This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE Globecom 2011 proceedings.

Robust Secure Transmission in MISO Channels With Imperfect ECSI

Jing Huang and A. Lee Swindlehurst
Electrical Engineering and Computer Science
University of California, Irvine, CA 92697
Email: {jing.huang; swindle}@uci.edu

***Abstract*—This paper studies robust transmission schemes for MISO wiretap channels with imperfect channel state information (CSI) for the eavesdropper link. Both the cases of direct transmission and cooperative jamming with a helper are investigated. The error in the eavesdropper's CSI is assumed to be norm-bounded, and robust transmit covariance matrices are obtained based on worst-case secrecy rate maximization, under both individual and global power constraints. Numerical results show the advantage of the proposed robust design. In particular, under a global power constraint, although cooperative jamming is not necessary for optimal transmission with perfect eavesdropper's CSI, we show that robust jamming support can increase the secrecy rate in the presence of channel mismatch.**

I. Introduction

Security is an important concern in wireless networks. There has recently been considerable interest in the use of physical layer mechanisms to improve the security of wireless transmissions. The theoretical basis of this area was initiated by Wyner, who introduced and studied the wiretap channel [1]. Recently, considerable research has investigated secrecy in wiretap channels with multiple antennas [2], [3]. In particular, for multiple-input single-output (MISO) wiretap cannels, the optimal transmit covariance matrix was found to be single-stream beamforming obtained via a closed-form solution [4], [5].

With the additional degrees of freedom in multi-antenna or multi-node systems, some work has considered improving the secrecy rate through the use of artificial interference [6], [7]. Some recent work has also considered using friendly helpers to provide jamming signals to confuse the eavesdropper [8]–[10]. This approach is often referred to as cooperative jamming. The optimal transmit weights for multiple single-antenna helpers was studied in [8], where a global power constraint was imposed. A similar case with individual power constraints was studied in [9]. However, most of the previous work on cooperative jamming assumes perfect global channel state information (CSI), including CSI for the eavesdropper (which we refer to as ECSI). This motivates us to investigate the case when the transmitters have only imperfect ECSI.

In this paper, we study robust transmit precoder design for MISO wiretap channels. We assume that perfect CSI for the legitimate links is available at both transmitters, while for the eavesdropper links there exist channel mismatches that are norm-bounded by some known constants. Following [4], Gaussian inputs are assumed in the paper. We focus on obtaining robust transmit covariance matrices for both direct transmission (DT) and the cooperative jamming (CJ) schemes with a helper (friendly jammer), based on maximizing the worst-case secrecy rate. We begin by studying the optimization problem under an individual power constraint, and then a more complicated case with a global power constraint is investigated.

The organization of the paper is as follows. Section II describes the system model. In Section III, robust design of the transmit covariance matrix is studied for the direct transmission scheme. The robust cooperative jamming scheme is then investigated in Section IV. Simulation examples are given in Section V, and conclusions are drawn in Section VI.

This work was supported by the U.S. Army Research Office under the Multi-University Research Initiative (MURI) grant W911NF-07-1-0318.

II. System Model

We consider a MISO communication system with a source node (Alice), a helper (Helper), a destination (Bob), and an eavesdropper (Eve). The number of antennas possessed by Alice and the Helper are denoted by N_a and N_h, respectively, while both Bob and Eve are single-antenna nodes. In this model, Alice sends private messages to Bob in the presence of Eve, who is able to eavesdrop on the link between Alice and Bob. The Helper can choose to be silent or to transmit artificial interference signals to confuse Eve. Both cases will be considered in the paper, and we refer to the former case as direct transmission (DT) and the latter as cooperative jamming (CJ).

A. Direct Transmission

When there is no support from the Helper, the received signals at Bob and Eve are given by

$$y_b = \mathbf{h}_b\mathbf{x} + n_b \tag{1a}$$

$$y_e = \mathbf{h}_e\mathbf{x} + n_e \tag{1b}$$

where $\mathbf{x}$ is the signal vector transmitted by Alice, the covariance matrix of $\mathbf{x}$ is denoted by $\mathbf{Q}_x = \mathbb{E}\{\mathbf{x}\mathbf{x}^H\}$, $\mathrm{tr}(\mathbf{Q}_x) \le P_S$ where P_S is the transmit power constraint on Alice, and $\{\mathbf{h}_b, \mathbf{h}_e\}$ are the $1 \times N_a$ channel vectors for Bob and Eve, respectively. The terms n_b and n_e represent naturally occurring noise at Bob and Eve, and we assume that n_b and n_e are zero-mean circular complex Gaussian with variance σ_b^2 and σ_e^2. We will assume without loss of generality that $\sigma_b^2 = \sigma_e^2 = \sigma^2$.

978-1-4244-9268-8/11/$26.00 ©2011 IEEE

B. Cooperative Jamming

For the case where the Helper joins the network by transmitting an i.i.d. Gaussian interference signal $\mathbf{z}$, Bob and Eve then receive

$$y_b = \mathbf{h}_b\mathbf{x} + \mathbf{g}_b\mathbf{z} + n_b \tag{2a}$$
$$y_e = \mathbf{h}_e\mathbf{x} + \mathbf{g}_e\mathbf{z} + n_e \tag{2b}$$

where we denote $\mathbf{Q}_z = \mathbb{E}\{\mathbf{z}\mathbf{z}^H\}$ and $\mathrm{tr}(\mathbf{Q}_z) \leq P_J$.

C. Channel Mismatch

For the channels between the transmitters and Eve, only estimates $\tilde{\mathbf{h}}_e$ and $\tilde{\mathbf{g}}_e$ are available at Alice and the Helper, respectively. We define the channel error vectors as

$$\mathbf{e}_h = \mathbf{h}_e - \tilde{\mathbf{h}}_e \tag{3a}$$
$$\mathbf{e}_g = \mathbf{g}_e - \tilde{\mathbf{g}}_e, \tag{3b}$$

and we assume that the channel mismatches lie in the bounded sets $\mathcal{E}_h = \{\mathbf{e}_h : ||\mathbf{e}_h||^2 \leq \epsilon_h^2\}$ and $\mathcal{E}_g = \{\mathbf{e}_g : ||\mathbf{e}_g||^2 \leq \epsilon_g^2\}$, where ϵ_h and ϵ_g are known constants.

III. Robust Direct Transmission

In this section, we consider the scenario where there is no jamming support from the Helper. According to the signal model (1) and (3), the secrecy rate is [4]

$$R_s = \log_2\left(1 + \frac{1}{\sigma^2}\mathbf{h}_b\mathbf{Q}_x\mathbf{h}_b^H\right) - \log_2\left(1 + \frac{1}{\sigma^2}(\tilde{\mathbf{h}}_e + \mathbf{e}_h)\mathbf{Q}_x(\tilde{\mathbf{h}}_e^H + \mathbf{e}_h)\right). \tag{4}$$

A power constraint is imposed such that $\mathbf{Q}_x \in \mathcal{Q}_x = \{\mathbf{Q}_x : \mathbf{Q}_x \succeq 0, \mathrm{tr}(\mathbf{Q}_x) \leq P_S\}$. For the case where perfect ECSI is available, the optimal $\mathbf{Q}_x$ has been found to be unit-rank and the corresponding beamformer is the generalized eigenvector of the matrix pencil $(\sigma^2\mathbf{I} + P_S\mathbf{h}_b^H\mathbf{h}_b, \sigma^2\mathbf{I} + P_S\mathbf{h}_e^H\mathbf{h}_e)$ corresponding to the largest generalized eigenvalue [4], [5].

We consider the case where Alice does not have perfect knowledge of the channel to Eve, but only has an estimate $\tilde{\mathbf{h}}_e$. We focus on optimizing the worst-case performance, where we maximize the secrecy rate for the worst-case channel mismatch $\mathbf{e}_h$ in the bounded set $\mathcal{E}_h$. Therefore, the optimization problem (4) becomes

$$\max_{\mathbf{Q}_x \in \mathcal{Q}_x} \min_{\mathbf{e}_h \in \mathcal{E}_h} \frac{\sigma^2 + \mathbf{h}_b\mathbf{Q}_x\mathbf{h}_b^H}{\sigma^2 + (\tilde{\mathbf{h}}_e + \mathbf{e}_h)\mathbf{Q}_x(\tilde{\mathbf{h}}_e + \mathbf{e}_h)^H}. \tag{5}$$

The difficulty in solving this problem comes from the inner minimization over $\mathbf{e}_h$. As will be discussed later, the minimization is actually a non-convex problem. However, we will show that through a proper transformation, problem (5) can be converted to a solvable quasiconvex optimization problem.

Proposition 1: Problem (5) is equivalent to the following problem

$$\min_{\mathbf{Q}_x, \mu, \mathbf{\Psi}} \quad \frac{\sigma^2 + \mu\epsilon_h^2 + \mathrm{tr}[(\mathbf{Q}_\mathrm{x} + \mathbf{\Psi})\tilde{\mathbf{h}}_\mathrm{e}^\mathrm{H}\tilde{\mathbf{h}}_\mathrm{e}]}{\sigma^2 + \mathrm{tr}(\mathbf{Q}_\mathrm{x}\mathbf{h}_\mathrm{b}^\mathrm{H}\mathbf{h}_\mathrm{b})} \tag{6a}$$
$$\text{s.t.} \quad \begin{bmatrix} \mu\mathbf{I}_{N_a} - \mathbf{Q}_x & \mathbf{Q}_x \\ \mathbf{Q}_x & \mathbf{\Psi} \end{bmatrix} \succeq 0 \tag{6b}$$
$$\mathrm{tr}(\mathbf{Q}_\mathrm{x}) \leq \mathrm{P_S} \tag{6c}$$
$$\mathbf{Q}_x \succeq 0, \mu \geq 0. \tag{6d}$$

Proof: The maximin problem (5) can be transformed to

$$\max_{\mathbf{Q}_x \in \mathcal{Q}_x, v} \quad \frac{\sigma^2 + \mathbf{h}_b\mathbf{Q}_x\mathbf{h}_b^H}{v}$$
$$\text{s.t.} \quad \sigma^2 + (\tilde{\mathbf{h}}_e + \mathbf{e}_h)\mathbf{Q}_x(\tilde{\mathbf{h}}_e + \mathbf{e}_h)^H \leq v, \ \forall \mathbf{e}_h : \mathbf{e}_h\mathbf{e}_h^H \leq \epsilon_h^2.$$

where the constraint can also be expressed as

$$-\mathbf{e}_h\mathbf{Q}_x\mathbf{e}_h^H - 2\mathrm{Re}(\tilde{\mathbf{h}}_e\mathbf{Q}_x\mathbf{e}_h^H) - \tilde{\mathbf{h}}_e\mathbf{Q}_x\tilde{\mathbf{h}}_e^H - \sigma^2 + v \geq 0, \quad \forall \mathbf{e}_h : -\mathbf{e}_h^H\mathbf{e}_h + \epsilon_h^2 \geq 0. \tag{8}$$

Using the $\mathcal{S}$-Procedure [11], we know that (8) holds if and only if there exists a $\mu \geq 0$ such that

$$\begin{bmatrix} \mu\mathbf{I}_{N_a} - \mathbf{Q}_x & -\mathbf{Q}_x\tilde{\mathbf{h}}_e^H \\ -\tilde{\mathbf{h}}_e\mathbf{Q}_x & -\tilde{\mathbf{h}}_e\mathbf{Q}_x\tilde{\mathbf{h}}_e^H - \sigma^2 - \mu\epsilon_h^2 + v \end{bmatrix} \succeq 0. \tag{9}$$

Then we can use the property of the generalized Schur complement [12] and rewrite (9) as

$$\sigma^2 + \mu\epsilon_h^2 + \tilde{\mathbf{h}}_e\mathbf{Q}_x\tilde{\mathbf{h}}_e^H + \tilde{\mathbf{h}}_e\mathbf{Q}_x(\mu\mathbf{I}_{N_a} - \mathbf{Q}_x)^\dagger\mathbf{Q}_x\tilde{\mathbf{h}}_e^H \leq v,$$

where $(\cdot)^\dagger$ represents the pseudo-inverse. Therefore, the maximin problem in (5) becomes a maximization problem

$$\max_{\mathbf{Q}_x \in \mathcal{Q}_x, \mu \geq 0} \frac{\sigma^2 + \mathbf{h}_b\mathbf{Q}_x\mathbf{h}_b^H}{\sigma^2 + \mu\epsilon_h^2 + \tilde{\mathbf{h}}_e\mathbf{Q}_x\tilde{\mathbf{h}}_e^H + \tilde{\mathbf{h}}_e\mathbf{Q}_x(\mu\mathbf{I}_{N_a} - \mathbf{Q}_x)^\dagger\mathbf{Q}_x\tilde{\mathbf{h}}_e^H}$$

which is equivalent to

$$\max_{\mathbf{Q}_x \in \mathcal{Q}_x, \mu \geq 0, \mathbf{\Psi}} \quad \frac{\sigma^2 + \mathbf{h}_b\mathbf{Q}_x\mathbf{h}_b^H}{\sigma^2 + \mu\epsilon_h^2 + \tilde{\mathbf{h}}_e\mathbf{Q}_x\tilde{\mathbf{h}}_e^H + \tilde{\mathbf{h}}_e\mathbf{\Psi}\tilde{\mathbf{h}}_e^H} \tag{10a}$$
$$\text{s.t.} \quad \mathbf{Q}_x(\mu\mathbf{I}_{N_a} - \mathbf{Q}_x)^\dagger\mathbf{Q}_x \preceq \mathbf{\Psi}. \tag{10b}$$

Next, we use the Schur complement to convert (10b) into a linear matrix inequality (LMI), and the maximization problem is then given by

$$\min_{\mathbf{Q}_x \in \mathcal{Q}_x, \mu \geq 0, \mathbf{\Psi}} \quad \frac{\sigma^2 + \mu\epsilon_h^2 + \mathrm{tr}[(\mathbf{Q}_\mathrm{x} + \mathbf{\Psi})\tilde{\mathbf{h}}_\mathrm{e}^\mathrm{H}\tilde{\mathbf{h}}_\mathrm{e}]}{\sigma^2 + \mathrm{tr}(\mathbf{Q}_\mathrm{x}\mathbf{h}_\mathrm{b}^\mathrm{H}\mathbf{h}_\mathrm{b})}$$
$$\text{s.t.} \quad \begin{bmatrix} \mu\mathbf{I}_{N_a} - \mathbf{Q}_x & \mathbf{Q}_x \\ \mathbf{Q}_x & \mathbf{\Psi} \end{bmatrix} \succeq 0,$$

which completes the proof. ■

Problem (6) consists of a linear fractional objective function (with a positive denominator), which is thus quasiconvex, with a set of LMI constraints. Therefore, we can solve this problem efficiently via the bisection method [11].

Note that the optimal covariance $\mathbf{Q}_x^*$ obtained from Proposition 1 is based on a hidden worst-case channel mismatch

$\mathbf{e}_h^*$. Next, we will explicitly determine $\mathbf{e}_h^*$ under the bounded constraint. The problem is formulated as

$$\max_{\mathbf{e}_h} \quad (\tilde{\mathbf{h}}_e + \mathbf{e}_h)\mathbf{Q}_x^*(\tilde{\mathbf{h}}_e + \mathbf{e}_h)^H \tag{11a}$$

$$\text{s.t.} \quad ||\mathbf{e}_h|| \leq \epsilon_h. \tag{11b}$$

This is a non-convex problem since we want to maximize a convex function. However, we can still obtain the global optimum by solving its dual problem, as explained in the following proposition.

Proposition 2: The worst-case channel mismatch for problem (11) is given by $\mathbf{e}_h = \mathbf{h}_e\mathbf{Q}_x^*(\lambda\mathbf{I} - \mathbf{Q}_x^*)^\dagger$, where λ is the solution of the following problem

$$\max_{\lambda\geq 0,\gamma} \quad \gamma \tag{12a}$$

$$\text{s.t.} \quad \begin{bmatrix} \lambda\mathbf{I} - \mathbf{Q}_x^* & \mathbf{Q}_x^*\tilde{\mathbf{h}}_e^H \\ \tilde{\mathbf{h}}_e\mathbf{Q}_x^* & -\tilde{\mathbf{h}}_e\mathbf{Q}_x^*\tilde{\mathbf{h}}_e^H - \lambda\epsilon_h^2 - \gamma \end{bmatrix} \succeq 0. \tag{12b}$$

Proof: Problem (11) can be rewritten as

$$\min_{\mathbf{e}_h} \quad -\mathbf{e}_h\mathbf{Q}_x^*\mathbf{e}_h^H - 2\text{Re}(\tilde{\mathbf{h}}_e\mathbf{e}_h^H) - \tilde{\mathbf{h}}_e\mathbf{Q}_x^*\tilde{\mathbf{h}}_e^H \tag{13a}$$

$$\text{s.t.} \quad \mathbf{e}_h\mathbf{e}_h^H \leq \epsilon_h^2. \tag{13b}$$

This is a non-convex problem since its Hessian is negative semidefinite, *i.e.* $-\mathbf{Q}_x^* \preceq 0$, and the Lagrangian is

$$\begin{aligned} &L(\mathbf{e}_h, \lambda) \\ &= -\mathbf{e}_h\mathbf{Q}_x^*\mathbf{e}_h^H - 2\text{Re}(\tilde{\mathbf{h}}_e\mathbf{Q}_x^*\mathbf{e}_h^H) - \tilde{\mathbf{h}}_e\mathbf{Q}_x^*\tilde{\mathbf{h}}_e^H + \lambda(\mathbf{e}_h\mathbf{e}_h^H - \epsilon_h^2) \\ &= \mathbf{e}_h(\lambda\mathbf{I} - \mathbf{Q}_x^*)\mathbf{e}_h^H + 2\text{Re}(-\tilde{\mathbf{h}}_e\mathbf{Q}_x^*\mathbf{e}_h^H) - \tilde{\mathbf{h}}_e\mathbf{Q}_x^*\tilde{\mathbf{h}}_e^H - \lambda\epsilon_h^2 \end{aligned}$$

where $\lambda \geq 0$ and the dual function is given by

$$\begin{aligned} g(\lambda) &= \inf_{\mathbf{e}_h} L(\mathbf{e}_h, \lambda) \\ &= -\tilde{\mathbf{h}}_e\mathbf{Q}_x^*\tilde{\mathbf{h}}_e^H - \lambda\epsilon_h^2 - \tilde{\mathbf{h}}_e\mathbf{Q}_x^*(\lambda\mathbf{I} - \mathbf{Q}_x^*)^\dagger\mathbf{Q}_x^*\tilde{\mathbf{h}}_e^H \end{aligned}$$

where $\lambda\mathbf{I} - \mathbf{Q}_x^* \succeq 0$ and $\mathbf{Q}_x^*\tilde{\mathbf{h}}_e^H \in \mathcal{R}(\lambda\mathbf{I} - \mathbf{Q}_x^*)$. The unconstrained minimization of $L(\mathbf{e}_h, \lambda)$ w.r.t. $\mathbf{e}_h$ is achieved when $\mathbf{e}_h = \mathbf{h}_e\mathbf{Q}_x^*(\lambda\mathbf{I} - \mathbf{Q}_x^*)^\dagger$. The dual problem is thus

$$\max_{\lambda} \quad -\tilde{\mathbf{h}}_e\mathbf{Q}_x^*\tilde{\mathbf{h}}_e^H - \lambda\epsilon_h^2 - \tilde{\mathbf{h}}_e\mathbf{Q}_x^*(\lambda\mathbf{I} - \mathbf{Q}_x^*)^\dagger\mathbf{Q}_x^*\tilde{\mathbf{h}}_e^H \tag{14a}$$

$$\text{s.t.} \quad \lambda\mathbf{I} - \mathbf{Q}_x^* \succeq 0, \ \mathbf{Q}_x^*\tilde{\mathbf{h}}_e^H \in \mathcal{R}(\lambda\mathbf{I} - \mathbf{Q}_x^*). \tag{14b}$$

Using a Schur complement, the dual problem becomes the following SDP

$$\max_{\lambda\geq 0,\gamma} \quad \gamma \tag{15a}$$

$$\text{s.t.} \quad \begin{bmatrix} \lambda\mathbf{I} - \mathbf{Q}_x^* & \mathbf{Q}_x^*\tilde{\mathbf{h}}_e^H \\ \tilde{\mathbf{h}}_e\mathbf{Q}_x^* & -\tilde{\mathbf{h}}_e\mathbf{Q}_x^*\tilde{\mathbf{h}}_e^H - \lambda\epsilon_h^2 - \gamma \end{bmatrix} \succeq 0. \tag{15b}$$

Note that (13) is usually called a *trust region subproblem* (TRS), and it has been proven that strong duality holds for TRS although the objective function is non-convex [13]. Thus the optimal value of (13) and (15) are the same. ■

Note that (12) is a semidefinite program (SDP) and hence can be solved efficiently using, for example, the interior-point method [11].

IV. Robust Cooperative Jamming

We now consider the case when the Helper provides cooperative jamming to improve the secrecy rate. According to the signal model in (2) and (3), the secrecy rate is

$$\begin{aligned} R_s = &\log_2\left(1 + \frac{\mathbf{h}_b\mathbf{Q}_x\mathbf{h}_b^H}{\mathbf{g}_b\mathbf{Q}_z\mathbf{g}_b^H + \sigma^2}\right) \\ &- \log_2\left(1 + \frac{(\tilde{\mathbf{h}}_e + \mathbf{e}_h)\mathbf{Q}_x(\tilde{\mathbf{h}}_e + \mathbf{e}_h)^H}{(\tilde{\mathbf{g}}_e + \mathbf{e}_g)\mathbf{Q}_z(\tilde{\mathbf{g}}_e + \mathbf{e}_g)^H + \sigma^2}\right). \end{aligned} \tag{16}$$

We will first consider the optimization problem under individual power constraints, *i.e.* $\mathbf{Q}_x \in \mathcal{Q}_x = \{\mathbf{Q}_x : \mathbf{Q}_x \succeq 0, \text{tr}(\mathbf{Q}_x) \leq P_S\}$ and $\mathbf{Q}_z \in \mathcal{Q}_z = \{\mathbf{Q}_z : \mathbf{Q}_z \succeq 0, \text{tr}(\mathbf{Q}_z) \leq P_J\}$, and then we investigate a more complicated case where a global power constraint is imposed. We will use a zero-forcing (ZF) constraint $\mathbf{Q}_z\mathbf{g}_b^H = \mathbf{0}$ on the jamming signal for the CJ problem, since the ZF jamming offers performance close to the optimal cooperative jamming solution for MISO wiretap channels [14]. With this constraint, the maximization of R_S with respect to $\mathbf{Q}_z$ does not depend on $\mathbf{Q}_x$, although the optimal $\mathbf{Q}_x$ still depends on $\mathbf{Q}_z$. Thus, we will first optimize $\mathbf{Q}_z$ and then the optimal $\mathbf{Q}_x$ can be calculated.

A. Individual Power Constraint

For the case of perfect ECSI, the optimal $\mathbf{Q}_z$ under the ZF constraint is given by $\mathbf{Q}_z = P_J\mathbf{w}\mathbf{w}^H$ [14], where $\mathbf{w}$ is the unit-norm one-dimensional beamformer for the Helper, and

$$\mathbf{w}^* = \frac{(\mathbf{I}_{N_h} - \mathbf{P}_{gb})\mathbf{g}_e^H}{||(\mathbf{I}_{N_h} - \mathbf{P}_{gb})\mathbf{g}_e^H||}$$

where $\mathbf{P}_{gb} = \mathbf{g}_b^H(\mathbf{g}_b\mathbf{g}_b^H)^{-1}\mathbf{g}_b$ is the orthogonal projection onto the subspace spanned by $\mathbf{g}_b^H$. The optimal information covariance matrix $\mathbf{Q}_x$, similar to the perfect ECSI case discussed in Section III, is unit-rank and the corresponding beamformer is the generalized eigenvector of the matrix pencil $(\sigma^2\mathbf{I} + P_S\mathbf{h}_b^H\mathbf{h}_b, \sigma_z^2\mathbf{I} + P_S\mathbf{h}_e^H\mathbf{h}_e)$ with the largest generalized eigenvalue, where $\sigma_z^2 = \sigma^2 + \mathbf{g}_e\mathbf{Q}_z\mathbf{g}_e^H$.

For the case of imperfect ECSI, we still solve for the jamming covariance $\mathbf{Q}_z$ first, and the optimization problem becomes

$$\max_{\mathbf{Q}_z\in\mathcal{Q}_z} \min_{\mathbf{e}_g\in\mathcal{E}_g} \quad (\tilde{\mathbf{g}}_e + \mathbf{e}_g)\mathbf{Q}_z(\tilde{\mathbf{g}}_e + \mathbf{e}_g)^H \tag{17a}$$

$$\text{s.t.} \quad \mathbf{g}_b\mathbf{Q}_z\mathbf{g}_b^H = 0. \tag{17b}$$

Proposition 3: Problem (17) is equivalent to the following problem

$$\max_{\mathbf{Q}_z,\mu,\mathbf{\Psi}} \quad \text{tr}[(\mathbf{Q}_z - \mathbf{\Psi})\tilde{\mathbf{g}}_e^H\tilde{\mathbf{g}}_e] - \mu\epsilon_g^2 \tag{18a}$$

$$\text{s.t.} \quad \begin{bmatrix} \mu\mathbf{I}_{N_h} + \mathbf{Q}_z & \mathbf{Q}_z \\ \mathbf{Q}_z & \mathbf{\Psi} \end{bmatrix} \succeq 0 \tag{18b}$$

$$\mathbf{Q}_z \succeq 0, \ \mu \geq 0, \ \text{tr}(\mathbf{Q}_z) \leq P_J \tag{18c}$$

$$\mathbf{g}_b\mathbf{Q}_z\mathbf{g}_b^H = 0. \tag{18d}$$

Proof: The proof is along the same line as that for Proposition 1 and is omitted. ■

Problem (18) is an SDP that consists of a linear objective function together with a set of LMI constraints. Therefore, we can solve this problem efficiently. Note that the corresponding $\mathbf{e}_g^*$ can also be expressed explicitly via a method similar to that in (11)-(12). With solutions for $\mathbf{Q}_z^*$ and $\mathbf{e}_g^*$, we can follow (5)-(6) and formulate the optimization problem over $\mathbf{Q}_x$ as

$$\max_{\mathbf{Q}_x \in \mathcal{Q}_x} \min_{\mathbf{e}_h \in \mathcal{E}_h} \frac{\sigma^2 + (\tilde{\mathbf{g}}_e + \mathbf{e}_g^*)\mathbf{Q}_z^*(\tilde{\mathbf{g}}_e + \mathbf{e}_g^*)^H + \mathbf{h}_b \mathbf{Q}_x \mathbf{h}_b^H}{\sigma^2 + (\tilde{\mathbf{h}}_e + \mathbf{e}_h)\mathbf{Q}_x(\tilde{\mathbf{h}}_e + \mathbf{e}_h)^H}, \tag{19}$$

which can be solved with the same procedure as in Section III.

B. Global Power Constraint

As with the previous case, we will assume a zero-forcing constraint for the helper's jamming signal at Bob. We investigate the joint optimization over $\mathbf{Q}_x$, $\mathbf{Q}_z$ and the power allocation between Alice and the Helper, under the constraint that $\text{tr}(\mathbf{Q}_x)+\text{tr}(\mathbf{Q}_z) = p_1+p_2 \le P$. Unfortunately, a one-step joint optimization of (16) over the variables $\mathbf{Q}_x$, $\mathbf{Q}_z$, p_1 and p_2 is difficult to perform. Thus we use the primal decomposition method [15] by decomposing the original problem into several subproblems controlled by a master problem, and using an iterative method to find the solution. In this case, from the previous section, we know that the subproblems involving $\mathbf{Q}_z$ and $\mathbf{Q}_x$ in (17) and (19) are both convex for given p_1 and p_2. Thus our first step will be to estimate $\mathbf{Q}_x$ and $\mathbf{Q}_z$ for some initial p_1 and p_2, then we will find the optimal p_1 and p_2 for the resulting $\mathbf{Q}_x$ and $\mathbf{Q}_z$, and continue in this iterative manner to find the beamformers and power allocation.

First, for given $\mathbf{Q}_x$ and $\mathbf{Q}_z$, let $\mathbf{Q}_x = p_1\bar{\mathbf{Q}}_x$ and $\mathbf{Q}_z = p_2\bar{\mathbf{Q}}_z$ where $\bar{\mathbf{Q}}_x$ and $\bar{\mathbf{Q}}_z$ are normalized such that $\text{tr}(\bar{\mathbf{Q}}_x) = 1$ and $\text{tr}(\bar{\mathbf{Q}}_z) = 1$. Hence the maximization of the secrecy rate (16) with respect to p_1 and p_2 is equivalent to

$$\max_{p_1,p_2 \ge 0} \quad \frac{p_1p_2c_1c_3 + p_1c_1\sigma^2 + p_2c_3\sigma^2 + \sigma^4}{p_1c_2 + p_2c_3 + \sigma^2} \tag{20a}$$

$$\text{s.t.} \quad p_1 + p_2 \le P \tag{20b}$$

where $c_1 = \mathbf{h}_b\bar{\mathbf{Q}}_x\mathbf{h}_b^H$, $c_2 = (\tilde{\mathbf{h}}_e + \mathbf{e}_h)\bar{\mathbf{Q}}_x(\tilde{\mathbf{h}}_e + \mathbf{e}_h)^H$, $c_3 = (\tilde{\mathbf{g}}_e + \mathbf{e}_g)\bar{\mathbf{Q}}_z(\tilde{\mathbf{g}}_e + \mathbf{e}_g)^H$.

Lemma 1: Problem (20) is convex, and the optimum is achieved when $p_1 + p_2 = P$.

Proof: The convexity of (20a) can be validated by examining its second derivative, and the details are omitted. The proof of $p_1+p_2 = P$ is straightforward: assuming that the best power strategy is obtained as p_1' and p_2' where $p_1' + p_2' < P$, we can always increase p_2' up to $P-p_1'$ in order to improve the secrecy rate in (16), since the jamming signal $\mathbf{z}$ only interferes with Eve due to the ZF constraint. Therefore, the optimum is achieved when the entire power budget is used. ■

According to Lemma 1, we replace p_2 with $P - p_1$ and rewrite (20a) as

$$f(p_1) = -\frac{c_1c_3p_1^2 - (c_1c_3P + c_1\sigma^2 - c_3\sigma^2)p_1 - (c_3\sigma^2P + \sigma^4)}{(c_2 - c_3)p_1 + c_3P + \sigma^2}. \tag{21}$$

We can then obtain the optimal power allocation by finding the stationary point of $f(p_1)$. Taking the first-order derivative of $f(p_1)$ and equating it to zero, we have

$$\begin{cases} p_{1,1} = -\frac{c_3P+\sigma^2}{c_2-c_3} + \frac{\sqrt{\Delta}}{2c_1c_3(c_2-c_3)} \\ p_{1,2} = -\frac{c_3P+\sigma^2}{c_2-c_3} - \frac{\sqrt{\Delta}}{2c_1c_3(c_2-c_3)} \end{cases}$$

where

$$\Delta = 4c_1c_3(c_3P + \sigma^2)(c_2c_3\sigma^2 + c_1c_2c_3P + c_1c_2\sigma^2 - c_2^2\sigma^2).$$

Since p_1 lies in the range $[0, P]$, it is easy to verify that $p_{1,2}$ is not a solution since

$$\begin{cases} -\frac{c_3P+\sigma^2}{c_2-c_3} - \frac{\sqrt{\Delta}}{2c_1c_3(c_2-c_3)} \le 0, & \text{for } c_2 > c_3 \\ -\frac{c_3P+\sigma^2}{c_2-c_3} - \frac{\sqrt{\Delta}}{2c_1c_3(c_2-c_3)} \ge -\frac{c_3P}{c_2-c_3} \ge P, & \text{for } c_2 < c_3. \end{cases}$$

For the case of $c_2 = c_3$, maximizing $f(p_1)$ in (21) amounts to minimizing

$$f_1(p_1) = c_1c_3p_1^2 - (c_1c_3P + c_1\sigma^2 - c_3\sigma^2)p_1 - (c_3\sigma^2P + \sigma^4),$$

which is still a convex function with the minimizer

$$p_1 = \frac{c_1c_3P + c_1\sigma^2 - c_3\sigma^2}{2c_1c_3}. \tag{22}$$

Therefore, the optimal solutions for (20) can be expressed as

$$\begin{cases} p_1^* = \\ \quad \begin{cases} \min\left\{\left[-\frac{c_3P+\sigma^2}{c_2-c_3} + \frac{\sqrt{\Delta}}{2c_1c_3(c_2-c_3)}\right]^+, P\right\}, & \text{for } c_2 \ne c_3 \\ \min\left\{\left[\frac{c_1c_3P+c_1\sigma^2-c_3\sigma^2}{2c_1c_3}\right]^+, P\right\}, & \text{for } c_2 = c_3 \end{cases} \\ p_2^* = P - p_1^*. \end{cases} \tag{23}$$

Now we can conduct the joint optimization that considers both the information/jamming covariances and the power allocation between them. The main steps are outlined as follows:

Algorithm Joint optimization for robust CJ

Initialize $p_1^{(0)} = p_2^{(0)} = \frac{P}{2}$.

For iteration k

1) Let $P_S = p_1^{(k-1)}$, $P_J = p_2^{(k-1)}$ and solve problem (17) and (19) to obtain $\mathbf{Q}_z^{(k)}$, $\mathbf{e}_g^{(k)}$, $\mathbf{Q}_x^{(k)}$, and $\mathbf{e}_h^{(k)}$ respectively.
2) Let $\bar{\mathbf{Q}}_x^{(k)} = \frac{\mathbf{Q}_x^{(k)}}{\text{tr}(\mathbf{Q}_x^{(k)})}$, $\bar{\mathbf{Q}}_z^{(k)} = \frac{\mathbf{Q}_z^{(k)}}{\text{tr}(\mathbf{Q}_z^{(k)})}$ and solve problem (20) to obtain $p_1^{(k)}$ and $p_2^{(k)}$.
3) Apply the resulting $p_1^{(k)}$ and $p_2^{(k)}$ to step 1 and loop until convergence.

Our extensive numerical experiments, some results of which are shown in Section V, further illustrate that the global optimum is obtained through this procedure.

V. Numerical Results

In this section, we present some numerical examples of the proposed robust transmission schemes. For all examples, we assume Alice and the Helper both have four antennas, *i.e.* $N_a = N_h = 4$, while Bob and Eve each has one. The channel matrices are assumed to be composed of independent, zero-mean Gaussian random variables with unit variance. All results

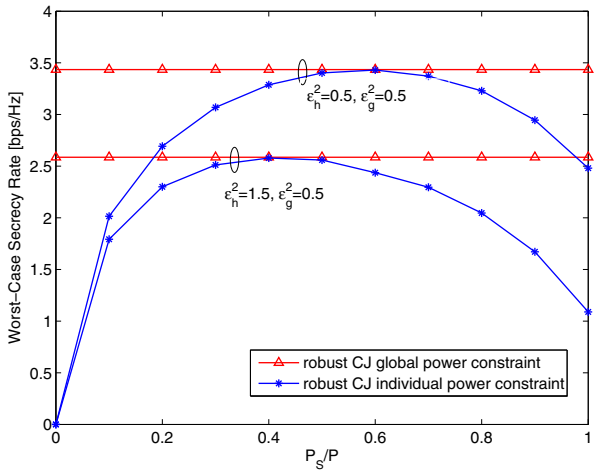

Fig. 1. Worst-case secrecy rate vs. transmit power fraction, $P = 10$dB.

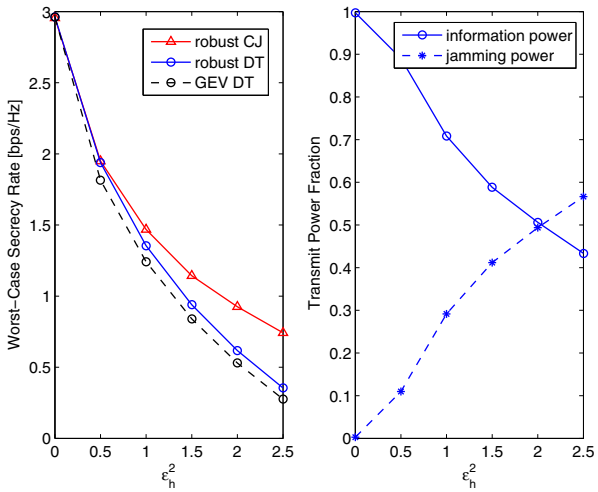

Fig. 2. Worst-case secrecy rate and transmit power fraction vs. channel mismatch ϵ_h^2, when $\epsilon_g^2 = 0.5$, $P = 3$dB.

are calculated based on an average of 1000 independent trials. The background noise power is assumed to be the same at Bob and Eve, $\sigma_b^2 = \sigma_e^2 = 1$, and the transmit power P is defined in dB relative to the noise power. In addition to the robust DT and CJ schemes, we also examine the non-robust generalized eigenvector scheme discussed in Section III for purposes of comparison, and we refer to it as GEV DT in the simulation.

In Fig. 1, we compare the performance of the robust CJ scheme under both global and individual power constraints. In this case, we assume the global power limit P is 10dB, P_S and P_J are the individual power constraints for Alice and the Helper respectively, and $P_S + P_J = P$. The benefit of having the flexibility associated with a global power constraint over fixed individual power constraints is clearly evident. Also it can be seen that the proposed joint optimization procedure achieves the optimal worst-case secrecy rate. When ϵ_h^2 increases, a larger fraction of the transmit power must be devoted to jamming in order to reach the higher secrecy rate.

The impact of ϵ_h^2 on the secrecy rate of the different schemes is presented in Fig. 2. The transmit power fraction for the robust CJ scheme is also plotted, and a global power constraint is used in this case. We assume P is 3dB, and the channel mismatch ϵ_g^2 between the Helper and Eve is fixed at 0.5. It can be observed that when $\epsilon_h^2 = 0$, a jamming signal is not necessary, and all schemes achieve the same secrecy rate. However, when ϵ_h^2 increases, the robustness of the CJ scheme is more obvious, and the jamming fraction of the total transmit power also increases.

VI. Conclusions

In this paper, we studied robust transmit design for MISO wiretap channels with imperfect ECSI. Robust transmit covariance matrices were obtained for both the direct transmission and cooperative jamming schemes, based on worst-case secrecy rate maximization. The benefits of the robust designs were illustrated through the numerical results. We conclude that although cooperative jamming is not helpful when perfect ECSI is available under a global power constraint, the worst-case secrecy rate can be increased by using jamming support from the helper when the ECSI is imperfect, provided that robust beamforming is employed.

References

[1] A. D. Wyner, "The wire-tap channel," *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, Jan. 1975.

[2] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," in *Proc. IEEE ISIT*, Jul. 2008, pp. 524–528.

[3] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas—part II: The MIMOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 11, pp. 5515–5532, Nov. 2010.

[4] S. Shafiee and S. Ulukus, "Achievable rates in Gaussian MISO channels with secrecy constraints," in *Proc. IEEE ISIT*, Jun. 2007, pp. 2466–2470.

[5] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas I: The MISOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 7, pp. 3088–3104, Jul. 2010.

[6] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, Jun. 2008.

[7] A. Mukherjee and A. L. Swindlehurst, "Robust beamforming for security in MIMO wiretap channels with imperfect CSI," *IEEE Trans. Signal Process.*, vol. 59, no. 1, pp. 351–361, Jan. 2011.

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

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

[10] J. Huang and A. L. Swindlehurst, "Cooperative jamming for secure communications in MIMO relay networks," *IEEE Trans. Signal Process.*, 2011, to appear.

[11] S. P. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge University Press, 2004.

[12] D. Carlson, E. Haynsworth, and T. Markham, "A generalization of the Schur complement by means of the Moore-Penrose inverse," *SIAM Journal on Applied Mathematics*, vol. 26, no. 1, pp. 169–175, Jan. 1974.

[13] R. J. Stern and H. Wolkowicz, "Indefinite trust region subproblems and nonsymmetric eigenvalue perturbations," *SIAM Journal on Optimization*, vol. 5, no. 2, pp. 286–313, May 1995.

[14] E. A. Jorswieck, "Secrecy capacity of single- and multi-antenna channels with simple helpers," in *Proc. Int Source and Channel Coding (SCC) ITG Conf.*, Jan. 2010, pp. 1–6.

[15] D. P. Palomar, "Convex primal decomposition for multicarrier linear MIMO transceivers," *IEEE Trans. Signal Process.*, vol. 53, no. 12, pp. 4661–4674, Dec. 2005.