Secure MISO Cognitive Radio System with Perfect and Imperfect CSI

Taesoo Kwon, Vincent W.S. Wong, and Robert Schober
Department of Electrical and Computer Engineering,
The University of British Columbia, Vancouver, Canada
Emails: {tskwon, vincentw, rschober}@ece.ubc.ca

***Abstract*—In cognitive radio (CR) systems, harmful interference from the secondary system degrades the data rate of the primary system. However, this interference may be beneficial to the primary system in terms of the secrecy rate, when unauthorized users eavesdrop on the primary link. This paper explores multiple-input single-output (MISO) CR systems where the secondary system secures the primary communication in return for permission to use the spectrum. In this context, the optimal transmission strategy has to be found which provides the best tradeoff between the useful and harmful effects of interference on the secrecy rate of the primary system. Considering the cases of perfect and imperfect channel state information of the eavesdroppers we formulate optimization problems for maximizing the primary secrecy rate under secondary data rate requirements. The resulting non-convex optimization problems are solved through a sequence of convex semidefinite programs. The simulation results reveal that the proposed schemes improve the secrecy level of the primary system while meeting the data rate requirements of the secondary system.**

I. Introduction

Cognitive radio (CR) is a promising technology to improve wireless spectrum utilization by conditionally allowing secondary systems to access the spectrum of the primary system. Thereby, the effect of the interference from the secondary system on the primary system should be minimized. In fact, in general, interference is harmful to the performance of wireless systems. However, recently it has been shown that in the context of secrecy, well-coordinated interference may actually be beneficial [1]–[5]. The idea of exploiting interference for secrecy can also be applied to CR systems [6]–[10].

The theoretical foundation of physical layer security dates back to the seminal work by Wyner [11], which showed that the source can deliver perfectly secure messages to the destination with a non-zero rate if the channel condition of the desired receiver is better than that of the eavesdropper. This basic concept was extended to actively degrading the link of the eavesdropper by exploiting artificial interference from other transmitters. The authors of [2], [3] studied scenarios where helper nodes cooperatively generate artificial noise to disturb the receptions of the eavesdroppers while minimizing interference to the legitimate receiver. In CR systems, if eavesdroppers overhear the primary link and treat interference as noise, the signals of secondary links can serve as both artificial noise for the secure primary link and data for their intended receivers. With respect to generating interference for secure communications, the operation of the secondary systems is similar to that of the helper nodes in [1]–[4], but helper nodes do not simultaneously serve their own receivers. This concept has recently been introduced in [6], [7]. The authors of [7] proposed a game-theoretic cooperation scenario between the primary and secondary systems where the primary users improve their secrecy level with the aid of secondary users. However, this work was limited to single-input single-output (SISO) systems. The work in [6] proposed a multiple-input single-output (MISO) beamforming algorithm for the secondary system. However, it only considered a CR system with a SISO primary link, a single MISO secondary link, and one eavesdropper, where the channel state information (CSI) of the eavesdropper is perfectly known. The authors of [9], [12] studied the case where the CSI of the eavesdroppers is estimated with a bounded error, but did not attempt to secure the primary communication through spectrum sharing.

This paper studies a general MISO system framework with a MISO primary link, multiple MISO secondary links, and multiple eavesdroppers. In this framework, the interference from a secondary transmitter is beneficial to the primary system while being harmful to other secondary links. Thus, the secondary system has to design its transmit beamforming vectors by taking into account the interference to the secondary users as well as the primary users and the eavesdroppers.

The main contributions of this paper are summarized as follows: To determine the optimal transmission strategy, we formulate the problem for maximizing primary secrecy rate under secondary data rate requirements using a semidefinite relaxation technique. We show that the relaxed non-convex optimization problem can be solved through a sequence of convex semidefinite programs (SDPs). Furthermore, we extend the problem to the case of imperfect eavesdropper CSI and find the optimal transmission strategy that maximizes the worst-case secrecy rate of the primary system. Finally, simulation results show that the proposed beamforming methods improve the secrecy rate and the worst-case secrecy rate of the primary system for the cases of perfect and imperfect eavesdropper CSI, respectively.

The rest of this paper is organized as follows: In Section II, we introduce the system model. In Sections III and IV, we present the design of the optimal transmit beamforming vectors for the cases of perfect and imperfect eavesdropper CSI, respectively. Simulation results are provided in Section V. Conclusions are given in Section VI.

Notation: Bold upper and lower case letters denote matrices and vectors, respectively. $(\cdot)^*$ denotes the conjugate transpose. $|\cdot|$ and $\|\cdot\|$ denote the absolute value of a scalar and the Euclidean norm of a vector, respectively. Matrix $\mathbf{I}_N$ denotes an $N \times N$ identity matrix. $\mathrm{Tr}(\mathbf{A})$ denotes the trace of matrix $\mathbf{A}$. $\mathbf{A} \succeq \mathbf{B}$ means that $\mathbf{A} - \mathbf{B}$ is positive semidefinite (PSD). $\mathbb{C}^N$ and $\mathbb{H}_+^N$ denote the sets of all N-dimensional complex vectors and PSD Hermitian matrices, respectively.

II. System Model

We consider a MISO CR system with a primary link, multiple eavesdroppers who overhear the primary signal, and multiple secondary links, as shown in Fig. 1. A primary transmitter with N_p antennas sends its signal to a primary receiver with a single antenna and needs to prevent eavesdroppers with a single antenna from overhearing its data. The secondary transmitters with N_s antennas want to send data to their own receivers using the spectrum of the primary system. They help to secure the primary communication in return for using the spectrum of the primary system. All primary and secondary receivers and eavesdroppers treat interference signals as noise. Eavesdroppers do not perform interference cancelation and are only interested in the primary signal. Under these assumptions the primary link achieves the following secrecy rate:

$$C^{(p)} = \log\left(1 + \Gamma^{(p)}\right) - \max_{k \in \mathcal{K}} \log\left(1 + \Gamma_k^{(e)}\right), \qquad (1)$$

where $\Gamma^{(p)}$ and $\Gamma_k^{(e)}$ denote the signal-to-interference-plus-noise ratios (SINRs) of the primary link and the k-th eavesdropper's link, respectively, and $\mathcal{K}$ denotes the set of eavesdroppers. Let $\mathcal{M}$ denote the set of secondary transmitters. Secondary transmitter m serves multiple secondary receivers denoted by (m,n) where $n \in \mathcal{N}_m$. Here, $\mathcal{N}_m$ is the set of secondary receivers served by secondary transmitter m. We use $\mathbf{h}^{(pp)}$, $\mathbf{h}_k^{(pe)}$, $\mathbf{h}_{mn}^{(ps)} \in \mathbb{C}^{N_p}$ and $\mathbf{h}_i^{(sp)}$, $\mathbf{h}_{ik}^{(se)}$, $\mathbf{h}_{imn}^{(ss)} \in \mathbb{C}^{N_s}$ to denote complex MISO channel vectors for the links between the nodes in the system; see Fig. 1 for details. Let the transmit beamforming vectors for serving the primary receiver and the (m,n)-th secondary receiver be denoted by $\mathbf{w}^{(p)}$ and $\mathbf{w}_{mn}^{(s)}$, respectively. Then, $\Gamma^{(p)}$ and $\Gamma_k^{(e)}$ are given by

$$\Gamma^{(p)} = \frac{|\mathbf{h}^{*(pp)}\mathbf{w}^{(p)}|^2}{\sum_{i\in\mathcal{M}}\sum_{j\in\mathcal{N}_i}|\mathbf{h}_i^{*(sp)}\mathbf{w}_{ij}^{(s)}|^2 + \sigma^2}\ , \qquad (2)$$

$$\Gamma_k^{(e)} = \frac{|\mathbf{h}_k^{*(pe)}\mathbf{w}^{(p)}|^2}{\sum_{i\in\mathcal{M}}\sum_{j\in\mathcal{N}_i}|\mathbf{h}_{ik}^{*(se)}\mathbf{w}_{ij}^{(s)}|^2 + \sigma^2}\ , \qquad (3)$$

where σ^2 denotes the noise variance. The SINR of secondary receiver (m,n), $\Gamma_{mn}^{(s)}$, is given by

$$\Gamma_{mn}^{(s)} = \frac{|\mathbf{h}_{mmn}^{*(ss)}\mathbf{w}_{mn}^{(s)}|^2}{|\mathbf{h}_{mn}^{*(ps)}\mathbf{w}^{(p)}|^2 + I_{mn}^{(ss)} + \sigma^2}\ , \qquad (4)$$

where $I_{mn}^{(ss)}$ is defined as $\sum_{j\in\mathcal{N}_m\setminus\{n\}}|\mathbf{h}_{mmn}^{*(ss)}\mathbf{w}_{mj}^{(s)}|^2 + \sum_{i\in\mathcal{M}\setminus\{m\}}\sum_{j\in\mathcal{N}_i}|\mathbf{h}_{imn}^{*(ss)}\mathbf{w}_{ij}^{(s)}|^2$. The achievable rate of the (m,n)-th secondary receiver is

$$C_{mn}^{(s)} = \log(1 + \Gamma_{mn}^{(s)})\ . \qquad (5)$$

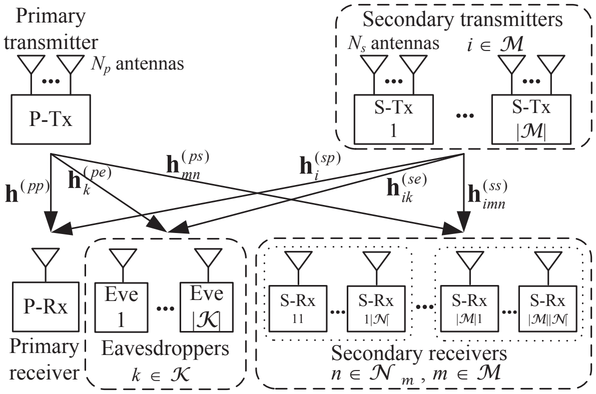

Fig. 1. System model for secure MISO cognitive radio system.

At first, we assume the full availability of CSI. As in the considered model the primary and secondary systems cooperate, they may share their CSI. Furthermore, the CSI of the eavesdroppers may be available when they are also users of the primary system. Nevertheless, accurate estimation of the eavesdroppers' CSI may still be difficult. Thus, in this paper, we consider the cases of perfect and imperfect eavesdropper CSI, respectively.

III. Primary Secrecy Rate with Perfect CSI

In this section, we aim to maximize the primary secrecy rate under constraints on the secondary data rates when the CSI of the eavesedroppers is perfectly known.

Considering that the primary transmitter and secondary transmitters have transmit power constraints of P_p and P_s, respectively, the problem can be formulated as

$$\underset{\mathbf{w}^{(p)},\{\mathbf{w}_{mn}^{(s)}\}}{\text{maximize}}\ C^{(p)} \qquad (6a)$$

$$\text{subject to } C_{mn}^{(s)} \geq R_{mn}^{(s)}, \quad \forall\, n \in \mathcal{N}_m, m \in \mathcal{M} \qquad (6b)$$

$$\|\mathbf{w}^{(p)}\|^2 \leq P_p \qquad (6c)$$

$$\sum_{n\in\mathcal{N}_m}\|\mathbf{w}_{mn}^{(s)}\|^2 \leq P_s,\ \forall\, m \in \mathcal{M}, \qquad (6d)$$

where the constant $R_{mn}^{(s)}$ is the minimum rate requirement of the (m,n)-th secondary receiver. This formulation is more general than the one in [6] which was limited to the optimization of one secondary beamforming vector to secure a SISO primary link against one eavesdropper. A primary transmitter with a single antenna cannot increase its secrecy level by itself while a primary transmitter with multiple antennas can maximize its secrecy rate through secure beamforming when the CSI of the eavesdroppers is known [12]. In problem (6), we consider the general case of a primary system with multiple transmit antennas and multiple eavesdroppers. In addition, problem (6) considers multiple secondary links, thus secondary transmit beamforming vectors are designed not only to secure a primary link but also to reduce the interference among secondary links. Problem (6) for the joint design of the primary and secondary beamforming vectors is non-convex and it is not easy to find its optimal solution. Thus, we relax and reformulate the problem in the following.

Let $\mathbf{W}^{(p)} = \mathbf{w}^{(p)}\mathbf{w}^{*(p)}$ and $\mathbf{W}^{(s)}_{mn} = \mathbf{w}^{(s)}_{mn}\mathbf{w}^{*(s)}_{mn}$. By using variables $\mathbf{W}^{(p)}$ and $\{\mathbf{W}^{(s)}_{mn}\}$ instead of $\mathbf{w}^{(p)}$ and $\{\mathbf{w}^{(s)}_{mn}\}$, the quadratic terms of $\mathbf{w}^{(p)}$ and $\{\mathbf{w}^{(s)}_{mn}\}$ in problem (6) can be expressed as PSD matrices, $\mathbf{W}^{(p)}$ and $\{\mathbf{W}^{(s)}_{mn}\}$, which have rank one. By relaxing the non-convex rank-one conditions of the PSD matrices, the relaxed constraint set of problem (6) becomes convex. Therefore, problem (6) is upper bounded by the following optimization problem:

$$\underset{\mathbf{W}^{(p)},\{\mathbf{W}^{(s)}_{mn}\}}{\text{maximize}} \quad \frac{1 + \frac{\mathrm{Tr}(\mathbf{W}^{(p)}\mathbf{H}^{(pp)})}{\sum_{i\in\mathcal{M}}\sum_{j\in\mathcal{N}_i}\mathrm{Tr}(\mathbf{W}^{(s)}_{ij}\mathbf{H}^{(sp)}_{i})+\sigma^2}}{1 + \max\limits_{k\in\mathcal{K}}\frac{\mathrm{Tr}(\mathbf{W}^{(p)}\mathbf{H}^{(pe)}_{k})}{\sum_{i\in\mathcal{M}}\sum_{j\in\mathcal{N}_i}\mathrm{Tr}(\mathbf{W}^{(s)}_{ij}\mathbf{H}^{(se)}_{ik})+\sigma^2}} \tag{7a}$$

$$\text{subject to} \quad \mathrm{Tr}(\mathbf{W}^{(s)}_{mn}\mathbf{H}^{(ss)}_{mmn}) - (2^{R^{(s)}_{mn}}-1)(I^{(s)}_{mn} + \sigma^2) \geq 0, \ \ \forall n\in\mathcal{N}_m, m\in\mathcal{M} \tag{7b}$$

$$\mathrm{Tr}(\mathbf{W}^{(p)}) \leq P_p \tag{7c}$$

$$\sum_{n\in\mathcal{N}_m}\mathrm{Tr}(\mathbf{W}^{(s)}_{mn}) \leq P_s, \ \forall m\in\mathcal{M} \tag{7d}$$

$$\mathbf{W}^{(p)} \succeq \mathbf{0} \tag{7e}$$

$$\mathbf{W}^{(s)}_{mn} \succeq \mathbf{0}, \quad \forall n\in\mathcal{N}_m, m\in\mathcal{M}, \tag{7f}$$

where $\mathbf{H}^{(pp)} = \mathbf{h}^{(pp)}\mathbf{h}^{*(pp)}$, $\mathbf{H}^{(pe)}_{k} = \mathbf{h}^{(pe)}_{k}\mathbf{h}^{*(pe)}_{k}$, $\mathbf{H}^{(ps)}_{mn} = \mathbf{h}^{(ps)}_{mn}\mathbf{h}^{*(ps)}_{mn}$, $\mathbf{H}^{(sp)}_{i} = \mathbf{h}^{(sp)}_{i}\mathbf{h}^{*(sp)}_{i}$, $\mathbf{H}^{(se)}_{ik} = \mathbf{h}^{(se)}_{ik}\mathbf{h}^{*(se)}_{ik}$, $\mathbf{H}^{(ss)}_{imn} = \mathbf{h}^{(ss)}_{imn}\mathbf{h}^{*(ss)}_{imn}$, and $I^{(s)}_{mn} = \mathrm{Tr}(\mathbf{W}^{(p)}\mathbf{H}^{(ps)}_{mn}) + \sum_{j\in\mathcal{N}_m\backslash\{n\}}\mathrm{Tr}(\mathbf{W}^{(s)}_{mj}\mathbf{H}^{(ss)}_{mmn}) + \sum_{i\in\mathcal{M}\backslash\{m\}}\sum_{j\in\mathcal{N}_i}\mathrm{Tr}(\mathbf{W}^{(s)}_{ij}\mathbf{H}^{(ss)}_{imn})$. Since the logarithm is a monotonic increasing function, objective function (6a) can be replaced by objective function (7a). Solving problem (7) is still difficult because objective function (7a) is non-concave. We introduce an auxiliary variable $\tau \triangleq 1 + \max_{k\in\mathcal{K}}\frac{\mathrm{Tr}(\mathbf{W}^{(p)}\mathbf{H}^{(pe)}_{k})}{\sum_{i\in\mathcal{M}}\sum_{j\in\mathcal{N}_i}\mathrm{Tr}(\mathbf{W}^{(s)}_{ij}\mathbf{H}^{(se)}_{ik})+\sigma^2}$. Using τ, problem (7) is rewritten as

$$\underset{\mathbf{W}^{(p)},\{\mathbf{W}^{(s)}_{mn}\},\tau}{\text{maximize}} \quad \frac{1}{\tau}\left(1 + \frac{\mathrm{Tr}(\mathbf{W}^{(p)}\mathbf{H}^{(pp)})}{\sum_{i\in\mathcal{M}}\sum_{j\in\mathcal{N}_i}\mathrm{Tr}(\mathbf{W}^{(s)}_{ij}\mathbf{H}^{(sp)}_{i}) + \sigma^2}\right) \tag{8a}$$

$$\text{subject to} \quad \mathrm{Tr}(\mathbf{W}^{(p)}\mathbf{H}^{(pe)}_{k}) - (\tau-1)(I^{(e)}_{k} + \sigma^2) \leq 0, \ \forall k\in\mathcal{K} \tag{8b}$$

$$\tau \leq 1 + \mathrm{Tr}(\mathbf{H}^{(pp)})P_p/\sigma^2 \tag{8c}$$

$$(7\text{b}) - (7\text{f}),$$

where $I^{(e)}_{k} = \sum_{i\in\mathcal{M}}\sum_{j\in\mathcal{N}_i}\mathrm{Tr}(\mathbf{W}^{(s)}_{ij}\mathbf{H}^{(se)}_{ik})$. By definition of τ, $\tau \geq 1$. In problem (8), the constraint of $\tau \geq 1$ is implicit in constraint (8b) because $\mathbf{W}^{(p)} \succeq \mathbf{0}$ and $\mathbf{W}^{(s)}_{mn} \succeq \mathbf{0}$. Constraint (8c) follows from the fact that the maximum SINR of eavesdroppers should not be larger than the primary SINR when we consider a nonnegative primary secrecy rate, i.e. $\tau \leq 1 + \frac{\mathrm{Tr}(\mathbf{W}^{(p)}\mathbf{H}^{(pp)})}{\sum_{i\in\mathcal{M}}\sum_{j\in\mathcal{N}_i}\mathrm{Tr}(\mathbf{W}^{(s)}_{ij}\mathbf{H}^{(sp)}_{i})+\sigma^2} \leq 1 + \mathrm{Tr}(\mathbf{H}^{(pp)})\frac{P_p}{\sigma^2}$.

The problem of maximizing a function can be solved by first maximizing over some of the variables, and then maximizing over the remaining ones [13].

Proposition 1: When τ is fixed, problem (8) can be represented as the following convex optimization problem, where $\mathbf{W}^{(p)} = \frac{\sigma^2}{\xi}\mathbf{Z}^{(p)}$ and $\mathbf{W}^{(s)}_{mn} = \frac{\sigma^2}{\xi}\mathbf{Z}^{(s)}_{mn}, \forall n\in\mathcal{N}_m, m\in\mathcal{M}$:

$$\underset{\mathbf{Z}^{(p)},\{\mathbf{Z}^{(s)}_{mn}\},\xi}{\text{maximize}} \ \mathrm{Tr}(\mathbf{Z}^{(p)}\mathbf{H}^{(pp)}) + \sum_{m\in\mathcal{M}}\sum_{n\in\mathcal{N}_m}\mathrm{Tr}(\mathbf{Z}^{(s)}_{mn}\mathbf{H}^{(sp)}_{m}) + \xi \tag{9a}$$

$$\text{subject to} \ \tau\left(\sum_{i\in\mathcal{M}}\sum_{j\in\mathcal{N}_i}\mathrm{Tr}(\mathbf{Z}^{(s)}_{ij}\mathbf{H}^{(sp)}_{i}) + \xi\right) = 1 \tag{9b}$$

$$\mathrm{Tr}(\mathbf{Z}^{(s)}_{mn}\mathbf{H}^{(ss)}_{mmn}) - (2^{R^{(s)}_{mn}}-1)(I'^{(s)}_{mn} + \xi) \geq 0, \ \forall n\in\mathcal{N}_m, m\in\mathcal{M} \tag{9c}$$

$$\mathrm{Tr}(\mathbf{Z}^{(p)}\mathbf{H}^{(pe)}_{k}) - (\tau-1)(I'^{(e)}_{k} + \xi) \leq 0, \ \forall k\in\mathcal{K} \tag{9d}$$

$$\mathrm{Tr}(\mathbf{Z}^{(p)}) \leq \xi P_p/\sigma^2 \tag{9e}$$

$$\sum_{n\in\mathcal{N}_m}\mathrm{Tr}(\mathbf{Z}^{(s)}_{mn}) \leq \xi P_s/\sigma^2, \ \forall m\in\mathcal{M} \tag{9f}$$

$$\mathbf{Z}^{(p)} \succeq \mathbf{0} \tag{9g}$$

$$\mathbf{Z}^{(s)}_{mn} \succeq \mathbf{0}, \quad \forall n\in\mathcal{N}_m, m\in\mathcal{M} \tag{9h}$$

$$\xi \geq 0, \tag{9i}$$

where $I'^{(s)}_{mn} = \mathrm{Tr}(\mathbf{Z}^{(p)}\mathbf{H}^{(ps)}_{mn}) + \sum_{j\in\mathcal{N}_m\backslash\{n\}}\mathrm{Tr}(\mathbf{Z}^{(s)}_{mj}\mathbf{H}^{(ss)}_{mmn}) + \sum_{i\in\mathcal{M}\backslash\{m\}}\sum_{j\in\mathcal{N}_i}\mathrm{Tr}(\mathbf{Z}^{(s)}_{ij}\mathbf{H}^{(ss)}_{imn})$, and $I'^{(e)}_{k} = \sum_{i\in\mathcal{M}}\sum_{j\in\mathcal{N}_i}\mathrm{Tr}(\mathbf{Z}^{(s)}_{ij}\mathbf{H}^{(se)}_{ik})$.

Proof: Please refer to Appendix A.

From Proposition 1, for given τ, problem (8) is a convex problem and the optimal solution can be found by the interior-point method [13]. When problem (9) is represented as a function of τ, $F(\tau)$, with domain $\{\tau \,|\, 1 \leq \tau \leq 1 + \mathrm{Tr}(\mathbf{H}^{(pp)})\frac{P_p}{\sigma^2}\}$, problem (7) is equivalent to

$$\underset{1\leq\tau\leq 1+\mathrm{Tr}(\mathbf{H}^{(pp)})\frac{P_p}{\sigma^2}}{\text{maximize}} \quad F(\tau). \tag{10}$$

Problem (10) is a single variable optimization problem which can be solved through a one-dimensional line search over τ. It means that relaxed problem (7) can be solved through a sequence of convex SDPs. If the optimal variables of problem (7) are of rank one, we can obtain the optimal beamforming vectors from them. Otherwise, in order to obtain an approximated solution for beamforming vectors, we can apply Gaussian randomization method [14]. However, an approximated solution yields a primary secrecy rate less than the optimal value of problem (10). The proposed beamforming design method is summarized in Algorithm 1.

IV. Worst-case Primary Secrecy Rate with Imperfect CSI

In this section, we model the imperfect eavesdropper CSI using an elliptically-bounded channel error model, and design robust beamforming vectors for maximization of the worst-case primary secrecy rate under secondary rate requirements.

Let $\bar{\mathbf{h}}^{(pe)}_{k} \in \mathbb{C}^{N_p}$ and $\bar{\mathbf{h}}^{(se)}_{mk} \in \mathbb{C}^{N_s}$ denote estimated CSI vectors, respectively. Then, $\mathbf{h}^{(pe)}_{k} = \bar{\mathbf{h}}^{(pe)}_{k} + \mathbf{e}^{(p)}_{k}$ and $\mathbf{h}^{(se)}_{mk} = \bar{\mathbf{h}}^{(se)}_{mk} + \mathbf{e}^{(s)}_{mk}$, where $\mathbf{e}^{(p)}_{k}$ and $\mathbf{e}^{(s)}_{mk}$ denote the channel error vectors such that $\mathbf{e}^{(p)}_{k} \in \mathcal{E}^{(p)}_{k} \triangleq \{\mathbf{e}^{(p)}_{k} \in$

Algorithm 1 Secure MISO Beamforming for CR System.

```
Initialization: Set $\tau_{max}$ to $1+\mathrm{Tr}(\mathbf{H}^{(pp)})P_p/\sigma^2$
Find $\hat{\tau}$ which maximizes $F(\tau)$ by applying one-dimensional line search method, e.g. the golden section method, on interval $[1,\tau_{max}]$
Set the optimal solution of (9) for $\hat{\tau}$ to $(\hat{\mathbf{Z}}^{(p)},\hat{\mathbf{Z}}^{(s)}_{mn},\hat{\xi})$
$\hat{\mathbf{W}}^{(p)} \leftarrow \frac{\sigma^2}{\hat{\xi}}\hat{\mathbf{Z}}^{(p)}$, $\hat{\mathbf{W}}^{(s)}_{mn} \leftarrow \frac{\sigma^2}{\hat{\xi}}\hat{\mathbf{Z}}^{(s)}_{mn}$, $\forall\,(m,n)$
if $\mathrm{rank}(\hat{\mathbf{W}}^{(p)})=1$ and $\mathrm{rank}(\hat{\mathbf{W}}^{(s)}_{mn})=1,\forall\,(m,n)$ then
    Apply matrix decomposition to find $\hat{\mathbf{w}}^{(p)}$ and $\{\hat{\mathbf{w}}^{(s)}_{mn}\}$
else
    Apply Gaussian randomization method [14] to find an approximated solution $(\hat{\mathbf{w}}^{(p)},\{\hat{\mathbf{w}}^{(s)}_{mn}\})$ of problem (6), from $(\hat{\mathbf{W}}^{(p)},\{\hat{\mathbf{W}}^{(s)}_{mn}\})$ with rank greater than one
end if
```

$\mathbb{C}^{N_p}\,|\,\mathbf{e}^{*(p)}_k\mathbf{Q}^{(p)}_k\mathbf{e}^{(p)}_k \le 1\},\forall\,k\in\mathcal{K}$ and $\mathbf{e}^{(s)}_{mk}\in\mathcal{E}^{(s)}_{mk}\triangleq\{\mathbf{e}^{(s)}_{mk}\in\mathbb{C}^{N_s}\,|\,\mathbf{e}^{*(s)}_{mk}\mathbf{Q}^{(s)}_{mk}\mathbf{e}^{(s)}_{mk}\le 1\},\forall\,m\in\mathcal{M},k\in\mathcal{K}$. Here, $\mathbf{Q}^{(p)}_k\in\mathbb{H}^{N_p}_+$ and $\mathbf{Q}^{(s)}_k\in\mathbb{H}^{N_s}_+$.

The worst-case secrecy rate, $\tilde{C}^{(p)}$, can be expressed as

$$\tilde{C}^{(p)}=\log\left(1+\Gamma^{(p)}\right) - \max_{k\in\mathcal{K}}\left(\max_{\mathbf{e}^{(p)}_k\in\mathcal{E}^{(p)}_k,\{\mathbf{e}^{(s)}_{mk}\in\mathcal{E}^{(s)}_{mk}\}}\log\left(1+\Gamma^{(e)}_k\right)\right).\tag{11}$$

We introduce an auxiliary variable $\tilde{\tau}\triangleq\max_{k\in\mathcal{K}}\left(\max_{\mathbf{e}^{(p)}_k\in\mathcal{E}^{(p)}_k,\{\mathbf{e}^{(s)}_{mk}\in\mathcal{E}^{(s)}_{mk}\}}1+\Gamma^{(e)}_k\right)$. Then, the problem for the design of secure and robust beamforming vectors can be formulated as

$$\underset{\mathbf{W}^{(p)},\{\mathbf{W}^{(s)}_{mn}\},\tilde{\tau}}{\text{maximize}}\ \frac{1}{\tilde{\tau}}\left(1+\frac{\mathrm{Tr}(\mathbf{W}^{(p)}\mathbf{H}^{(pp)})}{\sum_{i\in\mathcal{M}}\sum_{j\in\mathcal{N}_i}\mathrm{Tr}(\mathbf{W}^{(s)}_{ij}\mathbf{H}^{(sp)}_i)+\sigma^2}\right)\tag{12a}$$

$$\text{subject to}\quad \tilde{\tau}-1\ge\max_{\mathbf{e}^{(p)}_k\in\mathcal{E}^{(p)}_k,\{\mathbf{e}^{(s)}_{mk}\in\mathcal{E}^{(s)}_{mk}\}}\Gamma^{(e)}_k,\forall\,k\in\mathcal{K}\tag{12b}$$

$$\tilde{\tau}\le 1+\mathrm{Tr}(\mathbf{H}^{(pp)})P_p/\sigma^2\tag{12c}$$

$$(7\text{b})-(7\text{f}).$$

Similar to the case of perfect CSI, constraint (12c) follows from the definition of $\tilde{\tau}$ and the nonnegativity of primary secrecy rate. Using the same approach as in Proposition 1, it can be shown that, for a fixed τ, problem (12) can be rewritten as

$$\underset{\mathbf{Z}^{(p)},\,\{\mathbf{Z}^{(s)}_{mn}\},\,\xi}{\text{maximize}}\ \mathrm{Tr}(\mathbf{Z}^{(p)}\mathbf{H}^{(pp)})+\sum_{m\in\mathcal{M}}\sum_{n\in\mathcal{N}_m}\mathrm{Tr}(\mathbf{Z}^{(s)}_{mn}\mathbf{H}^{(sp)}_m)+\xi\tag{13a}$$

$$\text{subject to}\quad \tilde{\tau}\left(\sum_{i\in\mathcal{M}}\sum_{j\in\mathcal{N}_i}\mathrm{Tr}\left(\mathbf{Z}^{(s)}_{ij}\mathbf{H}^{(sp)}_i\right)+\xi\right)=1\tag{13b}$$

$$(12\text{b}),(9\text{c}),(9\text{e})-(9\text{i}).$$

However, constraint (12b) has a semi-infinite constraint for each k. This constraint can be transformed into linear matrix inequalities (LMIs) using the $\mathcal{S}$-procedure [13].

Proposition 2: Let $\mathbf{W}^{(p)}=\frac{\sigma^2}{\xi}\mathbf{Z}^{(p)}$ and $\mathbf{W}^{(s)}_{mn}=\frac{\sigma^2}{\xi}\mathbf{Z}^{(s)}_{mn},\forall\,n\in\mathcal{N}_m,m\in\mathcal{M}$. Problem (13) can be transformed to the following convex optimization problem.

$$\underset{\substack{\mathbf{Z}^{(p)},\{\mathbf{Z}^{(s)}_{mn}\},\xi\\\{u_{mk}\},\{\alpha_k\},\{\beta_{mk}\}}}{\text{maximize}}\ \mathrm{Tr}(\mathbf{Z}^{(p)}\mathbf{H}^{(pp)})+\sum_{m\in\mathcal{M}}\sum_{n\in\mathcal{N}_m}\mathrm{Tr}(\mathbf{Z}^{(s)}_{mn}\mathbf{H}^{(sp)}_m)+\xi\tag{14a}$$

$$\text{subject to}\quad (13\text{b}),(9\text{c}),(9\text{e})-(9\text{i})$$

$$\mathbf{\Phi}_k\succeq\mathbf{0},\qquad\forall\,k\in\mathcal{K}\tag{14b}$$

$$\mathbf{\Psi}_{mk}\succeq\mathbf{0},\qquad\forall\,m\in\mathcal{M},k\in\mathcal{K}\tag{14c}$$

$$\alpha_k\ge 0,\qquad\forall\,k\in\mathcal{K}\tag{14d}$$

$$\beta_{mk}\ge 0,\qquad\forall\,m\in\mathcal{M},k\in\mathcal{K},\tag{14e}$$

where

$$\mathbf{\Phi}_k=\begin{bmatrix}-\mathbf{Z}^{(p)}+\alpha_k\mathbf{Q}^{(p)}_k & -\mathbf{Z}^{(p)}\bar{\mathbf{h}}^{(pe)}_k\\ -\bar{\mathbf{h}}^{*(pe)}_k\mathbf{Z}^{(p)} & \phi_k\end{bmatrix},\tag{15}$$

$$\mathbf{\Psi}_{mk}=\begin{bmatrix}\mathbf{Z}^{(s)}_m+\beta_{mk}\mathbf{Q}^{(s)}_{mk} & \mathbf{Z}^{(s)}_m\bar{\mathbf{h}}^{(se)}_{mk}\\ \bar{\mathbf{h}}^{*(se)}_{mk}\mathbf{Z}^{(s)}_m & \psi_{mk}\end{bmatrix},\tag{16}$$

$\phi_k=-\bar{\mathbf{h}}^{*(pe)}_k\mathbf{Z}^{(p)}\bar{\mathbf{h}}^{(pe)}_k+(\tilde{\tau}-1)\left(\sum_{i\in\mathcal{M}}u_{ik}+\xi\right)-\alpha_k$, $\psi_{mk}=\bar{\mathbf{h}}^{*(se)}_{mk}\mathbf{Z}^{(s)}_m\bar{\mathbf{h}}^{(se)}_{mk}-u_{mk}-\beta_{km}$, and $\mathbf{Z}^{(s)}_m\triangleq\sum_{j\in\mathcal{N}_m}\mathbf{Z}^{(s)}_{mj}$.

Proof: This proof shows that problem (13) is equivalent to problem (14). In other words, it is shown that constraint (12b) can be rewritten as (14b)-(14e). Because all CSI errors are independent, the constraint in (12b) for $\mathbf{Z}^{(p)}$ and $\{\mathbf{Z}^{(s)}_{mn}\}$ can be rewritten as

$$\max_{\mathbf{e}^{(p)}_k\in\mathcal{E}^{(p)}_k}\left(\bar{\mathbf{h}}^{(pe)}_k+\mathbf{e}^{(p)}_k\right)^*\mathbf{Z}^{(p)}\left(\bar{\mathbf{h}}^{(pe)}_k+\mathbf{e}^{(p)}_k\right)\le(\tilde{\tau}-1)\left(\sum_{i\in\mathcal{M}}u_{ik}+\xi\right),\ \ \forall\,k\in\mathcal{K},\tag{17}$$

where $u_{ik}\triangleq\min_{\mathbf{e}^{(s)}_{ik}\in\mathcal{E}^{(s)}_{ik}}(\bar{\mathbf{h}}^{(se)}_{ik}+\mathbf{e}^{(s)}_{ik})^*\mathbf{Z}^{(s)}_i(\bar{\mathbf{h}}^{(se)}_{ik}+\mathbf{e}^{(s)}_{ik})$. Using the $\mathcal{S}$-procedure, (17) can be transformed into LMIs, i.e., (14b) and (14c). ■

When problem (14) is represented as a function $\tilde{F}(\tau)$, problem (12) can be reformulated into the following single variable optimization problem:

$$\underset{1\le\tilde{\tau}\le 1+\mathrm{Tr}(\mathbf{H}^{(pp)})\frac{P_p}{\sigma^2}}{\text{maximize}}\ \tilde{F}(\tilde{\tau}).\tag{18}$$

Therefore, an algorithm to find the optimal beamforming vectors can be designed, similar to Algorithm 1.

V. Performance Evaluation

In this section, we evaluate the performance of the beamforming design methods proposed in Sections III and IV, via simulations. Problems (7) and (12) may not always be feasible when the constraints are tight or the channel realizations are poor. If the problems are infeasible, the primary transmitter

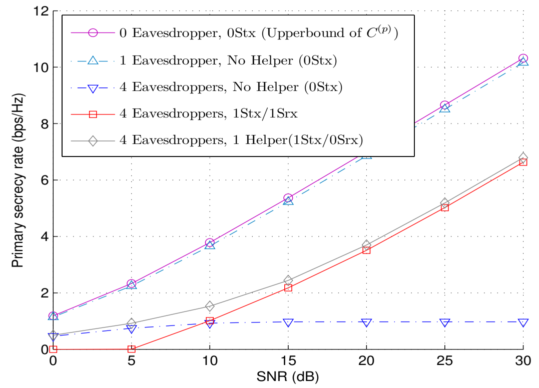

Fig. 2. Primary secrecy rate vs. SNR ($N_p = N_s = 2$, $R^{(s)} = 2$).

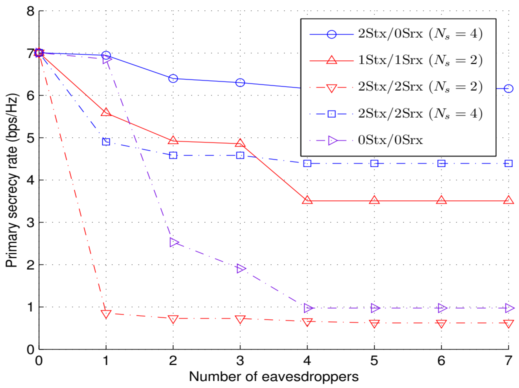

Fig. 4. Primary secrecy rate vs. number of eavesdroppers ($\text{SNR}_p = \text{SNR}_s = 20\,\text{dB}$, $R^{(s)} = 2$).

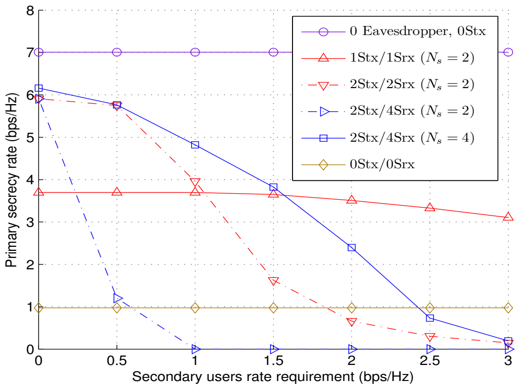

Fig. 3. Primary secrecy rate vs. secondary rate requirement ($\text{SNR}_p = \text{SNR}_s = 20\,\text{dB}$, four eavesdroppers).

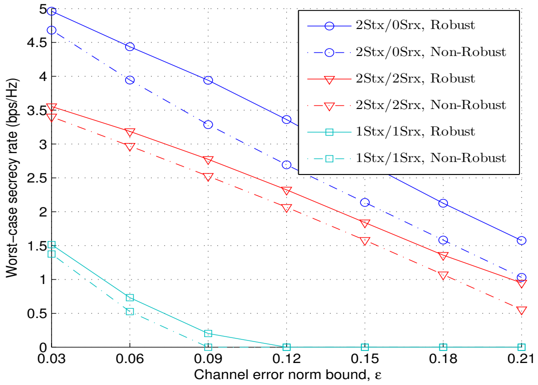

Fig. 5. Comparison of robust and non-robust beamforming design methods ($\text{SNR}_p = \text{SNR}_s = 20\,\text{dB}$, $N_p = N_s = 2$, $R^{(s)} = 1$).

cannot send secure messages to its desired receiver with a non-zero secrecy rate. In this section, we evaluate the performance only for the case when the problems are feasible. Figs. 2 - 4 show the results for perfectly-known eavesdropper CSI. For the transmit powers, $P_p = P_s$ holds, and all channels are randomly generated following an independent and identically distributed (i.i.d.) complex Gaussian distribution with zero mean and unit variance. In this section, a helper means a secondary transmitter that does not have its own receiver but only secures the primary communication. The notation MStx/NSrx in the legends of Figs. 3 - 5 means that there are M secondary transmitters, each of which serves N/M secondary receivers. The case of $M>0$ and $N=0$ means that M secondary transmitters serve only as helper nodes.

Fig. 2 presents the effect of secondary transmissions on the primary secrecy rate. When there is an eavesdropper, the primary system can achieve a secrecy rate similar to its data rate, which is the upper bound of $C^{(p)}$, by sending its data in the nullspace of eavesdroppers. In case of four eavesdroppers, the secrecy rate decreases abruptly. When a helper transmits artificial interference, the secrecy rate increases again. As long as the SNR is not too low, the secondary system can serve its own link with the required rate of 2 bps/Hz, with very small performance degradation of the primary system, compared to the case with no secondary receiver.

Fig. 3 shows the primary secrecy rate as a function of the secondary rate requirement for each secondary link. In this figure, a zero secondary rate requirement means that the secondary transmitters serve as helpers only. The results show that the secondary system does not only increase the primary secrecy rate by many folds, compared to the case of not sharing the spectrum, but also achieve non-zero data rate for each secondary link. Moreover, it is observed that there exists the rates that the secondary system can achieve without affecting the primary secrecy rate severely compared to the case where the secondary transmitters serve as helpers only, e.g. 0 to 1.5 bps/Hz in the scenario of 1Stx/1Srx in Fig. 3.

In Fig. 4, the effect of the number of eavesdroppers is investigated. In this figure, it is observed that the case of two secondary transmitters with two antennas, each of which has a single receiver, has a lower performance than the case without any helper. Because the secondary rate requirement is too tight to lead to a satisfactory performance for the case of only two antennas, the secondary system cannot help in securing the communication of the primary system. Thus, we need more spatial degrees of freedom for the secondary system to increase the secrecy rate.

In Fig. 5, we compare the non-robust beamforming design of Section III and the robust beamforming design of Section IV, when the eavesdroppers' channels are not known perfectly. The simulation assumes that $\mathbf{Q}_k^{(p)} = \frac{1}{\varepsilon^2}\mathbf{I}_{N_p}$ and $\mathbf{Q}_{mk}^{(s)} = \frac{1}{\varepsilon^2}\mathbf{I}_{N_s}$, i.e., the magnitude of the channel error vectors are bounded by ε. The performance measure is the worst-case secrecy rate. The non-robust method designs the beamforming vectors using estimated channels for the eavesdroppers' links while the robust method designs them based on the worst-case channel. Therefore, the non-robust method experiences a performance degradation because of these errors. Fig. 5 shows that the robust beamforming vector design yields much better worst-case secrecy rates than the non-robust design.

The beamforming vector design methods in Sections III and IV provide the optimal solution for maximizing the secrecy rate of the primary system when $\mathbf{W}^{(p)}$ and $\{\mathbf{W}_{mn}^{(s)}\}$ have rank-one. For all results presented in this section, the solutions were numerically found to have rank one.

VI. Conclusions

In this paper, we studied MISO cognitive radio (CR) systems where the primary system is more secured with the aid of secondary users. It is shown that the spectrum sharing with the secondary system can increase the primary secrecy rate much more, compared to the case where the primary system with multiple antennas improves its secrecy rate through only its own secure beamforming. The problem was formulated as a non-convex optimization problem to maximize the primary secrecy rate under constraints on the secondary date rates. Moreover, in case of imperfect CSI of the eavesdroppers' links, we formulated the problem as a non-convex optimization problem with semi-infinite constraints. We solved the considered problems via a sequence of convex semidefinite optimization problems. Simulation results showed that the proposed beamforming methods increased the secrecy rate and the worst-case secrecy rate of the primary system while meeting the secondary data rate requirements. An interesting topic for future work is the study of secure MISO CR systems for the case when the CSI of the eavesdroppers' links is completely unknown.

Appendix A
Proof of Proposition 1

For fixed τ, by the change of variables $\mathbf{W}^{(p)} = \frac{\sigma^2}{\xi}\mathbf{Z}^{(p)}$, $\mathbf{W}_{mn}^{(s)} = \frac{\sigma^2}{\xi}\mathbf{Z}_{mn}^{(s)}, \forall n \in \mathcal{N}_m, m \in \mathcal{M}$, where $\xi > 0$, problem (8) can be transformed into

$$\underset{\mathbf{Z}^{(p)},\{\mathbf{Z}_{mn}^{(s)}\},\xi}{\text{maximize}} \quad \frac{\mathrm{Tr}(\mathbf{Z}^{(p)}\mathbf{H}^{(pp)}) + \sum_{m\in\mathcal{M}}\sum_{n\in\mathcal{N}_m}\mathrm{Tr}(\mathbf{Z}_{mn}^{(s)}\mathbf{H}_m^{(sp)}) + \xi}{\tau\left(\sum_{m\in\mathcal{M}}\sum_{n\in\mathcal{N}_m}\mathrm{Tr}\left(\mathbf{Z}_{mn}^{(s)}\mathbf{H}_m^{(sp)}\right) + \xi\right)} \tag{19a}$$

$$\begin{aligned} \text{subject to} \quad & (9c) - (9h) \\ & \xi > 0. \end{aligned} \tag{19b}$$

By applying the Charnes-Cooper transformation [15], problem (19) is equivalent to

$$\underset{\mathbf{Z}^{(p)},\{\mathbf{Z}_{mn}^{(s)}\},\xi}{\text{maximize}} \quad \mathrm{Tr}(\mathbf{Z}^{(p)}\mathbf{H}^{(pp)}) + \sum_{m\in\mathcal{M}}\sum_{n\in\mathcal{N}_m}\mathrm{Tr}(\mathbf{Z}_{mn}^{(s)}\mathbf{H}_m^{(sp)}) + \xi \tag{20a}$$

$$\text{subject to} \quad \tau\left(\sum_{i\in\mathcal{M}}\sum_{j\in\mathcal{N}_i}\mathrm{Tr}\left(\mathbf{Z}_{ij}^{(s)}\mathbf{H}_i^{(sp)}\right) + \xi\right) = 1 \tag{20b}$$

$$(9c) - (9h)$$

$$\xi > 0. \tag{20c}$$

If ξ is equal to zero, then from constraints (9f) and (9h), we have $\mathbf{Z}_{mn}^{(s)} = \mathbf{0}, \forall n \in \mathcal{N}_m, m \in \mathcal{M}$. Because this violates constraint (9b), $\xi > 0$ must hold and $\xi \geq 0$ can be used instead of $\xi > 0$. Therefore, problem (9) is equivalent to problem (8) for fixed τ. ■

Acknowledgment

This research is supported by the Natural Sciences and Engineering Research Council (NSERC) of Canada.

References

[1] X. Tang, R. Liu, P. Spasojevic, and H. V. Poor, "Interference assisted secret communication," *IEEE Trans. on Information Theory*, vol. 57, no. 5, pp. 3153–3167, May 2011.

[2] J. Wang and A. L. Swindlehurst, "Cooperative jamming in MIMO ad-hoc networks," in *Proc. of Asilomar Conf. Signals, Systems and Computers*, Monterey, CA, Nov. 2009.

[3] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperative relays," *IEEE Trans. on Signal Processing*, vol. 58, no. 3, pp. 1875–1888, Mar. 2010.

[4] G. Zheng, L.-C. Choo, and K.-K. Wong, "Optimal cooperative jamming to enhance physical layer security using relays," *IEEE Trans. on Signal Processing*, vol. 59, no. 3, pp. 1317–1322, Mar. 2011.

[5] J. Li, A. P. Petropulu, and S. Weber, "On cooperative relaying schemes for wireless physical layer security," *IEEE Trans. on Signal Processing*, vol. 59, no. 10, pp. 4985–4997, Oct. 2011.

[6] K. Lee, O. Simeone, C.-B. Chae, and J. Kang, "Spectrum leasing via cooperation for enhanced physical-layer secrecy," in *Proc. of IEEE Int'l Conf. on Commun. (ICC)*, Kyoto, Japan, Jun. 2011.

[7] Y. Wu and K. J. R. Liu, "An information secrecy game in cognitive radio networks," *IEEE Trans. on Inf. Forensics and Security*, vol. 6, no. 3, pp. 831–842, Sep. 2011.

[8] Y. Pei, Y.-C. Liang, L. Zhang, K. C. Teh, and K. H. Li, "Secure communication over MISO cognitive radio channels," *IEEE Trans. on Wireless Commun.*, vol. 9, no. 4, pp. 1494–1502, Apr. 2010.

[9] Y. Pei, Y.-C. Liang, K. C. Teh, and K. H. Li, "Secure communication in multiantenna cognitive radio networks with imperfect channel state information," *IEEE Trans. on Signal Processing*, vol. 59, no. 4, pp. 1683–1693, Apr. 2011.

[10] J. Zhang and M. C. Gursoy, "Secure relay beamforming over cognitive radio channels," in *Proc. of Conf. Inform. Sci. and Systems (CISS)*, Princeton, NJ, Mar. 2011.

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

[12] Q. Li and W.-K. Ma, "Optimal and robust transmit designs for MISO channel secrecy by semidefinite programming," *IEEE Trans. on Signal Processing*, vol. 59, no. 8, pp. 3799–3812, Aug. 2011.

[13] S. Boyd and L. Vandenberghe, *Convex Optimization.* Cambridge University Press, 2007.

[14] Z. Q. Luo, W. K. Ma, A. M. C. So, Y. Ye, and S. Zhang, "Semidefinite relaxation of quadratic optimization problems," *IEEE Signal Processing Mag.*, vol. 27, no. 3, pp. 20–34, May 2010.

[15] A. Charnes and W. W. Coopper, "Programming with linear fractional functionals," *Naval Research Logistics Quarterly*, vol. 9, pp. 181–186, 1962.