Secure Communication in Multiantenna Cognitive Radio Networks With Imperfect Channel State Information

Yiyang Pei, *Student Member, IEEE*, Ying-Chang Liang, *Fellow, IEEE*, Kah Chan Teh, *Senior Member, IEEE*, and Kwok Hung Li, *Senior Member, IEEE*

***Abstract*—In this paper, we address the issue of optimal transmitter design to achieve physical layer security for a multiple-input single-output (MISO) cognitive radio network (CRN), in which a secondary user transmitter (SU-Tx) sends confidential information to a SU receiver (SU-Rx) on the same frequency band with a primary user (PU) in the presence of an eavesdropper receiver (ED-Rx). It is assumed that all the channel state information (CSI) of the secondary, primary and eavesdropper channels is not perfectly known at the SU-Tx. The optimal transmitter design, under the restriction of Gaussian signaling without preprocessing of information, involves a nonconvex semiinfinite optimization problem which maximizes the rate of the secondary link while avoiding harmful interference to the PU and keeping the eavesdropper totally ignorant of the messages sent regardless of the uncertainties in the CSI. We propose two approaches to solve this challenging optimization problem. The first one relates the original problem to a sequence of semiinfinite capacity-achieving transmitter design problems in an auxiliary CRN without any eavesdropper, which can then be solved through transformations and using convex semidefinite programs (SDPs). The second approach explores the hidden convexity of the problem and hence transforms it into a single SDP, which significantly reduces the computational complexity. Furthermore, a few heuristic beamforming solutions for the ease of implementation are also introduced. Finally, simulation results are presented to evaluate the performance of the proposed optimal and suboptimal solutions.**

***Index Terms*—Cognitive radio, imperfect channel state information, multiple antennas, secrecy rate, spectrum sharing.**

I. Introduction

THE use of cognitive radio (CR) has been widely recognized as an effective way to improve the utilization efficiency of the radio spectrum by allowing unlicensed secondary users (SUs) to coexist either opportunistically or concurrently with the licensed primary users (PUs). In the spectrum sharing cognitive radio networks (CRNs) where concurrent transmission is permitted, the quality of service (QoS) of the PUs is usually ensured by imposing the interference power constraints to restrict the interference power at the PU receivers (PU-Rx) to be below the *interference temperature limit* [1]. Under such a setup, many research works have been conducted from the information-theoretic perspective to identify the optimal transmission strategy to achieve *cognitive transmission*, i.e., the maximum rate of reliable communication over the secondary channel (i.e., channel from the SU transmitter (SU-Tx) to the SU receiver (SU-Rx)) while mitigating the interference over the primary channel (i.e., channel from the SU-Tx to the PU-Rx) [2]. In particular, the use of multiple antennas has been found to improve cognitive transmission substantially [3].

In addition to cognitive transmission, security issues are also crucial to CRNs. The unique characteristics of CR make CRNs even more susceptible to security threats than any conventional wireless communication systems. In particular, eavesdropping becomes much easier for a malicious user because of the capability for a future CR device to sense a wide range of radio spectrum. In this paper, we focus on the physical layer techniques to protect the confidentiality of information from the potential eavesdroppers. The theoretical foundation to study the secure communication at the physical layer is the wiretap channel and the information-theoretic notion of secrecy introduced by Wyner [4]. The basic wiretap channel describes the communication scenario involving three terminals: a transmitter, a legitimate receiver and an eavesdropper. The transmitter intends to transmit some information to the legitimate receiver but wants to keep the information secret from the eavesdropper. The level of secrecy is measured by the equivocation rate, which is defined as the entropy rate of the confidential information conditioned on the eavesdropper's observation. Clearly, higher equivocation rate indicates higher level of secrecy. In the extreme case, when the equivocation rate equals the transmission rate, we can achieve perfect secrecy, i.e., the eavesdropper cannot decode at any positive rate. The maximum rate of communication at which the information can be decoded with arbitrarily small probability of error at the legitimate receiver and with perfect secrecy rate at the eavesdropper is defined as *secrecy capacity*. Following Wyner's approach, many researchers have been working on extending the original degraded discrete memoryless wiretap channel to many other channel models and characterizing the corresponding secrecy capacity [5]–[7] etc. The use of multiple antennas for achieving secure transmission has also received a great deal of attention recently. In [8]–[10], the secrecy capacity for the point-to-point Gaussian multiple-antenna wiretap channels has been characterized.

The first attempt to address the secure transmission in a CRN from the information-theoretic perspective was made in [11]

Manuscript received February 25, 2010; revised August 10, 2010, December 01, 2010; accepted December 18, 2010. Date of publication February 14, 2011; date of current version March 09, 2011. The associate editor coordinating the review of this paper and approving it for publication was Prof. Amir Leshem.

Y. Pei and Y.-C. Liang are with the School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore 639798. They are also with Institute for Infocomm Research, Connexis, Singapore 138632 (e-mail: peiy0002@ntu.edu.sg; ycliang@i2r.a-star.edu.sg).

K. C. Teh and K. H. Li are with the School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore 639798 (e-mail: ekcteh@ntu.edu.sg; ekhli@ntu.edu.sg).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TSP.2011.2105479

and [12]. A *secure multiple-input single-output (MISO) CR channel*, in which a multiantenna SU-Tx sends confidential information to a single-antenna SU-Rx in the presence of a single-antenna PU-Rx and a single-antenna eavesdropper receiver (ED-Rx), was considered. The secrecy capacity is defined as the maximum rate of achieving both cognitive and secure transmission and has been characterized as a quasi-convex optimization problem involving transmit covariance matrix under the joint transmit power and interference power constraints. Efficient numerical solution has been developed to derive the optimal transmission strategy. However, the results presented in [11], [12] can only serve as the upper bounds for the secure transmission in the MISO CRN since the availability of perfect channel state information (CSI) of all the relevant channels is assumed at the SU-Tx. This CSI may not be obtained perfectly in practice due to the channel estimation and quantization errors, and the loose cooperation between the SU and the PU. This motivates the study of this paper, which aims to address the secure communication in the MISO CRNs in the context of imperfect knowledge of all the relevant channels at the SU-Tx. In such cases, robust design techniques have to be identified so that the cognitive and secure transmission strategy is less sensitive to the uncertainty in the CSI.

To address the system design in the context of imperfect CSI, two popular approaches have been adopted in the literature, namely, stochastic (Bayesian) approach and worst-case (maximin) approach. Assuming the CSI is a Gaussian random variable with only mean and covariance known to the transmitter, stochastic approach has been widely used to optimize the system performance with some statistical measures. Prior work along this line for multiantenna channels can be found in [13] and the references therein. On the other hand, in the worst-case approach, the CSI is assumed to belong to a given uncertainty set but the actual realization of the channel is not known to the transmitter. Under this scenario, the system is designed to optimize the worst-case performance measure. Prior work on the worst-case design for multiantenna systems can be found in [14]–[16]. The latter approach is adopted in this paper.

In the context of CRNs, studies on the robust transmitter design have been initiated by [17] for the MISO channel using the worst-case approach. However, the paper considered only the uncertainty in the primary channel. Later, the worst-case robust design has been investigated for MISO multicast channel [18] and MISO broadcast channel [19] when the uncertainty exists in both the secondary and primary channels under beamforming strategy.

In this paper, our objective is to design the transmission strategy under Gaussian signaling without preprocessing of information such that the secrecy rate of the secure MISO CRN is maximized and at the same time the PU-Rx is sufficiently protected under the interference power constraint for all the possible realizations of the CSI within the uncertainty sets. The design is formulated as a maximin nonconvex semiinfinite optimization problem, which is difficult to solve in its direct form. Two approaches are presented to find the optimal solution. Furthermore, a few beamforming solutions for the ease of implementation are proposed. Finally, the performance of the optimal and suboptimal algorithms is evaluated through computer simulations.

The rest of the paper is organized as follows. In Section II, we describe the system model of the secure MISO CRN with CSI uncertainties at the SU-Tx and formulate the optimization problem to maximize the secrecy rate under the joint transmit and interference power constraints for all the channel realizations within the uncertainty sets. Optimal and suboptimal algorithms to obtain the transmission strategies are proposed in Sections III and IV, respectively. The performance of the proposed algorithms is evaluated through simulations in Section V. Finally, conclusion is drawn in Section VI.

The following notations are used in this paper. Matrices and vectors are denoted using boldface upper and lower-case letters, respectively. The conjugate transpose and trace of a matrix $\boldsymbol{M}$ are denoted by $\boldsymbol{M}^{\dagger}$ and $\mathrm{tr}(\boldsymbol{M})$, respectively. $\boldsymbol{S} \succeq 0$ means that $\boldsymbol{S}$ is a positive semidefinite matrix. $\boldsymbol{I}$ denotes the identity matrix. The symbol $\triangleq$ denotes "defined as". $\mathbb{C}^{m\times n}$ denotes the complex space of a matrix with dimension $m \times n$. The distribution of a circularly symmetric complex Gaussian (CSCG) random variable with zero mean and variance σ^2 is denoted as $\mathcal{CN}(0,\sigma^2)$. $\mathrm{E}[\cdot]$ represents statistical expectation. $H(\cdot|\cdot)$ denotes the conditional entropy and $I(\cdot,\cdot)$ represents the mutual information.

II. System Model and Problem Formulation

As shown in Fig. 1, we are interested in a secure MISO CR channel, which consists of four terminals: a pair of SU-Tx and SU-Rx, a PU-Rx and an ED-Rx. The SU-Tx is sending a message W to the SU-Rx on the frequency band which is licensed to the PU-Rx. For security concern, the SU-Tx wants the message to be kept secret from the ED-Rx. It is assumed that each of the receive terminals has a single antenna while the SU-Tx is equipped with N antennas. This results in three MISO channels, namely, secondary channel, primary channel and eavesdropper channel, the channel responses of which are denoted by $\boldsymbol{h}_s$, $\boldsymbol{h}_p$ and $\boldsymbol{h}_e$, respectively, where $\boldsymbol{h}_s, \boldsymbol{h}_p, \boldsymbol{h}_e \in \mathbb{C}^{N\times 1}$. In this paper, we assume that the SU-Tx does not know the exact channel realizations of all the three channels but instead it has a knowledge of the uncertainty regions containing the actual channels, which are assumed to be described by the following ellipsoids:

$$\mathcal{H}_s = \left\{\boldsymbol{h}_s | \boldsymbol{h}_s = \hat{\boldsymbol{h}}_s + \Delta\boldsymbol{h}_s, \Delta\boldsymbol{h}_s^{\dagger}\boldsymbol{W}_s\Delta\boldsymbol{h}_s \le 1\right\} \quad (1)$$

$$\mathcal{H}_p = \left\{\boldsymbol{h}_p | \boldsymbol{h}_p = \hat{\boldsymbol{h}}_p + \Delta\boldsymbol{h}_p, \Delta\boldsymbol{h}_p^{\dagger}\boldsymbol{W}_p\Delta\boldsymbol{h}_p \le 1\right\} \quad (2)$$

$$\mathcal{H}_e = \left\{\boldsymbol{h}_e | \boldsymbol{h}_e = \hat{\boldsymbol{h}}_e + \Delta\boldsymbol{h}_e, \Delta\boldsymbol{h}_e^{\dagger}\boldsymbol{W}_e\Delta\boldsymbol{h}_e \le 1\right\} \quad (3)$$

where $\hat{\boldsymbol{h}}_s$, $\hat{\boldsymbol{h}}_p$ and $\hat{\boldsymbol{h}}_e$ are the erroneous estimates received at the SU-Tx; $\Delta\boldsymbol{h}_s$, $\Delta\boldsymbol{h}_p$, $\Delta\boldsymbol{h}_e$ are the corresponding channel estimation errors; $\boldsymbol{W}_s, \boldsymbol{W}_p, \boldsymbol{W}_e \succ 0$ determine the shape and size of each uncertainty region.

The justification of these uncertainty regions at the SU-Tx can be explained as follows. Similar to [20], we consider that the SU-Tx as a base station of the CRN and both the SU-Rx and ED-Rx are the SUs of the CRN. The ED-Rx is treated as an eavesdropper only because it is not the intended destination of message W. We can assume that both the SU-Rx and the ED-Rx have perfect knowledge of the realization of its own channel. This can be done by estimating the channel using the training sequence sent from the SU-Tx. The knowledge of $\boldsymbol{h}_s$ and $\boldsymbol{h}_e$ at the SU-Tx can be obtained through feedback channel from

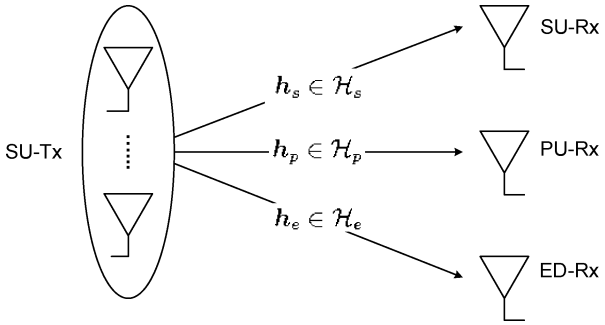


Fig. 1. System model for the secure MISO CRN.

the SU-Rx and the ED-Rx[1] assuming channel reciprocity. It is assumed to be imperfect because of various uncertainties such as the errors in the transmission through the feedback channel, the quantization error due to the limited capacity of the feedback channel, or the outdated feedback due to the time-varying nature of wireless environments. Furthermore, the knowledge of $\boldsymbol{h}_p$ at the SU-Tx can be obtained by periodically sensing the transmitted signal from the PU-Rx when it is in the transmission mode. However, besides the errors mentioned above, the estimation of $\boldsymbol{h}_p$ can be even more erroneous due to the limited cooperation with the PU. Hence, we consider that the SU-Tx only knows the erroneous estimates of the channels and wishes to ensure secure and cognitive transmission for the channel realizations that fall within the uncertainty regions around the estimates. These uncertainty regions show the extent to which the SU-Tx wants the secure and cognitive transmission to be. Larger uncertainty regions indicate that the SU-Tx takes a more conservative approach in securing the confidential information and protecting the PU.

The communication scenario of interest here can be considered as a special case of a compound wiretap channel [21]. Such a channel captures the transmission scenario over a wiretap channel with a number of possible channel realizations and secure transmission should be guaranteed no matter which realization it takes. When the channel realizations of the secondary channel and eavesdropper channel are $\boldsymbol{h}_s$ and $\boldsymbol{h}_e$, the signals received at the SU-Rx and the ED-Rx can be written as

$$y_m(\boldsymbol{h}_s) = \boldsymbol{h}_s^\dagger \boldsymbol{x}_m + w_m, \quad m = 1, \ldots, n \tag{4}$$

and

$$z_m(\boldsymbol{h}_e) = \boldsymbol{h}_e^\dagger \boldsymbol{x}_m + v_m, \quad m = 1, \ldots, n \tag{5}$$

respectively, where m is the time index; n is the length of the codeword; $\boldsymbol{x}_m \in \mathbb{C}^{N\times 1}$ is the signal transmitted from the SU-Tx; w_m and v_m are the zero-mean unit-variance CSCG noise components at the SU-Rx and the ED-Rx, respectively. The channel input is subject to the following power constraints:

$$\frac{1}{n}\sum_{m=1}^{n} \boldsymbol{x}_m^\dagger \boldsymbol{x}_m \le P, \tag{6}$$

$$\frac{1}{n}\sum_{m=1}^{n} \boldsymbol{h}_p^\dagger \boldsymbol{x}_m \boldsymbol{x}_m^\dagger \boldsymbol{h}_p \le \Gamma, \quad \forall \boldsymbol{h}_p \in \mathcal{H}_p \tag{7}$$

[1]It is reasonable to assume that ED-Rx feeds back its CSI to the SU-Tx since as another SU-Rx, it may also expect some confidential information from the SU-Tx.

where (6) is the transmit power constraint at the SU-Tx; and (7) is the interference power constraint at the PU-Rx with Γ denoting the interference temperature limit. Note that since the SU-Tx does not know the exact channel realization of the primary channel, to protect the PU at all times, such interference power constraint should be satisfied for all the possible realizations within the uncertainty set $\mathcal{H}_p$.

The information-theoretic security of the transmission, represented by the level of secrecy of the message W at the ED-Rx when the eavesdropper channel is $\boldsymbol{h}_e$, is measured by the equivocation rate, which is defined as the entropy rate of the confidential information given the channel outputs at the eavesdropper, i.e. $(1/n)H(W|z^n(\boldsymbol{h}_e))$, where $z^n(\boldsymbol{h}_e) = (z_1(\boldsymbol{h}_e), \ldots, z_n(\boldsymbol{h}_e))$. It shows the eavesdropper's uncertainty about the message W after receiving $z^n(\boldsymbol{h}_e)$. A higher equivocation rate indicates a higher level of secrecy. A secrecy rate R_s is said to be achieved with perfect secrecy if, for any $\epsilon > 0$, there exists a $(2^{nR_s}, n)$ code with the average error probability at the SU-Rx, $P_e^{(n)} \le \epsilon$, $\forall \boldsymbol{h}_s \in \mathcal{H}_s$, and the equivocation rate satisfying $R_s - (H(W|z^n(\boldsymbol{h}_e))/n) \le \epsilon$, $\forall \boldsymbol{h}_e \in \mathcal{H}_e$. The secrecy capacity of this channel is the maximum of all the achievable perfect secrecy rates.

In general, the characterization of the secrecy capacity for the general compound wiretap channel is an open research topic. In this paper, instead of characterizing the secrecy capacity for this channel, we restrict our attention to the case of Gaussian signaling with no preprocessing of information. It is pointed out that although such restriction achieves secrecy capacity for the degraded MIMO compound wiretap channel [21], it is potentially suboptimal for the general multiantenna channels.

Corollary 1: Under Gaussian signaling with no preprocessing of information, an achievable secrecy rate of the secure MISO CR channel with channel uncertainties can be found as the maximum objective value of the following problem:

$$Problem\ 1$$

$$\max_{\boldsymbol{S}\succeq 0} \quad \min_{\boldsymbol{h}_s\in\mathcal{H}_s, \boldsymbol{h}_e\in\mathcal{H}_e} \log_2 \frac{\left(1+\boldsymbol{h}_s^\dagger \boldsymbol{S}\boldsymbol{h}_s\right)}{\left(1+\boldsymbol{h}_e^\dagger \boldsymbol{S}\boldsymbol{h}_e\right)} \tag{8}$$

$$\text{s.t.} \quad \operatorname{tr}(\boldsymbol{S}) \le P \tag{9}$$

$$\boldsymbol{h}_p^\dagger \boldsymbol{S}\boldsymbol{h}_p \le \Gamma, \quad \forall\, \boldsymbol{h}_p \in \mathcal{H}_p \tag{10}$$

where $\boldsymbol{S}$ is the input transmit covariance matrix, i.e., $\boldsymbol{S} = \mathrm{E}[\boldsymbol{x}\boldsymbol{x}^\dagger]$.

Proof: For a general discrete memoryless compound wiretap channel, it has been shown in [21] that there exists a code to achieve the following secrecy rate[2]

$$R_s = \max_{p(\boldsymbol{u},\boldsymbol{x})} \min_{\boldsymbol{h}_s\in\mathcal{H}_s, \boldsymbol{h}_e\in\mathcal{H}_e} I\left(\boldsymbol{u}; y(\boldsymbol{h}_s)\right) - I\left(\boldsymbol{u}; z(\boldsymbol{h}_e)\right) \tag{11}$$

where $\boldsymbol{u}$ is an auxiliary random variable satisfying the Markov relation $\boldsymbol{u} \to \boldsymbol{x} \to (y(\boldsymbol{h}_s), z(\boldsymbol{h}_e))$; and $p(\cdot,\cdot)$ is the joint probability density function (pdf) of $\boldsymbol{u}$ and $\boldsymbol{x}$. By setting $\boldsymbol{u} = \boldsymbol{x}$, we have the following achievable secrecy rate

$$R_s = \max_{p(\boldsymbol{x})} \min_{\boldsymbol{h}_s\in\mathcal{H}_s, \boldsymbol{h}_e\in\mathcal{H}_e} I\left(\boldsymbol{x}; y(\boldsymbol{h}_s)\right) - I\left(\boldsymbol{x}; z(\boldsymbol{h}_e)\right). \tag{12}$$

[2]For the details of the coding strategy to achieve this secrecy rate, the readers are referred to [21]. For the practical code design for the wiretap channel, the readers are referred to [22] and the references therein.

This result can also be extended to a continuous-alphabet channel with average cost constraint. Hence, by restricting the channel input to be a Gaussian code, i.e., $\boldsymbol{u} = \boldsymbol{x} \sim \mathcal{CN}(0, \boldsymbol{S})$, then, under the matrix covariance constraint $\boldsymbol{S} \preceq \boldsymbol{K}$, where $\boldsymbol{K} \succeq 0$, we obtain the following achievable secrecy rate

$$R_s(\boldsymbol{K}) = \max_{0 \preceq \boldsymbol{S} \preceq \boldsymbol{K}} \min_{\boldsymbol{h}_s \in \mathcal{H}_s, \boldsymbol{h}_e \in \mathcal{H}_e} \log_2 \frac{1 + \boldsymbol{h}_s \boldsymbol{S} \boldsymbol{h}_s^\dagger}{1 + \boldsymbol{h}_e \boldsymbol{S} \boldsymbol{h}_e^\dagger}. \quad (13)$$

As shown in [23], the matrix covariance constraint $\boldsymbol{S} \preceq \boldsymbol{K}$ is a rather general constraint in the sense that it can be used to easily derive the achievable rate under any constraint that can be represented in terms of a compact set of $\boldsymbol{K}$. Hence, for our channel of interest, we define the compact set as $\mathcal{S} = \{\boldsymbol{K} \succeq 0 | \mathrm{tr}(\boldsymbol{K}) \leq P, \boldsymbol{h}_p^\dagger \boldsymbol{K} \boldsymbol{h}_p \leq \Gamma, \forall \boldsymbol{h}_p \in \mathcal{H}_p\}$, which corresponds to the set of covariance matrices satisfying both the transmit power constraint and worst-case interference power constraint. The maximum achievable secrecy rate under Gaussian signaling without preprocessing of information for the secure MISO CR channel with channel uncertainties is the maximum rate under this compact set constraint $\mathcal{S}$, denoted as $R_s(\mathcal{S})$. Then, according to Lemma 1 of [23], which states that the rate region achievable under the compact set constraint $\mathcal{S}$ is the union of all achievable rate regions for each $\boldsymbol{K} \in \mathcal{S}$, we have, for the maximum achievable secrecy rate

$$R_s(\mathcal{S}) = \max_{\boldsymbol{K} \in \mathcal{S}} R_s(\boldsymbol{K}) \quad (14)$$

$$= \max_{\boldsymbol{S} \succeq 0, \boldsymbol{S} \in \mathcal{S}} \min_{\boldsymbol{h}_s \in \mathcal{H}_s, \boldsymbol{h}_e \in \mathcal{H}_e} \log_2 \frac{1 + \boldsymbol{h}_s \boldsymbol{S} \boldsymbol{h}_s^\dagger}{1 + \boldsymbol{h}_e \boldsymbol{S} \boldsymbol{h}_e^\dagger}. \quad (15)$$

■

Corollary 1 formulates our main problem of interest. In the rest of the paper, our objective is to determine the optimal transmit covariance matrix $\boldsymbol{S}$ to achieve this secrecy rate, which is the maximum rate under the assumption of Gaussian signaling without preprocessing of information at which the information can be sent reliably to the SU-Rx but is kept perfectly secret from the ED-Rx and at the same time the PU-Rx is protected under the interference power constraint for all the possible channel realizations within the predefined channel uncertainty sets (1)–(3). We will deal with the following problem due to the monotonicity of the log function:

$Problem\ 2$:

$$\max_{\boldsymbol{S} \succeq 0} \min_{\boldsymbol{h}_s \in \mathcal{H}_s, \boldsymbol{h}_e \in \mathcal{H}_e} \frac{1 + \boldsymbol{h}_s^\dagger \boldsymbol{S} \boldsymbol{h}_s}{1 + \boldsymbol{h}_e^\dagger \boldsymbol{S} \boldsymbol{h}_e} \quad (16)$$

$$\text{s.t.} \quad \mathrm{tr}(\boldsymbol{S}) \leq P \quad (17)$$

$$\boldsymbol{h}_p^\dagger \boldsymbol{S} \boldsymbol{h}_p \leq \Gamma, \forall\, \boldsymbol{h}_p \in \mathcal{H}_p. \quad (18)$$

It can be shown that *Problem 2* is a maximin optimization of quasi-convex semiinfinite problem since the objective function is quasi-concave [24] and the constraint sets are defined by infinitely many linear constraints due to the uncertainty set $\mathcal{H}_p$. Therefore, *Problem 2* is challenging and no immediate algorithm can be applied to it in its direct form. In the next section, we will propose a few algorithms to find the optimal solution based on some equivalent transformations.

III. Optimal Solution

Since *Problem 2* belongs to the family of quasi-convex optimization problems, we first present an algorithm based on the general approach to conquer quasi-convex problems. However, this method may not be reliable for implementation. To overcome it, we present two alternative approaches. The first one relates the original problem to the robust design problems in an auxiliary CRN with two PUs and no ED, which can be transformed into a convex semidefinite program. As a result, the original problem can be solved by a sequence of semidefinite programs. In the second approach, we transform the original problem into a single convex semidefinite program by exploring its inherent convexity; hence, the computational complexity is significantly reduced.

A. Quasi-convex Optimization Approach

Quasi-convex optimization problem can be generally solved by a bisection search method, which requires the equivalent representation of the superlevel sets of a quasi-concave function via a set of convex inequalities [24]. Since our objective function is a ratio of two linear matrix inequalities of nonnegative semidefinite matrix, this can be easily done by taking the epigraph form of the original problem

$$\max_{\boldsymbol{S} \succeq 0, \tau \geq 0} \quad \tau \quad (19)$$

$$\text{s.t.} \quad \mathrm{tr}(\boldsymbol{S}) \leq P \quad (20)$$

$$\boldsymbol{h}_p^\dagger \boldsymbol{S} \boldsymbol{h}_p \leq \Gamma,\ \forall\, \boldsymbol{h}_p \in \mathcal{H}_p \quad (21)$$

$$1 + \boldsymbol{h}_s^\dagger \boldsymbol{S} \boldsymbol{h}_s \geq \tau \left(1 + \boldsymbol{h}_e^\dagger \boldsymbol{S} \boldsymbol{h}_e\right) \quad \forall\, \boldsymbol{h}_s \in \mathcal{H}_s,\ \boldsymbol{h}_e \in \mathcal{H}_e. \quad (22)$$

As a result, *Problem 2* is equivalently transformed into a problem with a linear objective function of τ and convex constraints with respect to $\boldsymbol{S}$ for each given value of τ, which enables the following bisection search method:

- **Given**, $\tau \in [0, \bar{\tau}]$
- **Initialize** $\tau_{\min} \leftarrow 0$, $\tau_{\max} \leftarrow \bar{\tau}$
- **Repeat**
  - $\tau \leftarrow (1/2)(\tau_{\min} + \tau_{\max})$
  - Check the feasibility of (20), (21), and (22). If it is feasible, set $\tau_{\min} \leftarrow \tau$; else, set $\tau_{\max} \leftarrow \tau$.
- **Until** $\tau_{\max} - \tau_{\min} \leq \varepsilon$, where ε is a small positive number that controls the accuracy of the algorithm.

Notice that at each search step, a convex feasibility test has to be performed but the feasibility of (21) and (22) cannot be determined directly since each of them corresponds to infinite number of constraints due to the uncertainty sets. Hence, reformulation is needed to transform them into finite number of constraints. Note that the uncertainty sets described in (1)–(3) are quadratic functions of the channel estimation errors. To resolve the semiinfiniteness of the constraints, the S-Procedure [25] is usually used to convert them into a finite number of convex semidefinite constraints. Since the uncertainties in $\boldsymbol{h}_s$ and $\boldsymbol{h}_e$ are constrained separately, we can first perform the S-Procedure with respect to the certainty set $\mathcal{H}_s$, and (22) is equivalently

transformed into

$$\begin{bmatrix} \boldsymbol{S}+s\boldsymbol{W}_s & \boldsymbol{S}\hat{\boldsymbol{h}}_s \\ \hat{\boldsymbol{h}}_s^{\dagger}\boldsymbol{S} & \boldsymbol{S}_1 \end{bmatrix} \succeq 0,\ \forall \boldsymbol{h}_e \in \mathcal{H}_e,\ \exists s \geq 0 \qquad (23)$$

where $\boldsymbol{S}_1 = \hat{\boldsymbol{h}}_s^{\dagger}\boldsymbol{S}\hat{\boldsymbol{h}}_s + 1 - \tau(\boldsymbol{h}_e^{\dagger}\boldsymbol{S}\boldsymbol{h}_e + 1) - s$. To further resolve the semidefiniteness of $\mathcal{H}_e$, we make use of the following extension of the S-Procedure ([26, Th. 3.5]).

Theorem 1: The relation

$$\begin{bmatrix} \boldsymbol{H} & \boldsymbol{F}+\boldsymbol{G}\boldsymbol{X} \\ (\boldsymbol{F}+\boldsymbol{G}\boldsymbol{X})^{\dagger} & \boldsymbol{C}+\boldsymbol{X}^{\dagger}\boldsymbol{B}+\boldsymbol{B}^{\dagger}\boldsymbol{X}+\boldsymbol{X}^{\dagger}\boldsymbol{A}\boldsymbol{X} \end{bmatrix} \succeq 0$$
$$\forall \boldsymbol{I}-\boldsymbol{X}^{\dagger}\boldsymbol{D}\boldsymbol{X} \succeq 0 \qquad (24)$$

is valid, if and only if,

$$\exists s \geq 0,\ \begin{bmatrix} \boldsymbol{H} & \boldsymbol{F} & \boldsymbol{G} \\ \boldsymbol{F}^{\dagger} & \boldsymbol{C}-s\boldsymbol{I} & \boldsymbol{B}^{\dagger} \\ \boldsymbol{G}^{\dagger} & \boldsymbol{B} & \boldsymbol{A}+s\boldsymbol{D} \end{bmatrix} \succeq 0. \qquad (25)$$

Then, according to Theorem 1, (23) can be finally reduced to a single convex constraint given by

$$\begin{bmatrix} \boldsymbol{S}+s\boldsymbol{W}_s & \boldsymbol{S}\hat{\boldsymbol{h}}_s & \boldsymbol{0}_{N\times N} \\ \hat{\boldsymbol{h}}_s^{\dagger}\boldsymbol{S} & \boldsymbol{S}_2 & -\tau\hat{\boldsymbol{h}}_e^{\dagger}\boldsymbol{S} \\ \boldsymbol{0}_{N\times N} & -\tau\boldsymbol{S}\hat{\boldsymbol{h}}_e & -\tau\boldsymbol{S}+e\boldsymbol{W}_e \end{bmatrix} \succeq 0,\ \exists s,e \geq 0 \quad (26)$$

where $\boldsymbol{S}_2 = \hat{\boldsymbol{h}}_s^{\dagger}\boldsymbol{S}\hat{\boldsymbol{h}}_s + 1 - \tau(\hat{\boldsymbol{h}}_e^{\dagger}\boldsymbol{S}\hat{\boldsymbol{h}}_e + 1) - s - e$. Similarly, (21) can also be equivalently transformed into the following single convex constraint:

$$\begin{bmatrix} -\hat{\boldsymbol{h}}_p^{\dagger}\boldsymbol{S}\hat{\boldsymbol{h}}_p + \Gamma - p & -\hat{\boldsymbol{h}}_p^{\dagger}\boldsymbol{S} \\ -\boldsymbol{S}\hat{\boldsymbol{h}}_p & -\boldsymbol{S}+p\boldsymbol{W}_p \end{bmatrix} \succeq 0,\ \exists p \geq 0. \qquad (27)$$

With the help of the S-Procedure and its extension, the constraint sets (20), (26), and (27) are finite and, in fact, they are all linear matrix inequalities (LMIs). As a result, the feasibility problem becomes testing the feasibility of a semidefinite program (SDP). Although many numerical solvers can solve the SDPs very efficiently, they are usually not good at distinguishing between a strictly infeasible problem and a possible numerical difficulty. Therefore, the algorithm based on numerical feasibility test is prone to errors.

B. Auxiliary CRN (ACRN) Transformation

In the conventional CRN where there is no eavesdropper, the SU-Tx has to control its antenna beams and power so that the interference power received at the PU-Rx is restricted. Similarly, in the conventional wiretap channel, the transmitter also has to restrict the receive power at the ED-Rx in order to achieve positive secrecy rate. The relationship between these two types of networks was first explored in [27], [28] in which a compound MISO wiretap channel with uncertainty only in the eavesdropper channel is transformed into a sequence of MISO CR channels with uncertainty only in the primary channel. In this subsection, we will first study the optimal robust transmitter design problem for a MISO CRN with two PUs in the case of uncertainties in all the relevant channels. Then, the relationship between this auxiliary CRN and our original system of interest is presented. Finally, an algorithm based on this transformation is proposed.

Consider a CRN with a pair of SU-Tx and SU-Rx and two PU-Rxs as shown in Fig. 2. Let $\boldsymbol{h}_s, \boldsymbol{h}_p$ and $\boldsymbol{h}_e$ denote the channel responses from the SU-Tx to the SU-Rx, PU-Rx1 and PU-Rx2, respectively. Due to the channel estimation or quantization error and limited cooperation with the PUs, it is assumed that the SU-Tx does not have perfect CSI of all the channels, but that it knows the uncertainty sets within which the exact CSI belongs to, which is defined by (1)–(3). The transmission strategy design in the presence of channel uncertainties can be formulated as an optimization problem to find the optimal transmit covariance matrix $\boldsymbol{S}$ such that the compound capacity, defined as the maximum worst-case rate [14] at which the message can be reliably delivered to the SU-Rx, is achieved, and at the same time the interference received at the PU-Rxs is kept below the predetermined thresholds for all the possible channel realizations within the uncertainty sets. Mathematically, it is given as

$$\begin{aligned} &Problem\ 3: \\ &\max_{\boldsymbol{S}\succeq 0} \quad \min_{\boldsymbol{h}_s\in\mathcal{H}_s} \log_2\left(1+\boldsymbol{h}_s^{\dagger}\boldsymbol{S}\boldsymbol{h}_s\right) && (28)\\ &\text{s.t.} \quad \operatorname{tr}(\boldsymbol{S}) \leq P && (29)\\ &\qquad \boldsymbol{h}_p^{\dagger}\boldsymbol{S}\boldsymbol{h}_p \leq \Gamma,\ \forall\, \boldsymbol{h}_p \in \mathcal{H}_p && (30)\\ &\qquad \boldsymbol{h}_e^{\dagger}\boldsymbol{S}\boldsymbol{h}_e \leq \gamma,\ \forall\, \boldsymbol{h}_e \in \mathcal{H}_e. && (31) \end{aligned}$$

Due to the monotonicity of the log function, *Problem 3* is equivalent to

$$\begin{aligned} &Problem\ 4: \\ &g(\gamma) \triangleq \max_{\boldsymbol{S}\succeq 0} \quad \min_{\boldsymbol{h}_s\in\mathcal{H}_s} \boldsymbol{h}_s^{\dagger}\boldsymbol{S}\boldsymbol{h}_s && (32)\\ &\qquad \text{s.t.} \quad \operatorname{tr}(\boldsymbol{S}) \leq P && (33)\\ &\qquad\qquad \boldsymbol{h}_p^{\dagger}\boldsymbol{S}\boldsymbol{h}_p \leq \Gamma,\ \forall\, \boldsymbol{h}_p \in \mathcal{H}_p && (34)\\ &\qquad\qquad \boldsymbol{h}_e^{\dagger}\boldsymbol{S}\boldsymbol{h}_e \leq \gamma,\ \forall\, \boldsymbol{h}_e \in \mathcal{H}_e. && (35) \end{aligned}$$

Note that the maximum objective value of the *Problem 4* is denoted as $g(\gamma)$, which is a function of the interference temperature limit γ at the PU-Rx2. It can be easily seen that *Problem 4* is a maximin convex semiinfinite program since the objective function is linear and the constraint sets are defined by the intersection of infinite number of convex sets. By taking the epigraph form and performing the S-procedure, we have the following convex problem with finite number of constraints:

$$\begin{aligned} &Problem\ 5: \\ &\max_{\boldsymbol{S}\succeq 0,t,s,p,e\geq 0} \quad t && (36)\\ &\text{s.t.} \quad \operatorname{tr}(\boldsymbol{S}) \leq P && (37)\\ &\qquad \begin{bmatrix} \hat{\boldsymbol{h}}_s^{\dagger}\boldsymbol{S}\hat{\boldsymbol{h}}_s - t - s & \hat{\boldsymbol{h}}_s^{\dagger}\boldsymbol{S} \\ \boldsymbol{S}\hat{\boldsymbol{h}}_s & \boldsymbol{S}+s\boldsymbol{W}_s \end{bmatrix} \succeq 0 && (38)\\ &\qquad \begin{bmatrix} -\hat{\boldsymbol{h}}_p^{\dagger}\boldsymbol{S}\hat{\boldsymbol{h}}_p + \Gamma - p & -\hat{\boldsymbol{h}}_p^{\dagger}\boldsymbol{S} \\ -\boldsymbol{S}\hat{\boldsymbol{h}}_p & -\boldsymbol{S}+p\boldsymbol{W}_p \end{bmatrix} \succeq 0 && (39)\\ &\qquad \begin{bmatrix} -\hat{\boldsymbol{h}}_e^{\dagger}\boldsymbol{S}\hat{\boldsymbol{h}}_e + \gamma - e & -\hat{\boldsymbol{h}}_e^{\dagger}\boldsymbol{S} \\ -\boldsymbol{S}\hat{\boldsymbol{h}}_e & -\boldsymbol{S}+e\boldsymbol{W}_e \end{bmatrix} \succeq 0. && (40) \end{aligned}$$

Problem 5 is a SDP with a linear objective function and LMI constraints. Hence, it can be solved very efficiently by some numerical solvers such as SeDuMi [29].

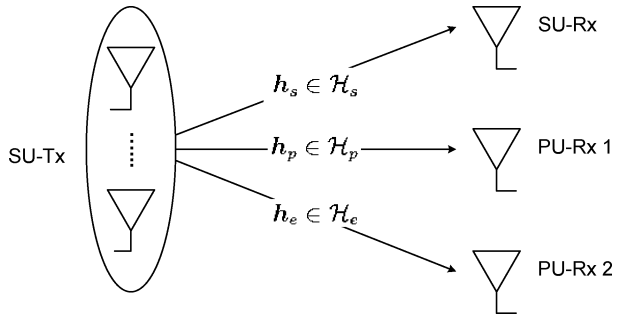


Fig. 2. System model for the conventional MISO CRN with 2 PUs.

The relationship between the original secure CR channel with uncertainties and this auxiliary CR channel with uncertainties, i.e., *Problem 2* and *Problem 4*, is revealed in the following proposition.

Proposition 1: Denote $\boldsymbol{S}^o$ as the optimal covariance matrix of *Problem 2* and define $\gamma^o = \max_{\boldsymbol{h}_e \in \mathcal{H}_e} \boldsymbol{h}_e \boldsymbol{S}^o \boldsymbol{h}_e$. Then, $\boldsymbol{S}^o$ is also optimal for *Problem 4* with $\gamma = \gamma^o$.

Proof: Please refer to Appendix A. ■

With this relationship, the following transformation for the original *Problem 2* can be obtained:

Proposition 2: Problem 2 is equivalent to

$$Problem\ 6: \quad \max_{\gamma \geq 0} \frac{1+g(\gamma)}{1+\gamma}. \tag{41}$$

Proof: Please refer to Appendix B. ■

As shown in Appendix C, *Problem 6* is an unconstrained quasi-convex optimization problem of a single variable γ. Therefore, an efficient golden section search algorithm can be applied, which is detailed as follows:

- **Given**, $\gamma \in [0, \bar{\gamma}]$, $c = (\sqrt{5}-1)/2$
- **Initialize** $a = 0, b = \bar{\gamma}, \gamma_1 \leftarrow (1-c)b, \gamma_2 \leftarrow cb$, compute $g(\gamma_1)$, $g(\gamma_2)$
- **Repeat**
  - **if** $(1+g(\gamma_1))/(1+\gamma_1)) > (1+g(\gamma_2))/(1+\gamma_2)$: set $b \leftarrow \gamma_2$, $\gamma_2 \leftarrow \gamma_1$, $g(\gamma_2) \leftarrow g(\gamma_1)$, $\gamma_1 \leftarrow b - c(b-a)$ compute $g(\gamma_1)$
  - **else**: set $a \leftarrow \gamma_1$, $\gamma_1 \leftarrow \gamma_2$, $g(\gamma_1) \leftarrow g(\gamma_2)$, $\gamma_2 \leftarrow a + c(b-a)$ compute $g(\gamma_2)$
- **Until** $|b-a| \leq \varepsilon$, where ε is a small positive number that controls the accuracy of the algorithm.

Note that the algorithm searches for the optimal γ over the region $[0, \bar{\gamma}]$. At each given γ, *Problem 5* has to be solved to obtain $g(\gamma)$. Therefore, the original maximin quasi-convex semiinfinite program is transformed into a sequence of convex optimization problems. Compared to the previous approach, no feasibility test of a SDP is involved and hence this approach is more reliable for implementation.

C. SDP Transformation

In [11] and [12], we have shown that the capacity-achieving transmission strategy design for the secure MISO CR channel with perfect CSI at the SU-Tx can be solved by transforming it into a single SDP. For *Problem 2*, it belongs to the family of generalized linear fraction programs since the objective function is the minimum of the ratio between two linear functions of semidefinite matrix $\boldsymbol{S}$. Generally, convex transformation does not apply. However, since the uncertainties in $\boldsymbol{h}_s$ and $\boldsymbol{h}_e$ are constrained separately, we will show that the convex transformation preserves as in the case of perfect CSI.

Proposition 3: Problem 2 is equivalent to *Problem 7*, which is given by

$$\begin{aligned} Problem\ 7: \quad & \\ \max_{\hat{\boldsymbol{S}} \succeq 0, t \geq 0} \quad & \min_{\boldsymbol{h}_s \in \mathcal{H}_s} t + \boldsymbol{h}_s^\dagger \hat{\boldsymbol{S}} \boldsymbol{h}_s && (42) \\ \text{s.t.} \quad & t + \boldsymbol{h}_e^\dagger \hat{\boldsymbol{S}} \boldsymbol{h}_e \leq 1, \ \forall\, \boldsymbol{h}_e \in \mathcal{H}_e && (43) \\ & \mathrm{tr}(\hat{\boldsymbol{S}}) - Pt \leq 0 && (44) \\ & \boldsymbol{h}_p^\dagger \hat{\boldsymbol{S}} \boldsymbol{h}_p - \Gamma t \leq 0, \ \forall\, \boldsymbol{h}_p \in \mathcal{H}_p && (45) \end{aligned}$$

and the optimal solution of *Problem 2* is $\boldsymbol{S}^* = \hat{\boldsymbol{S}}^o / t^o$, where $(\hat{\boldsymbol{S}}^o, t^o)$ is the optimal solution of *Problem 7*.

Proof: We first present a lemma, which is needed for the proof of Proposition 3.

Lemma 1: At the optimum of *Problem 7*, $(\hat{\boldsymbol{S}}^o, t^o)$ must satisfy that $t^o + \max_{\boldsymbol{h}_e \in \mathcal{H}_e} \boldsymbol{h}_e^\dagger \hat{\boldsymbol{S}}^o \boldsymbol{h}_e = 1$.

Proof: First, note that (43) is equivalent to $t^o + \max_{\boldsymbol{h}_e \in \mathcal{H}_e} \boldsymbol{h}_e^\dagger \hat{\boldsymbol{S}}^o \boldsymbol{h}_e \leq 1$. The proof can then be easily shown by contradiction. If we have $t^o + \max_{\boldsymbol{h}_e \in \mathcal{H}_e} \boldsymbol{h}_e^\dagger \hat{\boldsymbol{S}}^o \boldsymbol{h}_e < 1$ at the optimum, then we can always find a $t = t^o + \Delta t, \Delta t \geq 0$ such that the objective value is increased and the constraints (43)–(45) are still satisfied. This contradicts the assumption that $(\hat{\boldsymbol{S}}^o, t^o)$ is the optimal solution. This completes the proof. ■

We denote the optimal objective values of *Problem 2* and *Problem 7* as f^* and f^o, respectively. The proof can be divided into two parts. First, we will show that *Problem 7* can achieve an objective value of f^*, i.e., $f^* \leq f^o$. This can be easily verified by showing the pair $(\hat{\boldsymbol{S}} = \boldsymbol{S}^*/(1 + \max_{\boldsymbol{h}_e \in \mathcal{H}_e} \boldsymbol{h}_e^\dagger \boldsymbol{S}^* \boldsymbol{h}_e), t = 1/(1 + \max_{\boldsymbol{h}_e \in \mathcal{H}_e} \boldsymbol{h}_e^\dagger \boldsymbol{S}^* \boldsymbol{h}_e))$ is feasible for *Problem 7*.

Next, we will show that *Problem 2* can also achieve an objective value of f^o, i.e., $f^* \geq f^o$. Since $(\hat{\boldsymbol{S}}^o, t^o)$ is the optimal solution of *Problem 7*, it is clear that $\boldsymbol{S} = \hat{\boldsymbol{S}}^o / t^o$ is feasible for *Problem 2*. Then, by lemma 1, $f^o = t^o + \min_{\boldsymbol{h}_s \in \mathcal{H}_s} \boldsymbol{h}_s^\dagger \hat{\boldsymbol{S}}^o \boldsymbol{h}_s = (1 + \min_{\boldsymbol{h}_s \in \mathcal{H}_s} \boldsymbol{h}_s^\dagger \hat{\boldsymbol{S}}^o / t^o \boldsymbol{h}_s)/(1 + \max_{\boldsymbol{h}_e \in \mathcal{H}_e} \boldsymbol{h}_e^\dagger \hat{\boldsymbol{S}}^o / t^o \boldsymbol{h}_e)$ is achievable for *Problem 2*. Proposition 3 thus follows. ■

Problem 7 is a linear semiinfinite program, which can be transformed into a SDP by using the S-Procedure as in the previous two approaches.

$$\begin{aligned} Problem\ 8: \quad & \\ \max_{\hat{\boldsymbol{S}} \succeq 0, \tau, t, s, p, e \geq 0} \quad & \tau && (46) \\ \text{s.t.} \quad & \mathrm{tr}(\hat{\boldsymbol{S}}) - Pt \leq 0 && (47) \\ & \begin{bmatrix} \hat{\boldsymbol{h}}_s^\dagger \hat{\boldsymbol{S}} \hat{\boldsymbol{h}}_s + t - \tau - s & \hat{\boldsymbol{h}}_s^\dagger \hat{\boldsymbol{S}} \\ \hat{\boldsymbol{S}} \hat{\boldsymbol{h}}_s & \hat{\boldsymbol{S}} + s \hat{\boldsymbol{W}}_s \end{bmatrix} \succeq 0 && (48) \end{aligned}$$

$$\begin{bmatrix} -\hat{\boldsymbol{h}}_p^\dagger \hat{\boldsymbol{S}} \hat{\boldsymbol{h}}_p + t\Gamma - p & -\hat{\boldsymbol{h}}_p^\dagger \hat{\boldsymbol{S}} \\ -\hat{\boldsymbol{S}} \hat{\boldsymbol{h}}_p & -\hat{\boldsymbol{S}} + p\boldsymbol{W}_p \end{bmatrix} \succeq 0 \quad (49)$$

$$\begin{bmatrix} -\hat{\boldsymbol{h}}_e^\dagger \hat{\boldsymbol{S}} \hat{\boldsymbol{h}}_e - t + 1 - e & -\hat{\boldsymbol{h}}_e^\dagger \hat{\boldsymbol{S}} \\ -\hat{\boldsymbol{S}} \hat{\boldsymbol{h}}_e & -\hat{\boldsymbol{S}} + e\boldsymbol{W}_e \end{bmatrix} \succeq 0. \quad (50)$$

Compared to the Virtual CRN transformation, instead of solving a sequence of SDPs, this approach only requires to solve a single SDP, and hence the computational complexity is substantially reduced.

IV. Suboptimal Solutions

Although the optimal solution can be computed by the numerical approaches proposed in the previous section, the structure of the optimal solution, whether being beamforming or spatial multiplexing, is not yet known. For the practical implementation point of view, beamforming is preferred since it greatly simplifies the code design and the scalar wiretap channel code can be used. Nevertheless, finding the exact robust solution under the beamforming constraint (i.e., $\mathrm{rank}(\boldsymbol{S}) = 1$) may not be computationally tractable and usually some approximations have to be involved.[3] Therefore, in this section, we present a few heuristic beamforming solutions, the performance of which will be evaluated in the next section.

Before we present the heuristic beamforming solutions, we first show how the secrecy rate is computed for a given feasible beamforming vector. Note that when a beamforming vector is chosen as $\boldsymbol{w}$, the secrecy rate becomes $\log_2((1+\min_{\boldsymbol{h}_s\in\mathcal{H}_s}|\boldsymbol{w}^\dagger\boldsymbol{h}_s|^2)/(1+\max_{\boldsymbol{h}_e\in\mathcal{H}_e}|\boldsymbol{w}^\dagger\boldsymbol{h}_e|^2))$. According to the triangular inequality and the Cauchy-Schwarz inequality, we have

$$\begin{aligned} |\boldsymbol{w}^\dagger\boldsymbol{h}_s| &= |\boldsymbol{w}^\dagger\hat{\boldsymbol{h}}_s + \boldsymbol{w}^\dagger\Delta\boldsymbol{h}_s| && (51)\\ &\geq |\boldsymbol{w}^\dagger\hat{\boldsymbol{h}}_s| - \left|\boldsymbol{w}^\dagger\boldsymbol{W}_s^{-1/2}\boldsymbol{W}_s^{1/2}\Delta\boldsymbol{h}_s\right| && (52)\\ &\geq |\boldsymbol{w}^\dagger\hat{\boldsymbol{h}}_s| - \left\|\boldsymbol{w}^\dagger\boldsymbol{W}_s^{-1/2}\right\| \left\|\boldsymbol{W}_s^{1/2}\Delta\boldsymbol{h}_s\right\| && (53)\\ &\geq |\boldsymbol{w}^\dagger\hat{\boldsymbol{h}}_s| - \left\|\boldsymbol{w}^\dagger\boldsymbol{W}_s^{-1/2}\right\|. && (54) \end{aligned}$$

The minimum is $\min_{\boldsymbol{h}_s\in\mathcal{H}_s}|\boldsymbol{w}^\dagger\boldsymbol{h}_s| = |\boldsymbol{w}^\dagger\hat{\boldsymbol{h}}_s| - \|\boldsymbol{w}^\dagger\boldsymbol{W}_s^{-1/2}\|$ and it is achieved when $\Delta\boldsymbol{h}_s = -(\boldsymbol{W}_s^{-1}\boldsymbol{w}/\|\boldsymbol{w}^\dagger\boldsymbol{W}_s^{-1/2}\|)(\boldsymbol{w}^\dagger\hat{\boldsymbol{h}}_s/|\boldsymbol{w}^\dagger\hat{\boldsymbol{h}}_s|)$. Similarly, we have $\max_{\boldsymbol{h}_e\in\mathcal{H}_e}|\boldsymbol{w}^\dagger\boldsymbol{h}_e| = |\boldsymbol{w}^\dagger\hat{\boldsymbol{h}}_e| + \|\boldsymbol{w}^\dagger\boldsymbol{W}_e^{-1/2}\|$. The secrecy rate based on the feasible beamforming vector $\boldsymbol{w}$ is given as

$$\log_2 \frac{1+\left(|\boldsymbol{w}^\dagger\hat{\boldsymbol{h}}_s| - \left\|\boldsymbol{w}^\dagger\boldsymbol{W}_s^{-1/2}\right\|\right)^2}{1+\left(|\boldsymbol{w}^\dagger\hat{\boldsymbol{h}}_e| + \left\|\boldsymbol{w}^\dagger\boldsymbol{W}_e^{-1/2}\right\|\right)^2}. \quad (55)$$

One common approach to tackle the untractable beamforming problem is to solve a relaxed problem (i.e., dropping the rank-one constraint) and then use randomization techniques to generate an approximate beamforming solution based on the relaxed one [30], [31]. This suggests that we may solve the original problem by *Problem 7* and then generate an approximate solution using some randomization techniques. However, due to the complex forms of the constraints in *Problem 7*, conventional randomization techniques do not apply, and it is also likely to be complex to develop a randomization technique that is suitable to our problem. Besides, it is still unknown whether such an approximation is tight or not for our problem. Therefore, in all the beamforming approaches that will be presented subsequently, we will first generate some feasible rank-relaxation solutions (i.e., without the rank-one constraint) and then simply take the principle eigenvector of each solution as the beamforming vector, which can be easily seen to be feasible.

1) *Beamforming by the Exact Robust Solution* (BERS): The first approach is quite straightforward. After obtaining the optimal transmit covariance matrix based on *Problem 7*, we simply choose its principle eigenvector as the beamforming vector and calculate the corresponding secrecy rate from (55).
2) *Beamforming by the Approximate Robust Solution* (BARS): In this approach, we first consider an approximate robust beamforming design problem based on slightly strengthened uncertainty sets and then obtain the rank-relaxation solution of this approximate robust design problem. Notice that

$$\begin{aligned} &\left(|\boldsymbol{w}^\dagger\hat{\boldsymbol{h}}_s| - \left\|\boldsymbol{w}^\dagger\boldsymbol{W}_s^{-1/2}\right\|\right)^2 && (56)\\ &\quad= \boldsymbol{w}^\dagger\hat{\boldsymbol{h}}_s\hat{\boldsymbol{h}}_s^\dagger\boldsymbol{w} + \boldsymbol{w}^\dagger\boldsymbol{W}_s^{-1}\boldsymbol{w} \\ &\qquad - 2\left|\boldsymbol{w}^\dagger\boldsymbol{W}_s^{-1/2}\boldsymbol{W}_s^{1/2}\hat{\boldsymbol{h}}_s\right| \left\|\boldsymbol{w}^\dagger\boldsymbol{W}_s^{-1/2}\right\| && (57)\\ &\quad\geq \boldsymbol{w}^\dagger\hat{\boldsymbol{h}}_s\hat{\boldsymbol{h}}_s^\dagger\boldsymbol{w} + \boldsymbol{w}^\dagger\boldsymbol{W}_s^{-1}\boldsymbol{w} \\ &\qquad - 2\left\|\boldsymbol{w}^\dagger\boldsymbol{W}_s^{-1/2}\right\|^2 \left\|\boldsymbol{W}_s^{1/2}\hat{\boldsymbol{h}}_s\right\| && (58)\\ &\quad= \boldsymbol{w}^\dagger\boldsymbol{H}_s\boldsymbol{w} && (59) \end{aligned}$$

where $\boldsymbol{H}_s = \hat{\boldsymbol{h}}_s\hat{\boldsymbol{h}}_s^\dagger - \boldsymbol{W}_s^{-1}(1+2\|\boldsymbol{W}_s^{1/2}\hat{\boldsymbol{h}}_s\|)$. Hence, we have $\min_{\boldsymbol{h}_s\in\mathcal{H}_s}|\boldsymbol{w}^\dagger\boldsymbol{h}_s|^2 \geq \boldsymbol{w}^\dagger\boldsymbol{H}_s\boldsymbol{w}$. Note that for (58) to hold with equality, $\boldsymbol{W}_s^{-1/2}\boldsymbol{w}$ has to be linearly dependent on $\boldsymbol{W}_s^{1/2}\hat{\boldsymbol{h}}_s$. This condition may not be satisfied in the subsequent optimization with respect to $\boldsymbol{w}$. Hence, this minimum may not be achieved. Similarly, we also have $\max_{\boldsymbol{h}_e\in\mathcal{H}_e}|\boldsymbol{w}^\dagger\boldsymbol{h}_e|^2 \leq \boldsymbol{w}^\dagger\boldsymbol{H}_e\boldsymbol{w}$, where $\boldsymbol{H}_e = \hat{\boldsymbol{h}}_e\hat{\boldsymbol{h}}_e^\dagger + \boldsymbol{W}_e^{-1}(1+2\|\boldsymbol{W}_e^{1/2}\hat{\boldsymbol{h}}_e\|) \succ 0$. Therefore, an approximate robust design problem is given as

$$\begin{aligned} \max_{\boldsymbol{w}} \quad & \frac{1+\boldsymbol{w}^\dagger\boldsymbol{H}_s\boldsymbol{w}}{1+\boldsymbol{w}^\dagger\boldsymbol{H}_e\boldsymbol{w}} && (60)\\ \text{s.t.} \quad & \|\boldsymbol{w}\|^2 \leq P && (61)\\ & \boldsymbol{h}_p^\dagger\boldsymbol{w}\boldsymbol{w}^\dagger\boldsymbol{h}_p \leq \Gamma,\ \forall\, \boldsymbol{h}_p \in \mathcal{H}_p. && (62) \end{aligned}$$

Note that (60) is only a lower bound to the original objective function. Then, by rank-relaxation ($\boldsymbol{S} = \boldsymbol{w}\boldsymbol{w}^\dagger$) and SDP transformation as in Section III-C, the above problem can be transformed as

$$\begin{aligned} \max_{\boldsymbol{S}\succeq 0, t\geq 0} \quad & t + \mathrm{tr}(\boldsymbol{H}_s\hat{\boldsymbol{S}}) && (63)\\ \text{s.t.} \quad & \mathrm{tr}(\hat{\boldsymbol{S}}) \leq Pt && (64) \end{aligned}$$

[3] It is pointed out that when the number of antennas is large, it is possible to find the transmit directions which are favorable towards the SU-Rx and at the same time are null to both the eavesdropper and primary channels even though there are uncertainties involved. Hence, simple beamforming strategy can be used.

TABLE I
COMPLEXITY COMPARISON OF VARIOUS APPROACHES

	Number of Variables		Number of Constraints	
	complex semidefinite of size $N \times N$	positive scalar	complex semidefinite of size $(N+1) \times (N+1)$	real scalar
SDP	1	5	3	1
ACRN (at each γ)	1	4	3	1
BERS	1	5	3	1
BARS	1	1	1	2
BPRS	1	1	1	2

$$t + \mathrm{tr}(\boldsymbol{H}_s \hat{\boldsymbol{S}}) = 1 \tag{65}$$

$$\begin{bmatrix} -\hat{\boldsymbol{h}}_p^{\dagger} \hat{\boldsymbol{S}} \hat{\boldsymbol{h}}_p + t\Gamma - p & -\hat{\boldsymbol{h}}_p^{\dagger} \hat{\boldsymbol{S}} \\ -\hat{\boldsymbol{S}} \hat{\boldsymbol{h}}_p & -\hat{\boldsymbol{S}} + p\boldsymbol{W}_p \end{bmatrix} \succeq 0. \tag{66}$$

Finally, the beamforming vector is chosen as the principle eigenvector of $\hat{\boldsymbol{S}}^{\star}/t^{\star}$, where $(\hat{\boldsymbol{S}}^{\star}, t^{\star})$ is the optimal solution of the above problem.

3) *Beamforming by the Partially Robust Solution* (BPRS): Since we consider that both the SU-Rx and the ED-Rx are the secondary users of the CRN, it is natural to assume that the quality of the channel estimates for the secondary and eavesdropper channels are much better than that of the primary channel. In this approach, we simply ignore the channel uncertainties in $\boldsymbol{h}_s$ and $\boldsymbol{h}_e$ and choose the beamforming vector as the principle eigenvector of the optimal transmit covariance matrix based on $(\hat{\boldsymbol{h}}_s, \hat{\boldsymbol{h}}_e, \boldsymbol{h}_p)$. Mathematically, this corresponds to solving the following problem:

$$\max_{\boldsymbol{S} \succeq 0} \quad \frac{1 + \hat{\boldsymbol{h}}_s^{\dagger} \boldsymbol{S} \hat{\boldsymbol{h}}_s}{1 + \hat{\boldsymbol{h}}_e^{\dagger} \boldsymbol{S} \hat{\boldsymbol{h}}_e} \tag{67}$$

$$\text{s.t.} \quad \mathrm{tr}(\boldsymbol{S}) \le P \tag{68}$$

$$\boldsymbol{h}_p^{\dagger} \boldsymbol{S} \boldsymbol{h}_p \le \Gamma, \ \forall \, \boldsymbol{h}_p \in \mathcal{H}_p \tag{69}$$

which can be recast as the following SDP by the approach presented in Section III-C

$$\max_{\boldsymbol{S} \succeq 0, t \ge 0} \quad t + \hat{\boldsymbol{h}}_s^{\dagger} \hat{\boldsymbol{S}} \hat{\boldsymbol{h}}_s \tag{70}$$

$$\text{s.t.} \quad \mathrm{tr}(\hat{\boldsymbol{S}}) \le tP \tag{71}$$

$$\hat{\boldsymbol{h}}_e^{\dagger} \hat{\boldsymbol{S}} \hat{\boldsymbol{h}}_e + t = 1 \tag{72}$$

$$\begin{bmatrix} -\hat{\boldsymbol{h}}_p^{\dagger} \hat{\boldsymbol{S}} \hat{\boldsymbol{h}}_p + t\Gamma - p & -\hat{\boldsymbol{h}}_p^{\dagger} \hat{\boldsymbol{S}} \\ -\hat{\boldsymbol{S}} \hat{\boldsymbol{h}}_p & -\hat{\boldsymbol{S}} + p\boldsymbol{W}_p \end{bmatrix} \succeq 0. \tag{73}$$

Remark 1: The computational complexities of various proposed approaches will be briefly discussed here. Since all the proposed optimal and suboptimal approaches are based on SDP, the computational complexity depends significantly on the number and size of variables and constraints. In Table I, we summarize such information. For the optimal approaches, the SDP approach is almost of the same complexity as the ACRN at each given γ. However, since the ACRN has to solve a sequence of SDPs, the overall complexity of the ACRN is significantly higher than the optimal SDP one. The BERS has the same complexity as that of the optimal SDP since they solve the same optimization problem. The BARS and BPRS approaches are of the same complexity and they are simpler than the others.

V. SIMULATION RESULTS

In this section, we evaluate the performance of the proposed algorithms via computer simulations. Each entry of the channel vectors $\hat{\boldsymbol{h}}_s$, $\hat{\boldsymbol{h}}_e$ and $\hat{\boldsymbol{h}}_p$ is independent and identically distributed as $\mathcal{CN}(0,1)$. For simplicity, the uncertainty sets of all channels are assumed to be norm-bounded, i.e., $\boldsymbol{W}_s = (1/\epsilon_s)I$, $\boldsymbol{W}_p = (1/\epsilon_p)I$, $\boldsymbol{W}_e = (1/\epsilon_e)I$, where $(\epsilon_s, \epsilon_e, \epsilon_p)$ specifies the size of each uncertainty region, which is a measure of the quality of the channel estimations. Smaller values of ϵ imply better CSI knowledge at the SU-Tx. Monte Carlo simulations with 1000 randomly generated channel-triplets $(\hat{\boldsymbol{h}}_s, \hat{\boldsymbol{h}}_p, \hat{\boldsymbol{h}}_e)$ are performed and the average achievable secrecy rates are plotted. The transmit power and interference temperature limit are defined in dB with respect to the noise power.

We first consider a secure MISO CRN with $N = 4$ transmit antennas and the PU-Rx needs to be protected at the interference temperature limit of $\Gamma = -10$ dB. In Fig. 3, the secrecy rates achieved under different levels of channel uncertainties, as indicated by the triplet $(\epsilon_s, \epsilon_e, \epsilon_p)$, are plotted versus the transmit power level P. It is observed that the secrecy rates obtained by the two approaches, namely, ACRN transformation and SDP transformation, coincide perfectly since they are both optimal approaches. It is also observed that higher secrecy rate can be achieved when the uncertainty regions are smaller. This can be explained by the fact that more accurate CSI allows the SU-Tx to better direct its antenna beams towards the directions that are favorable to maximize its secrecy rate while avoiding harmful interference to the PU-Rx. Furthermore, we can also see that the secrecy rate becomes saturated at lower transmit power level when the uncertainty sets are larger. This is reasonable since injecting power into the channel does not necessarily help to increase the secrecy rate when the SU-Tx is less informed of the exact directions of the receivers. In Fig. 4, the achievable secrecy rate for a $N = 4$ transmit antenna MISO CR at the transmit power limit $P = 15$ dB is plotted against various interference temperature limits. The secrecy rates are also evaluated at different levels of channel uncertainties. Similarly, it is also observed that higher secrecy rates can be achieved with the increased accuracy in the CSI. We can also see that as the interference power constraint relaxes, the increase in secrecy rates is higher when there are uncertainties in the CSI. Fig. 5 shows the secrecy rate achieved with the use of different number of antennas at $P = 20$ dB when the level of uncertainty is $(10^{-3}, 10^{-3}, 10^{-2})$. We can observe that the secrecy

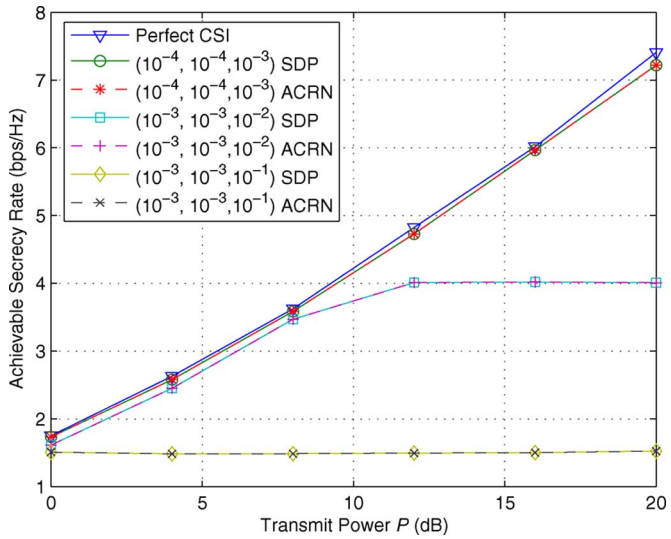


Fig. 3. Achievable secrecy rate versus transmit power with $N = 4$ antennas at $\Gamma = -10$ dB for different levels of channel uncertainties.

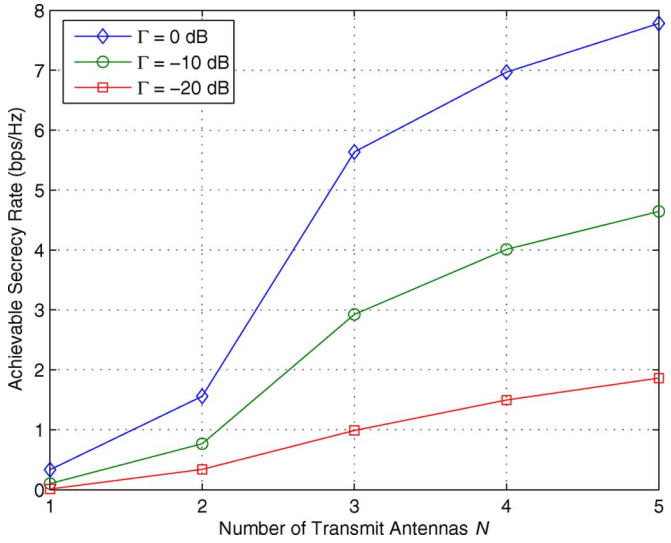


Fig. 5. Achievable secrecy rate versus number of transmit antennas at $P = 20$ dB and uncertainty level $(10^{-3}, 10^{-3}, 10^{-2})$.

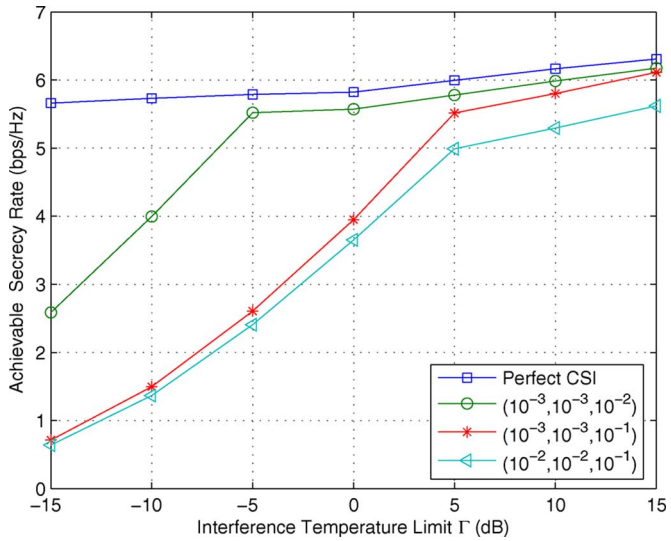


Fig. 4. Achievable secrecy rate versus interference power with $N = 4$ antennas at $P = 15$ dB for different levels of channel uncertainties.

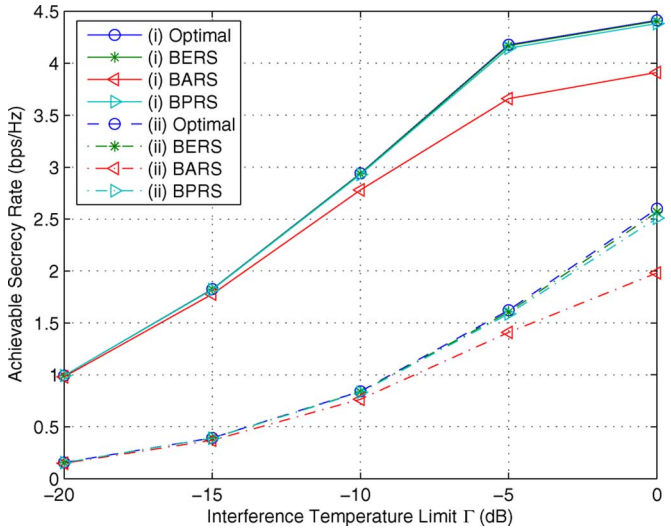


Fig. 6. Achievable secrecy rate versus interference temperature limit at $P = 15$ dB and uncertainty levels (i) $(10^{-3}, 10^{-3}, 10^{-2})$ and (ii) $(10^{-2}, 10^{-2}, 10^{-1})$.

rates are increased substantially with the use of multiple antennas. This demonstrates the effectiveness of multiple antennas in achieving simultaneous secure, robust and cognitive transmission. Fig. 6 plots the secrecy rate of both the optimal and three suboptimal solutions achieved using $N = 3$ antennas against various interference temperature limits at the transmit power $P = 15$ dB. For each evaluated Γ value, we consider two different sets of uncertainty regions: (i) $(10^{-3}, 10^{-3}, 10^{-2})$ and (ii) $(10^{-2}, 10^{-2}, 10^{-1})$. It is observed that BERS is very close to the optimal solution for almost all the cases. This implies that beamforming along the principle eigenvector of the optimal transmit covariance only suffers marginal rate loss, if any, which is favorable since beamforming is simpler to implement than spatial multiplexing. Furthermore, we can see that BPRS can also achieve close-to-optimal secrecy rate for the given uncertainty sets, which means that ignoring the uncertainty in the secondary and eavesdropper channels does not degrade the performance too much. Since it is practically reasonable to have good estimates of these two channels, BPRS is also a good choice since it is less complex than the optimal SDP approach and BERS. Last, BARS seems not to be an effective solution, which reveals that the techniques used in approximating the secrecy rate function significantly enlarge the uncertainty regions.

VI. Conclusion

In this paper, we have addressed the optimal robust transmitter design problem for the secure MISO CRN where the SU-Tx does not have perfect CSI of all the channels but only knows the associated uncertainty sets. Such a problem has been formulated as a maximin nonconvex semiinfinite optimization problem to maximize the achievable secrecy rate for the SU such that the interference received at the PU-Rx does not exceed the predefined threshold for all the possible channel realizations within the uncertainty regions. We have proposed two

approaches to solve the problem. In the first approach, we relate the original problem with the optimal robust transmitter design problem in an auxiliary CRN with two PUs where all the relevant channels are subject to uncertainty, and solve it by exploring the relationship between these two networks. The second approach effectively recasts the original problem as a single SDP by exploring its inherent convexity. Finally, some heuristic beamforming solutions for the ease of implementation have been presented and their performance has been evaluated via simulations.

APPENDIX A

Proof: Assume that $\boldsymbol{S}^*$ is the optimal covariance matrix of *Problem 4* with $\gamma = \gamma^o$, where $\boldsymbol{S}^* \neq \boldsymbol{S}^o$. If $\min_{\boldsymbol{h}_s \in \mathcal{H}_s} \boldsymbol{h}_s^\dagger \boldsymbol{S}^* \boldsymbol{h}_s < \min_{\boldsymbol{h}_s \in \mathcal{H}_s} \boldsymbol{h}_s^\dagger \boldsymbol{S}^o \boldsymbol{h}_s$, $\boldsymbol{S}^o$ is a better solution for *Problem 4* since it satisfies all the constraints. This contradicts the assumption that $\boldsymbol{S}^*$ is the optimal solution for *Problem 4*. If $\min_{\boldsymbol{h}_s \in \mathcal{H}_s} \boldsymbol{h}_s^\dagger \boldsymbol{S}^* \boldsymbol{h}_s > \min_{\boldsymbol{h}_s \in \mathcal{H}_s} \boldsymbol{h}_s^\dagger \boldsymbol{S}^o \boldsymbol{h}_s$, then $\boldsymbol{S}^*$ is a better solution for *Problem 2* since $\max_{\boldsymbol{h}_e \in \mathcal{H}_e} \boldsymbol{h}_e \boldsymbol{S}^* \boldsymbol{h}_e \leq \gamma^o$. This contradicts the assumption that $\boldsymbol{S}^o$ is the optimal solution for *Problem 2*. Therefore, $\min_{\boldsymbol{h}_s \in \mathcal{H}_s} \boldsymbol{h}_s^\dagger \boldsymbol{S}^* \boldsymbol{h}_s = \min_{\boldsymbol{h}_s \in \mathcal{H}_s} \boldsymbol{h}_s^\dagger \boldsymbol{S}^o \boldsymbol{h}_s$ and $\boldsymbol{S}^* = \boldsymbol{S}^o$. ■

APPENDIX B

Proof: The equivalency of the two problems can be shown via *Problem 4*. Denote the optimal objective values of *Problem 2* and *Problem 6* by f^o and $\tilde{f}$, respectively. The proof can be divided into two parts. First, we shall show that the optimal objective value of *Problem 2* can be achieved by *Problem 6*, i.e., $f^o \leq \tilde{f}$. Denote $t^o = \min_{\boldsymbol{h}_s \in \mathcal{H}_s} \boldsymbol{h}_s^\dagger \boldsymbol{S}^o \boldsymbol{h}_s$, then the maximum value of *Problem 2* is $f^o = (1 + t^o)/(1 + \gamma^o)$. By Proposition 1, $\boldsymbol{S}^o$ is also optimal for *Problem 4* with $\gamma = \gamma^o$. Then, we have $g(\gamma^o) = t^o$. Therefore, f^o is achievable for Problem 6. Next, we shall show by contradiction that the maximum objective value of *Problem 6* can also be achieved by *Problem 2*, i.e., $f^o \geq \tilde{f}$. Denote the optimal solution of *Problem 6* by $\tilde{\gamma}$ and the optimal solution of *Problem 4* with $\gamma = \tilde{\gamma}$ by $\tilde{\boldsymbol{S}}$. If $f^o < \tilde{f}$, then we have $f^o < (1 + \min_{\boldsymbol{h}_s \in \mathcal{H}_s} \boldsymbol{h}_s^\dagger \tilde{\boldsymbol{S}} \boldsymbol{h}_s)/(1 + \tilde{\gamma}) \leq (\min_{\boldsymbol{h}_s \in \mathcal{H}_s} (1 + \boldsymbol{h}_s^\dagger \tilde{\boldsymbol{S}} \boldsymbol{h}_s)/\max_{\boldsymbol{h}_e \in \mathcal{H}_e} (1 + \boldsymbol{h}_e^\dagger \tilde{\boldsymbol{S}} \boldsymbol{h}_e))$, which indicates that $\tilde{\boldsymbol{S}}$ is a better solution for *Problem 2* than $\boldsymbol{S}^o$. This contradicts the assumption that $\boldsymbol{S}^o$ is the optimal solution for *Problem 2*. Hence, we have $f^o \leq \tilde{f}$. The proof is thus completed by combining the two parts. ■

APPENDIX C

Proof: We will first show that $g(\gamma)$ is a concave function. Note that *Problem 4* and *Problem 5* are equivalent with the same objective value, and strong duality holds for the convex *Problem 5*. Thus, we have

$$g(\gamma) = \min_{\boldsymbol{\Phi} \succeq 0} \max_{(\boldsymbol{S}, t, s, p, e) \in \mathcal{F}} L(\boldsymbol{S}, t, s, p, e, \boldsymbol{\Phi}, \gamma) \tag{74}$$

where $\boldsymbol{\Phi}$ is the Lagrange multiplier associated with (40); $\mathcal{F}$ is the combined constraint set defined by (37), (38), and (39), i.e., $\mathcal{F} = \{\boldsymbol{S} \succeq 0, t, s, p, e \geq 0 | (37), (38), (39)\}$; and $L(\boldsymbol{S}, t, s, p, e, \boldsymbol{\Phi}, \gamma)$ is the partial Lagrangian with respect to the constraint (40). Furthermore, denoting

$$\boldsymbol{\Phi} = \begin{bmatrix} \phi_a & \boldsymbol{\Phi}_{b,1\times N} \\ \boldsymbol{\Phi}_{b,1\times N}^\dagger & \boldsymbol{\Phi}_{c,N\times N} \end{bmatrix} \tag{75}$$

$$\boldsymbol{A}(\boldsymbol{S}, e) = \begin{bmatrix} -\hat{\boldsymbol{h}}_e^\dagger \boldsymbol{S} \hat{\boldsymbol{h}}_e - e & -\hat{\boldsymbol{h}}_e^\dagger \boldsymbol{S} \\ -\boldsymbol{S} \hat{\boldsymbol{h}}_e & -\boldsymbol{S} + e\boldsymbol{W}_e \end{bmatrix} \tag{76}$$

$$\boldsymbol{B}(\gamma) = \begin{bmatrix} \gamma & \boldsymbol{0}_{1\times N} \\ \boldsymbol{0}_{N\times 1} & \boldsymbol{0}_{N\times N} \end{bmatrix} \tag{77}$$

we have

$$L(\boldsymbol{S}, t, s, p, e, \boldsymbol{\Phi}, \gamma) = t + \operatorname{tr}(\boldsymbol{\Phi}(\boldsymbol{A}(\boldsymbol{S}, e) + \boldsymbol{B}(\gamma))) \tag{78}$$

$$= t + \operatorname{tr}(\boldsymbol{\Phi}\boldsymbol{A}(\boldsymbol{S}, e))) + \phi_a \gamma. \tag{79}$$

Then, the concavity of $g(\gamma)$ will be shown by the definition of convexity. Suppose $\gamma_1, \gamma_2 \geq 0$. Then, for any $0 \leq \theta \leq 1$, we have

$$\begin{aligned} & g(\theta\gamma_1 + (1-\theta)\gamma_2) \\ &= \min_{\boldsymbol{\Phi} \succeq 0} \max_{(\boldsymbol{S}, t, s, p, e) \in \mathcal{F}} L(\boldsymbol{S}, t, s, p, e, \boldsymbol{\Phi}, \theta\gamma_1 + (1-\theta)\gamma_2) \\ &= \min_{\boldsymbol{\Phi} \succeq 0} \max_{(\boldsymbol{S}, t, s, p, e) \in \mathcal{F}} (\theta L(\boldsymbol{S}, t, s, p, e, \boldsymbol{\Phi}, \gamma_1) \\ &\qquad + (1-\theta) L(\boldsymbol{S}, t, s, p, e, \boldsymbol{\Phi}, \gamma_2)) \\ &\geq \min_{\boldsymbol{\Phi} \succeq 0} \max_{(\boldsymbol{S}, t, s, p, e) \in \mathcal{F}} \theta L(\boldsymbol{S}, t, s, p, e, \boldsymbol{\Phi}, \gamma_1) \\ &\quad + \min_{\boldsymbol{\Phi} \succeq 0} \max_{(\boldsymbol{S}, t, s, p, e) \in \mathcal{F}} (1-\theta) L(\boldsymbol{S}, t, s, p, e, \boldsymbol{\Phi}, \gamma_2) \\ &= \theta g(\gamma_1) + (1-\theta) g(\gamma_2). \end{aligned} \tag{80}$$

Therefore, $g(\gamma)$ is a concave function of γ. Furthermore, it can be easily shown that the superlevel set of (41) is concave. Therefore, by the definition of quasi-convexity, (41) is quasi-concave [24]. ■

REFERENCES

[1] S. Haykin, "Cognitive radio: Brain-empowered wireless communications," *IEEE J. Sel. Areas Commun.*, vol. 23, no. 2, pp. 201–220, Feb. 2005.

[2] R. Zhang, Y.-C. Liang, and S. Cui, "Dynamic resource allocation in cognitive radio networks: A convex optimization perspective," *IEEE Signal Process. Mag.*, vol. 27, no. 3, pp. 102–114, May 2010.

[3] R. Zhang and Y.-C. Liang, "Exploiting multi-antennas for opportunistic spectrum sharing in cognitive radio networks," *IEEE J. Sel. Topics Signal Process.*, vol. 2, no. 1, pp. 88–102, Feb. 2008.

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

[5] S. K. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 24, no. 4, pp. 451–456, Jul. 1978.

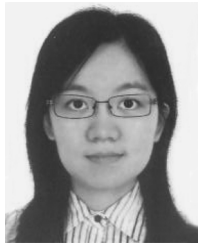
[6] Y. Liang, H. V. Poor, and S. Shamai, "Secure communication over fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2470–2492, Jun. 2008.

[7] E. Tekin and A. Yener, "The general Gaussian multiple-access and two-way wiretap channels: Achievable rates and cooperative jamming," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2735–2751, Jun. 2008.

[8] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," 2007 [Online]. Available: http://aps.arxiv.org/abs/0710.1920

[9] T. Liu and S. Shamai (Shitz), "A note on the secrecy capacity of the multiple-antenna wiretap channel," *IEEE Trans. Inf. Theory*, vol. 55, no. 6, pp. 2547–2553, Jun. 2009.

[10] R. Bustin, R. Liu, H. V. Poor, and S. Shamai (Shitz), "An MMSE approach to the secrecy capacity of the MIMO Gaussian wiretap channel," in *EURASIP J. Wireless Commun. Netw.*, 2009.
[11] Y. Pei, Y.-C. Liang, K. C. Teh, and K. H. Li, "Achieving cognitive and secure transmissions using multiple antennas," in *Proc. IEEE Int. Symp. Pers., Indoor and Mobile Radio Commun. (PIMRC'09)*, Sep. 2009, pp. 1–5.
[12] Y. Pei, Y.-C. Liang, K. C. Teh, and K. H. Li, "Secure communication over MISO cognitive radio channels," *IEEE Trans. Wireless Commun.*, vol. 9, no. 4, pp. 1494–1502, Apr. 2010.
[13] X. Zhang, D. P. Palomar, and B. Ottersten, "Statistically robust design of linear MIMO transceivers," *IEEE Trans. Signal Process.*, vol. 56, no. 8, pp. 3678–3689, Aug. 2008.
[14] A. Wiesel, Y. C. Eldar, and S. Shamai, "Optimization of the MIMO compound capacity," *IEEE Trans. Wireless Commun.*, vol. 6, no. 3, pp. 1094–1101, Mar. 2007.
[15] M. B. Shenouda and T. N. Davidson, "Convex conic formulations of robust downlink precoder designs with quality of service constraints," *IEEE J. Sel. Topics Signal Process.*, vol. 1, no. 4, pp. 714–724, Dec. 2007.
[16] A. Pascual-Iserte, D. P. Palomar, A. I. Pérez-Neira, and M. A. Lagunas, "A robust maximin approach for MIMO communications with imperfect channel state information based on convex optimization," *IEEE Trans. Signal Process.*, vol. 54, no. 1, pp. 346–360, Jan. 2006.
[17] L. Zhang, Y.-C. Liang, Y. Xin, and H. V. Poor, "Robust cognitive beamforming with partial channel state information," *IEEE Trans. Wireless Commun.*, vol. 8, no. 8, pp. 4143–4153, Aug. 2009.
[18] K. T. Phan, S. A. Vorobyov, N. D. Sidiropoulos, and C. Tellambura, "Spectrum sharing in wireless networks via QoS-aware secondary multicast beamforming," *IEEE Trans. Signal Process.*, vol. 57, no. 6, pp. 2323–2335, Jun. 2009.
[19] G. Zheng, K.-K. Wong, and B. Ottersten, "Robust cognitive beamforming with bounded channel uncertainties," *IEEE Trans. Signal Process.*, vol. 57, no. 12, pp. 4871–4881, Dec. 2009.
[20] Y. Liang and H. V. Poor, "Secure communication over fading channels," in *Proc. 44th Annu. Allerton Conf. Commun., Contr. Comput.*, Sep. 2006, pp. 817–823.
[21] Y. Liang, G. Kramer, H. V. Poor, and S. Shamai, "Compound wiretap channels," in *Proc. 45th Annu. Allerton Conf. on Commun., Contr. Comput.*, Sep. 2007, pp. 136–143.
[22] Y. Liang, H. V. Poor, and S. Shamai (Shitz), "Information theoretic security," *Found. Trends in Commun. Inf. Theory*, vol. 5, no. 4–5, pp. 355–580, 2008.
[23] H. Wiengarten, Y. Steinberg, and S. Shamai (Shitz), "The capacity region of the Gaussian multiple-input multiple-output broadcast channel," *IEEE Trans. Inf. Theory*, vol. 52, no. 9, pp. 3936–3964, Sep. 2006.
[24] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge, U.K.: Cambridge Univ. Press, 2004.
[25] S. Boyd, L. E. Ghaoui, E. Feron, and V. Balakrishnan, *Linear Matrix Inequalities in System and Control Theory*. Philadelphia, PA: SIAM, 1994.
[26] Z.-Q. Luo, J. F. Sturm, and S. Zhang, "Multivariate nonnegative quadratic mappings," *SIAM J. Optimiz.*, vol. 14, pp. 1140–1162, 2004.
[27] L. Zhang, Y.-C. Liang, Y. Pei, and R. Zhang, "Robust beamforming design: From cognitive radio MISO channels to secrecy MISO channels," in *Proc. IEEE Global TeleCommun. Conf. (GLOBECOM'09)*, Dec. 2009, pp. 1–5.
[28] L. Zhang, R. Zhang, Y.-C. Liang, Y. Xin, and S. Cui, "On the relationship between the multi-antenna secrecy communications and cognitive radio communications," *IEEE Trans. Commun.*, vol. 58, no. 6, pp. 1877–1886, Jun. 2010.
[29] J. F. Sturm, "Using SeDuMi 1.02, a MATLAB toolbox for optimization over symmetric cones," *Optimiz. Methods Software*, pp. 625–653, 1999.
[30] N. D. Sidiropoulos, T. N. Davidson, and Z.-Q. Luo, "Transmit beamforming for physical-layer multicasting," *IEEE Trans. Signal Process.*, vol. 54, no. 6, pp. 2239–2251, Jun. 2006.
[31] Z.-Q. Luo, W.-K. Ma, A. M.-C. So, Y. Ye, and S. Zhang, "Semidefinite relaxation of quadratic optimization problems," *IEEE Signal Process. Mag.*, vol. 27, no. 3, pp. 20–34, May 2010.



Yiyang Pei (S'09) received the B.E. degree in electrical and electronic engineering from Nanyang Technological University (NTU), Singapore, in 2007.

She is currently working toward the Ph.D degree in the School of Electrical and Electronic Engineering, NTU, and with the Institute for Infocomm Research (I2R), A*STAR, Singapore. Her research interests are in the area of wireless communications, with current emphasis on resource allocation in cognitive radio networks.

Ying-Chang Liang (A'00–SM'00–F'11) received the B.Eng. and Ph.D. degrees in electrical engineering from Jilin University, Changchun, China, in 1989 and 1993, respectively.

He is currently a Senior Scientist with the Institute for Infocomm Research (I2R), A*STAR, and holds an Associate Professorship position with Nanyang Technological University, both in Singapore. He was a visiting scholar with the Department of Electrical Engineering, Stanford University, Stanford, CA, from December 2002 to December 2003. His research interest includes cognitive radio, dynamic spectrum access, reconfigurable signal processing for broadband communications, space-time wireless communications, wireless networking, information theory, and statistical signal processing.

Dr. Liang is an Associate Editor of the IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY. He served as an Associate Editor of the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS from 2002 to 2005, Lead Guest-Editor of the IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, Special Issue on Cognitive Radio: Theory and Applications, and the Special Issue on Advances in Cognitive Radio Networking and Communications, Lead Guest-Editor of EURASIP *Journal on Advances in Signal Processing* Special Issue on Advanced Signal Processing for Cognitive Radio, as well as Guest Editor of *Computer Networks Journal* (Elsevier) Special Issue on Cognitive Wireless Networks. He received the Best Paper Awards from IEEE VTC-Fall in 1999, IEEE PIMRC in 2005, and EURASIP *Journal on Wireless Communications and Networking* in 2010. He also received the Institute of Engineers Singapore (IES) Prestigious Engineering Achievement Award in 2007.

Kah Chan Teh (S'96–M'99–SM'07) received the B.Eng. and Ph.D. degrees in electrical engineering from Nanyang Technological University (NTU), Singapore, in 1995 and 1999, respectively.

Since July 1999, he has been with NTU where he is currently an Associate Professor with the Division of Communication Engineering. His research interests are in the areas of signal processing for communications, performance evaluations of interference suppression for spread-spectrum communication systems, multiuser detection in CDMA systems, cognitive radios, and cooperative communication systems.

Dr. Teh received the Best Teacher of the Year Award from NTU in 2005.

Kwok Hung Li (S'87–M'89–SM'99) received the B.Sc. degree in electronics from the Chinese University of Hong Kong in 1980 and the M.Sc. and Ph.D. degrees in electrical engineering from the University of California, San Diego, in 1983 and 1989, respectively.

Since December 1989, he has been with the Nanyang Technological University, Singapore. He is currently an Associate Professor with the Division of Communication Engineering and serves as the Head of the Division. His research interest has centered on the area of digital communication theory with emphasis on spread-spectrum communications, mobile communications, coding and signal processing.