathrm{Tr}\left(\left(\mathbf{I}+\frac{P_J}{N_0}\mathbf{E}_J\right)\mathbf{Q}_J\right)}{\mathrm{Tr}\left(\mathbf{E}_T\mathbf{Q}_T\right)}\right) = t.
\end{aligned} \tag{4.30}$$

Next, notice that (4.29) is independent to $\mathrm{Tr}(\mathbf{Q}_T)$ and $\mathrm{Tr}(\mathbf{Q}_J)$. If $\mathbf{Q}_T^*$,$\mathbf{Q}_J^*$ are an optimal solution to (4.29), then $\alpha\mathbf{Q}_T^*$,$\beta\mathbf{Q}_J^*$ is also an optimal solution where α,β are positive constants. Following this reason, without changing the essence of problem (4.30), the last constraint of (4.30) can be replaced by

$$\begin{cases}
\min\limits_{(\mathbf{R}_T,\mathbf{R}_J)\in\Omega_r}\dfrac{\mathrm{Tr}\left(\mathbf{R}_T\mathbf{Q}_T\right)}{\mathrm{Tr}\left(\left(\mathbf{I}+\frac{P_J}{N_0}\mathbf{R}_J\right)\mathbf{Q}_J\right)} = t\\
\min\limits_{(\mathbf{E}_T,\mathbf{E}_J)\in\Omega_e}\dfrac{\mathrm{Tr}\left(\left(\mathbf{I}+\frac{P_J}{N_0}\mathbf{E}_J\right)\mathbf{Q}_J\right)}{\mathrm{Tr}\left(\mathbf{E}_T\mathbf{Q}_T\right)} = 1
\end{cases}. \tag{4.31}$$

Moreover, the above two equality constraints can be relaxed to inequality constraints and problem (4.30) is equivalent to

$$\begin{aligned}
&\max_{t,\mathbf{Q}_T,\mathbf{Q}_J} \quad t\\
\text{s.t.}\quad &\mathbf{Q}_T\succeq 0,\quad \mathbf{Q}_J\succeq 0,\\
&\min_{(\mathbf{R}_T,\mathbf{R}_J)\in\Omega_r}\frac{\mathrm{Tr}\left(\mathbf{R}_T\mathbf{Q}_T\right)}{\mathrm{Tr}\left(\left(\mathbf{I}+\frac{P_J}{N_0}\mathbf{R}_J\right)\mathbf{Q}_J\right)}\geq t,\\
&\min_{(\mathbf{E}_T,\mathbf{E}_J)\in\Omega_e}\frac{\mathrm{Tr}\left(\left(\mathbf{I}+\frac{P_J}{N_0}\mathbf{E}_J\right)\mathbf{Q}_J\right)}{\mathrm{Tr}\left(\mathbf{E}_T\mathbf{Q}_T\right)}\geq 1.
\end{aligned} \tag{4.32}$$

The only difference between (4.32) and (4.30) is that $\mathbf{Q}_T^*$,$\mathbf{Q}_J^*$ optimal to (4.32) is a scaled version of $\mathbf{Q}_T^*$,$\mathbf{Q}_J^*$ optimal to (4.30).

Finally, (4.32) can be rewritten into a quasiconvex optimization form

$$\begin{aligned} \max_{t,\mathbf{Q}_T,\mathbf{Q}_J} \quad & t \\ \text{s.t.} \quad & \mathbf{Q}_T \succeq 0, \quad \mathbf{Q}_J \succeq 0, \\ & \mathrm{Tr}\left(\mathbf{R}_T\mathbf{Q}_T\right) \geq t \times \mathrm{Tr}\left(\left(\mathbf{I}+\frac{P_J}{N_0}\mathbf{R}_J\right)\mathbf{Q}_J\right), \forall\left(\mathbf{R}_T,\mathbf{R}_J\right) \in \Omega_r, \\ & \mathrm{Tr}\left(\left(\mathbf{I}+\frac{P_J}{N_0}\mathbf{E}_J\right)\mathbf{Q}_J\right) \geq \mathrm{Tr}\left(\mathbf{E}_T\mathbf{Q}_T\right), \forall\left(\mathbf{E}_T,\mathbf{E}_J\right) \in \Omega_e. \end{aligned} \tag{4.33}$$

Problem (4.33) can be solved by solving a sequence of feasibility problems as the following bisection method shows.

Bisection method for solving (4.33)

1: Given a lower bound l and an upper bound u, such that the interval $[l,u]$ is guaranteed to contain the optimal objective J^*.

2: Let $t=\frac{l+u}{2}$. Solve the feasibility problem: finding $\mathbf{Q}_T$ and $\mathbf{Q}_J$ such that the constraints in (4.33) are satisfied.

   If a feasible solution can be found, then $l \leftarrow t$, else $u \leftarrow t$.

3: Repeat step 2 until the bounding interval $[l,u]$ is small enough.

Note that $\mathbf{Q}_T^*$ to (4.6) has the maximum power referring to (**Case 2**), and $\mathbf{Q}_J^*$ to (4.6) has the maximum power referring to (**Case 2-2**). Thus after obtaining $\mathbf{Q}_T'^*, \mathbf{Q}_J'^*$ to (4.33), we scale the power of $\alpha\mathbf{Q}_T'^*, \beta\mathbf{Q}_J'^*$ to their full powers and use the scaled solution $(\alpha\mathbf{Q}_T'^*, \beta\mathbf{Q}_J'^*)$ as the approximate solution to (4.4).

4.4 Numerical Results

We present numerical examples to demonstrate the effectiveness of the proposed cooperative jamming in combating location uncertainties of the Rx and jamming the Ev's at multiple locations.

In the first example, a multiple-antenna transmitter wants to transmit towards a certain range of desired directions where the Rx might be located, and to jam the other insecure

directions where the Ev might be. The locations of the Rx and the Ev are as follows. The distance of the Rx and the Ev are assumed to be $d_R = 1$ and $d_E = 1$. The desired direction range is $\theta_R \in [-5°, 5°]$, and the insecure directions is $\theta_E \in [-90°, -15°] \cup [15°, 90°]$. The discretized samples in place of the continuous direction range, shown in Fig. 4.2, are used to generate the channel uncertainty.

The transmitter is equipped with $L = 6$ linear antenna elements spaced half wavelength apart, and has a maximum power $P = 20\text{dB}\times N_0$. The antenna elements are assumed to be omni-isotropic and have unit gains. The signals arrived at the Rx and the Ev are modeled as far-field signals, so that the channel at location (d, θ) can expressed as

$$\mathbf{h}\left(d,\theta\right) = \frac{1}{d^{\alpha/2}}\left[1, e^{-j\pi\sin(\theta)}, e^{-j2\pi\sin(\theta)}, \cdots, e^{-j(L-1)\pi\sin(\theta)}\right]^T, \tag{4.34}$$

where d is the distance, $\alpha = 2$ is the path loss exponent, and angle θ is the direction. The discrete samples of Rx's and Ev's locations along with (4.2) are used to generate the uncertainty sets of the channels.

In Fig. 4.2(a), the transmitter plays the roles of both the Tx and the Jm in Fig. 4.1 by transmitting the message signal and the superposing jamming noise. The total power is $P = 20\text{dB}\times N_0$, which is allocated into the signal power $P_T = 30N_0$ and the jamming power $P_J = 70N_0$. Fig. 4.2(a) plots the SINR in gray scale as well as beampatterns of the message signal and the jamming noise, that is, $BP_T(\theta) = \mathbf{h}^H\left(1,\theta\right)\mathbf{Q}_T\mathbf{h}\left(1,\theta\right)$ and $BP_J(\theta) = \mathbf{h}^H\left(1,\theta\right)\mathbf{Q}_J\mathbf{h}\left(1,\theta\right)$. The main beam of the message signal points to the Rx's direction range. Four side lobes inevitably exists due to the geometry of the linear array. These side lobes are protected by the jamming noise, whose beams point to the side lobes' direction and avoid the Rx's direction range. The overall result of this cooperative jamming design is that $\text{SINR}_R \geq 24.5\text{dB}$ and $\text{SINR}_E \leq -2.6\text{dB}$. The worst-case secrecy rate under this cooperative design is $\underline{C_{\text{sec}}} = 7.52\text{bps/Hz}$.

To compare the performance with or without cooperative jamming, Fig. 4.2(b) is the optimal transmit design without jamming to maximize the worst-case rate. The total transmit powers with or without jamming are the same $20\text{dB}\times N_0$ for a fair comparison. Without jamming, the transmitter sends only the message signal which steers towards the Rx's direction and simultaneously nulls the direction of the eavesdropper. The optimal transmit

design maximizes the worst-case secrecy rate

$$\begin{aligned} & \max_{\substack{\mathbf{Q}_T \succeq 0 \\ \mathrm{Tr}(\mathbf{Q}_T) \le P_T}} \min_{\substack{\mathbf{r}_T \in \Delta_r \\ \mathbf{e}_T \in \Delta_e}} \log \left(\frac{1+\mathrm{SNR}_R}{1+\mathrm{SNR}_E} \right) \\ = & \max_{\substack{\mathbf{Q}_T \succeq 0 \\ \mathrm{Tr}(\mathbf{Q}_T) \le P_T}} \min_{\substack{\mathbf{r}_T \in \Delta_r \\ \mathbf{e}_T \in \Delta_e}} \log \left(\frac{1+\frac{\mathbf{r}_T^H \mathbf{Q}_T \mathbf{r}_T}{N_0}}{1+\frac{\mathbf{e}_T^H \mathbf{Q}_T \mathbf{e}_T}{N_0}} \right). \end{aligned} \tag{4.35}$$

This non-jamming design is effective when the direction range of the Ev is small. For the large direction range of the Ev here, as in the case of Fig. 4.2, the non-jammingx design is not as effective. The side lobes of the message signal exists inevitably and are unprotected, as shown in Fig. 4.2(b). The worst-case SNR's are $\mathrm{SINR}_R \ge 26.7$dB and $\mathrm{SINR}_E \le 15.3$dB. The worst-case secrecy rate under this non-jamming design is 3.74bps/Hz.

In the second example, the goal is to transmit the signal to a certain region and nulls the other insecure locations where the Ev might be. A corresponding battlefield scenario is that a commanding unit and some jamming helpers all equipped with multi antennas wants to transmit to mobile soldiers that are only able to carry small-sized single antenna and are located within a certain region. Meanwhile, the signal leaking to the insecure locations should be protected by the jamming noise. Fig. 4.3 shows a such scenario where a Tx and two Jm's each with 4-antenna linear array are at coordinate $(0,0)$, $(-1.2,1.5)$ and $(1.2,1.5)$, respectively. The total power for the three units is $25\mathrm{dB}\times N_0 = 316N_0$, which consists of $P_s = 116N_0$ at the Tx and $P_n = 200N_0$ together at the two Jm's. In Fig. 4.3, the Tx steers its main beam to the Rx's region. The message signal level at the bottom region is higher than that at the Rx's region, because the bottom region is closer to the Tx. Cooperatively, the Jm are able to deploy a lobe of large jamming power towards the bottom region to make small the SINR at the bottom. The Jm also have two lobes of small power to jam the upper region where the signal level is low. The SINR result is that $\mathrm{SINR}_R \ge 19.8$dB and $\mathrm{SINR}_E \le 6.7$dB. The worst-case secrecy rate under the jamming design is 4.08bps/Hz. Note that using only the Tx and without the Jm's at other locations, even if the Tx can transmit message signal and overlapping jamming noise at the same time as in our first example, the worst-case secrecy rate will be zero, because the Tx alone can not prevent the bottom region from having higher SINR than the Rx's region.

4.5 Conclusion

We study the worst-case secrecy rate of MISOSE wiretap channels. We propose to solve the joint optimization of transmit and jamming design for the approximate worst-case SINR-ratio problem. A minimax solution is shown to exist for the problem, based on which some insightful results of the optimal transmit and jamming covariances are obtained. We also show that the worst-case design can be viewed as a special case of the average design, and is in fact the worst case of the average design. A quasi-convex optimization algorithm that is tractable and efficient is provided for solving the worst-case SINR-ratio problem. In the first numerical example, we demonstrate that a linear array successfully transmits towards a certain direction range and jams the other directions simultaneously. In the second example, three arrays cooperate to transmit to a certain location and jam the other locations.

4.6 Appendix 4.A: Equivalent between Max-min and Min-Max Problems

Lemma 4.2:

$$\begin{aligned} & \min_{\substack{(\mathbf{R}_T,\mathbf{R}_J)\in\Omega_r \\ (\mathbf{E}_T,\mathbf{E}_J)\in\Omega_e}} \frac{\mathrm{Tr}\left(\mathbf{R}_T\mathbf{Q}_T\right)}{\mathrm{Tr}\left(\mathbf{E}_T\mathbf{Q}_T\right)} \frac{\mathrm{Tr}\left(\mathbf{E}_J\mathbf{Q}_J\right)+N_0}{\mathrm{Tr}\left(\mathbf{R}_J\mathbf{Q}_J\right)+N_0} \\ = & \min_{\substack{(\mathbf{R}_T,\mathbf{R}_J)\in\mathrm{conv}(\Omega_r) \\ (\mathbf{E}_T,\mathbf{E}_J)\in\mathrm{conv}(\Omega_e)}} \frac{\mathrm{Tr}\left(\mathbf{R}_T\mathbf{Q}_T\right)}{\mathrm{Tr}\left(\mathbf{E}_T\mathbf{Q}_T\right)} \frac{\mathrm{Tr}\left(\mathbf{E}_J\mathbf{Q}_J\right)+N_0}{\mathrm{Tr}\left(\mathbf{R}_J\mathbf{Q}_J\right)+N_0}, \forall \mathbf{Q}_T, \mathbf{Q}_J. \end{aligned} \tag{4.36}$$

Proof:

On the one hand, since $\Omega_r \subseteq \mathrm{conv}(\Omega_r)$ and $\Omega_e \subseteq \mathrm{conv}(\Omega_e)$, the left-hand-side of (4.36) will be greater than the right-hand-side of (4.36).

On the other hand, $\forall\,(\mathbf{R}_{0,T}, \mathbf{R}_{0,J}) \in \mathrm{conv}(\Omega_r)$, there must exist a $(\mathbf{R}_T, \mathbf{R}_J) \in \Omega_r$ such that $\frac{\mathrm{Tr}\left(\mathbf{R}_{i,T}\mathbf{Q}_T\right)}{\mathrm{Tr}\left(\mathbf{R}_{i,J}\mathbf{Q}_J\right)+N_0} \leq \frac{\mathrm{Tr}\left(\mathbf{R}_{0,T}\mathbf{Q}_T\right)}{\mathrm{Tr}\left(\mathbf{R}_{0,J}\mathbf{Q}_J\right)+N_0}$. The reason is as follows. Suppose $(\mathbf{R}_{0,T}, \mathbf{R}_{0,J})$ can be decomposed as a convex combination of $\{(\mathbf{R}_{i,T}, \mathbf{R}_{i,J})\}_{i=1}^{N} \subseteq \Omega_r$ with the coefficients $\{\nu_i\}_{i=1}^{N}$:

$$\left(\begin{array}{l} \mathbf{R}_{0,T} = \sum \nu_i \mathbf{R}_{i,T} \\ \mathbf{R}_{0,J} = \sum \nu_i \mathbf{R}_{i,J} \end{array} \right). \tag{4.37}$$

Suppose $\frac{\mathrm{Tr}(\mathbf{R}_{0,T}\mathbf{Q}_T)}{\mathrm{Tr}(\mathbf{R}_{0,J}\mathbf{Q}_J)+N_0} = K$, and substituting the above into $\mathrm{Tr}(\mathbf{R}_{0,T}\mathbf{Q}_T) - K\left(\mathrm{Tr}\left(\mathbf{R}_{0,J}\mathbf{Q}_J\right) + N_0\right) = 0$ yields

$$\sum_i \left[\mathrm{Tr}\left(\mathbf{R}_{i,T}\mathbf{Q}_T\right) - K\left(\mathrm{Tr}\left(\mathbf{R}_{i,J}\mathbf{Q}_J\right) + N_0\right)\right] = 0. \tag{4.38}$$

By the above equality, there must exist at least one i such that

$$\mathrm{Tr}\left(\mathbf{R}_{i,T}\mathbf{Q}_T\right) - K\left(\mathrm{Tr}\left(\mathbf{R}_{i,J}\mathbf{Q}_J\right) + N_0\right) \leq 0, \tag{4.39}$$

and thus

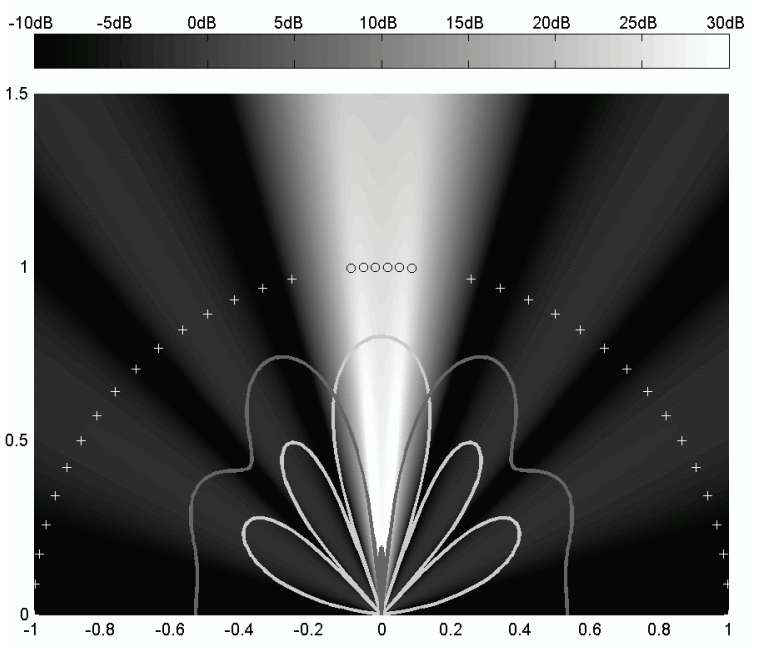
$$\begin{aligned} \forall\left(\mathbf{R}_{0,T}, \mathbf{R}_{0,J}\right) &\in \mathrm{conv}\left(\Omega_r\right), \text{and } \forall\mathbf{Q}_T\forall\mathbf{Q}_J, \\ \exists\left(\mathbf{R}_{i,T}, \mathbf{R}_{i,J}\right) &\in \Omega_r \text{ such that} \\ \frac{\mathrm{Tr}\left(\mathbf{R}_{i,T}\mathbf{Q}_T\right)}{\mathrm{Tr}\left(\mathbf{R}_{i,J}\mathbf{Q}_J\right) + N_0} &\leq \frac{\mathrm{Tr}\left(\mathbf{R}_{0,T}\mathbf{Q}_T\right)}{\mathrm{Tr}\left(\mathbf{R}_{0,J}\mathbf{Q}_J\right) + N_0}. \end{aligned} \tag{4.40}$$

For the similar reason,

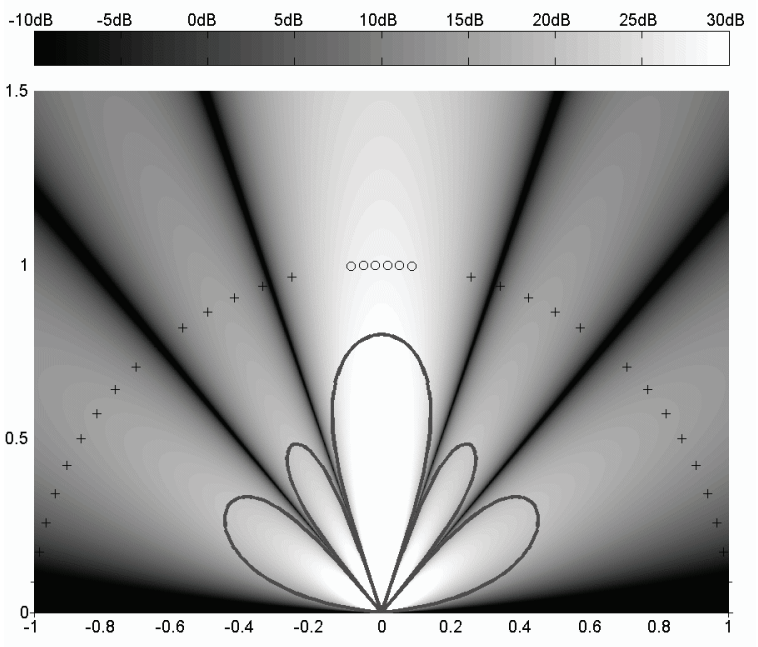
$$\begin{aligned} \forall\left(\mathbf{E}_{0,T}, \mathbf{E}_{0,J}\right) &\in \mathrm{conv}\left(\Omega_e\right), \text{and } \forall\mathbf{Q}_T\forall\mathbf{Q}_J, \\ \exists\left(\mathbf{E}_{j,T}, \mathbf{E}_{j,J}\right) &\in \Omega_e \text{ such that} \\ \frac{\mathrm{Tr}\left(\mathbf{E}_{j,J}\mathbf{Q}_J\right) + N_0}{\mathrm{Tr}\left(\mathbf{E}_{j,T}\mathbf{Q}_T\right)} &\leq \frac{\mathrm{Tr}\left(\mathbf{E}_{0,J}\mathbf{Q}_J\right) + N_0}{\mathrm{Tr}\left(\mathbf{E}_{0,T}\mathbf{Q}_T\right)}. \end{aligned} \tag{4.41}$$

From (4.40) and (4.41), we can conclude the left-hand-side of (4.36) will be smaller than the right-hand-side of (4.36).

Therefore, the left-hand-side of (4.36) will be equal to the right-hand-side of (4.36). ■



(a) the cooperative jamming scheme



(b) without artificial noise

Figure 4.2: Gray-scale images show the SINR at different locations yielded by a 6-antenna transmitter, under a) the proposed cooperative jamming scheme and b) without jamming noise. The transmit power for the both cases is 20dB. The Rx is assumed to be located at distance $d_R = 1$ and direction $\theta_R \in [-5°, 5°]$, and its location samples are plotted as "o". The Ev is assumed to be at distance $d_E = 1$ and direction $\theta_E \in [-90°, -15°] \cup [15°, 90°]$, and its location samples are plotted as "+". In (a), the beampattern of the message signal is plotted as the bright curve, while that of the jamming signal the dark curve. In (b), the beampattern of the message signal is plotted as the dark curve.

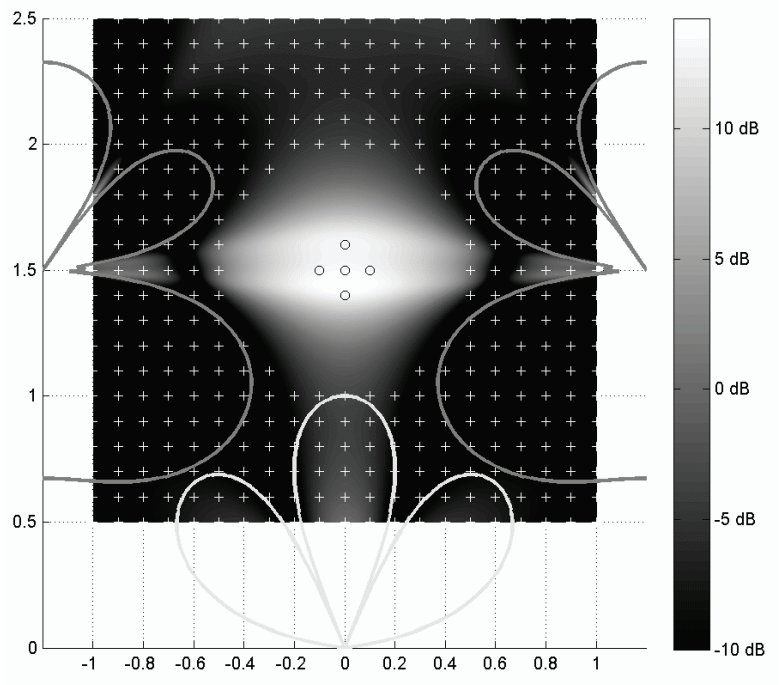


Figure 4.3: Gray-scale image shows the SINR at different locations yielded by the joint efforts of one Tx and two Jm's. The Rx is assumed to be in the center region marked by "o", and the Ev may be at the rest region marked by "+". The beampattern of the Tx is plotted as the bright curve, while that of the Jm the dark curve.

Chapter 5

DISTRIBUTED JAMMING FOR SECURE COMMUNICATION NETWORKS

5.1 Motivation

Recently, secure wireless communications at the physical layer is intriguing renewed interests among research area. Many research areas have been gaining renewed interests by their applications on the physical layer secrecy. Geol and Negi [18] proposed artificial noise enhancement to improve security. The secrecy of communication between the legitimate transmitter-receiver pair is improved by having external helpers simultaneously send independent signals to confuse the eavesdropper. Haenggi [20] and Pinto *et al.* [45] study the in-degree and out-degree distributions under the security constraints. The independence of fading channels is exploited to generate noise to suppress eavesdroppers' channels taking advantage of cooperative schemes [44]. It is shown in [3] that theoretic information secrecy can be achieved by fading alone if channel state information (CSI) is available.

Many research focuses on distinctive techniques to enhance the security of a single link. Security is more expensive and difficult to achieve in large distributed networks, unlike point-to-point communications. A few work has been carried out to study secrecy impacts on network performance, especially in large scale wireless networks. Vasudevan *et al.* [62] study the secrecy capacity issue in a large-scale network. The impact of secrecy guard zone or mobility on capacity is investigated by Koyluoglu *et al.* [27], Zhou *et al.* [70] and reference within. All these works are based on the assumption of either the known CSI information or some pre-known location information of eavesdroppers which can be used by transmitters to differentiate receivers' channels from eavesdroppers'. However, since in real-world scenarios it is difficult to obtain such information, it is of significant interest to study secrecy improvement, if both the CSI and location information are unknown to legitimate nodes.

We study networks having both legitimate and eavesdropper nodes whose locations follow independent homogeneous Poisson point processes (PPPs). The locations and CSI of eavesdropper are assumed completely unknown, and jammers' location are also unknown since we assume they operate in a fairly decentralized manner. We propose a transmission/jamming protocol modified from the RTS/CTS protocol. During packet transmission, the nearby jammers within a certain range of the receiver will broadcast artificial noise that only harms eavesdroppers' received signal. The performance of the network is assess by a MAC-level metric called *secure throughput*. A closed-form expression of the secure throughput is derived and to allow us to numerically optimize the design parameters. Note that the major difference between our work and the related works such as [63] and [71], is the effective usage of multi-antenna systems. The additional degree of freedom of multi-antenna systems is used to degrade eavesdropping ability without harming the legitimate receiver.

5.2 System Models and Jamming Protocol

Consider an ad hoc network of both legitimate and eavesdropper nodes over a large two-dimensional area. We model the locations of all legitimate Tx and jammers as a homogeneous PPP with density λ_t and λ_j, respectively. This assumption of Poisson spatial distribution is suitable for nodes having substantial mobility. Each Tx has an intended receiver at a distance d_{tr} in a random direction. In addition, the locations of the Eves are also drawn according to another homogeneous PPP with density λ_e. Furthermore, we assume that the Eves do not collude and, hence, must decode the messages individually.

We assume that Tx, Rx and jammers are drawn from the pool of legitimate nodes and are equipped with N_l antennas. Eves are equipped with N_e antennas. A single stream of data is transmitted by each Tx, and let $\mathbf{c}_{t_i}$ and s_i denote the beamforming vector and the scalar signal from the i-th Tx. At the same time of transmission, each jammer broadcasts a single stream of artificial noise, and let $\mathbf{c}_j$ and z_j denote the beamforming vector and the artificial noise from the j-th jammer. The signal received at the legitimate receiver and the

Table 5.1: A jamming protocol based on RTS/CTS

	Operation at communicating nodes
1)	A Tx sends a RTS requesting transmission to a Rx. If available for communication, the Rx replies with a CTS.
2)	After successful RTS/CTS, the channel estimation is performed either at the Tx or Rx, and this information is feedback to the other end. The channel information is used to determine the Tx and Rx beamformers.
3)	The Rx then broadcasts a packet using the receive beamformer determined in Step 2, for surrounding jammers to estimate the channel and choose their artificial noise orthogonal to the receiver.
4)	The transmitter sends a data packet.
5)	If successfully received, the receiver sends back an ACK to the transmitter.
	Operation at jammers
1)	Upon reception of a RTS or CTS, the jammer is aware of the intent of transmission.
2)	A jammer, if inside the guard zone of the Rx, estimates the Rx's channel.
3)	Start jamming after either the notifying packet from the receiver is fully decoded or detected. If channel information can be estimated, the jammer will chose artificial noise orthogonal to the channel. Else if the jammer has no channel information, the jammer randomly broadcast artificial noise.
3)	Stop jamming after a packet transmission duration.

k-th eavesdropper are modeled as, respectively,

$$\begin{aligned}
\mathbf{y}_R &= d_{t_0r}^{-\alpha/2}\mathbf{H}_{t_0r}\cdot\mathbf{c}_{t_0}s_0 + \sum_{i\neq 0} d_{t_ir}^{-\alpha/2}\mathbf{H}_{t_ir}\cdot\mathbf{c}_{t_i}s_i \\
&\quad + \sum_j d_{jr}^{-\alpha/2}\mathbf{H}_{jr}\cdot\mathbf{c}_j z_j + \mathbf{n}_r, \\
\mathbf{y}_{E_k} &= d_{t_0k}^{-\alpha/2}\mathbf{H}_{t_0k}\cdot\mathbf{c}_{t_0}s_0 + \sum_{i\neq 0} d_{t_ik}^{-\alpha/2}\mathbf{H}_{t_ik}\cdot\mathbf{c}_{t_i}s_i \\
&\quad + \sum_j d_{jk}^{-\alpha/2}\mathbf{H}_{jk}\cdot\mathbf{c}_j z_j + \mathbf{n}_k,
\end{aligned} \tag{5.1}$$

where subscripts $\{t_0, t_1, \cdots\}$, r, $\{j = 1, 2, \cdots\}$ and $\{k = 1, 2, \cdots\}$ represent the Tx's, Rx, jammers and eavesdroppers, respectively. To include geometric information, scaling components $d^{-\alpha/2}$ is used to model the pathloss effect, where d denotes distance and $\alpha > 2$ the pathloss exponent. We also assume the fading channel matrices $\mathbf{H}$ is independent of each other. Assuming Rayleigh fading environment, the elements of $\mathbf{H}$ is an independent zero-mean complex Gaussian random variable. The noise received by the receiver and eavesdroppers $\mathbf{n}_r$ and $\mathbf{n}_k, k = 1, \cdots, m$ are complex Gaussian vector with variance $\sigma_r^2\mathbf{I}$ and $\sigma_e^2\mathbf{I}$, respectively.

During the CTS phase, the Rx will reply with pilot symbols for channel estimation at the surrounding jammers. We assume that the jammers within a guard zone (a circular region $\mathcal{B}_b$ of radius b) around the receiver can successfully decode pilot symbols and perform channel estimation. The size of the circle $\mathcal{B}_b$ is determined by the signal strength of the CTS packet. After estimating the channel information, the surrounding jammers can choose their artificial noise to be zero-forcing to the Rx's. In other words, the receiver are only affected by the artificial noise from the jammer outside $\mathcal{B}_b$. If a jammer is in multiple Rx's guard zone, we assume that a jammer has enough number of antennas to be zero-forcing to all the Rx's channel. Let $\mathbf{w}_R$ and $\mathbf{w}_{E_k}$ denote the receive beamformer at the receiver and eavesdropper respectively. After applying the above assignments of the zero-forcing

jamming noise, (5.1) can be rewritten as

$$\begin{aligned} y_R &= \mathbf{w}_R^H \begin{pmatrix} d_{t_0r}^{-\alpha/2}\mathbf{h}_{t_0r}s_0 + \sum_{i\neq 0} d_{t_ir}^{-\alpha/2}\mathbf{h}_{t_ir}s_i \\ + \sum_{j\notin\mathcal{B}_b} d_{jr}^{-\alpha/2}\mathbf{h}_{jr}z_j + \mathbf{n}_r \end{pmatrix}, \\ y_{E_k} &= \mathbf{w}_{E_k}^H \begin{pmatrix} d_{t_0k}^{-\alpha/2}\mathbf{h}_{t_0k}s_0 + \sum_{i\neq 0} d_{t_ik}^{-\alpha/2}\mathbf{h}_{t_ik}s_i \\ + \sum_{j} d_{jk}^{-\alpha/2}\mathbf{h}_{jk}z_j + \mathbf{n}_k \end{pmatrix}. \end{aligned} \tag{5.2}$$

The effective MISO channels are $\mathbf{h}_{t_0r} = \mathbf{H}_{t_0r} \cdot \mathbf{c}_{t_0}$and so on. The effective channels $\mathbf{h}_{t_0r}$ etc. are still Gaussian random vectors, because a linear combination of rows of $\mathbf{H}$ is still Gaussian.

Assuming the receiver and the eavesdroppers use optimum combining (in other words, MMSE) to maximize their received SINR, the resulting SINRs can be expressed as the following well-known form

$$\begin{aligned} \mathrm{SINR}_R &= d_{t_0r}^{-\alpha} P_t \cdot \mathbf{h}_{t_0r}^H \begin{pmatrix} P_t \sum_{i\neq 0} d_{t_ir}^{-\alpha}\mathbf{h}_{t_ir}\mathbf{h}_{t_ir}^H + \\ P_j \sum_{j\notin\mathcal{B}_b} d_{jr}^{-\alpha}\mathbf{h}_{jr}\mathbf{h}_{jr}^H + \sigma_r^2\mathbf{I} \end{pmatrix}^{-1} \mathbf{h}_{t_0r}, \\ \mathrm{SINR}_{E_k} &= d_{t_0k}^{-\alpha/2} P_t \cdot \mathbf{h}_{t_0k}^H \begin{pmatrix} P_t \sum_{i\neq 0} d_{t_ik}^{-\alpha}\mathbf{h}_{t_ik}\mathbf{h}_{t_ik}^H + \\ P_j \sum_{j} d_{jk}^{-\alpha}\mathbf{h}_{jk}\mathbf{h}_{jk}^H + \sigma_e^2\mathbf{I} \end{pmatrix}^{-1} \mathbf{h}_{t_0k}. \end{aligned} \tag{5.3}$$

We will consider interference limited scenario where interference dominantes the SINR outages, so $\sigma_r^2\mathbf{I}$ and $\sigma_e^2\mathbf{I}$ are omitted in the above expressions.

5.3 Secure Throughput and Main Results

One of the link-level performance metrics of secure communications is secrecy capacity. The *secrecy capacity* of a wireless link is the maximum transmission rate at which the source can communicate with the receiver without the eavesdropper being able to acquire any information. For practical scenarios, the recent work [62] defines *per-node secure throughput* as a measure of secrecy that relies on simple link-layer parameters, much like the throughput of a link (defined as the probability of successful transmission) is a link-layer alternative to the channel capacity (defined as the maximum achievable rate). A successful secure transmission is the event that the transmitted message is successfully received by the legitimate Rx, and unsuccessfully received by every Eves. This definition leads to the *network-level*

secure throughput which is the successful secure transmission that happens in a unit area,

$$\begin{aligned} & \text{Secure Throughput } T \\ = \; & \lambda_t \cdot \Pr\{\text{Rx can decode}\} \cdot \Pr\{\text{all Eves cannot decode}\} \\ = \; & \lambda_t \cdot \Pr\{\,\text{SINR}_R > v |\, d_{t_0 r}\} \cdot \Pr\left\{\bigcup_k \{\text{SINR}_{E_k} < v\}\right\}. \end{aligned}$$

Here we only consider a fixed Tx-Rx distance $d_{t_0 r}$. Extension to the case of random $d_{t_0 r}$ can be made by taking expectation of the above equation, if $d_{t_0 r}$ is assumed to a random variable.

In the following, we derive the successful transmission probability and outage probability for all Eves.

5.3.1 Successful transmission probability

Given the jamming protocol shown in Table I, a Rx will be interfered by other Tx's and jammers outside of the guard zone. The other interfering Tx's forms a PPP on the infinite 2-dim plane with the same density λ_t, conditional on the fixed location of the intended Tx. The jammer outside of the guard zone forms another PPP with density λ_j on the region $\mathbb{R}^2/\mathcal{B}_b$. Following the SINR outage of a MMSE receiver under multiple interfering PPPs given in the next chapter, the successful transmission of a MMSE Rx is expressed as

$$\begin{aligned} & \Pr\{\,\text{SINR}_R > v |\;\; d_{t_0 r}\} \\ = \; & \sum_{i=0}^{N_l - 1} \frac{\left(\Omega_{\text{Tx}} + \Omega_{\text{Jam}} + \sigma^2 v\right)^i}{i!} \cdot \exp\left(-\Omega_{\text{Tx}} - \Omega_{\text{Jam}} - \sigma^2 v\right) \qquad (5.4) \\ = \; & \sum_{i=0}^{N_l - 1} \frac{\left(\lambda_t \Delta d_{t_0 r}^2 v^{2/\alpha} + \lambda_j \Delta' \left(d_{t_0 r}^{\alpha} \frac{P_j}{P_t} v\right)^{2/\alpha} + \sigma^2 v\right)^i}{i!} \cdot \\ & \times \exp\left(-\lambda_t \Delta d_{t_0 r}^2 v^{2/\alpha} - \lambda_j \Delta' \left(d_{t_0 r}^{\alpha} \frac{P_j}{P_t} v\right)^{2/\alpha} - \sigma^2 v\right) \qquad (5.5) \end{aligned}$$

The other parameters are transmitter density λ_t, jammer density λ_j, transmit power P_t, jamming power λ_t, and eavesdropper antenna number N_e. The *effective interference* from the PPP of interfering Tx's is

$$\Omega_{\mathrm{Tx}} = \lambda_t \left(d_{t_0 r}^2 v^{2/\alpha} \right) \Delta, \tag{5.6}$$

$$\text{where } \Delta = \frac{2\pi}{\alpha} \Gamma\left(\frac{2}{\alpha}\right) \Gamma\left(1 - \frac{2}{\alpha}\right), \tag{5.7}$$

and the *effective interference* from the PPP of jammers outside the guard zone is

$$\begin{aligned}
\Omega_{\mathrm{Jam}} &= \lambda_i \iint_{\mathbb{R}^2/\mathcal{B}_b} \frac{|X|^{-\alpha} \left(d_{t_0 r}^{\alpha} \frac{P_j}{P_t} v \right)}{1 + |X|^{-\alpha} \left(d_{t_0 r}^{\alpha} \frac{P_j}{P_t} v \right)} \mathrm{d}X \\
&= \lambda \left(d_{t_0 r}^{\alpha} \frac{P_j}{P_t} v \right)^{2/\alpha} \cdot \frac{2\pi}{\alpha} B\left(\frac{\left(d_{t_0 r}^{\alpha} \frac{P_j}{P_t} v \right) b^{-\alpha}}{1 + \left(d_{t_0 r}^{\alpha} \frac{P_j}{P_t} v \right) b^{-\alpha}}; 1 - \frac{2}{\alpha}, \frac{2}{\alpha} \right) \qquad (5.8) \\
&= \lambda \left(d_{t_0 r}^{\alpha} \frac{P_j}{P_t} v \right)^{2/\alpha} \Delta', \qquad (5.9) \\
\text{where } \Delta' &= \frac{2\pi}{\alpha} B\left(\frac{\left(d_{t_0 r}^{\alpha} \frac{P_j}{P_t} v \right) b^{-\alpha}}{1 + \left(d_{t_0 r}^{\alpha} \frac{P_j}{P_t} v \right) b^{-\alpha}} \middle| 1 - \frac{2}{\alpha}, \frac{2}{\alpha} \right). \qquad (5.10)
\end{aligned}$$

where b denotes radius of the guard zone, and $B\left(x \middle| z, w\right)$ denotes incomplete Beta function with parameters (z, w).

5.3.2 Outage probability for all Eves

Next we derive outage probability of one Eve at fixed distance $d_{t_0 k}$ away from the Tx and that of all Eves on the infinite plane. A Eve will be interfered by other Tx's and jammers on the whole plane. The SINR outage of a MMSE Eve at distance $d_{t_0 k}$ is expressed as

$$\begin{aligned}
&\Pr\left\{ \mathrm{SINR}_{E_k} < v \middle| \, d_{t_0 k} \right\} \\
= \; & 1 - \sum_{i=0}^{N_e - 1} \frac{\left(\lambda_t \Delta d_{t_0 k}^2 v^{2/\alpha} + \lambda_j \Delta \left(d_{t_0 k}^{2/\alpha} \frac{P_j}{P_t} v \right)^{2/\alpha} + \sigma^2 v \right)^i}{i!} \cdot \\
& \times \exp\left(-\lambda_t \Delta d_{t_0 k}^2 v^{2/\alpha} - \lambda_j \Delta \left(d_{t_0 k}^{2/\alpha} \frac{P_j}{P_t} v \right)^{2/\alpha} - \sigma^2 v \right), \qquad (5.11)
\end{aligned}$$

where $\lambda_t \Delta d_{t_0 k}^2 v^{2/\alpha}$ represents the effective interference from other unwanted Tx's and $\lambda_j \Delta \left(d_{t_0 k}^{2/\alpha} \frac{P_j}{P_t} v \right)^{2/\alpha}$ the interference from jammers. To ensure that none Eve on the 2-dim infinite plane can

decode the transmitted message, we consider Poisson distributed Eves on the entire plane and find the outage probability of all Eves:

$$\begin{aligned} & \Pr\left\{\bigcup_k \{\mathrm{SINR}_{E_k} < v\}\right\} \\ = \quad & \exp\left(-\frac{\pi\lambda_e N_e}{\Delta\left(\lambda_t + \lambda_j\left(\frac{P_j}{P_t}\right)^{2/\alpha}\right)v^{2/\alpha}}\right), \end{aligned} \tag{5.12}$$

where λ_e denotes eavesdropper density. The detailed derivation from (5.11) to (5.12) can be found in Appendix 5.A.

5.4 Numerical Results

A number of numerical results are plotted below to illustrate the impact of Tx/Rx, jammer and eavesdropper densities, as well as that of the zero-forcing range (guard zone) on the secure throughput.

Fig. 5.1 shows how the secure throughput varies as Tx/Rx pairs density λ_t increases. The effect of λ_t on the secure throughput is similar to the conventional throughput without secure consideration [64]. When λ_t is small, the throughput is limited by the number of transmission happens per unit area. When λ_t is large, the throughput is limited by the excessive interference caused by other Tx's.

In Fig. 5.2 the effect of jammers density λ_j is plotted. When λ_j is small, the secure throughput increase as λ_j increases. This is because that the increasing jamming noise helps block eavesdropping. When λ_j is large, too much jamming noise decreases the successful transmission probability of the legitimate nodes so the throughput also decreases.

The effect of Eves density λ_e is shown in Fig. 5.3. It is straightforward that the secure throughput drops as λ_e increases.

Finally, the effect of the guard zone can be seen in the figures. The guard zone plays an important role in the performance, because the total interference to a Rx is dominated by a few nearest interferers. However the size of the guard zone is limited by the power of channel estimation packet, and only nearby jammers are able to estimate channel. The size is also limited by the number of antennas of jammers, because a jammer inside in multiple

Rxs' guard zone might not have enough degree of freedoms for the artificial noise to be zero-forcing to all Rx's.

A number of numerical results are also plotted below to illustrate the impact of transmitter, jammer and eavesdropper densities, as well as that of the zero-forcing range on the secure throughput.

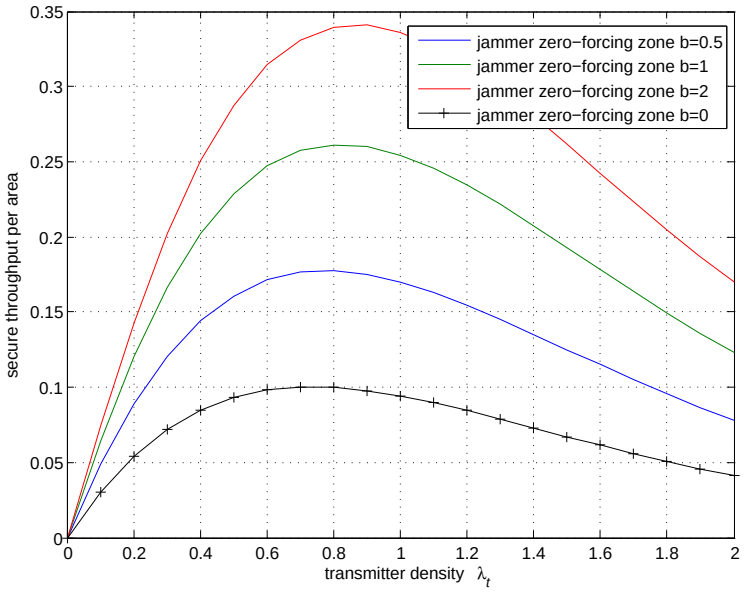


Figure 5.1: The secure throughput versus density of legitimate transmitters λ_t. The other network parameters are densities $\lambda_j = 1\text{m}^{-2}$, $\lambda_e = 0.2\text{m}^{-2}$, transmit power $P_t = P_j = 1$, and number of antennas $N_l = N_e = 2$.

5.5 Conclusion

We have studied secure communication networks where both the locations and the channels of eavesdroppers are unknown. We proposed a distributed jamming protocol for secure communication, in which jammers inside a Rx's guard zone will broadcast artificial noise that only harms eavesdroppers. Under the assumption of Poisson spatial distributions, we have derived the successful transmission probability of a MMSE Rx and outage probability of all Poisson distributed eavesdroppers. A secure throughput is defined as secure transmission

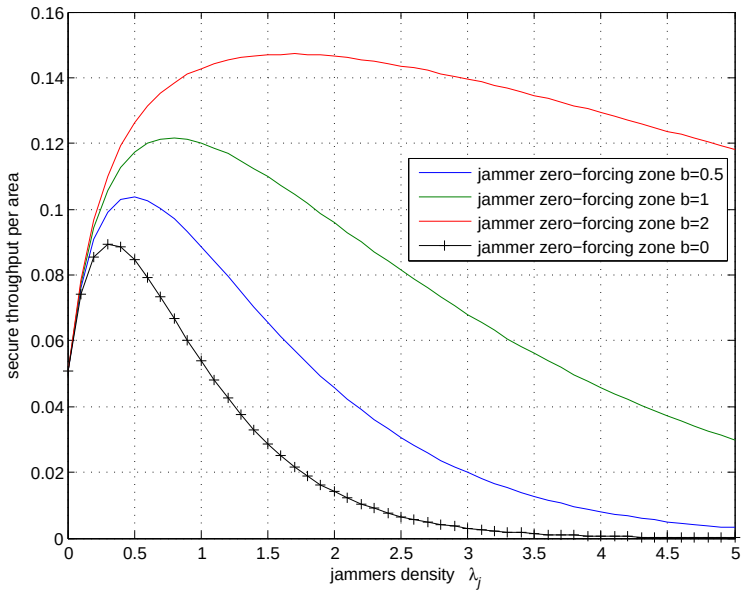


Figure 5.2: The secure throughput versus density of jammers λ_j. The other network parameters are densities $\lambda_t = 0.1\text{m}^{-2}$, $\lambda_e = 0.2\text{m}^{-2}$, transmit power $P_t = P_j = 1$, and number of antennas $N_l = N_e = 2$.

happening per unit area, and is expressed in closed form in terms of parameters such as densities, transmit power, jamming power etc. Numerical results show the effect of densities and guard zones on the secure throughput. Insights for network design can be obtained from the closed-form expression or the numerical results.

5.6 Appendix 5.A: Derivation of outage probability of all Eves

Considering a Tx located at the center of a circular area of radius r, the number of Eves in the area is a Poisson random variable:

$$\Pr\left[M_e = m\right] = \frac{\left(\lambda_e \pi r^2\right)^m}{m!} \exp\left(-\lambda_e \pi r^2\right) \tag{5.13}$$

The SINR outage of one Eve at a distance $d_{t_o k}$ away from the Tx is given by (5.3). Next we derive the outage probability of all SINRs of all the Eves.

The outage probability of all the Eves is

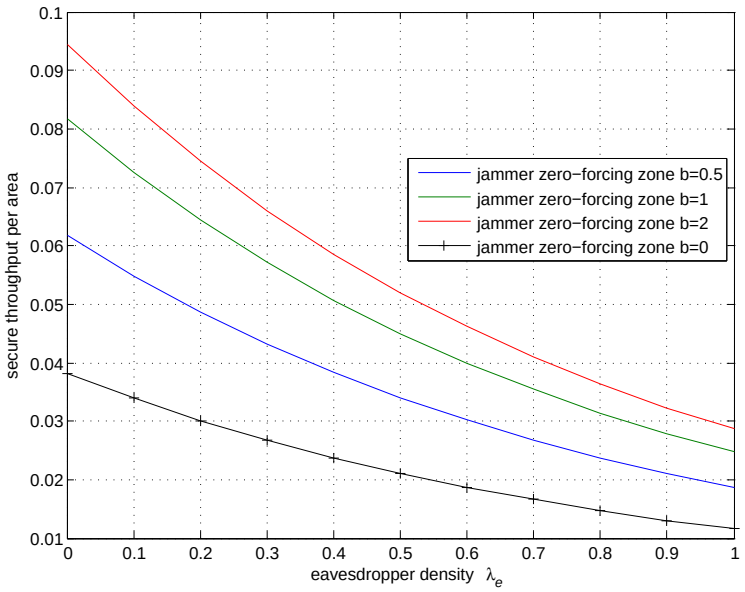


Figure 5.3: The secure throughput versus density of eavesdroppers λ_e. The other network parameters are densities $\lambda_t = 0.1\text{m}^{-2}$, $\lambda_j = 1\text{m}^{-2}$, transmit power $P_t = P_j = 1$, and number of antennas $N_l = N_e = 2$.

$$\begin{aligned} & \Pr\left[\bigcup_k \{\text{SINR}_{E_k} < v\}\right] \\ = & \sum_{k=0}^{\infty} \Pr\left[M_e = m\right] \cdot \left\{E_{d_{t_0k}}\left[\Pr\left\{\text{SINR}_{E_k} < v \middle| d_{t_0k}\right\}\right]\right\}^m \end{aligned}$$

where the above equation follows from that each Eve is distributed indepedently given the total number of Eves. Each Eve is independently in the 2-dim circular area, and thus their squared distances obey uniform distribution: $d_{t_0k}^2 \sim U\left[0, r^2\right]$. The expected outage probability of one Eve is

$$
\begin{aligned}
& E_{d_{t_0k}}\left[\Pr\left\{\mathrm{SINR}_{E_k} < v \middle| d_{t_0k}\right\}\right] \\
= & \int_0^{r^2} \Pr\left\{\mathrm{SINR}_{E_k} < v \middle| d_{t_0k}\right\} f\left(d_{t_0k}^2 = t^2\right)\, \mathrm{d}t \\
= & \int_0^{r^2} \Pr\left\{\mathrm{SINR}_{E_k} < v \middle| t\right\} \frac{1}{t^2}\, \mathrm{d}t \\
= & 1 - \frac{1}{r^2} \frac{N_e}{\left(\lambda_t + \lambda_j \left(\frac{P_j}{P_t}\right)^{2/\alpha}\right) \Delta v^{2/\alpha}} + o\left(\frac{1}{r^2}\right). \qquad (5.14)
\end{aligned}
$$

Therefore, all Eves in an infinite 2-dim plane are in SINR outage with probability

$$
\begin{aligned}
& \Pr\left[\bigcup_k \{\mathrm{SINR}_{E_k} < v\}\right] \\
= & \sum_{k=0}^{\infty} \frac{\left(\lambda_e \pi r^2\right)^m}{m!} \exp\left(-\lambda_e \pi r^2\right) \\
& \cdot \left\{1 - \frac{1}{r^2} \frac{N_e}{\left(\lambda_t + \lambda_j \left(\frac{P_j}{P_t}\right)^{2/\alpha}\right) \Delta v^{2/\alpha}} + o\left(\frac{1}{r^2}\right)\right\}^m \\
\to & \exp\left(-\frac{\lambda_e \pi N_e}{\left(\lambda_t + \lambda_j \left(\frac{P_j}{P_t}\right)^{2/\alpha}\right) \Delta v^{2/\alpha}}\right), \text{as } r \to \infty. \qquad (5.15)
\end{aligned}
$$

Chapter 6

PERFORMANCE ANALYSIS OF MMSE RECEIVERS IN LARGE NETWORKS

In distributed multiple access networks, such as ad hoc networks, the mutual interference between nodes poses a fundamental limit on the throughput of peer-to-peer communication. Antenna arrays is a promising technique to improve the performance of wireless networks by increasing robustness through diversity, and data rates through spatial multiplexing, beamforming and interference mitigation. Multi-antenna systems employed in these networks depends heavily on propagation characteristics and spatial distribution of the interferers scattered in the network. Hence performance analysis of multi-antenna systems in spatially distributed networks have received significant attention in recent years.

6.1 Background and Related Work

For distributed random networks, the number and the locations of interferers are commonly characterized by a spatial node distribution. The Poisson point process (PPP) [54] is widely adopted in the literature to model spatial node positions over an infinite plane [65] [2]. For sensor networks , the PPP assumption is usually justified by claiming that sensor nodes are dropped from aircraft in large numbers; for mobile ad hoc networks , it may be argued that terminals move and transmit independently from each other. Besides the spatial distribution, inter-node channel modeling such as pathloss, multipath fading and shadowing also impacts interference statistics. Once the interference statistics are derived, system performance measures, such as the SINR outage probability, the average throughput per unit area or the error probability, can then be analyzed [65] –[21]. Given this spatial model, the link outage is described as the probability that the SINR of a representative receiver is below a certain threshold.

The performance of multi-antenna receiver under PPP interferers has been studied in several works. Lower and upper bounds on the outage probability for sectorized antenna,

maximal ratio combining and space time coding techniques is derived in [21]. Partial zero-forcing receiver was considered in [23] and it is possible to linearly increase the area spectral efficiency by simultaneously increasing the number of antennas and density of simultaneous transmissions. Ali *et. al.* [1] found the exact SINR outage for a MMSE receiver under PPP single-stream interferences. Louie *et. al.* [39] found the SINR outage of multi-antenna receiver with maximum-ratio-combining and zero-forcing combining, under PPP multi-stream interferers. In later works, spatial node distributions are considered non-homogeneous in order to model more realistic scenarios such as hot-spots. Interference modeling in non-homogenous single antenna systems have been studied in several works such as [12, 13] and references within. The performance of multi-antenna systems has also been studied in relatively fewer works. Interference-alignment in clustered wireless networks was considered in [61]. [22] considered multi-antenna systems in networks with Carrier-Sensing-Multiple-Access (CSMA) which induces correlation between actively transmitting nodes and [73] used an asymptotic analysis to analyze the spectral efficiency of non-homogenous networks with linear MMSE receivers.

In this chapter, we extend the outage analysis in [1] to that under more sophisticated Poisson spatial distributions such as multiple PPPs and Poisson clustered networks. Multiple PPPs arises when the network nodes can not be simply modeled as one PPP, e.g. coexistence of UWB and narrow-band nodes, coexistence of ZigBee and WiFi nodes, or a cognitive radio network where primary users form a PPP and secondary users another PPP. Clustered networks are often seen when the clustering is introduced by geographical factors such as mobile nodes clustered around a base station, or by some MAC protocols. Our contribution is summarized as follows.

1. Considering a L-antenna receiver surrounded by multiple PPPs of interferers, the outage probability is derived in a closed form. Specifically, the outage is expressed as a probability that a Gamma r.v. with shape parameter L and scale parameter 1 being smaller than an effective interference plus noise. Comparing this expression to that under a single PPP, a superposition property exhibits such that the net interference caused by the multiple PPPs is the sum of the interference caused each PPP

individually.

2. The superposition property is used to extend the outage analysis to Poisson clustered interferers. Cluster locations (parent locations) are distributed as a homogeneous PPP and each cluster consists of a Poisson number of i.i.d. children. The net interference of the whole clustered process is the sum of effective interference caused by each cluster, and can be treated as a shot-noise r.v. We prove that the shot-noise r.v. has a mean equal to the effective interference caused by a PPP with the same node density. In other words, the expected interference depends only on the node density. That the net interference being a r.v. is consistent with our intuition that by clustering the net interference depends on the parent locations and fluctuates from realization to realization, whereas PPP is a more uniform spatial distribution so that the effective interference of a PPP is a constant. This result reveals that any clustering process is beneficial than a PPP, which can be explained by that a receiver under opportunistically low interference has better outage than under constant interference. The more clustering, such as smaller number of clusters with larger number of children per each cluster or more compact children distribution, the better outage. Finally to facilitate simplified calculations, we approximate the shot-noise r.v. as a Gamma r.v. and then obtain an outage expression in the form of incomplete Beta function.

6.2 Spatial Distributions

6.2.1 Poisson Point Process (PPP)

A stationary Poisson point process (PPP) of density λ is is a random countable collection of points such that

- The number of points in any set $B \subset \mathcal{R}^2$ is a Poisson random variable with mean $\lambda|B|$.

- The number of points in disjoint sets are independent random variables.

An inhomogeneous PPP is defined in a similar manner as the stationary PPP, except that the number of points in a set B is a Poisson random variable with mean $\Lambda(B)$. A non-homogeneous PPP is modeled by a spatial density function which determines the probability of nodes occurring in a small region. Let $\Lambda(X)$ describe the spatial density function of the non-homogeneous PPP. For a region $\mathcal{R}$, the number of nodes is a Poisson random variable with mean $\mu = \iint_{\mathcal{R}} \Lambda(X)\,\mathrm{d}X$. Each node is distributed independently and the probability of occurrence in a small region is proportion to $\Lambda(X)$.

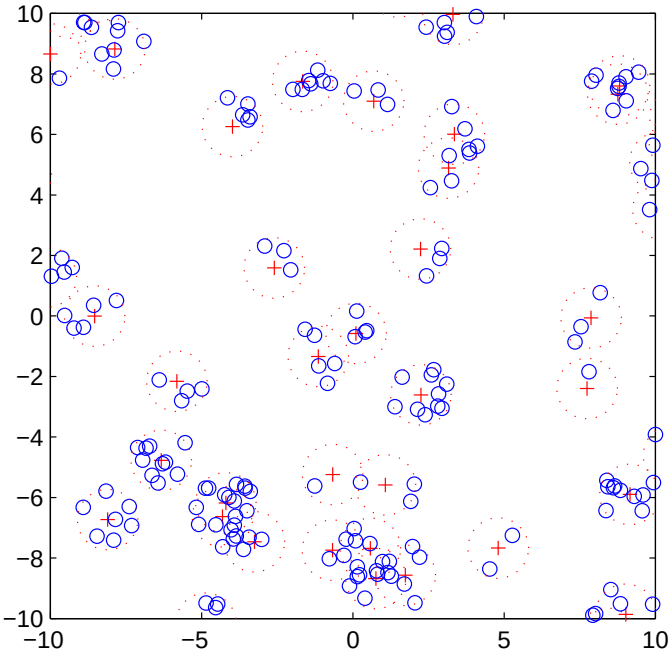
6.2.2 Poisson Cluster Process (PCP)

The assumption of homogeneous Poisson point process for the node distribution is common and analytically convenient. This assumption may be the case for certain networks, such as sensor networks where sensor nodes are dropped from aircraft in large numbers and mobile ad hoc networks where terminals move independently from each other. In many other cases, the node distribution is not completely spatially random but clustered. For example, the communicating nodes inside a building or groups of nodes moving in a coordinated fashion tends to be clustered. On the other hand, some MAC protocols may artificially induce the clustering. As shown in Fig. 6.1, a cluster process can exhibit a different spatial characteristic than a homogeneous PPP does.

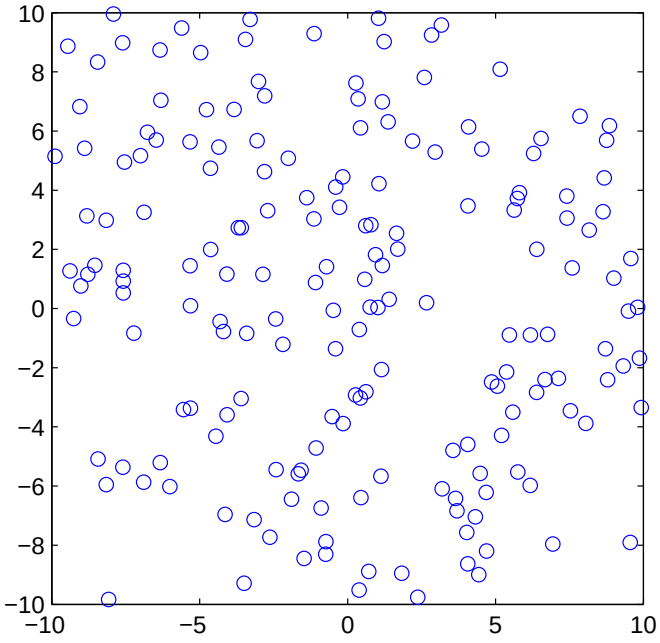
Neyman-Scott cluster processes [54]. Let $\{X_k\}$ be a Poisson point process on $\mathbb{R}^d$. Conditional on $\{X_k\}$, associate with each X_k is a finite Poisson point process $\mathcal{Z}_k$ of points 'centered' at X_k and assume that these processes are independent of one another. Then $\mathcal{Z} = \bigcup_{X_k \in \{X_k\}} \mathcal{Z}_k$ is a Neyman-Scott cluster process.

Assume that parent point process $\{X_k\}$ are homogeneously Poisson distributed with density λ_p, and $\bar{c}$ denotes the expected number of children per cluster. The children points are scattered independently and with identical distribution, around the parent point. The complete process is given by the union of all children points. Note that the parent points themselves are not included. The density of the cluster process is $\lambda = \lambda_p \bar{c}$. We also assume that the children scattering is isotropic, which makes the cluster process isotropic.

We will focus on two representative cases of the Neyman-Scott processes, namely Matern



(a) Matern Cluster Process



(b) Homogeneous PPP

Figure 6.1: (a) A realization of the Matern cluster process with parent density $\lambda_p = 0.1$, expected children number $\bar{c} = 5$ and radius $d_c = 1$. Parent points are plotted in red '+' and children in blue 'o' enclosed in dotted circles. (b) A realization of a homogeneous PPP with density $\lambda = 0.5$. Note that the two processes have the same density $\lambda_p \bar{c} = \lambda$.

cluster process and Thomas cluster process. For the Matern cluster process, the children are uniformly distributed around the parent within a circle of radius d_c. So the children density function at location Z is given by

$$\Lambda_{\text{Matern}}(Z - X_k) = \begin{cases} \bar{c}\frac{1}{\pi d_c^2}, & |Z - X_k| \leq d_c \\ 0, & \text{otherwise.} \end{cases} . \tag{6.1}$$

In the Thomas cluster process, each child is distributed by a 2-dim symmetric Gaussian distribution with covariance matrix $\sigma^2\mathbf{I}$. The density function is

$$\Lambda_{\text{Thomas}}(Z - X_k) = \bar{c}\frac{1}{2\pi\sigma^2}\exp\left(-\frac{(|Z - X_k|)^2}{2\sigma^2}\right). \tag{6.2}$$

6.3 System Model and Prior Results

In [14], the paper considers a complex-baseband communication system consisting of a L-antenna receiver, a desired source s_0 and several interfering sources $\{s_i\}_{i=1}^n$. Let P_0 denote the received power of the desired sources and $P_i, i = 1, \cdots, N$ the power of other sources. Let $\mathbf{n}$ denote an additive vector of Gaussian noise with mean zero and variance σ^2. The received signal is given by

$$\mathbf{y} = \sqrt{P_0}\mathbf{g}_0 s_0 + \sum_{i=1}^{n}\sqrt{P_i}\mathbf{g}_i s_i + \mathbf{n} \tag{6.3}$$

where $\mathbf{g}_0$ and $\{\mathbf{g}_i\}_{i=1}^n$ denote channels that are independent zero-mean unit-gain complex Gaussian random vectors. Assume that the receiver adjusts its combining weights according to MMSE criterion, i.e. optimum combining in the context of array processing, to maximize the resulting SINR. The SINR is given by the following well-known expression

$$\text{SINR} = P_0\mathbf{g}_0^H\left(\sum_{i=1}^{n}P_i\mathbf{g}_i\mathbf{g}_i^H + \sigma^2\mathbf{I}\right)^{-1}\mathbf{g}_0. \tag{6.4}$$

It is shown in [14] that SINR outage, the probability of the SINR below a threshold γ, is given by

$$\Pr\left[\frac{\text{SINR}}{P_0} < \gamma\right] = 1 - \frac{\sum_{i=1}^{L-1}a_i\gamma^i}{\exp(\sigma^2\gamma)(1 + P_1\gamma)\cdots(1 + P_n\gamma)}, \tag{6.5}$$

where a_i is the coefficient of the i-th order in the expansion of the denominator.

The later work [1] studies the outage probability under a homogeneous PPP of interferers. In a distributed network, the number and locations of the nodes are usually unknown to the receiver, but can be characterized as a homogeneous PPP for the simple case of random access strategy. In a planar network, in a closed region with area A, the number of transmitters is distributed according to the Poisson distribution with mean λA, where λ denotes density of the PPP. The locations of these nodes $\{X_i\}$ are uniformly distributed in the region.

Assume the receiver is located at the origin without loss of generality. The distance between the transmitter and the receiver is fixed at d_0, and those between the interferers and the receiver are $|X_i|$. Each node transmits with a single antenna and unit power. The channel is represented as a combination of path loss with an exponent $\alpha > 2$ and independent Rayleigh fading which is independent among antennas and nodes. The received signal vector can be represented by

$$\mathbf{y} = d_0^{-\alpha/2}\mathbf{g}_0 s_0 + \sum_{i=1}^{n} |X_i|^{-\alpha/2}\,\mathbf{g}_i s_i + \mathbf{n} \tag{6.6}$$

where the entries of $\mathbf{g}_0$ and $\mathbf{g}_i$ are independent identically distributed (i.i.d.) complex Gaussian random variables with mean zero and unit variance. The noise vector consists of complex Gaussian random variables with mean zero and variance σ^2. The resulting SINR for the MMSE receiver is given by

$$\text{SINR} = d_0^{-\alpha}\mathbf{g}_0^H \left(\sum_{i=1}^{n} |X_i|^{-\alpha}\,\mathbf{g}_i\mathbf{g}_i^H + \sigma^2\mathbf{I} \right)^{-1} \mathbf{g}_0. \tag{6.7}$$

Furthermore, we leave d_0 out of consideration and define normalized SINR as $\text{SINR}d_0^{\alpha}$.

The outage probability $F(\gamma) = \Pr\left[\text{SINR}d_0^{\alpha} < \gamma\right]$, assuming that interferers follow from a homogeneous PPP with density λ on an infinite plane, is given by [1]

$$F(\gamma) = 1 - \sum_{i=0}^{L-1} \frac{1}{i!} \left(\Omega(\gamma) + \sigma^2\gamma\right)^i \exp\left(-\Omega(\gamma) - \sigma^2\gamma\right) \tag{6.8}$$

where

$$\Omega(\gamma) = \lambda \iint_{\mathbb{R}^2} \frac{|X|^{-\alpha}\gamma}{1+|X|^{-\alpha}\gamma}\,\mathrm{d}x \tag{6.9}$$

$$= \lambda\gamma^{2/\alpha} \cdot \frac{2\pi}{\alpha}\Gamma\left(\frac{2}{\alpha}\right)\Gamma\left(1-\frac{2}{\alpha}\right). \tag{6.10}$$

Notice the equality that

$$1-\sum_{i=0}^{L-1}\frac{1}{i!}x^i\exp(-x) = 1-\int_x^\infty \frac{1}{L!}t^{L-1}\exp(-t)\ \mathrm{d}t \tag{6.11}$$

$$= 1-\int_x^\infty f_\Gamma(t;L,1)\ \mathrm{d}t \tag{6.12}$$

$$= \Pr\left[\Gamma_{(L,1)} < x\right] \tag{6.13}$$

where $\Gamma_{(L,1)}$ denotes a Gamma random variable with shape and scale parameters $(L,1)$, and $f_\Gamma(t;L,1)$ the probability density function (PDF) of the Gamma random variable. Consequently, (6.8) can be written as

$$F(\gamma) = \Pr\left[\Gamma_{(L,1)} < \Omega(\gamma) + \sigma^2\gamma\right]. \tag{6.14}$$

In the above equation, $\Gamma_{(L,1)}$ reflects the anti-interference ability of the receiver, and the more antennas the less outage; $\Omega(\gamma)$ can be viewed as *expectation of effective interference* exerted by the whole PPP.

6.4 Superposition Property for Multiple PPPs

In this section we extend the outage expression under a homogeneous PPP [1] to that under multiple PPPs.

Theorem 6.1: **Superposition property of multiple homogeneous PPPs**. Assume the interferers are union of K homogeneous PPPs on region $\mathcal{R}_i$ each with density $\lambda_i, i = 1,\cdots,K$. The SINR outage for a L-antenna MMSE receiver is given by

$$F(\gamma) = \Pr\left[\Gamma_{(L,1)} < \Omega_1(\gamma) + \cdots + \Omega_K(\gamma) + \sigma^2\gamma\right] \tag{6.15}$$

where the effective interference from the i-th PPP is

$$\Omega_i(\gamma) = \lambda_i \iint_{\mathcal{R}_i} \frac{|X|^{-\alpha}\gamma}{1+|X|^{-\alpha}\gamma} \mathrm{d}X, \quad i = 1, \cdots, K. \tag{6.16}$$

Additionally, if transmit power and channel shadowing are incorporated in model (6.6), i.e. a node in the i-th PPP transmits with i.i.d. random power P_i and its channel gain experiences i.i.d. random shadowing g_i, then $\Omega_i(\gamma)$ is modified accordingly as

$$\Omega_i(\gamma) = \lambda_i \iint_{\mathcal{R}_i} E_{g_i,P_i}\left\{\frac{g_i P_i |X|^{-\alpha}\gamma}{1+g_i P_i |X|^{-\alpha}\gamma}\right\} \mathrm{d}X, \quad i = 1, \cdots, K. \tag{6.17}$$

A proof is given in Appendix 6.A. This theorem states that the net effective interference caused by two or more PPPs is the sum of the effective interference caused by each PPP individually.

Next we focus on the superposition property for non-homogeneous PPP. Spatial node distributions in many systems may not be homogenous, such as in networks with hot-spots. Performance of single antenna systems under non-homogenous networks have been studied in several works. Multi-antenna in non-homogeneous networks have been studied in relatively fewer works [73].

A non-homogeneous PPP is modeled by a spatial density function which determines the probability of nodes occurring in a small region. Let $\Lambda(X)$ describe the spatial density function of the non-homogeneous PPP. For a region $\mathcal{R}$, the number of nodes is a Poisson random variable with mean $\mu = \iint_{\mathcal{R}} \Lambda(X)\,\mathrm{d}X$. Each node is distributed independently and the probability of occurrence in a small region is proportion to $\Lambda(X)$.

Corollary 6.1: **Superposition property of multiple non-homogeneous PPPs.** Assume the interferers are union of K non-homogeneous PPPs each with density function $\Lambda_i(X), i = 1, \cdots, K$ on region $\mathcal{R}_i, i = 1, \cdots, K$. The SINR outage for a L-antenna MMSE receiver is given by the same equation (6.15) with

$$\Omega_i(\gamma) = \iint_{\mathcal{R}_i} \Lambda_i(X) \frac{|X|^{-\alpha}\gamma}{1+|X|^{-\alpha}\gamma}\,\mathrm{d}X. \tag{6.18}$$

Proof: This corollary can be proved in a rigorous way similar to Appendix 6.A. Here we present a loose but simple proof by directly using Theorem 6.1.

A PPP on a large region, which can be divided into several small regions, can be viewed as a union of several PPPs on these small regions. As the segments get fine enough, a non-homogeneous PPP on the large region can be viewed as many fine segments of homogeneous PPP with their local fixed densities, which enables us to directly extend the outage results of homogeneous interferers to non-homogeneous interferers.

For simplicity, first consider the case of one non-homogeneous PPP with density $\Lambda(X)$ on region $\mathcal{R}$. Partition the region $\mathcal{R}$ into a large number of small regions denoted as $\mathcal{R} = \mathcal{R}_1 \cup \cdots \cup \mathcal{R}_N$. As the number of the regions increases and the area of each region decreases, the spatial node distribution on an infinitesimal region $\mathcal{R}_j$ can be viewed as a homogeneous PPP with a constant density λ_j since the value of $\Lambda(X)$ is almost constant on $\mathcal{R}_j$. Using Theorem 6.1, the outage is written in terms of a superposition of the N homogeneous PPPs:

$$F(\gamma) = \Pr\left[\Gamma_{(L,1)} < \Omega_1(\gamma) + \cdots + \Omega_N(\gamma) + \sigma^2\gamma\right] \tag{6.19}$$

where

$$\Omega_j(\gamma) = \Lambda_j \iint_{\mathcal{R}_j} \frac{|X|^{-\alpha}\gamma}{1+|X|^{-\alpha}\gamma} \mathrm{d}X, \quad j = 1, \cdots, N. \tag{6.20}$$

Because $\Lambda(X)$ on $\mathcal{R}_j$ equals the constant λ_j, the above equation can be rewritten as

$$\Omega_j(\gamma) = \iint_{\mathcal{R}_j} \Lambda(X) \frac{|X|^{-\alpha}\gamma}{1+|X|^{-\alpha}\gamma} \mathrm{d}X, \quad j = 1, \cdots, N. \tag{6.21}$$

Noticing that

$$\begin{aligned} \Omega(\gamma) &= \iint_{\mathcal{R}} \Lambda(X) \frac{|X|^{-\alpha}\gamma}{1+|X|^{-\alpha}\gamma} \mathrm{d}X & (6.22)\\ &= \Omega_1(\gamma) + \cdots + \Omega_N(\gamma), & (6.23) \end{aligned}$$

thus the outage can be rewritten as

$$F(\gamma) = \Pr\left[\Gamma_{(L,1)} < \Omega(\gamma) + \sigma^2\gamma\right]. \tag{6.24}$$

Second, for multiple layers of non-homogeneous PPPs, partition can be similarly applied to each PPP. Combining the partitions of each non-homogeneous PPP, it is then straightforward to complete the proof. ■

6.5 MMSE Receiver under Clustered Poisson Interferers

Each cluster consists of a Poisson random number of i.i.d. children interferers, and can be viewed as a layer of Poisson field. Given the number of the clusters and parent locations, from Theorem 6.1, the conditional outage of the SINR of a L-antenna receiver can be expressed in the form of

$$F(\gamma|K, X_1, \cdots, X_K) = \Pr\left[\Gamma_{(L,1)} < \sum_{k=1}^{K} \Omega\left(X_k, \gamma\right) + \sigma^2\gamma\right], \tag{6.25}$$

where

$$\Omega\left(X_k, \gamma\right) = \iint_{\mathbb{R}^2} \Lambda\left(Z - X_k\right) \frac{|Z|^{-\alpha}\gamma}{1 + |Z|^{-\alpha}\gamma} dZ \tag{6.26}$$

represents the effective interference yielded by the k-th cluster located at X_k. $\Omega\left(X_k, \gamma\right)$ can also be written as

$$\Omega\left(X_k, \gamma\right) = \bar{c}\tilde{\Omega}\left(X_k, \gamma\right) = \bar{c} \iint_{\mathbb{R}^2} f\left(Z - X_k\right) \frac{|Z|^{-\alpha}\gamma}{1 + |Z|^{-\alpha}\gamma} dZ \tag{6.27}$$

where $\tilde{\Omega}\left(X_k, \gamma\right)$ denotes normalized effective interference and $f\left(\cdot\right)$ is a PDF function describing children distribution. The calculation of $\Omega\left(X_k, \gamma\right)$ for the Matern and the Thomas processes can be found in Appendix 6.B.

To obtain the outage $F(\gamma)$, the only remaining in the above equation is the stochastic characteristics of $\sum_{k=1}^{K} \Omega\left(X_k, \gamma\right)$.

Definition 6.1: **Shot noise (SN) process and Laplace transform of a PPP SN** [54]. A SN process, a real-valued random process $\{\sum_h (x)\}$, is a functional of an underlying stationary point process $\{X_i\} \subset \mathbb{R}^d$:

$$\sum\nolimits_h (x) \equiv \sum_{i \in \{X_i\}} h\left(|X_i - x|\right), \tag{6.28}$$

where $h\left(\cdot\right)$ is a impulse response function. The SN random variable $\sum_h (o)$ for a 2-dim PPP with density λ, where o denotes the origin, has a Laplace transform

$$\mathcal{L}\left[\sum\nolimits_{h}(o)\right](s)=\exp\left\{-\lambda 2\pi\int_{0}^{\infty}\left(1-e^{-sh(r)}\right)r\ \mathrm{d}r\right\} \tag{6.29}$$

for all $s\in\mathbb{C}$ for which the integral exists.

Because the parent points follows a homogeneous PPP, by Definition 6.1, $\sum_{\Omega}\equiv\sum_{k=1}^{K}\Omega\left(X_k,\gamma\right)$ in (6.25) can be viewed as a SN random variable with impulse response function $\Omega\left(\cdot,\gamma\right)$. The Laplace transform of $\sum_{\Omega}$ is given by

$$\mathcal{L}\left[\sum\nolimits_{\Omega}\right](s)=\exp\left\{-\lambda_p 2\pi\int_{0}^{\infty}\left(1-e^{-s\Omega(r,\gamma)}\right)r\ \mathrm{d}r\right\}. \tag{6.30}$$

The Laplace transform of $\Gamma_{(L,1)}$ is known to be $\frac{1}{(1+s)^L}$. The PDF of $\left[\Gamma_{(L,1)}-\sum_{\Omega}\right]$ can be computed by inverse Laplace transform

$$\mathrm{PDF}(t)=\frac{1}{2\pi j}\int_{c-j\infty}^{c+j\infty}e^{st}\mathcal{L}\left[\Gamma_{(L,1)}-\sum\nolimits_{\Omega}\right](s)\ \mathrm{d}s \tag{6.31}$$

where the integration is in the complex plane, $j=\sqrt{-1}$ is the imaginary unit and c is an appropriate constant. The CDF of $\left[\Gamma_{(L,1)}-\sum_{\Omega}\right]$ is given by

$$\mathrm{CDF}(t)=\frac{1}{2\pi j}\int_{c-j\infty}^{c+j\infty}\frac{1}{s}e^{st}\mathcal{L}\left[\Gamma_{(L,1)}-\sum\nolimits_{\Omega}\right](s)\ \mathrm{d}s. \tag{6.32}$$

The Laplace transform of $\left[\Gamma_{(L,1)}-\sum_{\Omega}\right]$ can be written as

$$\begin{aligned}
&\mathcal{L}\left[\Gamma_{(L,1)}-\sum\nolimits_{\Omega}\right](s)\\
=\ & E\left[e^{s\left(\Gamma_{(L,1)}-\sum_{\Omega}\right)}\right] &(6.33)\\
=\ & E\left[e^{s\Gamma_{(L,1)}}\right]E\left[e^{-s\sum_{\Omega}}\right]\\
=\ & \frac{1}{(1+s)^L}\mathcal{L}\left[\sum\nolimits_{\Omega}\right](-s). &(6.34)
\end{aligned}$$

Substituting (6.34) and (6.30) into (6.32), the outage can be expressed as

$$
\begin{aligned}
F(\gamma) &= \Pr\left[\Gamma_{(L,1)} - \sum\nolimits_{\Omega} < \sigma^2\gamma\right] && (6.35)\\
&= \mathrm{CDF}(\sigma^2\gamma) && (6.36)\\
&= \frac{1}{2\pi j}\int_{c-j\infty}^{c+j\infty}\frac{1}{s}e^{s\sigma^2\gamma}\frac{1}{(1+s)^L}\exp\left\{-\lambda_p 2\pi\int_0^{\infty}\left(1-e^{s\Omega(r,\gamma)}\right)r\ \mathrm{d}r\right\}\ \mathrm{d}s. && (6.37)
\end{aligned}
$$

The funtion to be integrated has two poles at $s = 0$ and $s = -1$, so c cannot be 0 and -1.

Fig. 6.2 plots the theoretic calculation (6.37) and simulation results using (6.5). The simulation is averaged over 10^6 independent runs. The figure shows that the theoretic calculation is accurate.

6.5.1 Mean of $\sum_{\Omega}$

Moments of any order can be derived from (6.30). The mean and variance of $\sum_{\Omega}$ are given by

$$
\begin{aligned}
E\left[\sum\nolimits_{\Omega}\right] &= \lambda_p 2\pi\int_0^{\infty} r\Omega\left(r,\gamma\right)\ \mathrm{d}r = \lambda_p\bar{c}2\pi\int_0^{\infty} r\tilde{\Omega}\left(r,\gamma\right)\ \mathrm{d}r, && (6.38)\\
\mathrm{var}\left[\sum\nolimits_{\Omega}\right] &= \lambda_p 2\pi\int_0^{\infty} r\Omega^2\left(r,\gamma\right)\ \mathrm{d}r = \lambda_p\bar{c}^2 2\pi\int_0^{\infty} r\tilde{\Omega}^2\left(r,\gamma\right)\ \mathrm{d}r. && (6.39)
\end{aligned}
$$

Proposition 6.1: For any children distribution, the mean of $\sum_{\Omega}$ is equal to the effective interference of a homogeneous PPP with equivalent density $\lambda = \lambda_p\bar{c}$:

$$
E_{K,X_1,\cdots,X_K}\left\{\sum\nolimits_{\Omega}\right\} = \lambda_p\bar{c}\gamma^{2/\alpha}\cdot\frac{2\pi}{\alpha}\Gamma\left(\frac{2}{\alpha}\right)\Gamma\left(1-\frac{2}{\alpha}\right). \qquad (6.40)
$$

A proof is given in Appendix 6.C. This proposition immediately results in the following conclusion that clustering is always beneficial in terms of SINR outage.

Proposition 6.2: For a Neyman-Scott cluster process with homogeneous Poisson parent process and arbitrary children distribution function, the outage is strictly less than that under a homogeneous PPP with equivalent density $\lambda = \lambda_p\bar{c}$.

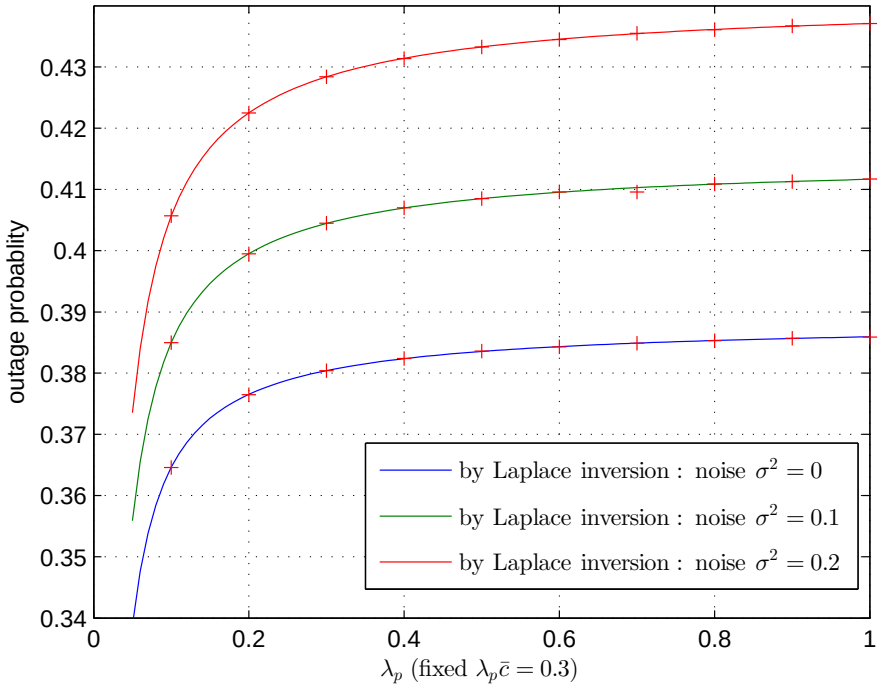


Figure 6.2: Comparison of the simulated SINR outage and the theoretic SINR outage by Laplace inversion. We fix the density $\lambda_p \bar{c} = 0.3$ for better illustration (the resulting outage will vary within a small range). Matern process with $d_c = 1$ is used as the children process. The SINR threshold is set to $\gamma = 0$dB, and antenna number is $L = 3$. The theoretic results are plotted in solid curves, and the simulation results in '+'. The comparison shows that the theoretic calculation is accurate.

Proof: The outage under any clustering is given by (6.25), and that under the homogeneous PPP (6.8). Because $\sum_{\Omega}$ in (6.25) is a random variable with mean $\lambda_p \bar{c}\gamma^{2/\alpha} \cdot \frac{2\pi}{\alpha}\Gamma\left(\frac{2}{\alpha}\right)\Gamma\left(1-\frac{2}{\alpha}\right)$ and non-zero variance, the outage for clustering is strictly less than that for the homogeneous PPP. ■

Remark: For a homogeneous PPP, the interfering nodes are more uniformly distributed, so the receiver is consistently affected by interference. On the contrary, for a cluster process, $\sum_{\Omega}$ depends on the realization of clusters' locations. The amount of $\sum_{\Omega}$ will fluctuate from realization to realization. Even though occasionally a cluster is close to the receiver to block the desired signal, with some chances all the cluster is far away enough for the receiver to communicate.

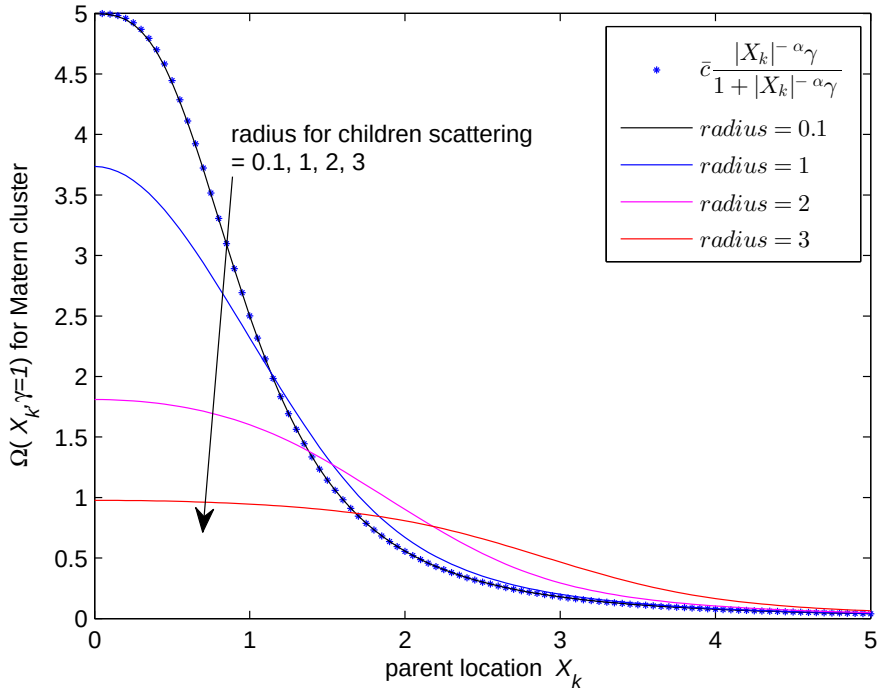
6.5.2 Effect of Cluster Parameters on $\Omega(X_k, \gamma)$

1. Scaling: Consistent with intuition, the effective cluster interference is proportional to the expected number of children. That is, $\Omega(X_k, \gamma) = \bar{c}\tilde{\Omega}(X_k, \gamma) \propto \bar{c}$.

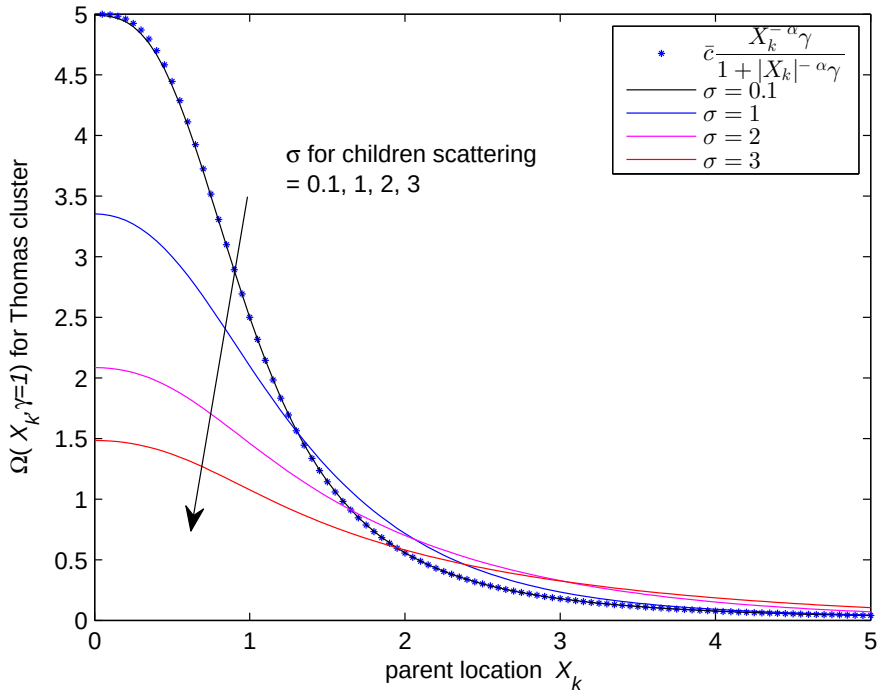
2. Monotonicity and asymptotic decay: $\Omega(X_k, \gamma)$ is strictly decreasing in X_k, and strictly increasing in γ. Bounds are $0 < \Omega(X_k, \gamma) < \bar{c}$. Moreover, as $X_k \to \infty$, $\Omega(X_k, \gamma) \to \bar{c}|X_k|^{-\alpha}\gamma$; in other words, at enough distance, the effective interference of a cluster follows the same pathloss decay as the interference of a node.

3. Effect of cluster scattering: As seen in Fig. 6.3,

   - If clusters are very compact, e.g. $d_c \to 0$ and $\sigma \to 0$ for the Matern and the Thomas processes respectively, then $\Omega(X_k, \gamma) \to \bar{c}\frac{|X_k|^{-\alpha}\gamma}{1+|X_k|^{-\alpha}\gamma}$. And $\Omega(X_k, \gamma)$ decays rapidly as the cluster moves away.
   - As cluster becomes more scattering, a cluster near the origin produces less interference, but will maintain for a longer distance as the cluster moves away.
   - If clusters have huge children scattering, e.g. $d_c \to \infty$ and $\sigma \to \infty$ for the two representative processes, then $\Omega(X_k, \gamma)$ becomes irrelevant to the cluster location. In fact, not only children within the same cluster is i.i.d., but also



(a) Matern Cluster



(b) Thomas Cluster

Figure 6.3: Effective interference $\Omega(X_k, \gamma)$ for the Matern and the Thomas cluster process for different values of d_c and σ, respectively. Expected number of children per cluster is $\bar{c} = 5$.

children among clusters tends to be i.i.d. This means the cluster process becomes a homogeneous PPP with equivalent density $\lambda = \lambda_p \bar{c}$.

6.5.3 Effect of Cluster Parameters on $\sum_\Omega$

The effect of cluster parameters is discussed below.

1. Scaling: $E\left[\sum_\Omega\right] \propto \lambda_p \bar{c}$, $\text{var}\left[\sum_\Omega\right] \propto \lambda_p \bar{c}^2$. A more general result is that, the n-th order moment $E\left[\left(\sum_\Omega\right)^n\right] \propto \lambda_p \bar{c}^n$.

2. With $\lambda_p \bar{c}$ fixed and changing $\lambda_p, \bar{c}$, the conclusion is that more clustering is more beneficial to the outage, as seen in Fig. 6.4. From the above remark, for fixed $\lambda_p \bar{c}$, $E\left[\sum_\Omega\right]$ is constant and $E\left[\left(\sum_\Omega\right)^n\right] \propto (\lambda_p \bar{c})\, \bar{c}^{n-1}$, $n \geq 2$.

   - As $\lambda_p \to \infty$ and $\bar{c} \to 0$, higher (≥ 2) moments of $\sum_\Omega$ tends to zero, meaning $\sum_\Omega$ tends to a constant, which suggests that the cluster process becomes a homogeneous PPP. On the other hand, intuitively thinking as $\bar{c} \to 0$, Poisson number of children per cluster tends to Bernoulli trail: a cluster has one child with probabilty $\bar{c}$ and no child with $1 - \bar{c}$. Then by the Poisson splitting, this forms a PPP with density $\lambda_p \bar{c}$.
   - As $\bar{c}$ increases, $\text{var}\left[\sum_\Omega\right]$ increases and the outage decreases accordingly. Intuitively image that a small number of clusters with large children population per cluster. Occasionally a cluster is close to the receiver so that the receiver is completely blocked by nearby cluster. But with some chance all the clusters are too far away to interfere the receiver.

3. Effect of cluster scattering: another instance of that more clustering is more beneficial, as seen in Fig. 6.5.

   - If clusters have huge children scattering, e.g. $d_c \to \infty$ and $\sigma \to \infty$, the cluster process tends to a homogeneous PPP, which is undesirable.

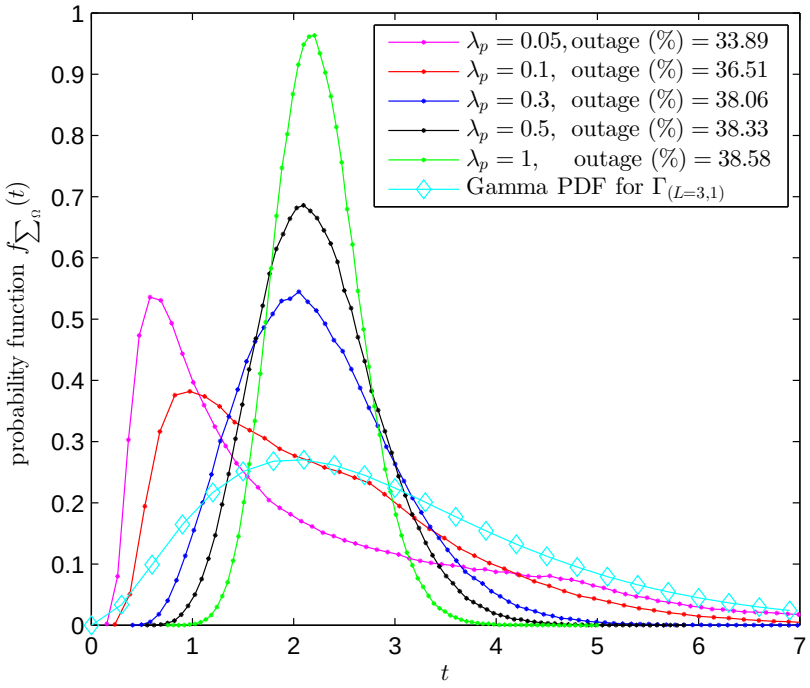


Figure 6.4: Simulated PDF of $\sum_\Omega$ for varying $\lambda_p, \bar{c}$, given fixed $\lambda_p \bar{c} = 0.3$. The SINR threshold is set to $\gamma = 0$dB, and antenna number is $L = 3$. Gamma PDF $\Gamma_{(L=3,1)}$ is also plotted. As λ_p increases ($\bar{c}$ decreases), var$\left[\sum_\Omega\right]$ decreases and results in higher outage.

- As clusters become more compact, var$\left[\sum_{\Omega}\right]$ increases and the outage decreases. This can also be explained by Fig. 6.3. Let us name "high-interference region" the region where $\Omega\left(X_k, \gamma\right)$ is larger than a threshold, and "low-interference zone" the rest of the 2-dim plane. As seen in Fig. 6.3, $\Omega\left(X_k, \gamma\right)$ decays faster for more compact cluster. Consequently the "high-interference region" gets smaller and this reduces the outage by increasing the chance that all interfering clusters are in the "low-interference zone".

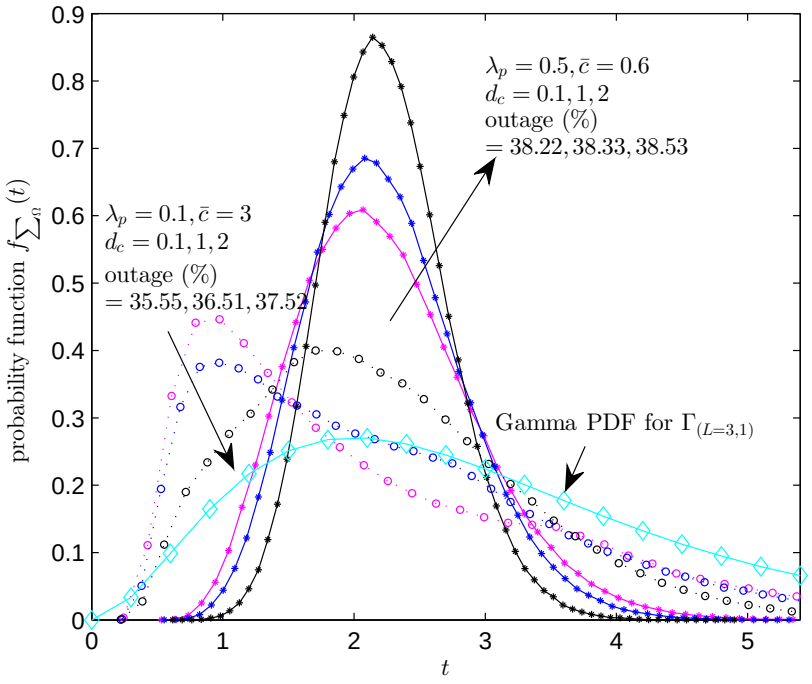


Figure 6.5: Simulated PDF of $\sum_{\Omega}$ for varying levels of children scattering (in this figure, varying d_c for the Matern cluster). The dotted curves are for $\lambda_p = 0.1, \bar{c} = 3$, and the solid curves $\lambda_p = 0.5, \bar{c} = 0.6$. The SINR threshold is set to $\gamma = 0$dB, and antenna number is $L = 3$. As d_c increases, children become more scattering, and the resulting outage increases.

6.5.4 Gamma Approximation

The Laplace transform (6.30) is a full characterization $\sum_{\Omega}$, but this characterization is largely numerical and complex. In favor of a simple final expression for the outage, we seek to approximate $\sum_{\Omega}$ as a tractable distribution. Because each X_k is i.i.d. distributed, $\sum_{\Omega}$ is a sum of positive i.i.d. $\Omega(X_k, \gamma)$. By the central limit theorem, a large number of i.i.d. random variables will sum up to approach Gaussian distribution. As early as 1944-1945 it is shown in [47] that the probability distribution of a SN random variable tends to Gaussian distribution, as the density tends to infinity. The SN random variable also tends to Gamma distribution, since Gamma distribution itself with a large shape parameter converges to Gaussian distribution. Here we choose to approximate $\sum_{\Omega}$ as a Gamma random variable for the reason that the final expression of the outage can be concisely expressed as an incomplete Beta function, as seen later.

The parameters of Gamma distribution can be determined by mean and variance. The mean is given in (6.8). Approximating $\sum_{\Omega}$ to a Gamma random variable $\Gamma_{\left(\hat{k},\hat{\theta}\right)}$, the shape parameter $\hat{k}$ and scale parameter $\hat{\theta}$ can be determined as

$$\hat{k} = \frac{\left(E\left[\sum_{\Omega}\right]\right)^2}{\mathrm{var}\left[\sum_{\Omega}\right]} = \frac{\left(\lambda_p \bar{c}^2 2\pi \int_0^{\infty} r\tilde{\Omega}(r,\gamma)\,\mathrm{d}r\right)^2}{\lambda_p \bar{c}^2 2\pi \int_0^{\infty} r\tilde{\Omega}^2(r,\gamma)\,\mathrm{d}r} \propto \lambda_p, \tag{6.41}$$

$$\hat{\theta} = \frac{\mathrm{var}\left[\sum_{\Omega}\right]}{E\left[\sum_{\Omega}\right]} = \frac{\lambda_p \bar{c}^2 2\pi \int_0^{\infty} r\tilde{\Omega}^2(r,\gamma)\,\mathrm{d}r}{\lambda_p \bar{c}^2 2\pi \int_0^{\infty} r\tilde{\Omega}(r,\gamma)\,\mathrm{d}r} \propto \bar{c}. \tag{6.42}$$

This approximation is precise as $\lambda_p \to \infty$, as shown in Fig. 6.6. Note that $\bar{c}$ does not affect the goodness of the approximation, because scaling $\bar{c}$ will scale $\sum_{\Omega}$ and $\Gamma_{\left(\hat{k},\hat{\theta}\right)}$ but will not change the shapes of them.

For the interference limited scenario where interference dominates, by ignoring the noise term $\sigma^2\gamma$ in (6.25), the approximate outage is the probability $\Pr\left[\Gamma_{(L,1)} < \Gamma_{\left(\hat{k},\hat{\theta}\right)}\right]$. It is known that Beta random variable is the ratio of a Gamma random variable divided by the sum of itself and another independent Gamma random variable. Then the outage can be

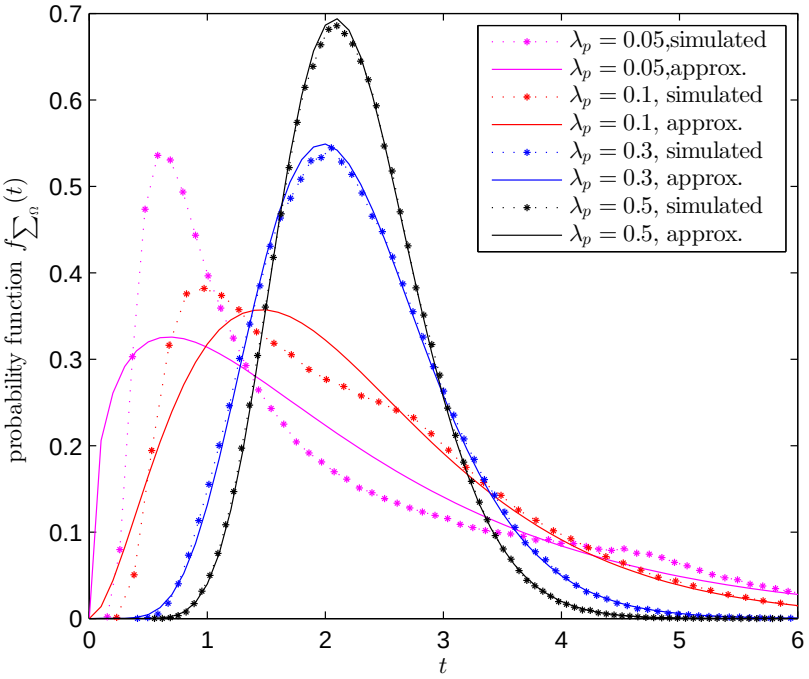
derived as an incomplete Beta function

$$\begin{aligned} F(\gamma) &\approx \Pr\left[\Gamma_{(L,1)} < \Gamma_{\left(\hat{k},\hat{\theta}\right)}\right] && (6.43)\\ &= \Pr\left[\Gamma_{(L,1)} < \hat{\theta}\Gamma_{\left(\hat{k},1\right)}\right] && (6.44)\\ &= \Pr\left[\frac{\Gamma_{(L,1)}}{\Gamma_{(L,1)}+\Gamma_{\left(\hat{k},1\right)}} < \frac{\hat{\theta}}{1+\hat{\theta}}\right] && (6.45)\\ &= \Pr\left[B_{\left(L,\hat{k}\right)} < \frac{\hat{\theta}}{1+\hat{\theta}}\right] && (6.46)\\ &= I_{\frac{\hat{\theta}}{1+\hat{\theta}}}\left(L,\hat{k}\right) && (6.47) \end{aligned}$$

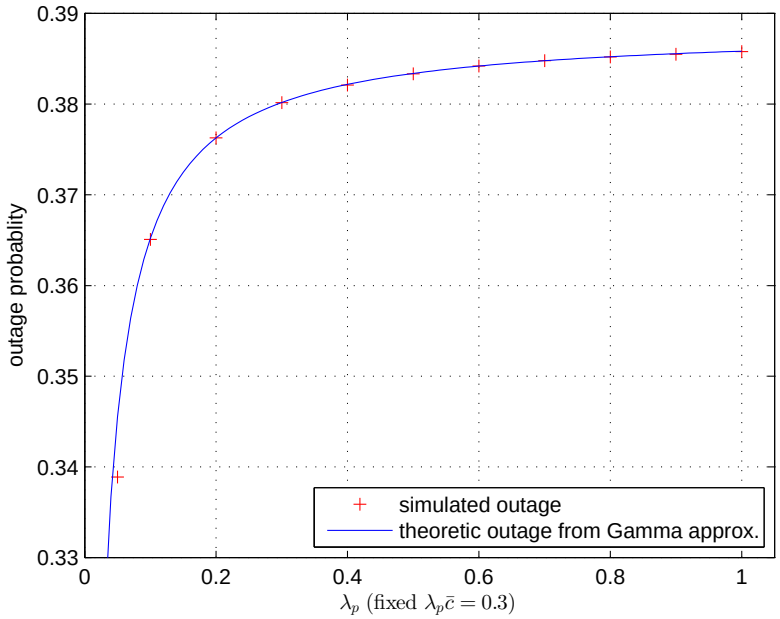
where $B_{\left(L,\hat{k}\right)}$ denotes a Beta random variable with parameters $\left(L,\hat{k}\right)$ and $I_x(a,b)$ the regularized incomplete Beta function. Numerical results in Fig. 6.6 show that this approximation achieves good precision.

6.6 Conclusion

Previous work characterizing outage in large random networks focused on the homogeneous PPP as the node distribution. We have extended the previous results to multiple homogeneous/nonhomogeneous PPPs and Poisson clustered processes. It is shown that the resulting total interference under multiple PPPs is a sum of the effective interferences from each PPP, which is referred to as the superposition property. For Poisson clustered processes, the total interference is a sum of the effective interferences from each cluster, and can be treated as a shot noise model. We have proved that any clustered process is better than a homogeneous PPP, by showing that the total interference of a clustered process is a random variable whose mean is equal to the effective interference of the homogeneous PPP. It is further shown that the more clustering (e.g., smaller number of clusters with larger number of children, more compact children scattering) leads to the better outage performance. In fact, as parent density tends to infinity while children number tends to zero, or as children scattering becomes infinitely large, the clustered process tends to a homogeneous PPP. Finally we derive a concise expression of the SINR outage for fast and theoretical calculation, by approximating the total interference as a Gamma random variable.



(a) simulated PDF and approx. Gamma PDF



(b) simulated and approx. outage

Figure 6.6: Goodness of Gamma approximation: (a) comparison of simulated PDF and Gamma PDF, (b) comparison of the simulated and approximate SINR outage. The SINR threshold is set to $\gamma = 0$dB, and antenna number is $L = 3$. It can be seen in (a) that PDF curves differ at small λ_p but converges at large λ_p, and in (b) that slight mismatches of the outage show at small λ_p. Note that the goodness of approximation depends on λ_p but not on $\bar{c}$. The reason to choose fixed $\lambda_p\bar{c} = 0.3$ is that the values of the resulting PDF and outage are close to be shown in a single figure.

6.7 Appendix 6.A: Proof of the Superposition Property

Here we give a proof for Theorem 6.1 for two layers of PPPs. The proof for three or more layers is essentially the same and thus omitted for brevity.

Proof: Assume two homogeneous PPPs with density λ_X, λ_Y on region $\mathcal{R}_X$, $\mathcal{R}_Y$, respectively. Let $\{N, X_1, \cdots, X_N\}$ and $\{M, Y_1, \cdots, Y_M\}$ denote the number and the locations of nodes respectively. Assume every node transmit with unit power. The conditional SINR outage is given as [14]

$$\begin{aligned} & F(\gamma|\, N, X_1, \cdots, X_N, M, Y_1, \cdots, Y_M) \\ = \; & 1 - \frac{\sum_{i=0}^{L-1} a_i \gamma^i}{\exp\left(\sigma^2\gamma\right) \prod_{n=1}^{N} \left(1 + |X_n|^{-\alpha}\,\gamma\right) \prod_{m=1}^{M} \left(1 + |Y_m|^{-\alpha}\,\gamma\right)}, \end{aligned} \tag{6.48}$$

where $a_i, i = 0, \cdots, L-1$ are the first L coefficients of the Taylor expansion of the denominator of (6.48).

The coefficient a_i can be expressed by the inverse z-tranform,

$$a_i = \mathcal{Z}^{-1}\left\{\exp\left(\sigma^2 z\right) \prod_{n=1}^{N} \left(1 + |X_n|^{-\alpha}\, z\right) \prod_{m=1}^{M} \left(1 + |Y_m|^{-\alpha}\, z\right)\right\} \tag{6.49}$$

$$= \frac{1}{2\pi j} \oint_C \left[\exp\left(\sigma^2 z\right) \prod_{n=1}^{N} \left(1 + |X_n|^{-\alpha}\, z\right) \prod_{m=1}^{M} \left(1 + |Y_m|^{-\alpha}\, z\right)\right] z^{i-1}\, \mathrm{d}z \tag{6.50}$$

where C is a counterclockwise closed path encircling the origin and entirely in the region of convergence. Replacing a_i with (6.50), we have

$$\frac{a_i \gamma^i}{\exp\left(\sigma^2\gamma\right) \prod_{n=1}^{N} \left(1 + |X_n|^{-\alpha}\,\gamma\right) \prod_{m=1}^{M} \left(1 + |Y_m|^{-\alpha}\,\gamma\right)} \tag{6.51}$$

$$= \gamma^i \exp\left(-\sigma^2\gamma\right) \times \tag{6.52}$$

$$\frac{1}{2\pi j} \oint_C \exp\left(\sigma^2 z\right) \prod_{n=1}^{N} \left(\frac{1 + |X_n|^{-\alpha}\, z}{1 + |X_n|^{-\alpha}\,\gamma}\right) \prod_{m=1}^{M} \left(\frac{1 + |Y_m|^{-\alpha}\, z}{1 + |Y_m|^{-\alpha}\,\gamma}\right) z^{i-1}\, \mathrm{d}z. \tag{6.53}$$

Taking expectation of $\{N, X_1, \cdots, X_N\}$ and $\{M, Y_1, \cdots, Y_M\}$,

$$
\begin{aligned}
& E_{N,X_1,\cdots,X_N}\left\{\prod_{n=1}^{N}\left(\frac{1+|X_n|^{-\alpha}z}{1+|X_n|^{-\alpha}\gamma}\right)\right\} \\
= \; & E_{N,X_1}\left\{\frac{1+|X_1|^{-\alpha}z}{1+|X_1|^{-\alpha}\gamma}\right\}^{N} \qquad (6.54) \\
= \; & \sum_{N=0}^{\infty}\left(E_{X_1}\left\{\frac{1+|X_1|^{-\alpha}z}{1+|X_1|^{-\alpha}\gamma}\right\}\right)^{N}\frac{(\lambda_X A_{\mathcal{R}_X})^N}{N!}\exp\left(-\lambda_X A_{\mathcal{R}_X}\right) \\
= \; & \exp\left(\lambda_X A_{\mathcal{R}_X} E_{X_1}\left\{\frac{1+|X_1|^{-\alpha}z}{1+|X_1|^{-\alpha}\gamma}\right\}\right)\exp\left(-\lambda_X A_{\mathcal{R}_X}\right) \\
= \; & \exp\left(\lambda_X A_{\mathcal{R}_X} E_{X_1}\left\{\frac{|X_1|^{-\alpha}z-|X_1|^{-\alpha}\gamma}{1+|X_1|^{-\alpha}\gamma}\right\}\right) \qquad (6.55)
\end{aligned}
$$

where equality (6.54) follows from that $X_1, \cdots, X_N$ are i.i.d., and $A_{\mathcal{R}_X}$ denotes the area of $\mathcal{R}_X$. Similarly,

$$
\begin{aligned}
& E_{M,Y_1,\cdots,Y_M}\left\{\prod_{m=1}^{M}\left(\frac{1+|Y_m|^{-\alpha}z}{1+|Y_m|^{-\alpha}\gamma}\right)\right\} \qquad (6.56) \\
= \; & \exp\left(\lambda_Y A_{\mathcal{R}_Y} E_{Y_1}\left\{\frac{|Y_1|^{-\alpha}z-|Y_1|^{-\alpha}\gamma}{1+|Y_1|^{-\alpha}\gamma}\right\}\right). \qquad (6.57)
\end{aligned}
$$

Substituting (6.55) and (6.57) into (6.53), we have

$$
\begin{aligned}
& 1-F(\gamma) \\
= & \sum_{i=0}^{L-1} \gamma^i \exp\left(-\sigma^2\gamma\right) \frac{1}{2\pi j} \oint_C \left(\begin{array}{c} \exp\left(\sigma^2 z\right) \times \\ \exp\left(\lambda_X A_{\mathcal{R}_X} E_{X_1}\left\{\frac{|X_1|^{-\alpha} z - |X_1|^{-\alpha}\gamma}{1+|X_1|^{-\alpha}\gamma}\right\}\right) \times \\ \exp\left(\lambda_Y A_{\mathcal{R}_Y} E_{Y_1}\left\{\frac{|Y_1|^{-\alpha} z - |Y_1|^{-\alpha}\gamma}{1+|Y_1|^{-\alpha}\gamma}\right\}\right) \end{array} \right) z^{i-1}\,\mathrm{d}z \\
= & \sum_{i=0}^{L-1} \gamma^i \exp\left(\begin{array}{c} -\sigma^2\gamma + \\ \lambda_X A_{\mathcal{R}_X} E_{X_1}\left\{\frac{-|X_1|^{-\alpha}\gamma}{1+|X_1|^{-\alpha}\gamma}\right\} + \\ \lambda_Y A_{\mathcal{R}_Y} E_{Y_1}\left\{\frac{-|Y_1|^{-\alpha}\gamma}{1+|Y_1|^{-\alpha}\gamma}\right\} \end{array} \right) \times \\
& \frac{1}{2\pi j} \oint_C \exp\left[\left(\begin{array}{c} \sigma^2 + \\ \lambda_X A_{\mathcal{R}_X} E_{X_1}\left\{\frac{|X_1|^{-\alpha}}{1+|X_1|^{-\alpha}\gamma}\right\} + \\ \lambda_Y A_{\mathcal{R}_Y} E_{Y_1}\left\{\frac{|Y_1|^{-\alpha}}{1+|Y_1|^{-\alpha}\gamma}\right\} \end{array} \right) z \right] z^{i-1}\,\mathrm{d}z \qquad (6.58) \\
= & \sum_{i=0}^{L-1} \exp\left(\begin{array}{c} -\sigma^2\gamma - \\ \lambda_X A_{\mathcal{R}_X} E_{X_1}\left\{\frac{|X_1|^{-\alpha}\gamma}{1+|X_1|^{-\alpha}\gamma}\right\} - \\ \lambda_Y A_{\mathcal{R}_Y} E_{Y_1}\left\{\frac{|Y_1|^{-\alpha}\gamma}{1+|Y_1|^{-\alpha}\gamma}\right\} \end{array} \right) \gamma^i \frac{1}{i!} \left(\begin{array}{c} \sigma^2 + \\ \lambda_X A_{\mathcal{R}_X} E_{X_1}\left\{\frac{|X_1|^{-\alpha}}{1+|X_1|^{-\alpha}\gamma}\right\} + \\ \lambda_Y A_{\mathcal{R}_Y} E_{Y_1}\left\{\frac{|Y_1|^{-\alpha}}{1+|Y_1|^{-\alpha}\gamma}\right\} \end{array} \right)^i \\
= & e^{-\sigma^2\gamma - \Omega_X - \Omega_Y} \sum_{i=0}^{L-1} \frac{1}{i!} \left(\sigma^2\gamma + \Omega_X + \Omega_Y\right)^i
\end{aligned}
$$

where equality (6.58) follows from that

$$
\begin{aligned}
& \frac{1}{2\pi j} \oint_C \exp\left(bz\right) z^{i-1}\,\mathrm{d}z & (6.59) \\
= & \; i\text{-th order coefficient of Taylor expansion of} \exp\left(bz\right) & (6.60) \\
= & \frac{1}{i!} b^i, & (6.61)
\end{aligned}
$$

and

$$
\begin{aligned}
& \Omega_X \\
= & \; \lambda_X A_{\mathcal{R}_X} E_{X_1}\left\{\frac{|X_1|^{-\alpha}\gamma}{1+|X_1|^{-\alpha}\gamma}\right\} \\
= & \; \lambda_X \iint_{\mathcal{R}_X} \frac{|X|^{-\alpha}\gamma}{1+|X|^{-\alpha}\gamma} \mathrm{d}X, & (6.62)
\end{aligned}
$$

and

$$\begin{aligned}
&\Omega_Y \\
=\ & \lambda_Y A_{\mathcal{R}_Y} E_{Y_1}\left\{\frac{|Y_1|^{-\alpha}\gamma}{1+|Y_1|^{-\alpha}\gamma}\right\} \\
=\ & \lambda_Y \iint_{\mathcal{R}_Y} \frac{|Y|^{-\alpha}\gamma}{1+|Y|^{-\alpha}\gamma}\mathrm{d}Y. \qquad (6.63)
\end{aligned}$$

■

6.8 Appendix 6.B: Derivation of $\Omega(X_k,\gamma)$ for the Matern and the Thomas Processes

For the Matern cluster process, given the expected number of children $\bar{c}$ and the radius d_c, the effective interference of the k-th cluster is given by

$$\Omega_{\text{Matern}}(X_k,\gamma) = \iint_{\mathcal{B}(X_k,d_c)} \Lambda_{\text{Matern}}(Z)\,\frac{|Z|^{-\alpha}\gamma}{1+|Z|^{-\alpha}\gamma}\,\mathrm{d}Z \qquad (6.64)$$

where $\mathcal{B}(X_k,d)$ is a ball of radius d_c centered at X_k. Representing Z in polar coordination $Z = X_k + \begin{bmatrix} \rho\cos(\theta+\theta_0) \\ \rho\sin(\theta+\theta_0) \end{bmatrix}$ where θ_0 is the angle of X_k, the above integral is derived to be

$$\begin{aligned}
&\Omega_{\text{Matern}}(X_k,\gamma) \\
=\ & \frac{\bar{c}}{\pi d_c^2}\int_0^d\int_0^{2\pi} \frac{\left(\rho^2+|X_k|^2-2\rho|X_k|\cos\theta\right)^{-\alpha/2}\gamma}{1+\left(\rho^2+|X_k|^2-2\rho|X_k|\cos\theta\right)^{-\alpha/2}\gamma}\cdot\rho\,\mathrm{d}\theta\mathrm{d}\rho \\
=\ & \frac{\bar{c}}{\pi d_c^2}\int_0^d\int_0^{2\pi} \frac{\gamma}{\left(\rho^2+|X_k|^2-2\rho|X_k|\cos\theta\right)^{\alpha/2}+\gamma}\rho\,\mathrm{d}\theta\mathrm{d}\rho,
\end{aligned}$$

where $\left(\rho^2+|X_k|^2-2\rho|X_k|\cos\theta\right)^{1/2}$ is the distance from Z to the origin according to the law of cosine.

For the Thomas cluster process, the children points of the k-th cluster is Gaussian distributed with density (6.1). In polar representation $Z = X_k + \begin{bmatrix} \rho\cos(\theta+\theta_0) \\ \rho\sin(\theta+\theta_0) \end{bmatrix}$, the density function can be expressed as

$$\Lambda_{\text{Thomas}}(\rho,\theta) = \frac{\bar{c}}{(2\pi)^{3/2}\sigma\rho}\exp\left(-\frac{\rho^2}{2\sigma^2}\right).$$

The effective interference is

$$\Omega_{\text{Thomas}}(X_k,\gamma) \tag{6.65}$$

$$= \int_0^{\infty}\int_0^{2\pi} \frac{\left(\rho^2+|X_k|^2-2\rho|X_k|\cos\theta\right)^{-\alpha/2}\gamma}{1+\left(\rho^2+|X_k|^2-2\rho|X_k|\cos\theta\right)^{-\alpha/2}\gamma}\cdot\frac{\bar{c}}{(2\pi)^{3/2}\sigma\rho}\exp\left(-\frac{\rho^2}{2\sigma^2}\right)\cdot\rho\,\mathrm{d}\theta\mathrm{d}\rho$$

$$= \frac{\bar{c}}{(2\pi)^{3/2}\sigma}\int_0^{\infty}\int_0^{2\pi}\frac{\gamma}{\left(\rho^2+|X_k|^2-2\rho|X_k|\cos\theta\right)^{\alpha/2}+\gamma}\exp\left(-\frac{\rho^2}{2\sigma^2}\right)\mathrm{d}\theta\mathrm{d}\rho. \tag{6.66}$$

6.9 Appendix 6.C: Proof of Proposition 6.1

For any children distribution, $E_{K,X_1,\cdots,X_K}\left\{\sum_{k=1}^{K}\Omega(X_k,\gamma)\right\} = \lambda_p\bar{c}\gamma^{2/\alpha}\cdot\frac{2\pi}{\alpha}\Gamma\left(\frac{2}{\alpha}\right)\Gamma\left(1-\frac{2}{\alpha}\right)$.

Proof: By Definition 6.1, we assume that the children distribution at location Z is independent of parent location X_k, but only depends on $Z-X_k$. Thus the children density function can be written as

$$\Lambda(Z) = \bar{c}f(Z-X_k) \tag{6.67}$$

where $\bar{c}$ is the expected number of children, $f(\cdot)$ is a probability density function.

By Campbell's theorem,

$$E_{K,X_1,\cdots,X_K}\left\{\sum_{k=1}^{K}\Omega(X_k,\gamma)\right\} \tag{6.68}$$

$$= \lambda_p\iint_{\mathbb{R}^2}\Omega(X_k,\gamma)\,\mathrm{d}X_k. \tag{6.69}$$

Substituting (6.67) into the above expression, we have

$$E_{K,X_1,\cdots,X_K}\left\{\sum_{k=1}^{K}\Omega(X_k,\gamma)\right\} \tag{6.70}$$

$$= \lambda_p\bar{c}\iint_{\mathbb{R}^2}\iint_{\mathbb{R}^2} f(Z-X_k)\,\frac{|Z|^{-\alpha}\gamma}{1+|Z|^{-\alpha}\gamma}\,\mathrm{d}Z\mathrm{d}X_k. \tag{6.71}$$

Exchanging order of the integrals,

$$E_{K,X_1,\cdots,X_K}\left\{\sum_{k=1}^{K}\Omega\left(X_k,\gamma\right)\right\} \tag{6.72}$$

$$= \lambda_p\bar{c}\iint_{\mathbb{R}^2}\frac{|Z|^{-\alpha}\gamma}{1+|Z|^{-\alpha}\gamma}\iint_{\mathbb{R}^2}f\left(Z-X_k\right)\,\mathrm{d}X_k\mathrm{d}Z \tag{6.73}$$

$$= \lambda_p\bar{c}\iint_{\mathbb{R}^2}\frac{|Z|^{-\alpha}\gamma}{1+|Z|^{-\alpha}\gamma}\iint_{\mathbb{R}^2}f\left(Y\right)\,\mathrm{d}Y\mathrm{d}Z \tag{6.74}$$

$$= \lambda_p\bar{c}\iint_{\mathbb{R}^2}\frac{|Z|^{-\alpha}\gamma}{1+|Z|^{-\alpha}\gamma}\mathrm{d}Z \tag{6.75}$$

$$= \lambda_p\bar{c}\gamma^{2/\alpha}\cdot\frac{2\pi}{\alpha}\Gamma\left(\frac{2}{\alpha}\right)\Gamma\left(1-\frac{2}{\alpha}\right) \tag{6.76}$$

where the change of variable is $Y = Z - X_k$. This completes the proof. ■

Chapter 7

CONCLUSIONS

In this thesis, we have analyzed and optimized multi-antenna systems for physical-layer security. We have also studied the performance of multi-antenna receivers in large distributed networks. Our contributions are listed below.

- For MISOSE wiretap channel with perfect CSI, we optimize joint transmit and collaborative jamming to maximize the secrecy rate. In particular, we reduce the problem of maximizing the secrecy rate to the problem of finding the optimal jamming levels. Moreover, finding the optimal jamming levels can be solved by a one-dimensional search that is computationally affordable. The numerical result demonstrates an example that the optimized jamming significantly improves the secrecy rate, compared to the traditional zero-forcing jamming.

  For MIMOME wiretap channel with perfect CSI, we study optimal transmit/jamming under an additional constraint of transmit beamforming (the rank-1 constraint on the transmit covariance matrix). By relating the MIMOME channel to the effective MISOSE channel, we propose an iterative algorithm that in each iteration searches the jamming covariance on the 1-dim space defined by the effective MISOSE channel. Numerical results show that our proposed algorithm converges within a few iterations and it achieves higher secrecy rate than the existing artificial noise schemes.

- For MISOSE wiretap channel with imperfect CSI, we have studied the problem of optimizing the transmit covariance, assuming that the CSI of the receiver and the eavesdropper channel belong to given uncertainty sets. By proving the saddle-point solution, we transformed the worst-case optimization problem into a quasi-convex optimization problem. The result of the worst-case optimization problem can be expressed in the form of generalized eigenvalue, which is the same form as that of

the conventional case. We also have shown that the average design serves as an upper bound on the worst-case design, and the worst-case design meets the lowest of the average design. Two numerical examples of the receivers and the eavesdroppers location uncertainties demonstrated the effectiveness of our proposed design.

- For jamming-aided MISOSE wiretap channel with imperfect CSI, we optimize the transmit/jamming covariances. We propose to solve the joint optimization of transmit and jamming design for the approximate worst-case SINR-ratio problem. A minimax solution is shown to exist for the problem, based on which some insightful results of the optimal transmit and jamming covariances are obtained. A quasiconvex optimization algorithm that is tractable and efficient is provided for solving the worst-case SINR-ratio problem. One application of this method demonstrates that a linear array successfully transmits towards a certain direction range and jams the other directions simultaneously. In the second application, three arrays cooperate to transmit to a certain location and jam the other locations.

In the end, we analyze the performance of multi-antenna receiver under sophisticated Poisson spatial node distribution. We have extended the previous results for interferers distributed as an homogeneous PPP to that for interferes as multiple homogeneous/nonhomogeneous PPPs and Poisson clustered processes. The resulting total interference under multiple PPPs is a sum of the effective interferences from each PPP, which is referred to as the superposition property. For Poisson clustered processes, we have proved that any clustered process is better than a homogeneous PPP. It is further shown that the more clustering (e.g., smaller number of clusters with larger number of children, more compact children scattering) leads to the better outage performance. Potential applications of these results include interference characterization of femto-cell cellular networks, cognitive radio networks, coexisting networks etc.

BIBLIOGRAPHY

[1] O.B.S. Ali, C. Cardinal, and F. Gagnon. Performance of optimum combining in a poisson field of interferers and rayleigh fading channels. *Wireless Communications, IEEE Transactions on*, 9(8):2461–2467, 2010.

[2] F. Baccelli, B. Blaszczyszyn, and P. Muhlethaler. An aloha protocol for multihop mobile wireless networks. *Information Theory, IEEE Transactions on*, 52(2):421–436, 2006.

[3] M. Bloch, J. Barros, M.R.D. Rodrigues, and S.W. McLaughlin. Wireless information-theoretic security. *Information Theory, IEEE Transactions on*, 54(6):2515–2534, 2008.

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

[5] Ronit Bustin, Ruoheng Liu, H. Vincent Poor, and Shlomo Shamai. An mmse approach to the secrecy capacity of the mimo gaussian wiretap channel. *EURASIP J. Wireless Commun. Network*, 2009:3:1–3:8, March 2009.

[6] I. Csiszar and J. Korner. Broadcast channels with confidential messages. *IEEE Trans. on Inform. Theory*, 24(3):339–348, May 1978.

[7] DingZhu Du and Panos M. Pardalos. *Minimax and Applications*. Kluwer Academic Publishers, Dordrecht, 1995.

[8] Artur Ekert and Richard Jozsa. Quantum computation and shor's factoring algorithm. *Rev. Mod. Phys.*, 68(3):733–753, Jul 1996.

[9] E. Ekrem and S. Ulukus. Secrecy capacity region of the gaussian multi-receiver wiretap channel. In *ISIT 2009.*, 28 2009.

[10] Ersen Ekrem and Sennur Ulukus. On the secrecy of multiple access wiretap channel. In *In 46th Annual Allerton Conference on Communications, Control and Computing*, 2008.

[11] S.A. Fakoorian, A.L. Swindlehurst, et al. Optimal power allocation for gsvd-based beamforming in the mimo wiretap channel. *arXiv preprint arXiv:1006.1890*, 2010.

[12] R.K. Ganti, J.G. Andrews, and M. Haenggi. High-sir transmission capacity of wireless networks with general fading and node distribution. *Information Theory, IEEE Transactions on*, 57(5):3100–3116, 2011.

[13] R.K. Ganti and M. Haenggi. Interference and outage in clustered wireless ad hoc networks. *IEEE transactions on information theory*, 55(9):4067–4086, 2009.

[14] Hongsheng Gao, Peter J. Smith, and Martin V. Clark. Theoretical reliability of mmse linear diversity combining in rayleigh-fading additive interference channels. *IEEE Transactions on Communications*, 46(5):666–672, 1998.

[15] S. Gerbracht, A. Wolf, and E.A. Jorswieck. Beamforming for fading wiretap channels with partial channel information. In *Smart Antennas (WSA), 2010 International ITG Workshop on*, pages 394–401. IEEE, 2010.

[16] E.N. Gilbert. Random plane networks. *Journal of the Society for Industrial & Applied Mathematics*, 9(4):533–543, 1961.

[17] EN Gilbert. Random subdivisions of space into crystals. *The Annals of Mathematical Statistics*, 33(3):958–972, 1962.

[18] S. Goel and R. Negi. Guaranteeing secrecy using artificial noise. *IEEE Trans. on Wireless Commun.*, 7(6):2180–2189, 2008.

[19] S. Govindasamy, D.W. Bliss, and D.H. Staelin. Spectral efficiency in single-hop ad-hoc wireless networks with interference using adaptive antenna arrays. *Selected Areas in Communications, IEEE Journal on*, 25(7):1358–1369, 2007.

[20] M. Haenggi. The secrecy graph and some of its properties. In *Information Theory, 2008. ISIT 2008. IEEE International Symposium on*, pages 539–543. IEEE, 2008.

[21] A.M. Hunter, J. Andrews, and S. Weber. Transmission capacity of ad hoc networks with spatial diversity. *Wireless Communications, IEEE Transactions on*, 7(12):5058–5071, 2008.

[22] A.M. Hunter, R.K. Ganti, and J.G. Andrews. Transmission capacity of multi-antenna ad hoc networks with csma. In *Signals, Systems and Computers (ASILOMAR), 2010 Conference Record of the Forty Fourth Asilomar Conference on*, pages 1577–1581. IEEE, 2010.

[23] N. Jindal, J.G. Andrews, and S. Weber. Multi-antenna communication in ad hoc networks: Achieving mimo gains with simo transmission. *Communications, IEEE Transactions on*, 59(2):529–540, 2011.

[24] A. Khisti and G. Wornell. Secure transmission with multiple antennas ii: The mimome wiretap channel. *arXiv preprint arXiv:1006.5879*, 2010.

[25] A. Khisti and G.W. Wornell. Secure transmission with multiple antennas i: The misome wiretap channel. *IEEE Trans. on Inform. Theory*, 56(7):3088–3104, 2010.

[26] M. Kobayashi and M. Debbah. On the secrecy capacity of frequency-selective fading channels : A practical vandermonde precoding. In *Personal, Indoor and Mobile Radio Communications, 2008. PIMRC 2008. IEEE 19th International Symposium on*, pages 1–5, 2008.

[27] O.O. Koyluoglu, C.E. Koksal, and H.E. Gamal. On secrecy capacity scaling in wireless networks. *Information Theory, IEEE Transactions on*, 58(5):3000–3015, 2012.

[28] Lifeng Lai and H. El Gamal. The relay-eavesdropper channel: Cooperation for secrecy. *IEEE Trans. on Inform. Theory*, 54(9):4005–4019, 2008.

[29] S. Leung-Yan-Cheong and M. Hellman. The gaussian wire-tap channel. *IEEE Trans. on Inform. Theory*, 24(4):451–456, 1978.

[30] S. Levy. *Crypto.* Allen Lane, 2001.

[31] J. Li and A.P. Petropulu. On ergodic secrecy rate for gaussian miso wiretap channels. *Wireless Communications, IEEE Transactions on*, 10(4):1176–1187, 2011.

[32] Zang Li, W. Trappe, and R. Yates. Secret communication via multi-antenna transmission. In *41st Annual Conference on Information Sciences and Systems, 2007. CISS '07.*, pages 905–910, 2007.

[33] Y. Liang, H.V. Poor, et al. Physical layer security in broadcast networks. *Security and Communication Networks*, 2(3):227–238, 2009.

[34] Y. Liang, A. Somekh-Baruch, H.V. Poor, S. Shamai, and S. Verdú. Capacity of cognitive interference channels with and without secrecy. *Information Theory, IEEE Transactions on*, 55(2):604–619, 2009.

[35] Yingbin Liang, Gerhard Kramer, H. Vincent Poor, and Shlomo Shamai. Compound wiretap channels. *EURASIP J. Wirel. Commun. Netw.*, 2009:5:1–5:12, March 2009.

[36] Yingbin Liang and H.V. Poor. Multiple-access channels with confidential messages. *IEEE Trans. on Inform. Theory*, 54(3):976–1002, 2008.

[37] Ruoheng Liu and H.V. Poor. Multi-antenna gaussian broadcast channels with confidential messages. In *ISIT 2008.*, pages 2202–2206, 2008.

[38] Tie Liu and Shlomo Shamai. A note on the secrecy capacity of the multiple-antenna wiretap channel. *IEEE Trans. Info. Theory*, 55:2547–2553, June 2009.

[39] R.H.Y. Louie, M.R. McKay, and I.B. Collings. Open-loop spatial multiplexing and diversity communications in ad hoc networks. *Information Theory, IEEE Transactions on*, 57(1):317–344, 2011.

[40] A. Mukherjee and A.L. Swindlehurst. Fixed-rate power allocation strategies for enhanced secrecy in mimo wiretap channels. In *Signal Processing Advances in Wireless Communications, 2009. SPAWC '09.*, pages 344–348, 2009.

[41] A. Mukherjee and A.L. Swindlehurst. Robust beamforming for security in mimo wiretap channels with imperfect csi. *IEEE Trans. on Signal Process.*, 59(1):351–361, 2011.

[42] F. Oggier and B. Hassibi. The secrecy capacity of the mimo wiretap channel. In *ISIT 2008.*, pages 524–528, 2008.

[43] P. Parada and R. Blahut. Secrecy capacity of simo and slow fading channels. In *ISIT 2005.*, pages 2152–2155, 2005.

[44] E. Perron, S. Diggavi, and E. Telatar. On cooperative wireless network secrecy. In *INFOCOM 2009, IEEE*, pages 1935–1943. IEEE, 2009.

[45] P.C. Pinto, J. Barros, and M.Z. Win. Wireless secrecy in large-scale networks. In *Information Theory and Applications Workshop (ITA), 2011*, pages 1–10. IEEE, 2011.

[46] Zouheir Rezki, François Gagnon, and Vijay K. Bhargava. The ergodic capacity of the mimo wire-tap channel. *Arxiv.org*, abs/0902.0189, 2009.

[47] S.O. Rice. Mathematical analysis of random noise-conclusion. *Bell Systems Tech. J., Volume 24, p. 46-156*, 24:46–156, 1945.

[48] R. L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM*, 21:120–126, February 1978.

[49] S. Shafiee, Nan Liu, and S. Ulukus. Towards the secrecy capacity of the gaussian mimo wire-tap channel: The 2-2-1 channel. *IEEE Trans. on Inform. Theory*, 55(9):4033–4039, 2009.

[50] Shabnam Shafiee and Sennur Ulukus. Achievable rates in gaussian miso channels with secrecy constraints. In *ISIT 2007.*, pages 2466–2470, 2007.

[51] C.E. Shannon. Communication theory of secrecy systems. *Bell Syst. Tech.*, 28(4):656–715, 1949.

[52] W. Shi and J. Ritcey. Optimal transmit design for worst-case secrecy rate over uncertain miso channels. *IEEE Trans. on Commun.*, submitted.

[53] W. Shi and J. Ritcey. Optimal cooperative transmit and jamming design for maximizing secrecy rate of gaussian miso wiretap channels. *IEEE Trans. on Commun.*, to be published 2013.

[54] D. Stoyan, W.S. Kendall, J. Mecke, and L. Ruschendorf. *Stochastic geometry and its applications*, volume 2. Wiley New York, 1987.

[55] A.L. Swindlehurst. Fixed sinr solutions for the mimo wiretap channel. In *Acoustics, Speech and Signal Processing, 2009. ICASSP 2009. IEEE International Conference on*, pages 2437–2440. IEEE, 2009.

[56] R. Tanbourgi, H. Jakel, L. Chaichenets, and F.K. Jondral. Interference and throughput in aloha-based ad hoc networks with isotropic node distribution. In *Information Theory Proceedings (ISIT), 2012 IEEE International Symposium on*, pages 616–620. IEEE, 2012.

[57] E. Tekin, S. Serbetli, and A. Yener. On secure signaling for the gaussian multiple access wire-tap channel. In *Signals, Systems and Computers, 2005. Conference Record of the Thirty-Ninth Asilomar Conference on*, 28 2005.

[58] E. Tekin and A. Yener. The gaussian multiple access wire-tap channel. *IEEE Trans. on Inform. Theory*, 54(12):5747–5755, 2008.

[59] E. Tekin and A. Yener. The general gaussian multiple-access and two-way wiretap channels: Achievable rates and cooperative jamming. *IEEE Trans. on Inform. Theory*, 54(6):2735–2751, 2008.

[60] Ender Tekin and Aylin Yener. Achievable rates for the general gaussian multiple access wire-tap channel with collective secrecy. *CoRR*, abs/cs/0612084, 2006.

[61] R. Tresch and M. Guillaud. Performance of interference alignment in clustered wireless ad hoc networks. In *Information Theory Proceedings (ISIT), 2010 IEEE International Symposium on*, pages 1703–1707. IEEE, 2010.

[62] S. Vasudevan, D. Goeckel, and D.F. Towsley. Security-capacity trade-off in large wireless networks using keyless secrecy. In *Proceedings of the eleventh ACM international symposium on Mobile ad hoc networking and computing*, pages 21–30. ACM, 2010.

[63] J.P. Vilela, P.C. Pinto, and J. Barros. Position-based jamming for enhanced wireless secrecy. *Information Forensics and Security, IEEE Transactions on*, 6(3):616–627, 2011.

[64] S. Weber, J.G. Andrews, and N. Jindal. An overview of the transmission capacity of wireless networks. *Communications, IEEE Transactions on*, 58(12):3593–3604, 2010.

[65] M.Z. Win, P.C. Pinto, and L.A. Shepp. A mathematical theory of network interference and its applications. *Proceedings of the IEEE*, 97(2):205–230, 2009.

[66] A. Wolf and E.A. Jorswieck. On the zero forcing optimality for friendly jamming in miso wiretap channels. In *Signal Processing Advances in Wireless Communications (SPAWC), 2010*, pages 1–5, 2010.

[67] A. D. Wyner. The Wire-tap Channel. *Bell Systems Technical Journal*, 54(8):1355–1387, January 1975.

[68] R. D. Yates, D. Tse, and Z. Li. Secure communication on interference channels. In *ISIT 2008*, 2008.

[69] L. Zhang, Y.C. Liang, Y. Pei, and R. Zhang. Robust beamforming design: From cognitive radio miso channels to secrecy miso channels. In *Global Telecommunications Conference, 2009. GLOBECOM 2009. IEEE*, pages 1–5. IEEE, 2009.

[70] X. Zhou, R.K. Ganti, J.G. Andrews, and A. Hjorungnes. On the throughput cost of physical layer security in decentralized wireless networks. *Wireless Communications, IEEE Transactions on*, 10(8):2764–2775, 2011.

[71] X. Zhou, M. Tao, and R. A. Kennedy. Cooperative jamming for secrecy in decentralized wireless networks. In *Proc. IEEE ICC*. IEEE, 2012.

[72] Xiangyun Zhou and M.R. McKay. Physical layer security with artificial noise: Secrecy capacity and optimal power allocation. In *3rd International Conference on Signal Processing and Communication Systems, 2009. ICSPCS 2009.*, pages 1–5, 2009.

[73] J. Zhu and S. Govindasamy. Performance of multi-antenna mmse receivers in non-homogeneous poisson networks. *arXiv preprint arXiv:1109.2964*, 2011.

VITA

Wei Shi was born in Zhuzhou City, Hunan Province, China, in 1982. He received the B.S. and M.S. degrees both from Automation Department from Tsinghua University, Beijing, China, in 2004 and 2007 respectively. He was an research intern at Mitsubishi Research Lab, Cambridge, MA, during summer 2011. Since January 2010, He has been working towards his Ph.D. degree working with Prof. James A. Ritcey in the Department of Electrical Engineering, University of Washington, Seattle. His research interests include multi-antenna communication systems, physical-layer security, stochastic geometry, and signal processing for wireless communications.

Publications

- Journals

1. W. Shi and J. A. Ritcey, "Cooperative transmit and jamming for maximizing secrecy rate of Gaussian MISO wiretap channels," *IEEE Trans. Commun.*, to be published.
2. W. Shi and J. A. Ritcey, "Performance of MMSE receiver: superposition property of multiple Poisson fields and its application to Poisson clustered interferers," *IEEE Trans. Wireless Commun.*, to be submitted.
3. W. Shi and J. A. Ritcey, "Distributed jamming protocol and secure throughput for Poisson fields of legitimate nodes and eavesdroppers," *IEEE Trans. Wireless Commun.*, to be submitted.
4. W. Shi and J. A. Ritcey, "Cooperative transmit and jamming design for uncertain MISO wiretap channels," in preparation for re-submission.
5. W. Shi and J. A. Ritcey, "Optimal transmit design for worst-case secrecy rate over uncertain MISO channels," in preparation for re-submission.

- Conferences

1. W. Shi and J. A. Ritcey, "Performance of MMSE multi-antenna receiver under hierarchial Poisson random fields of interferences," in *Proc. 46th Asilomar Conf. Signals, Systems and Computers*, Pacific Grove, CA, Nov. 2012.
2. W. Shi and J. A. Ritcey, "Distributed jamming for secure communication in a Poisson field of legitimate nodes and eavesdroppers," in *Proc. 46th Asilomar Conf. Signals, Systems and Computers*, Pacific Grove, CA, Nov. 2012.
3. W. Shi, R. Annavajjala, P. V. Orlik, and A. F. Molisch, "Non-coherent ToA estimation for UWB multipath channels using max-eigenvalue detection," in *Proc. of IEEE Int. Conf. Commun.*, Ottawa, Canada, June 2012.
4. W. Shi and J. A. Ritcey, "Transmit beamforming and cooperative jamming for MIMOME wiretap channels," in *Proc. 45th Asilomar Conf. Signals, Systems and Computers*, Pacific Grove, CA, Nov. 2011.
5. W. Shi and J. A. Ritcey, "Robust beamforming for MISO wiretap channel by optimizing the worst-case secrecy capacity," in *Proc. 44th Asilomar Conf. Signals, Systems and Computers*, Pacific Grove, CA, Nov. 2010.
6. W. Shi and S. Roy, "Achieving full diversity by selection in arbitrary multi-hop amplify-and-forward relay networks," *IEEE Globecom*, Honolulu, Hawaii, Dec. 2009.

- Software

1. Interference Analyzer for Multi-antenna Wireless Network (IA-MWiN) available at https://catalyst.uw.edu/workspace/jar7/33304/