Optimal Cooperative Jamming for Security

Han-Ting Chiang and James S. Lehnert
School of Electrical and Computer Engineering
Purdue University, West Lafayette, IN 47907-2035
{hchiang, lehnert}@purdue.edu

***Abstract*—In this paper, based on a cooperative jamming scheme, the design of the optimal covariance matrix of the artificial noise produced by a helper that maximizes the secret rate between a source and legitimate destination pair in the presence of multiple eavesdroppers is addressed. It is shown that the original nonconvex design problem can be transformed into a sequence of convex optimization problems. The rank property of the optimal covariance matrix is investigated. In the presence of multiple eavesdroppers, the optimality of beamforming is established. Further, in the presence of two eavesdroppers, it is shown that generally the zero-forcing solution does not maximize the secret rate. Finally, the robust design under imperfect channel state information is considered.**

***Index Terms*—Artificial noise, cooperative jamming, secrecy.**

I. Introduction

Secrecy is a critical issue in wireless communications because of the information leakage resulting from the broadcast nature of the wireless medium. To improve security, besides cryptographic techniques, physical layer approaches that restrict the decoding or demodulation capability of the eavesdroppers have also been studied. The research dates back to the simple wire-tap channel proposed by Wyner [1]. An overview of subsequent works and recent developments can be found in [2]. These studies reveal the possibility of conveying confidential messages between the source and legitimate destinations while keeping eavesdroppers ignorant if the channels from the source to the destinations are better then those from the source to the eavesdroppers.

To enhance security, the idea of cooperative communication has been adapted. An overview is provided in [3]. There are two types of cooperation. One is cooperative relay (CR), which includes amplify-and-forward (AF) and decode-and-forward (DF) schemes [4]-[6], and the other is cooperative jamming (CJ) [5]-[9]. In this paper, we focus on the CJ scheme because its demand on the helpers is smaller than that on the relays in the CR schemes. In the CJ scheme, helpers generate artificial noise (AN) to interfere with the eavesdroppers. The idea of using AN to confuse eavesdroppers is first presented in [7]. The suboptimal weight design for the AN at the helpers for secrecy is considered in [5] with the additional constraint that the AN at the destination is nulled out. This reduces the difficulty of the design problem but may also sacrifice the performance. Without the additional constraint, in the presence of a single eavesdropper, the optimal weight design is studied in [6], [8], [9], and conditions under which a positive secret rate is achievable are derived in [6]. In addition, for a source with multiple antennas (no cooperation), the secret rate can be improved by employing the AN along with the messages. This model is studied in [10] based on quality-of-service constraints with channel state information (CSI) and in [7], [11] without CSI for the channels to the eavesdroppers.

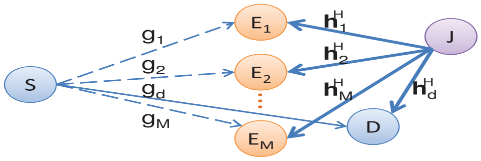

Fig. 1. System model.

In this paper, we consider the optimal system design for security based on the CJ scheme. The network considered consists of a source, a legitimate destination, a helper and multiple eavesdroppers while in [6], [8], [9] only a single eavesdropper is considered. We presume that the helper is equipped with multiple antennas while others each have a single antenna. The goal is to design the optimal covariance matrix of the AN that maximizes the secret rate. Considering the two-layer (TL) idea proposed in [12] (also in [6], [9]), we transform the original nonconvex design problem into a sequence of convex optimization problems. This greatly reduces the complexity of the design. We show that to achieve the maximal secret rate, generally the dimension of the AN must be less than or equal to M, where M is the number of eavesdroppers, and it is sufficient for the helper to generate the AN with dimension no more then $\sqrt{M+1}$. In [6], [13], it is shown that, in the presence of one eavesdropper, the zero-forcing (ZF) solution does not maximize the secret rate. Here, we further show that in the presence of two eavesdroppers this is still true in general. Finally, we consider the robust design with imperfect CSI. The S-Lemma, which is also employed in [14], [15], is utilized to modify the proposed method.

II. System Model

The system model is illustrated in Fig. 1. The wireless communication network based on the CJ scheme consists of a source S, a legitimate destination D, a helper J and M eavesdroppers $\{\mathrm{E}_i\}_{i=1}^M$ who act independently. The source S wishes to send confidential messages to the destination D while keeping the eavesdroppers $\{\mathrm{E}_i\}_{i=1}^M$ ignorant; meanwhile, the helper J assists the source S by producing the AN to interfere with the eavesdroppers $\{\mathrm{E}_i\}_{i=1}^M$. Although the goal of the helper J is to create interference at the eavesdroppers, we do not restrict its signal to be interference free at the destination as in [5] (i.e., ZF to the destination). Sometimes, it is worth tolerating some interference at the destination to create a higher noise level at the eavesdroppers. We assume that the helper J has $N_t \geq 2$ antennas while due to cost or size limitations, other units each only have one antenna. We assume that the source S employs Gaussian codewords and denote the message signal by $x_s \in \mathbb{C}$ with $\mathbb{E}[|x_s|^2] = P_s$, where $P_s > 0$ is the power budget of the source. We denote the AN, which is independent of x_s and generated by the helper J, by $\mathbf{x}_f \in \mathbb{C}^{N_t \times 1}$, where $\mathbf{x}_f \sim \mathcal{CN}(\mathbf{0}, \mathbf{Q})$ and $\mathcal{CN}(\mathbf{m}, \mathbf{C})$ denotes the circularly symmetric complex Gaussian distribution with mean $\mathbf{m}$ and covariance matrix $\mathbf{C}$. We assume that all channels are quasi-static flat-fading, invariant during the transmission blocks, and independent of each other. We use $g_d, g_i \in \mathbb{C}\backslash\{0\}$ to stand for the channels from the source S to the destination D and to the ith eavesdropper E$_i$, respectively. We denote by $\mathbf{h}_d^H, \mathbf{h}_i^H \in \mathbb{C}^{1\times N_t} \backslash\{\mathbf{0}^H\}$ the channels from the helper J to the destination D and to the ith eavesdropper E$_i$, respectively.

The signals received at the destination D, $y_d \in \mathbb{C}$, and the ith eavesdropper E$_i$, $y_i \in \mathbb{C}$, are expressed, respectively, as

$$y_d = g_d x_s + \mathbf{h}_d^H \mathbf{x}_f + n_d, \tag{1}$$

$$y_i = g_i x_s + \mathbf{h}_i^H \mathbf{x}_f + n_i, \tag{2}$$

where $n_d \sim \mathcal{CN}(0, \sigma_d^2)$, $n_i \sim \mathcal{CN}(0, \sigma_i^2)$ are, respectively, the thermal noise at the destination D and at the ith eavesdropper E$_i$. Given a realization of the channels and the covariance matrix $\mathbf{Q}$ of the AN, from [16], an achievable secret rate from the source S to the destination D is given by

$$\min_i \left[R_d - R_i\right]^+ = \left[R_d - \max_i R_i\right]^+, \tag{3}$$

where $[\cdot]^+$ denotes $\max[\cdot, 0]$ and

$$R_d = \log_2\left(1 + \frac{P_s|g_d|^2}{\mathbf{h}_d^H\mathbf{Q}\mathbf{h}_d + \sigma_d^2}\right), \tag{4}$$

$$R_i = \log_2\left(1 + \frac{P_s|g_i|^2}{\mathbf{h}_i^H\mathbf{Q}\mathbf{h}_i + \sigma_i^2}\right). \tag{5}$$

R_d and R_i are the capacities of the channels from the source S to the destination D and to the ith eavesdropper E$_i$, respectively. The $[\cdot]^+$ operator in (3) indicates that sometimes a positive secret rate cannot be achieved (i.e., $R_d \leq \max_i R_i$). The goal is to design the optimal covariance matrix $\mathbf{Q}$ of the AN, $\mathbf{x}_f$, under the power budget $P_f > 0$ at the helper such that the secret rate (3) is maximized.

III. Perfect CSI

In this section, we assume that perfect CSI is available. The CSI of channels (from the source or helper) to the destination can be obtained from feedback. For channels to the eavesdroppers, we assume that the eavesdroppers do not only snoop passively, but also communicate with other units in the network actively, and therefore, we can monitor the channels. The system design problem of maximizing the secret rate (3) is formulated without the $[\cdot]^+$ operator as

$$\textbf{Problem 1 (P1)} \quad \max_{\mathbf{Q}\succeq\mathbf{0},\ \mathrm{Tr}(\mathbf{Q})\leq P_f} \left[R_d - \max_i R_i\right].$$

To achieve a positive secret rate, from (3)-(5), there must exist a $\mathbf{Q} \succeq \mathbf{0}$ satisfying $\mathrm{Tr}(\mathbf{Q}) \leq P_f$ with $\frac{(\mathbf{h}_i^H\mathbf{Q}\mathbf{h}_i+\sigma_i^2)/|g_i|^2}{(\mathbf{h}_d^H\mathbf{Q}\mathbf{h}_d+\sigma_d^2)/|g_d|^2} > 1$, $\forall i$. Whether such a $\mathbf{Q}$ exists or not can be tested by examining

$$\textbf{P1T} \quad \max_{\mathbf{Q}\succeq\mathbf{0},\ \mathrm{Tr}(\mathbf{Q})\leq P_f} \frac{\min_i(\mathbf{h}_i^H\mathbf{Q}\mathbf{h}_i + \sigma_i^2)/|g_i|^2}{(\mathbf{h}_d^H\mathbf{Q}\mathbf{h}_d + \sigma_d^2)/|g_d|^2}.$$

If the optimal objective value of **P1T** is greater than one, a positive secret rate is achievable, and otherwise not. Using a common scheme for dealing with linear fractional functions, we can transform the quasi-convex optimization problem **P1T** to the convex optimization problem

$$\begin{aligned}\textbf{P1T}' \quad &\max_{t\geq 0,\ \hat{\mathbf{Q}}\succeq\mathbf{0},\ \mathrm{Tr}(\hat{\mathbf{Q}})\leq tP_f}\ \min_i\ (\mathbf{h}_i^H\hat{\mathbf{Q}}\mathbf{h}_i + t\sigma_i^2)/|g_i|^2\\ &\text{subject to}\quad \mathbf{h}_d^H\hat{\mathbf{Q}}\mathbf{h}_d + t\sigma_d^2 = |g_d|^2,\end{aligned}$$

where we set $t = |g_d|^2/(\mathbf{h}_d^H\mathbf{Q}\mathbf{h}_d + \sigma_d^2)$ and $\hat{\mathbf{Q}} = t\mathbf{Q}$ to simplify the testing. We notice that **P1T** and **P1T′** have the same optimal objective value, and we only proceed to solve **P1** if a positive secret rate is achievable.

In general, **P1** is not a convex optimization problem. Considering the TL idea in [12], [9], instead of directly solving the nonconvex **P1**, which has $N_t(N_t+1)/2$ real variables, we consider the following alternative TL optimization problem:

$$\textbf{P2 (Outer)} \quad \max_{T\in[T_{zf}\ \ T_{ub}]} \frac{1 + 1/g(T)}{1 + 1/T}$$

where

$$\begin{aligned}\textbf{P3 (Inner)}\ \ g(T) = &\min_{\mathbf{Q}\succeq\mathbf{0},\ \mathrm{Tr}(\mathbf{Q})\leq P_f} \frac{\mathbf{h}_d^H\mathbf{Q}\mathbf{h}_d + \sigma_d^2}{P_s|g_d|^2}\\ &\text{subject to}\quad \frac{\mathbf{h}_i^H\mathbf{Q}\mathbf{h}_i + \sigma_i^2}{P_s|g_i|^2} \geq T,\ \ \forall i. \end{aligned} \tag{6}$$

We will show later that we can find the optimal $\mathbf{Q}$ of **P1** with less complexity by solving the above TL problem. We denote by $g(T)$ the optimal object value of **P3** for a given T. In **P2**, T_{zf} is set to be the optimal objective value of the following convex optimization problem:

$$\begin{aligned}\textbf{P4} \quad &\max_{\mathbf{Q}\succeq\mathbf{0},\ \mathrm{Tr}(\mathbf{Q})\leq P_f}\ \min_i\ \frac{\mathbf{h}_i^H\mathbf{Q}\mathbf{h}_i + \sigma_i^2}{P_s|g_i|^2}\\ &\text{subject to}\quad \mathbf{h}_d^H\mathbf{Q}\mathbf{h}_d = 0.\end{aligned} \tag{7}$$

T_{ub} is defined as the optimal objective value of **P4** without the constraint (7) and is the maximal T such that the feasible set of **P3** is nonempty. For each T, **P3** can be viewed as a subproblem of **P1** with the additional constraint $(\max_i R_i) \leq \log_2(1+1/T)$, which restricts the rates between the source and the eavesdroppers, and the T corresponding to the optimal $\mathbf{Q}$ of **P1** is searched in **P2**. We denote by $\mathcal{Q}(T)$ the optimal set of **P3** for a given T, i.e., $\mathcal{Q}(T) = \{\mathbf{Q} \,|\, \mathbf{Q}\,\text{is an optimal point of}\ \mathbf{P3}\ \text{for the given}\, T\}$. Then, T_{zf} is the largest T such that $\mathbf{h}_d^H\mathbf{Q}\mathbf{h}_d = 0$ for $\mathbf{Q} \in \mathcal{Q}(T)$. This means

$$R_{zf} = \left[\log_2\left(1 + \frac{P_s|g_d|^2}{\sigma_d^2}\right) - \log_2\left(1 + \frac{1}{T_{zf}}\right)\right]^+ \tag{8}$$

is the maximal secret rate of **P1** under the additional ZF constraint (7), which prohibits the AN from interfering with the destination. Under the additional ZF constraint, the optimal $\mathbf{Q}$ of **P1** can be found by solving the convex **P4**, and the corresponding optimal set is equal to $\mathcal{Q}(T_{zf})$. We refer to $\mathcal{Q}(T_{zf})$ as the ZF solution. Although the additional ZF constraint reduces the design complexity to solving a convex optimization problem, as we will discuss later, this may sacrifice the performance. Given T, **P3** is a semidefinite programming (SDP) problem [17] and, therefore, can be solved efficiently. Further, denoting by $R_s(T)$ the objective function of **P2**, we have the following lemma:

Lemma 1: $R_s(T)$ is quasi-concave, or at least can be uniformly approximated by a quasi-concave function $\forall\, \epsilon_s > 0$ on the set $\mathcal{T} = \{T : g(T) < T\}$.

Proof: Please refer to the Appendix.

We notice that $g(T) < T$ implies $R_s(T) > 1$ and $\mathcal{T} \neq \emptyset$ implies that a positive secret rate is achievable. Lemma 1 indicates that practically, if $\mathcal{T} \neq \emptyset$, the optimal T of **P2** can be found by efficient one dimension search algorithms. More importantly, we have Lemma 2, which shows how to find an optimal $\mathbf{Q}$ of the nonconvex **P1**. We can instead solve **P2**, which involves solving a sequence of convex optimization problems (**P3**), to reduce the complexity. We refer to this technique as the TL method. The proof is omitted due to the space limitation.

Lemma 2: $\mathbf{Q}$ is an optimal point of **P1** if and only if (iff) $\mathbf{Q} \in \mathcal{Q}(T)$ for a T that is an optimal point of **P2**.

Further, we define $\mathcal{P} = \{i \mid \exists\, c_i \in \mathbb{C}\, s.t.\, \mathbf{h}_i = c_i \mathbf{h}_d,\ 1 \leq i \leq M\}$. $\mathcal{P} = \emptyset$ indicates that every channel from the helper to an eavesdropper is not parallel to the channel from the helper to the destination, and this is generally true. Then, we have Lemma 3, which gives the rank properties of the optimal set of **P1**.

Lemma 3: There is an optimal $\mathbf{Q}$ of **P1** with rank$\,(\mathbf{Q}) \leq \min(\sqrt{M+1}, N_t)$. Moreover, if $\mathcal{P} = \emptyset$, all optimal $\mathbf{Q}$ of **P1** must satisfy rank$\,(\mathbf{Q}) \leq \min(M, N_t)$.

Proof: Please refer to the Appendix.

Lemma 3 means, to achieve the maximal secret rate, the dimension of the AN must be less than or equal to $\min(M, N_t)$ if $\mathcal{P} = \emptyset$, and it is sufficient for the helper to generate the AN with dimension no more then $\min(\sqrt{M+1}, N_t)$. In the presence of one or two eavesdroppers, i.e., $M \leq 2$, Lemma 3 implies beamforming is optimal in the sense that it can achieve the maximal secret rate. Further, when $M = 1$, Lemma 3 indicates that **P1** includes the design problem in [9] with the total power constraint as a special case. Utilizing Lemma 3, we can derive the optimal structure of the beamformer when $M = 1$. This has been accomplished in [8] (see also [6]), and we do not repeat the result here.

Now, we proceed to study the optimality of the ZF solution, i.e., $\mathcal{Q}(T_{zf})$. We presume the ZF solution can achieve a positive secret rate (i.e.,$R_{zf} > 0$) in the following discussion. When there exists a single eavesdropper, in [6], [13], it is shown that if $\mathcal{P} = \emptyset$ and $\mathbf{h}_d^H \mathbf{h}_1 \neq 0$, then the ZF solution is not the optimal set of **P1**, i.e., $\mathbf{Q} \in \mathcal{Q}(T_{zf})$ does not maximize the secret rate (3). The assumption $\mathbf{h}_d^H \mathbf{h}_1 \neq 0$ is necessary; otherwise, it is obvious that the ZF solution is optimal. Here, we investigate the optimality of the ZF solution when there exist two eavesdroppers, and obtain the following Lemma:

Lemma 4: When $M = 2$, suppose $\mathcal{P} = \emptyset$ and $\mathbf{h}_d^H \mathbf{h}_i \neq 0$, $i = 1, 2$. If there is a vector $\mathbf{v} \in \mathbb{C}^{N_t \times 1}$ such that $\mathbf{v}\mathbf{v}^H \in \mathcal{Q}(T_{zf})$ (guaranteed, see the proof of Lemma 3) and one of the following conditions is satisfied:

1) $\exists\, \theta_1, \theta_2 \in [0\ 2\pi)\ \ s.t.\ \ \mathbf{v}^H \mathbf{h}_1 e^{j\theta_1} > 0,\ \ \mathbf{v}^H \mathbf{h}_2 e^{j\theta_2} > 0$ ($\Leftrightarrow$ $\mathbf{v}^H \mathbf{h}_1 \neq 0, \mathbf{v}^H \mathbf{h}_2 \neq 0$), and the argument $\mathrm{Arg}\left(\frac{\mathbf{h}_d^H \mathbf{h}_1 e^{j\theta_1}}{\mathbf{h}_d^H \mathbf{h}_2 e^{j\theta_2}}\right) \neq \pi$,
2) $\mathbf{v}^H \mathbf{h}_1 \neq 0, \mathbf{v}^H \mathbf{h}_2 = 0, \frac{\sigma_2^2}{P_s |g_2|^2} > \frac{\left|\mathbf{v}^H \mathbf{h}_1\right|^2 + \sigma_1^2}{P_s |g_1|^2}$,
3) $\mathbf{v}^H \mathbf{h}_2 \neq 0, \mathbf{v}^H \mathbf{h}_1 = 0, \frac{\sigma_1^2}{P_s |g_1|^2} > \frac{\left|\mathbf{v}^H \mathbf{h}_2\right|^2 + \sigma_2^2}{P_s |g_2|^2}$,

then $\mathcal{Q}(T_{zf})$ is not the optimal set of **P1**, i.e., T_{zf} is not an optimal point of **P2**.

Proof: Please refer to the Appendix.

Condition 1 corresponds to the case in which the AN needs to interfere with both eavesdroppers to maximize the secret rate under the ZF constraint (7). Condition 2 and 3 correspond to the case in which the AN is only required to interfere with one of the two eavesdroppers to maximize the secret rate under the ZF constraint (7). Generally, one of the conditions will be satisfied. The assumption $\mathcal{P} = \emptyset$ indicates that at least one of the two numbers $\mathbf{v}^H \mathbf{h}_1$ and $\mathbf{v}^H \mathbf{h}_2$ is not zero. Further, $\mathbf{v}^H \mathbf{h}_1 \neq 0$ and $\mathbf{v}^H \mathbf{h}_2 = 0$ imply $\frac{\sigma_2^2}{P_s |g_2|^2} \geq \frac{\left|\mathbf{v}^H \mathbf{h}_1\right|^2 + \sigma_1^2}{P_s |g_1|^2}$; $\mathbf{v}^H \mathbf{h}_2 \neq 0$ and $\mathbf{v}^H \mathbf{h}_1 = 0$ imply $\frac{\sigma_1^2}{P_s |g_1|^2} \geq \frac{\left|\mathbf{v}^H \mathbf{h}_2\right|^2 + \sigma_2^2}{P_s |g_2|^2}$. Lemma 4 means that, in the presence of two eavesdroppers, the ZF solution is generally not optimal in the sense of maximizing the secret rate.

IV. Imperfect CSI

In the previous section, we assume that perfect CSI is available. This assumption may not hold. For example, when the eavesdroppers are less active, then channels to the eavesdroppers cannot be estimated accurately. In addition, channels may also vary too fast to be tracked precisely. To take this into account in this section, we consider the effect of imperfect CSI. We assume that only the nominal channel coefficients $\hat{g}_d$, $\hat{g}_i$, $\hat{\mathbf{h}}_d^H$, and $\hat{\mathbf{h}}_i^H$ are available. The actual channel coefficients g_d, g_i, $\mathbf{h}_d^H$, and $\mathbf{h}_i^H$ are contained, respectively, in the uncertainty ellipsoids

$$\mathcal{G}_d = \{g_d \mid |g_d - \hat{g}_d| \leq \epsilon_d\}, \tag{9}$$

$$\mathcal{G}_i = \{g_i \mid |g_i - \hat{g}_i| \leq \epsilon_i\}, \tag{10}$$

$$\mathcal{H}_d = \left\{\mathbf{h}_d^H \mid \left\|(\mathbf{h}_d - \hat{\mathbf{h}}_d)^H \mathbf{R}_d^{1/2}\right\| \leq 1\right\}, \tag{11}$$

$$\mathcal{H}_i = \left\{\mathbf{h}_i^H \mid \left\|(\mathbf{h}_i - \hat{\mathbf{h}}_i)^H \mathbf{R}_i^{1/2}\right\| \leq 1\right\}, \tag{12}$$

where $\epsilon_d > 0$, $\epsilon_i > 0$, $\mathbf{R}_d \succ \mathbf{0}$, and $\mathbf{R}_i \succ \mathbf{0}$ depend on the shapes and volumes of the corresponding uncertainty ellipsoids. Under this new model, given the nominal channel gains and the covariance matrix $\mathbf{Q}$, an achievable secret rate from the source to the destination for any channel gains

$g_d \in \mathcal{G}_d$, $\{g_i \in \mathcal{G}_i\}_1^M$, $\mathbf{h}_d^H \in \mathcal{H}_d$, and $\{\mathbf{h}_i^H \in \mathcal{H}_i\}_1^M$ is given as

$$\min_{g_d \in \mathcal{G}_d, \mathbf{h}_d^H \in \mathcal{H}_d, i, g_i \in \mathcal{G}_i, \mathbf{h}_i^H \in \mathcal{H}_i} [R_d - R_i]^+ . \qquad (13)$$

The robust system design problem can be expressed as

$$\textbf{P5} \quad \max_{\mathbf{Q} \succeq \mathbf{0},\, \mathrm{Tr}(\mathbf{Q}) \leq P_f} \left[\min_{g_d \in \mathcal{G}_d, \mathbf{h}_d^H \in \mathcal{H}_d} R_d - \max_{i, g_i \in \mathcal{G}_i, \mathbf{h}_i^H \in \mathcal{H}_i} R_i \right].$$

As indicated in Section III, it is too complicated to solve **P5** directly. Instead, we can show that the optimal **Q** of **P5** can be obtained by solving the following TL optimization problem:

$$\textbf{P6 (Outer)} \quad \max_{T \in [T_{lb}\ T_{ub}]} \frac{1 + 1/\tilde{g}(T)}{1 + 1/T}$$

where

$$\textbf{P7(Inner)}\ \tilde{g}(T) = \min_{\mathbf{Q} \succeq \mathbf{0}, \mathrm{Tr}(\mathbf{Q}) \leq P_f} \max_{g_d \in \mathcal{G}_d, \mathbf{h}_d^H \in \mathcal{H}_d} \frac{\mathbf{h}_d^H \mathbf{Q} \mathbf{h}_d + \sigma_d^2}{P_s |g_d|^2}$$
$$\text{subject to} \quad \frac{\mathbf{h}_i^H \mathbf{Q} \mathbf{h}_i + \sigma_i^2}{P_s |g_i|^2} \geq T,$$
$$\forall g_i \in \mathcal{G}_i, \ \forall \mathbf{h}_i^H \in \mathcal{H}_i, \ \forall i. \qquad (14)$$

We denote by $\tilde{g}(T)$ the optimal objective value of **P7** for a given T. In **P6**, $T_{lb} = \min_i (\sigma_i^2 / (P_s |\hat{g}_i|^2 (1 + \epsilon_i / |\hat{g}_i|)^2))$ is the maximal T such that $\mathbf{Q} = \mathbf{0}$ is a feasible point of **P7**. T_{ub} is defined as the maximal T such that the feasible set of **P7** is nonempty. However, it is infeasible to solve **P7** directly because (14) consists of an infinite number of constraints and the objective function is composed of an infinite number of functions. Hence, we need to reformulate **P7**. First, it is easy to verify that

$$\min_{g_d \in \mathcal{G}_d} |g_d|^2 = |\hat{g}_d|^2 (1 - \frac{\epsilon_d}{|\hat{g}_d|})^2 = |\hat{g}_d|^2 (1 - \epsilon_d')^2, \qquad (15)$$

$$\max_{g_i \in \mathcal{G}_i} |g_i|^2 = |\hat{g}_i|^2 (1 + \frac{\epsilon_i}{|\hat{g}_i|})^2 = |\hat{g}_i|^2 (1 + \epsilon_i')^2, \qquad (16)$$

where $\epsilon_d' = \epsilon_d / |\hat{g}_d|$, $\epsilon_i' = \epsilon_i / |\hat{g}_i|$, and we assume $\epsilon_d' < 1$ (Otherwise, a positive secret rate can not be achieved). With (15), (16), we can rewrite **P7** as

$$\textbf{P7}'\ \tilde{g}(T) = \min_{\mathbf{Q} \succeq \mathbf{0}\ \mathrm{Tr}(\mathbf{Q}), \leq P_f} \max_{\mathbf{h}_d^H \in \mathcal{H}_d} \frac{\mathbf{h}_d^H \mathbf{Q} \mathbf{h}_d + \sigma_d^2}{P_s |\hat{g}_d|^2 (1 - \epsilon_d')^2}$$
$$\text{subject to} \quad \frac{\mathbf{h}_i^H \mathbf{Q} \mathbf{h}_i + \sigma_i^2}{P_s |\hat{g}_i|^2 (1 + \epsilon_i')^2} \geq T, \ \forall \mathbf{h}_i^H \in \mathcal{H}_i, \ \forall i.$$

Further, by rewriting **P7′** into epigraph form and then applying the S-Lemma [20, Th. 2.1], which has also been used in [14], [15] for robust system design, we make the solution of **P7** practical by reformulating it as

$$\textbf{P7}''\ \ \tilde{g}(T) = \min_{\nu \geq 0,\ \mathbf{Q} \succeq \mathbf{0},\ \mathrm{Tr}(\mathbf{Q}) \leq P_f,\ \alpha_d \geq 0,\ \{\alpha_i \geq 0\}_1^M} \nu$$
$$\text{subject to} \quad \begin{bmatrix} -\mathbf{Q} + \alpha_d \mathbf{R}_d & -\mathbf{Q}\hat{\mathbf{h}}_d \\ -\hat{\mathbf{h}}_d^H \mathbf{Q} & -q_d(\nu) - \alpha_d \end{bmatrix} \succeq \mathbf{0},$$
$$\begin{bmatrix} \mathbf{Q} + \alpha_i \mathbf{R}_i & \mathbf{Q}\hat{\mathbf{h}}_i \\ \hat{\mathbf{h}}_i^H \mathbf{Q} & q_i(T) - \alpha_i \end{bmatrix} \succeq \mathbf{0}, \ \forall i,$$

where $q_d(\nu) = \hat{\mathbf{h}}_d^H \mathbf{Q} \hat{\mathbf{h}}_d + \sigma_d^2 - P_s |\hat{g}_d|^2 (1 - \epsilon_d')^2 \nu$ and $q_i(T) = \hat{\mathbf{h}}_i^H \mathbf{Q} \hat{\mathbf{h}}_i + \sigma_i^2 - P_s |\hat{g}_i|^2 (1 + \epsilon_i')^2 T$. Details appears in [15], where the same procedure is applied to a similar problem formulation. **P7″** is a SDP problem with $2M + 5$ constraints, and the objective function of **P6** has the same property as $R_s(T)$ as given in Lemma 1. Hence, we can now find an optimal **Q** of **P5** efficiently by solving **P6**. We also notice that, as in Section III, a convex problem can be formulated to examine if a positive secret rate is possible. We only proceed to solve **P6** if a positive secret rate is achievable.

V. Simulations

In this section, we demonstrate the effectiveness of the proposed methods via Monte-Carlo simulations. We use CVX [18] to solve the design problems. We assume unit power thermal noise at all nodes. All channels are generated independently and $g_d, g_i \sim \mathcal{CN}(0, 1)$, $\mathbf{h}_d, \mathbf{h}_i \sim \mathcal{CN}(\mathbf{0}, \mathbf{I}_{N_t})$. In the presence of imperfect CSI, we set $\mathbf{R}_d = (1/\xi_d)\mathbf{I}_{N_t}$, $\mathbf{R}_i = (1/\xi_i)\mathbf{I}_{N_t}$, $\xi_d, \xi_i > 0$, which means the uncertainty ellipsoids $\mathcal{H}_d$, $\mathcal{H}_i$ are bounded balls.

In the first example, we assume that perfect CSI is available. We assume that there exist three eavesdroppers and the helper has two antennas. We vary the power of the source P_s and helper P_f, and the average achieved secret rates of the proposed TL method and the ZF approach (8) (i.e., $\mathbf{Q} \in \mathcal{Q}(T_{zf})$) are depicted in Fig. 2. The results show that the CJ scheme greatly improves the secret rate even when the helper only transmits with 2dB power. Without the helper, the secret rate increases slightly with the increase of P_s. However, it increases greatly with the increase of P_f. This justifies that CJ indeed can facilitate secure transmissions. Further, the TL (optimal) method outperforms the ZF approach, especially when P_f is small, because of the additional degree of freedom for the AN. The gaps between the two methods would be larger than in the figure if the channel realizations that do not achieve positive secret rates are excluded. For example, when $P_f = 2$dB, the gap doubles if those channel realizations are excluded. (Approximately half of the channel realizations in the simulation will be excluded in this case.) Also, we notice that, for a fixed P_s, as P_f goes to infinity, the performance gap between the TL and ZF methods will approach zero. This is because, in this case, the helper can destroy the channels from the source to the eavesdroppers simply by transmitting the AN in the null space of the channel from the helper to the destination.

In the second example, we consider the effect of imperfect CSI. We investigate the environment which has two eavesdroppers and a helper with four antennas. We set $\epsilon_d = \xi_d = \epsilon_i = \xi_i = \epsilon$. Two cases: $\epsilon = 0.01$ and $\epsilon = 0.1$ are considered. The results are plotted in Fig. 3. The imperfect CSI does downgrade the system performance and the achieved secret decreases as the channel uncertainty increases. However, CJ still greatly improves the secret rate when compared with the direct transmission in which the achieved secret rate increases only slightly as the the source power increases.

VI. Conclusion

In this paper, based on the CJ scheme, we address the optimal design for secure communications in the presence of multiple eavesdroppers. A TL method is proposed to simplify the original nonconvex design problem. Several properties of the optimal AN are studied. Further, the proposed TL method is modified to adapt to imperfect CSI.

VII. Appendix

A. Proof of Lemma 1

First, note that $g(T)$ is convex [17, Exercise 5.32], and hence so is the set $\mathcal{T}$. With the assumption of the existence of the first and second order derivatives of $g(T)$, following the proof of [9, Theorem 3], one can verify that $R_s(T)$ is a quasi-concave function on $\mathcal{T}$. In addition, if the assumption does not hold, we can still show that there exists a quasi-concave function $\hat{R}_s(T)$ such that $|R_s(T) - \hat{R}_s(T)| < \epsilon_s$ on $\mathcal{T}$ for all $\epsilon_s > 0$. Because $g(T)$ is continuous on $\mathcal{T}$ (due to the convexity), there exists a infinite differentiable convex function $\hat{g}(T)$ such that $|g(T) - \hat{g}(T)| < \epsilon_g$ on $\mathcal{T}$ for all $\epsilon_g > 0$. This further implies the existence of $\hat{R}_s(T)$.

B. Proof of Lemma 3

We prove Lemma 3 by showing that, $\forall\ T \in [T_{zf}\ T_{ub}]$, $\mathcal{Q}(T)$ satisfies the statement therein. We presume $M < N_t$ and $\sqrt{M+1} < N_t$. Part of the techniques used here are similar as in [21], [10]. To present concisely, we assume $P_s|g_d|^2 = P_s|g_i|^2 = 1$. Recall $\mathcal{P} = \{i \mid \exists\ c_i \in \mathbb{C}\ s.t.\ \mathbf{h}_i = c_i \mathbf{h}_d,\ 1 \leq i \leq M\}$ and denote $\overline{\mathcal{P}} = \{i \mid 1 \leq i \leq M, i \notin \mathcal{P}\}$. For now, we assume $\mathcal{P} = \emptyset$ and divide the proof into three cases.

1) $T_{zf} < T < T_{ub}$: Since **P3** is a SDP problem (also convex) with finite optimal object value (bounded below) and Slater's condition is satisfied in this case, the strong duality holds and the dual problem of **P3** attains the optimal objective value. Further, **P3** attains the optimal objective value because the objective function is a continuous function and the feasible set is compact and nonempty. Then, from [19, Th. 3.2], we conclude that **P3** has an optimal $\mathbf{Q} \in \mathcal{Q}(T)$ with rank$\,(\mathbf{Q}) \leq \sqrt{M+1}$. In addition, since the duality gap is zero, the Karush-Kuhn-Tucker (KKT) conditions are necessary and sufficient for any optimal primal and dual variable pair. Associate the interference constraints (6), power constraint, and positive-semidefinite constraint with the Lagrange multipliers $\{\lambda_i \geq 0\}_1^M, v \geq 0$, and $\mathbf{\Psi} \in \mathbb{C}^{N_t \times N_t}$, $\mathbf{\Psi} \succeq \mathbf{0}$, respectively. Then, part of the KKT conditions of **P3** are given by
$$\mathbf{h}_d \mathbf{h}_d^H + v\mathbf{I} = \sum_{i=1}^{M} \lambda_i \mathbf{h}_i \mathbf{h}_i^H + \mathbf{\Psi}, \tag{17}$$
$$\text{Tr}\,(\mathbf{\Psi}\mathbf{Q}) = 0. \tag{18}$$
First, we consider $v > 0$. From (17), we have rank$\,(\mathbf{I}) = $ rank$\left(\sum_{i=1}^M \lambda_i \mathbf{h}_i \mathbf{h}_i^H + \mathbf{\Psi}\right) = N_t$. By the property, rank$\left(\sum_{i=1}^M \lambda_i \mathbf{h}_i \mathbf{h}_i^H\right) +$ rank$(\mathbf{\Psi}) \geq$ rank$\left(\sum_{i=1}^M \lambda_i \mathbf{h}_i \mathbf{h}_i^H + \mathbf{\Psi}\right)$, we get rank$(\mathbf{\Psi}) \geq \max(N_t - M, 0)$. Also, (18) and $\mathbf{\Psi} \succeq 0$ together imply that $\mathbf{\Psi}\mathbf{Q} = \mathbf{0}$. Following Sylvester's rank inequality, rank$\,(\mathbf{\Psi})+$rank$\,(\mathbf{Q}) - N_t \leq$ rank$\,(\mathbf{\Psi}\mathbf{Q})$, we conclude that rank$\,(\mathbf{Q}) \leq M$ for all $\mathbf{Q} \in \mathcal{Q}(T)$ if $v > 0$. Next, we consider $v = 0$. From (17), we have $\mathbf{\Psi} = \mathbf{h}_d \mathbf{h}_d^H - \sum_{i=1}^M \lambda_i \mathbf{h}_i \mathbf{h}_i^H \succeq \mathbf{0}$. This indicates that $\lambda_i = 0,\ \forall\ i$ (note $\mathcal{P} = \emptyset$) and $\mathbf{\Psi} = \mathbf{h}_d \mathbf{h}_d^H$. With (18), this further implies if there exists an optimal primal and dual variable pair satisfying the KKT conditions, the optimal objective value is σ_d^2, i.e., $\mathbf{h}_d^H \mathbf{Q} \mathbf{h}_d = 0$, which contradicts $T > T_{zf}$. Therefore, there exists no optimal primal and dual variable pair with $v = 0$. Hence, the proof is complete in this case.

2) $T = T_{ub}$: In this case, it is not obvious whether Slater's condition holds. However, consider the following SDP optimization problem
$$\begin{aligned} \textbf{P8} \quad & \min_{\mathbf{Q} \succeq \mathbf{0}} \quad \text{Tr}(\mathbf{Q}) \\ & \text{subject to} \quad \mathbf{h}_i^H \mathbf{Q} \mathbf{h}_i + \sigma_i^2 \geq T_{ub},\ \ \forall i \\ & \qquad\qquad\quad \mathbf{h}_d^H \mathbf{Q} \mathbf{h}_d + \sigma_d^2 = g(T_{ub}). \end{aligned} \tag{19}$$
The optimal objective value of **P8** is P_f. Suppose the optimal objective value of **P8** is less than P_f. Since $\mathcal{P} = \emptyset$, then it is easy to construct a $\mathbf{Q}$ that is a feasible point of **P3** with $T > T_{ub}$, which contradicts the definition of T_{ub}. Hence, an optimal point of **P8** is also an optimal point of **P3**. Because Slater's condition holds for **P8** and the optimal objective value P_f is attained (by the definition of T_{ub}), from [19, Th. 3.2], **P8** has an optimal $\mathbf{Q}$ with rank$\,(\mathbf{Q}) \leq \sqrt{M+1}$. Therefore, **P3** has an optimal $\mathbf{Q}$ with rank$\,(\mathbf{Q}) \leq \sqrt{M+1}$. In addition, consider **P8′** in which we remove the last constraint (19) of **P8**. It is easy to verify that $\mathbf{Q}$ is a feasible point of **P3** (note $T = T_{ub}$) iff $\mathbf{Q}$ is an optimal point of **P8′**. Then, following a similar analysis of the KKT conditions of **P8′** as in the above case, we can show that any optimal point of **P8′** must satisfy rank$\,(\mathbf{Q}) \leq M$ and so does the optimal point of **P3**.

3) $T = T_{zf}$: Similar to the above case.

Now, consider when $\mathcal{P} \neq \emptyset$. In this scenario, we can replace constraints $\frac{\mathbf{h}_i^H \mathbf{Q} \mathbf{h}_i + \sigma_i^2}{P_s |g_i|^2} \geq T_{ub},\ \ i \in \bar{\mathcal{P}}$, by a single constraint. Then, the proof follows as above.

C. Proof of Lemma 4

To begin, we notice that **P1** with $\mathbf{h}_d = \bar{\mathbf{h}}_d e^{j\theta_d}$, $\mathbf{h}_i = \bar{\mathbf{h}}_i e^{j\theta_i}$ for all $\theta_d, \theta_i \in [0\ 2\pi)$ share the same optimal point set and optimal objective value. In addition, $\mathbf{v}\mathbf{v}^H = \mathbf{v}e^{j\theta_v}\left(\mathbf{v}e^{-j\theta_v}\right)^H$ for all $\theta_v \in [0\ 2\pi)$, and $\mathbf{v}^H \mathbf{h}_d = 0$.

First, consider the case where Condition 1 is satisfied. From the discussion above, we can assume that, for $i = 1, 2$, $\mathbf{v}^H \mathbf{h}_i > 0$ (i.e., Re$[\mathbf{v}^H \mathbf{h}_i] > 0$, Im$[\mathbf{v}^H \mathbf{h}_i] = 0$) and Re$[\mathbf{h}_d^H \mathbf{h}_i] > 0$. The last follows because, given $\mathbf{h}_1$ and $\mathbf{h}_2$, we can select a $\theta_d \in [0\ 2\pi)$ such that Re$[e^{j\theta_d} \mathbf{h}_d^H \mathbf{h}_i] > 0$ for $i = 1, 2$ if the phase difference of the two complex numbers

$\mathbf{h}_d^H\mathbf{h}_1$ and $\mathbf{h}_d^H\mathbf{h}_2$ is not π. Consider $\mathbf{Q}(\lambda) = P_f(\sqrt{\lambda}\bar{\mathbf{h}}_d + \sqrt{1-\lambda}\bar{\mathbf{v}})(\sqrt{\lambda}\bar{\mathbf{h}}_d+\sqrt{1-\lambda}\bar{\mathbf{v}})^H$, $\lambda \in [0\ 1]$, where $\bar{\mathbf{h}} = \mathbf{h}/\|\mathbf{h}\|$ and $\bar{\mathbf{v}} = \mathbf{v}/\|\mathbf{v}\|$. Given λ, the secret rate (3) can be expressed as

$$R_s(\lambda) = \min(R_{s,1}(\lambda), R_{s,2}(\lambda)), \tag{20}$$

where

$$\begin{aligned} R_{s,i}(\lambda) = {} & \log_2\left(1 + \frac{P_s|g_d|^2}{P_f\lambda\left\|\mathbf{h}_d\right\|^2 + \sigma_d^2}\right) \\ & - \log_2\left(1 + \frac{P_s|g_i|^2}{P_f\left|\sqrt{\lambda}\bar{\mathbf{h}}_d^H\mathbf{h}_i + \sqrt{1-\lambda}\bar{\mathbf{v}}^H\mathbf{h}_i\right|^2 + \sigma_i^2}\right) \end{aligned} \tag{21}$$

and we ignore the $[\cdot]^+$ operator. Then, we can verify that $\lim_{\lambda\downarrow 0}\frac{dR_{s,i}(\lambda)}{d\lambda} = \infty$ for $i = 1, 2$. This implies that $\mathcal{Q}(T_{zf})$ is not the optimal set of **P1** since $R_s(0) = R_{zf}$.

Next, assume that Condition 2 is satisfied. In this case, we can assume that $\mathbf{v}^H\mathbf{h}_1 > 0$ and $\mathbf{h}_d^H\mathbf{h}_1 > 0$. Consider the same $\mathbf{Q}(\lambda)$ as in the previous case. It is easy to verify now that $\lim_{\lambda\downarrow 0}\frac{dR_{s,1}(\lambda)}{d\lambda} = \infty$, $\left|\lim_{\lambda\downarrow 0}\frac{dR_{s,2}(\lambda)}{d\lambda}\right| < \infty$. Further, the condition $\frac{\sigma_2^2}{P_s|g_2|^2} > \frac{\left|\mathbf{v}^H\mathbf{h}_1\right|^2+\sigma_1^2}{P_s|g_1|^2}$ implies that $R_{s,1}(0) < R_{s,2}(0)$. Hence, we conclude that $\mathcal{Q}(T_{zf})$ is not the optimal set of **P1**.

The proof of the case where Condition 3 is satisfied is the same as that of Condition 2. Hence, the proof is complete.

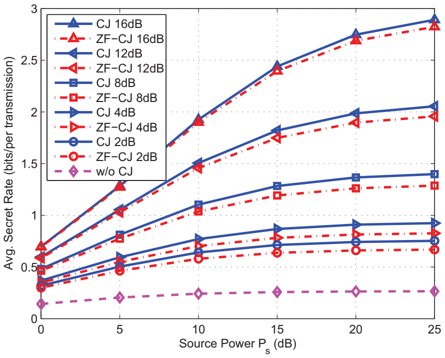

Fig. 2. Average secret rate with perfect CSI for $M = 3$, $N_t = 2$.

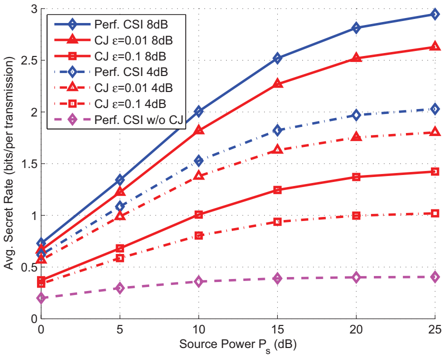

Fig. 3. Average secret rate with imperfect CSI for $M = 2$, $N_t = 4$

Acknowledgment

This work was supported in part by the Air Force Office of Scientific Research under Grant FA9550-07-1-0456.

References

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

[2] Y. Liang, H. V. Poor, and S. Shamai, *Information theoretic security source*, Now Publishers, 2009.

[3] E. Ekrem and S. Ulukus, "Cooperative secrecy in wireless communications," in *Securing wireless coommunications at the physical layer*, Springer Science and Business Media LLC, 2010.

[4] J. Zhang and M. C. Gursoy, "Collaborative relay beamforming for secure broadcasting," submitted to *IEEE Trans. Inf. Theory* in Jun. 2010. [Online]. Available at http://arxiv.org/abs/1006.4386

[5] 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.

[6] J. Li, A. P. Petropulu, and S. Weber, "Optimal cooperative relaying schemes for improving wireless physical layer security," submitted to *IEEE Trans. Inf. Theory* in Jan. 2010. [Online]. Available at http://arxiv.org/abs/1001.1389

[7] R. Negi and S. Goelm, "Secret communication using artifical noise," in *Proc. IEEE Vehicular Tech. Conf.*, vol. 3, Dallas TX, pp. 1906-1910, Sept. 2005.

[8] E. A. Jorswieck, "Secrecy capacity of single- and multi-antenna channels with simple helpers," *2010 Int. ITG Conf. Source and Channel Coding (SCC)*, Siegen, Germany, Jan. 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] W. C. Liao, T. H. Chang, W.K. Ma, and C. Y. Chi, "QoS-based transmit beamforming in the presence of eavesdroppers: an optimized artificial-noise-aided approach," *IEEE Trans. Signal Process.*, vol. 59, no. 3, pp. 1202-1216, Mar. 2011.

[11] J. Wang and A. L. Swindlehurst, "Cooperative jamming in MIMO Ad-Hoc networks," *43th Asilomar Conf. Signals, Systems and Computers*, Pacific Grove, CA, USA, Nov. 2009.

[12] 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," *47th Annu. Allerton Conf. Commun., Control, Comput.*, Monticello, IL, USA, Sept.- Oct. 2009.

[13] A. Wolf and E. Jorswieck, "On the zero forcing optimality for friendly jamming in MISO wiretap channels," *2010 IEEE Int. Workshop on Signal Process. Advances for Wireless Commun. (SPAWC)*, Marrakech, Morocco, Jun. 2010.

[14] 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.

[15] Y. Pei, Y. C. Liang, K. C. Teh, and K. H. Li, "Achieving robust, secure and cognitive transmissions using multiple antennas," in *Proc. 2010 IEEE Int. Conf. Commun. (ICC)*, Cape Town, South Africa, May 2010.

[16] Y. Liang, G. Kramer, H. V. Poor, and S. Shamai (Shitz), "Compound wire-tap channels," *EURASIP J. Wireless Commun. Netw.*, vol. 2009, Article ID 142374, 12 pages, 2009. doi:10.1155/2009/142374

[17] S.Boyd and L. Vandenberghe, *Convex optimization*, Cambridge University Press, 2004.

[18] M. Grant and S. Boyd, "CVX: Matlab software for disciplined convex programming," [Online]. Available at http://cvxr.com/cvx/

[19] Y. Huang and D. P. Palomar, "Rank-constrained separable semidefinite programming with applications to optimal beamforming," *IEEE Trans. Signal Process.*, vol. 58, no. 2, pp. 664-678, Feb. 2010.

[20] A. Beck and Y. C. Eldar, "Strong duality in nonconvex quadratic optimization with tow quadratic constraints," *SIAM J. Optimiz.*, vol. 17, no. 3, pp. 844-860, 2006.

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