Robust Transmit Design for Secure AF Relay Networks Based on Worst-Case Optimization

Lingxiang Li, Zhi Chen, *Member, IEEE*, and Jun Fang *Member, IEEE*
National Key Laboratory on Communications, University of Electronic Science and Technology of China
Email: lingxiang_li_uestc@hotmail.com; {chenzhi, JunFang }@uestc.edu.cn

***Abstract*—This paper studies robust transmit design to maximize the worst-case secrecy rate in AF networks under both total and individual relay power constraints. Channel state information (CSI) in the network is assumed to be perfectly known except for that associated with the eavesdroppers whose imperfection is modeled as deterministic bounded errors. To use the power at the relay nodes more efficiently, a joint cooperative relaying and jamming scheme is considered. Through some matrix manipulations, we recast the original nonconvex optimization problem as a sequence of semidefinite programs (SDPs), which enables us to obtain the optimal relay weights and the optimal covariance matrix of the jamming signal. Numerical results are presented to show the efficacy of the proposed scheme.**

***Index Terms*—Physical-layer security, Worst-case secrecy capacity, Cooperative communications.**

I. Introduction

Exploiting cooperation of multiple single-antenna nodes to enhance security has attracted considerable attention very recently [1]–[3]. There are two kinds of cooperation [1], cooperative relaying (CR) and cooperative jamming (CJ). Both of them aim to increase the secrecy rate while with different means: cooperative relaying makes efforts to improve the source-destination channel quality, whereas cooperative jamming attempts to degrade the source-eavesdropper channel quality. However, optimal solutions to the secrecy rate maximization (SRM) problem are difficult to get due to the correlated generalized eigenvector problems it involves. To deal with this issue, a suboptimal null-space beamforming scheme was proposed in [1]. Further, to get optimal solutions, a one-dimensional search which involves solving a sequence of semidefinite programs (SDPs) was proposed in [3].

A rigorous assumption in the above works is that the source node knows the perfect CSI, even including that of the eavesdroppers. This assumption, however, may not hold valid in practical scenarios. In some recent works, a more practical scenario is considered where the CSI of eavesdroppers is unknown or partially known [4]–[6]. Specifically, [4] proposed a suboptimal but tractable scheme to enhance security for the unknown CSI case. In [5], [6], suboptimal and optimal solutions were obtained to maximize the worst-case secrecy rate for the partial CSI case, respectively. In this paper, we consider a secure AF networks where only partial CSI of eavesdroppers is available. Deterministically bounded CSI error model is employed and a robust transmit design at relays is studied to maximize the worst-case secrecy rate.

Different from [5], [6] where each node engages in either cooperative relaying or cooperative jamming, we consider each relay to forward the information bearing signal and transmit artificial noise simultaneously. The idea of cooperative jamming comes from the artificial noise (AN) aided approach which was proposed in [7]–[9] to confuse the eavesdropper under the condition of no CSI or partial CSI of the eavesdroppers. Results have shown that such AN aided approach is helpful to improve security. Moreover, since there exists a rate floor for the source-relay-destination (SRD) link due to the noise amplification at relays, spending extra power in relaying will not help increase the secrecy rate when a certain point is reached. On the other hand, distributing a portion of power to AN to confuse the eavesdropper can be helpful. Based on these observations, we propose a strategy where the relay nodes relay the signal and transmit artificial noise simultaneously.

Our main contribution consists of the following two aspects:

1) We maximize the worst-case secrecy rate which guarantees perfect secrecy for any admissible CSI uncertainties, including the worst. Joint cooperative relaying and jamming is considered. Optimal solutions are obtained by reformulating the original nonconvex optimization problem into a sequence of SDPs.
2) We conjecture that the AN aided approach can enhance security in AF relay networks even when Global CSI is available. Numerical results are provided to show the efficacy of the proposed scheme.

II. System Model

As depicted in Fig. 1, a source node aims to send confidential messages to the destination in the presence of multiple eavesdroppers with the help of a set of relays. Two phases including the broadcasting phase and the relaying phase are required. In the broadcasting phase, the source broadcasts its message s, $\mathrm{E}\{|s|^2\} = P_s$, and the signals received at relays are

$$\mathbf{y}_R = \mathbf{h}_{SR} s + \mathbf{n}_R \tag{1}$$

where $\mathbf{h}_{SR} \in \mathbb{C}^{N\times 1}$ represent the channel vector from the source to the relay. The noise vector at relays $\mathbf{n}_R$ are assumed to be additive white Gaussian noise (AWGN), with i.i.d. entries distributed as $\mathcal{CN}(0, \sigma_R^2)$. In the relaying phase, the relays forward a weighted version of the received signal with the

This work was supported in part by the Fundamental Research Funds for the Central Universities (China) under Grant ZYGX2010X002, and by the National High-Tech R&D Program of China under Grant 2012AA011402.

978-1-4799-2893-4/14/$31.00 ©2014 IEEE

weight vector $\mathbf{v}$. Concurrently, the relays transmit artificial noise $\mathbf{n}_J$, $\mathbf{Q}_J = \mathrm{E}\{\mathbf{n}_J\mathbf{n}_J^H\}$, to confuse the eavesdropper. Finally, the signal transmitted by the relays is

$$\mathbf{x} = \mathrm{diag}\{\mathbf{v}\}(\mathbf{h}_{SR}s + \mathbf{n}_R) + \mathbf{n}_J \tag{2}$$

We focus our study on the relaying link, so we assume that both the destination and the eavesdropper cannot hear the message sent by the source but only the message sent by the relays. The signals received at the destination and the mth eavesdropper can thus be expressed as, respectively,

$$y_D = \mathbf{h}_{RD}^H \mathrm{diag}\{\mathbf{v}\}(\mathbf{h}_{SR}s + \mathbf{n}_R) + \mathbf{h}_{RD}^H\mathbf{n}_J + n_D$$

$$y_{E,m} = \mathbf{g}_{RE,m}^H \mathrm{diag}\{\mathbf{v}\}(\mathbf{h}_{SR}s + \mathbf{n}_R) + \mathbf{g}_{RE,m}^H\mathbf{n}_J + n_E$$

in which $n_D \sim \mathcal{CN}(0, \sigma_D^2)$ and $n_E \sim \mathcal{CN}(0, \sigma_E^2)$ are the AWGN at each receiver. In addition, $\mathbf{h}_{RD} \in \mathbb{C}^{N\times 1}$ and $\mathbf{g}_{RE,m} \in \mathbb{C}^{N\times 1}$ represent the channel vector from the relay to the destination and the mth eavesdropper, respectively.

Channel state information in the network is assumed to be perfectly known except that of the eavesdroppers

$$\mathbf{g}_{RE,m} = \hat{\mathbf{g}}_{RE,m} + \Delta\mathbf{g}_{RE,m} \quad m = 1, \ldots, M \tag{3}$$

where $\Delta\mathbf{g}_{RE,m}$ denotes the channel uncertainty whose magnitude is bounded by a constant β_m, i.e.,

$$\|\Delta\mathbf{g}_{RE,m}\|_F \le \beta_m \quad m = 1, \ldots, M \tag{4}$$

In this paper, we aim to maximize the worst-case secrecy rate [1] subject to both total and individual relay power constraints, i.e.,

$$\begin{aligned}\max_{\{\mathbf{Q}_\mathbf{v}, \mathbf{Q}_J\}} \min_{m\in\{1,\cdots,M\}} \min_{\{\Delta\mathbf{g}_{RE,m}\}} &\{\frac{1}{2}\log(1+\gamma_D) - \frac{1}{2}\log(1+\gamma_{E,m})\} \\ \text{s.t.} \quad &\mathrm{tr}\{P_s\mathbf{h}_{SR}\mathbf{h}_{SR}^H\mathrm{diag}\{\mathbf{Q}_\mathbf{v}\} + \sigma_R^2\mathbf{Q}_\mathbf{v} + \mathbf{Q}_J\} \le P_r \\ &\left[P_s\mathbf{h}_{SR}\mathbf{h}_{SR}^H\mathrm{diag}\{\mathbf{Q}_\mathbf{v}\} + \sigma_R^2\mathbf{Q}_\mathbf{v} + \mathbf{Q}_J\right]_{k,k} \le P_k \\ &\qquad k = 1, \cdots, N \end{aligned} \tag{5}$$

in which the covariance matrix $\mathbf{Q}_\mathbf{v} = \mathbf{v}\mathbf{v}^H$, $\mathbf{Q}_\mathbf{v} \succeq \mathbf{0}$. And the received signal to interference-plus-noise ratios (SINRs) at the destination and the mth eavesdropper are, respectively,

$$\gamma_D = \frac{P_s\mathbf{h}^H\mathbf{Q}_\mathbf{v}\mathbf{h}}{\sigma_D^2 + \mathbf{h}_{RD}^H(\sigma_R^2\mathrm{diag}\{\mathbf{Q}_\mathbf{v}\} + \mathbf{Q}_J)\mathbf{h}_{RD}}$$

$$\gamma_{E,m} = \frac{P_s\mathbf{g}_m^H\mathbf{Q}_\mathbf{v}\mathbf{g}_m}{\sigma_E^2 + \mathbf{g}_{RE,m}^H(\sigma_R^2\mathrm{diag}\{\mathbf{Q}_\mathbf{v}\} + \mathbf{Q}_J)\mathbf{g}_{RE,m}}$$

where the channel from the source to the destination $\mathbf{h} = \mathrm{diag}\{\mathbf{h}_{SR}\}\mathbf{h}_{RD}$, and the channel from the source to the mth eavesdropper $\mathbf{g}_m = \mathrm{diag}\{\mathbf{h}_{SR}\}\mathbf{g}_{RE,m}$.

III. Robust Joint Relaying and Jamming Schemes

The focus of this section is to solve the max-min optimization problem in (5) which is a nonconvex problem and challenging to solve directly. To this end, the two-layer (TL) idea [10] is utilized. The key insight is to recast the original optimization problem in (5) as a two-level optimization problem. The inner-level part is dealt with convex optimization methods

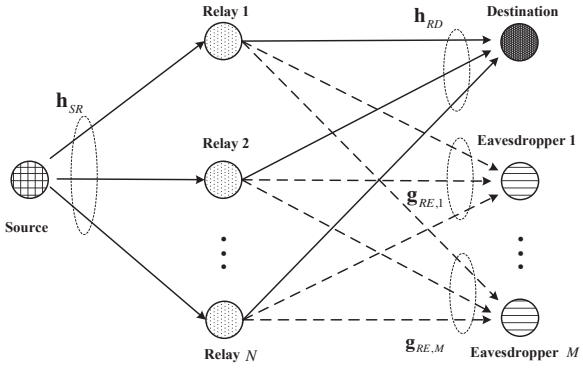

Fig. 1. AF relay network with single-antenna nodes

[11], and the outer-level part is dealt with a one-dimensional search. Specifically, the outer-level part is

$$\max_{\tau\in[\tau_{lb},\tau_{ub}]} \frac{1+f(\tau)}{1+\tau} \tag{6}$$

where $f(\tau)$ is obtained through solving the following inner-level part optimization problem for a given τ

$$\begin{aligned} f(\tau) = \max_{\{\mathbf{Q}_\mathbf{v}\succeq\mathbf{0}, \mathbf{Q}_J\succeq\mathbf{0}\}} &\frac{P_s\mathbf{h}^H\mathbf{Q}_\mathbf{v}\mathbf{h}}{\sigma_D^2 + \mathbf{h}_{RD}^H(\sigma_R^2\mathrm{diag}\{\mathbf{Q}_\mathbf{v}\} + \mathbf{Q}_J)\mathbf{h}_{RD}} \\ \text{s.t.} \quad \max_{\{\Delta\mathbf{g}_{RE,m}\}} &\frac{P_s\mathbf{g}_m^H\mathbf{Q}_\mathbf{v}\mathbf{g}_m}{\sigma_E^2 + \mathbf{g}_{RE,m}^H(\sigma_R^2\mathrm{diag}\{\mathbf{Q}_\mathbf{v}\} + \mathbf{Q}_J)\mathbf{g}_{RE,m}} \le \tau \\ &\qquad m = 1, \cdots, M \\ &\mathrm{tr}\{P_s\mathbf{h}_{SR}\mathbf{h}_{SR}^H\mathrm{diag}\{\mathbf{Q}_\mathbf{v}\} + \sigma_R^2\mathbf{Q}_\mathbf{v} + \mathbf{Q}_J\} \le P_r \\ &\left[P_s\mathbf{h}_{SR}\mathbf{h}_{SR}^H\mathrm{diag}\{\mathbf{Q}_\mathbf{v}\} + \sigma_R^2\mathbf{Q}_\mathbf{v} + \mathbf{Q}_J\right]_{k,k} \le P_k \\ &\qquad k = 1, \cdots, N \\ &\mathrm{rank}\{\mathbf{Q}_\mathbf{v}\} = 1 \end{aligned} \tag{7}$$

Letting $\eta = \frac{1}{\sigma_D^2 + \mathbf{h}_{RD}^H(\sigma_R^2\mathrm{diag}\{\mathbf{Q}_\mathbf{v}\} + \mathbf{Q}_J)\mathbf{h}_{RD}} > 0$, $\tilde{\mathbf{Q}}_\mathbf{v} = \eta\mathbf{Q}_\mathbf{v}$, $\tilde{\mathbf{Q}}_J = \eta\mathbf{Q}_J$, and using the Charnes-Cooper transformation, we can recast the problem in (7) as

$$\begin{aligned} f(\tau) = \max_{\{\tilde{\mathbf{Q}}_\mathbf{v}\succeq\mathbf{0}, \tilde{\mathbf{Q}}_J\succeq\mathbf{0}, \eta>0\}} &P_s\mathbf{h}^H\tilde{\mathbf{Q}}_\mathbf{v}\mathbf{h} \\ \text{s.t.} \quad &\sigma_D^2\eta + \mathbf{h}_{RD}^H(\sigma_R^2\mathrm{diag}\{\tilde{\mathbf{Q}}_\mathbf{v}\} + \tilde{\mathbf{Q}}_J)\mathbf{h}_{RD} = 1 \\ &\max_{\{\Delta\mathbf{g}_{RE,m}\}} \frac{P_s\mathbf{g}_m^H\tilde{\mathbf{Q}}_\mathbf{v}\mathbf{g}_m}{\sigma_E^2\eta + \mathbf{g}_{RE,m}^H(\sigma_R^2\mathrm{diag}\{\tilde{\mathbf{Q}}_\mathbf{v}\} + \tilde{\mathbf{Q}}_J)\mathbf{g}_{RE,m}} \le \tau \\ &\qquad m = 1, \cdots, M \\ &\mathrm{tr}\{P_s\mathbf{h}_{SR}\mathbf{h}_{SR}^H\mathrm{diag}\{\tilde{\mathbf{Q}}_\mathbf{v}\} + \sigma_R^2\tilde{\mathbf{Q}}_\mathbf{v} + \tilde{\mathbf{Q}}_J\} \le \eta P_r \\ &\left[P_s\mathbf{h}_{SR}\mathbf{h}_{SR}^H\mathrm{diag}\{\tilde{\mathbf{Q}}_\mathbf{v}\} + \sigma_R^2\tilde{\mathbf{Q}}_\mathbf{v} + \tilde{\mathbf{Q}}_J\right]_{k,k} \le \eta P_k \\ &\qquad k = 1, \cdots, N \\ &\mathrm{rank}\{\tilde{\mathbf{Q}}_\mathbf{v}\} = 1 \end{aligned} \tag{8}$$

in which the perfect CSI $\mathbf{g}_{RE,m}$ is not available. To handle this imperfect-CSI induced constraints in (8), we need the following *S-procedure* in [11]

Lemma 1: [11] Let $\varphi_k(\mathbf{x}) = \mathbf{x}^H\mathbf{A}_k\mathbf{x} + 2\Re\{\mathbf{b}_k^H\mathbf{x}\} + c_k$, where $\mathbf{A}_k \in \mathbb{H}^n$, $\mathbf{b}_k \in \mathbb{C}^n$, $c_k \in \mathbb{R}$. The implication $\varphi_1(\mathbf{x}) \le$

$0 \Rightarrow \varphi_2(\mathbf{x}) \leq 0$ holds if and only if there exists a $\mu \geq 0$ such that

$$\mu \begin{bmatrix} \mathbf{A}_1 & \mathbf{b}_1 \\ \mathbf{b}_1^H & c_1 \end{bmatrix} - \begin{bmatrix} \mathbf{A}_2 & \mathbf{b}_2 \\ \mathbf{b}_2^H & c_2 \end{bmatrix} \succeq \mathbf{0}$$

provided that there exists a point $\hat{\mathbf{x}}$ such that $\varphi_1(\hat{\mathbf{x}}) < 0$.

For ease of exposition, we first rewrite the second constraint in (8) as

$$\mathbf{g}_{RE,m}^H \mathbf{\Phi} \mathbf{g}_{RE,m} - \tau\eta\sigma_E^2 \leq 0 \tag{9}$$

where $\mathbf{\Phi} = P_s \mathrm{diag}\{\mathbf{h}_{SR}\}^H \tilde{\mathbf{Q}}_{\mathbf{v}} \mathrm{diag}\{\mathbf{h}_{SR}\} - \sigma_R^2 \tau \mathrm{diag}\{\tilde{\mathbf{Q}}_{\mathbf{v}}\} - \tau\tilde{\mathbf{Q}}_J$. Substituting (3) into (9) yields

$$\begin{aligned} \Delta\mathbf{g}_{RE,m}^H \mathbf{\Phi} \Delta\mathbf{g}_{RE,m} + 2\Re\{\hat{\mathbf{g}}_{RE,m}^H \mathbf{\Phi} \Delta\mathbf{g}_{RE,m}\} \\ + \hat{\mathbf{g}}_{RE,m}^H \mathbf{\Phi} \hat{\mathbf{g}}_{RE,m} - \tau\eta\sigma_E^2 \leq 0 \end{aligned} \tag{10}$$

Combined with the *S-procedure* in Lemma 1, (4)⇒(10) if and only if, for some $\mu_m \geq 0$,

$$\begin{bmatrix} \mu_m \mathbf{I} - \mathbf{\Phi} & -\mathbf{\Phi}^H \hat{\mathbf{g}}_{RE,m} \\ -\hat{\mathbf{g}}_{RE,m}^H \mathbf{\Phi} & -\beta_m^2 \mu_m - \hat{\mathbf{g}}_{RE,m}^H \mathbf{\Phi} \hat{\mathbf{g}}_{RE,m} + \tau\eta\sigma_E^2 \end{bmatrix} \succeq \mathbf{0} \tag{11}$$

Further, $\mathrm{diag}\{\tilde{\mathbf{Q}}_{\mathbf{v}}\} = \sum_{i=1}^N \mathbf{E}_i \tilde{\mathbf{Q}}_{\mathbf{v}} \mathbf{E}_i$ where $\mathbf{E}_i$ is the matrix with all 0 entries except that the ith diagonal entry is 1. Thus for any matrix $\mathbf{A}$, we have $\mathrm{tr}\{\mathbf{A}\mathrm{diag}\{\tilde{\mathbf{Q}}_{\mathbf{v}}\}\} = \mathrm{tr}\{\mathrm{diag}\{\mathbf{A}\}\tilde{\mathbf{Q}}_{\mathbf{v}}\}$ which enables us to rewrite the optimization problem in (8) as

$$\begin{aligned} f(\tau) = \max_{\{\tilde{\mathbf{Q}}_{\mathbf{v}} \succeq \mathbf{0}, \tilde{\mathbf{Q}}_J \succeq \mathbf{0}, \eta > 0, \mu_m \geq 0, \forall m\}} & P_s \mathrm{tr}\{\mathbf{h}\mathbf{h}^{\mathrm{H}} \tilde{\mathbf{Q}}_{\mathbf{v}}\} \\ \text{s.t. } \sigma_D^2 \eta + \mathrm{tr}\{\sigma_R^2 \mathrm{diag}\{\mathbf{h}_{\mathrm{RD}} \mathbf{h}_{RD}^H\} \tilde{\mathbf{Q}}_{\mathbf{v}} + \mathbf{h}_{\mathrm{RD}} \mathbf{h}_{RD}^H \tilde{\mathbf{Q}}_J\} = 1 & \\ \begin{bmatrix} \mu_m \mathbf{I} - \mathbf{\Phi} & -\mathbf{\Phi}^H \hat{\mathbf{g}}_{RE,m} \\ -\hat{\mathbf{g}}_{RE,m}^H \mathbf{\Phi} & -\beta_m^2 \mu_m - \hat{\mathbf{g}}_{RE,m}^H \mathbf{\Phi} \hat{\mathbf{g}}_{RE,m} + \tau\eta\sigma_E^2 \end{bmatrix} \succeq \mathbf{0} & \\ m = 1, \cdots, M & \\ \mathrm{tr}\{P_s \mathrm{diag}\{\mathbf{h}_{SR} \mathbf{h}_{SR}^H\} \tilde{\mathbf{Q}}_{\mathbf{v}} + \sigma_R^2 \tilde{\mathbf{Q}}_{\mathbf{v}} + \tilde{\mathbf{Q}}_J\} \leq \eta P_r & \\ \left[P_s \mathrm{diag}\{\mathbf{h}_{SR} \mathbf{h}_{SR}^H\} \tilde{\mathbf{Q}}_{\mathbf{v}} + \sigma_R^2 \tilde{\mathbf{Q}}_{\mathbf{v}} + \tilde{\mathbf{Q}}_J\right]_{k,k} \leq \eta P_k & \\ k = 1, \cdots, N & \\ \mathrm{rank}\{\tilde{\mathbf{Q}}_{\mathbf{v}}\} = 1 & \end{aligned} \tag{12}$$

which is still a nonconvex problem due to the rank-one constraint on $\mathbf{Q}_{\mathbf{v}}$. To this end, we resort to the semidefinite relaxation (SDR) technique [12] and drop the rank-one constraint. The resulting optimization problem is a SDP and can be efficiently solved by available softwares, e.g., CVX [11]. Moreover, in Appendix A, we get Proposition 1 as follows

Proposition 1: *There exists an optimal solution* $\{\mathbf{Q}_{\mathbf{v}}^\star, \mathbf{Q}_J^\star\}$ *of (12) such that* $\mathrm{rank}\{\mathbf{Q}_{\mathbf{v}}^\star\} = 1$*, provided that a positive secrecy rate is achieved.*

Thus, optimal solutions obtained by the SDR technique are also optimal solutions to (12). So far, the inner-level part is solved and $f(\tau)$ is dertamined for any given τ. The remaining issue now is to resolve the optimal $\tau^\star$ maximizing the objective function in (6). In (6), τ_{lb} and τ_{ub} denote the lower and upper bound of $\gamma_{E,m}$, respectively. Firstly since $\gamma_{E,m}$ is no less than 0, thus we have $\tau_{lb} = 0$. Secondly, according to the security requirement, $\gamma_{E,m}$ should be no more than γ_D. Further, γ_D is upper bounded by the maximal received SINR value at the destination that can be achieved by the no-eavesdropper case (SRD Link). Therefore, τ_{ub} can be determined by solving the following optimization problem

$$\begin{aligned} \tau_{ub} = \max_{\mathbf{v}} \quad & \frac{P_s \mathbf{v}^H \mathbf{h}\mathbf{h}^H \mathbf{v}}{\sigma_D^2 + \sigma_R^2 \mathbf{v}^H \mathbf{H}_{RD} \mathbf{v}} \\ \text{s.t.} \quad & \mathbf{v}^H (\sigma_R^2 \mathbf{I} + P_s \mathbf{H}_{SR}) \mathbf{v} \leq P_r \end{aligned} \tag{13}$$

where $\mathbf{H}_{RD} = \mathrm{diag}\{\mathbf{h}_{\mathrm{RD}} \mathbf{h}_{\mathrm{RD}}^{\mathrm{H}}\}$ and $\mathbf{H}_{SR} = \mathrm{diag}\{\mathbf{h}_{\mathrm{SR}} \mathbf{h}_{\mathrm{SR}}^{\mathrm{H}}\}$. Solving the optimization problem in (13) which is a generalized eigenvector problem, we get

$$\tau_{ub} = P_s \mathbf{h}^H (\sigma_D^2 (\sigma_R^2 \mathbf{I} + P_s \mathbf{H}_{SR})/P_r + \sigma_R^2 \mathbf{H}_{RD})^{-1} \mathbf{h}$$

By performing one dimension search on τ, the optimal $\tau^\star$ maximizing the objective function in (6) could be found. Correspondingly, the optimal solution $\mathbf{v}^\star$, $\mathbf{Q}_J^\star$ to the original optimization problem (5) are obtained.

IV. Numerical Results

Channels are are assumed to be independent of each other with elements distributed as complex Gaussian with zero-mean and unit covariance. Results are averaged over 1000 independent trials. We set parameters as follows: $\sigma_D^2 = \sigma_E^2 = \sigma_R^2 = 1$, $M = 5$, $N = 10$, $\beta_m/\sqrt{N} = \varepsilon$ for all $\mathbf{g}_m$, $P_k = 0.5P_r/N$ for $k = 1, \cdots, N/2$, and $P_k = 2P_r/N$ for $k = N/2+1, \cdots, N$.

Fig.2 plots the worst-case secrecy rate performance with varying ε. Note that the proposed robust scheme also applies to the perfect CSI case where worst-case secrecy rate equals to secrecy rate. Here, the line labeled as SRD link shows the data rate that can be achieved by the no-eavesdropper case, which provides an upper bound on the secrecy rate of all security schemes. Results show that the worst-case secrecy rate decreases with the increase of channel uncertainties. However, perfect secrecy can always be guaranteed. Especially when the total relay power is large enough, such performance degradation eases up. In addition, the line labeled as AF Without Jamming plots the secrecy rate that can be achieved by the AF scheme without transmitting artificial noise. It can be observed that even when Global CSI is available, i.e., the $\varepsilon = 0$ case, the proposed joint cooperative relaying and jamming scheme outperforms the AF Without Jamming scheme. Correspondingly, Fig.3 plots the optimal percent results of power distributed to the artificial noise. Results show that the power distributed to the AN increases with both the total relay power budget and the channel uncertainties. Besides, we see that even when Global CSI is available, distributing part of the total relay power to AN is necessary.

V. Conclusion

The problem of robust transmit design aiming to maximize the worst-case secrecy rate for secure AF relay networks was considered. To utilize the power at relays more effectively, a joint cooperative relaying and jamming scheme was proposed. Optimal relay weight vector and AN covariance matrix were obtained by carefully reformulating the original nonconvex optimization problem into a sequence of SDPs.

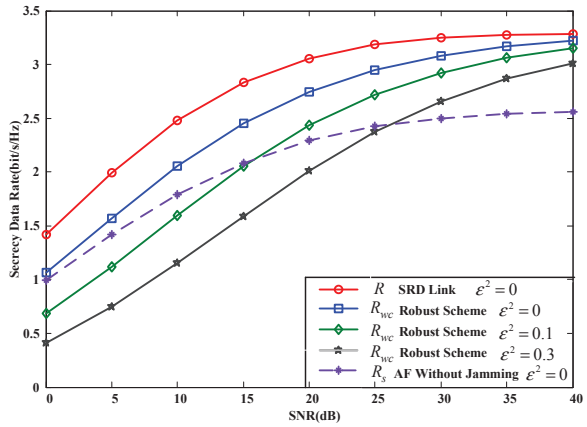

Fig. 2. Worst-case secrecy rate versus total relay power for P_s=10dB

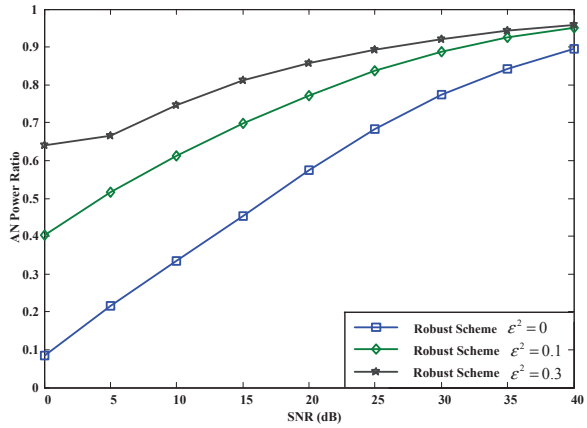

Fig. 3. Power distributed to AN versus total relay power for P_s=10dB

Appendix A
Proof of Proposition 1

Through simple extensions of the results in [8], omitted for the lack of space, optimal solutions to the following power minimization problem are also optimal solutions to the original optimization problem in (7).

$$\begin{aligned}
&\min_{\{\mathbf{Q_v}\succeq\mathbf{0},\mathbf{Q}_J\succeq\mathbf{0}\}} \mathrm{tr}\{P_s\mathbf{h}_{SR}\mathbf{h}_{SR}^H\mathrm{diag}\{\mathbf{Q_v}\}+\sigma_R^2\mathbf{Q_v}+\mathbf{Q}_J\}\\
&\text{s.t. } \frac{P_s\mathbf{h}^H\mathbf{Q_v}\mathbf{h}}{\sigma_D^2+\mathbf{h}_{RD}^H(\sigma_R^2\mathrm{diag}\{\mathbf{Q_v}\}+\mathbf{Q}_J)\mathbf{h}_{RD}}\geq f(\tau)\\
&\max_{\{\Delta\mathbf{g}_{RE,m}\}}\frac{P_s\mathbf{g}_m^H\mathbf{Q_v}\mathbf{g}_m}{\sigma_E^2+\mathbf{g}_{RE,m}^H(\sigma_R^2\mathrm{diag}\{\mathbf{Q_v}\}+\mathbf{Q}_J)\mathbf{g}_{RE,m}}\leq\tau\\
&\qquad\qquad m=1,\cdots,M\\
&\left[P_s\mathbf{h}_{SR}\mathbf{h}_{SR}^H\mathrm{diag}\{\mathbf{Q_v}\}+\sigma_R^2\mathbf{Q_v}+\mathbf{Q}_J\right]_{k,k}\leq P_k\\
&\qquad\qquad k=1,\cdots,N\\
&\mathrm{rank}\{\mathbf{Q_v}\}=1 \qquad (14)
\end{aligned}$$

Applying the same derivation steps from (8) to (12) in Part III, and letting $\mathbf{\Psi}=P_s\mathrm{diag}\{\mathbf{h}_{SR}\}^H\mathbf{Q_v}\mathrm{diag}\{\mathbf{h}_{SR}\}-\sigma_R^2\tau\mathrm{diag}\{\mathbf{Q_v}\}-\tau\mathbf{Q}_J$, we can recast the optimization problem in (14) as

$$\begin{aligned}
&\min_{\{\mathbf{Q_v}\succeq\mathbf{0},\mathbf{Q}_J\succeq\mathbf{0},\mu_m\geq0,\forall m\}}\mathrm{tr}\{P_s\mathrm{diag}\{\mathbf{h}_{SR}\mathbf{h}_{SR}^H\}\mathbf{Q_v}+\sigma_R^2\mathbf{Q_v}+\mathbf{Q}_J\}\\
&\text{s.t. } f(\tau)\sigma_D^2+f(\tau)\mathrm{tr}\{\sigma_R^2\mathrm{diag}\{\mathbf{h}_{RD}\mathbf{h}_{RD}^H\}\mathbf{Q_v}+\mathbf{h}_{RD}\mathbf{h}_{RD}^H\mathbf{Q}_J\}\\
&\quad\leq P_s\mathrm{tr}\{\mathbf{h}\mathbf{h}^H\mathbf{Q_v}\}\\
&\begin{bmatrix}\mu_m\mathbf{I}-\mathbf{\Psi} & -\mathbf{\Psi}^H\hat{\mathbf{g}}_{RE,m}\\ -\hat{\mathbf{g}}_{RE,m}^H\mathbf{\Psi} & -\beta_m^2\mu_m-\hat{\mathbf{g}}_{RE,m}^H\mathbf{\Psi}\hat{\mathbf{g}}_{RE,m}+\tau\sigma_E^2\end{bmatrix}\succeq\mathbf{0}\\
&\qquad\qquad m=1,\cdots,M\\
&\left[P_s\mathrm{diag}\{\mathbf{h}_{SR}\mathbf{h}_{SR}^H\}\mathbf{Q_v}+\sigma_R^2\mathbf{Q_v}+\mathbf{Q}_J\right]_{k,k}\leq P_k\\
&\qquad\qquad k=1,\cdots,N\\
&\mathrm{rank}\{\mathbf{Q_v}\}=1 \qquad (15)
\end{aligned}$$

Further, resorting to the SDR technique [12] and dropping the rank-one constraint, the resulting optimization problem of (15) is convex with part of the KKT conditions as follows

$$\begin{aligned}
\mathbf{Y}=&P_s\mathrm{diag}\{\mathbf{h}_{SR}\mathbf{h}_{SR}^H\}+\sigma_R^2\mathbf{I}\\
&+\lambda[\sigma_R^2f(\tau)\mathrm{diag}\{\mathbf{h}_{RD}\mathbf{h}_{RD}^H\}-P_s\mathbf{h}\mathbf{h}^H]\\
&+\sum\nolimits_{m=1}^{M}\mathrm{diag}\{\mathbf{h}_{SR}\}\mathbf{G}_m\mathbf{B}_m\mathbf{G}_m^H\mathrm{diag}\{\mathbf{h}_{SR}\}^H\\
&-\sum\nolimits_{m=1}^{M}\sigma_R^2\tau\mathrm{diag}\{\mathbf{G}_m\mathbf{B}_m\mathbf{G}_m^H\}\\
&+\sum\nolimits_{k=1}^{N}v_k[P_s\mathrm{diag}\{\mathbf{E}_k\mathbf{h}_{SR}\mathbf{h}_{SR}^H\}+\sigma_R^2\mathbf{E}_k] \qquad (16a)\\
\mathbf{X}=&\mathbf{I}+\lambda f(\tau)\mathbf{h}_{RD}\mathbf{h}_{RD}^H-\sum\nolimits_{m=1}^{M}\tau\mathbf{G}_m\mathbf{B}_m\mathbf{G}_m^H\\
&+\sum\nolimits_{k=1}^{N}v_k\mathbf{E}_k \qquad (16b)\\
&\mathbf{Y}\mathbf{Q}_{\mathbf{v}}^{\star}=\mathbf{0} \qquad (16c)\\
&\mathbf{Y}\succeq\mathbf{0},\mathbf{X}\succeq\mathbf{0},\mathbf{B}_m\succeq\mathbf{0},\forall m,v_k\geq0,\forall k,\lambda\geq0 \qquad (16d)
\end{aligned}$$

in which $\mathbf{G}_m=[\mathbf{I},\ \hat{\mathbf{g}}_{RE,m}]$. $\mathbf{Y}$ and $\mathbf{X}$ are dual variables associated with $\mathbf{Q}_{\mathbf{v}}^{\star}$ and $\mathbf{Q}_J^{\star}$, respectively. In addition, λ, $\mathbf{B}_m$ and v_k are dual variables associated with corresponding inequalities in (15). Substituting (16-b) into (16-a), we get

$$\begin{aligned}
\mathbf{Y}=&P_s\mathrm{diag}\{\mathbf{h}_{SR}\mathbf{h}_{SR}^H\}+\sigma_R^2\mathrm{diag}\{\mathbf{X}\}\\
&+\sum\nolimits_{m=1}^{M}\mathrm{diag}\{\mathbf{h}_{SR}\}\mathbf{G}_m\mathbf{B}_m\mathbf{G}_m^H\mathrm{diag}\{\mathbf{h}_{SR}\}^H\\
&+\sum\nolimits_{k=1}^{N}v_k[P_s\mathrm{diag}\{\mathbf{E}_k\mathbf{h}_{SR}\mathbf{h}_{SR}^H\}]\\
&-\lambda P_s\mathbf{h}\mathbf{h}^H\\
=&\tilde{\mathbf{Y}}-\lambda P_s\mathbf{h}\mathbf{h}^H \qquad (17)
\end{aligned}$$

where we define $\tilde{\mathbf{Y}}=\mathbf{Y}+\lambda P_s\mathbf{h}\mathbf{h}^H$. Since $\mathbf{X}\succeq\mathbf{0}$, so $\mathrm{diag}\{\mathbf{X}\}\succeq\mathbf{0}$. Moreover, $\mathrm{diag}\{\mathbf{h}_{SR}\mathbf{h}_{SR}^H\}\succ\mathbf{0}$ holds in general, and the other two terms in the sum expression of $\tilde{\mathbf{Y}}$ are always non-negative hermite matrix, therefore $\tilde{\mathbf{Y}}\succ\mathbf{0}$.

Combing (16c) and (17), we get $\tilde{\mathbf{Y}}\mathbf{Q}_{\mathbf{v}}^{\star}=\lambda P_s\mathbf{h}\mathbf{h}^H\mathbf{Q}_{\mathbf{v}}^{\star}$. Firstly, because $\mathrm{rank}\{\tilde{\mathbf{Y}}\mathbf{Q}_{\mathbf{v}}^{\star}\}=\mathrm{rank}\{\lambda P_s\mathbf{h}\mathbf{h}^H\mathbf{Q}_{\mathbf{v}}^{\star}\}\leq1$ and $\tilde{\mathbf{Y}}\succ\mathbf{0}$, so $\mathrm{rank}\{\mathbf{Q}_{\mathbf{v}}^{\star}\}=\mathrm{rank}\{\tilde{\mathbf{Y}}\mathbf{Q}_{\mathbf{v}}^{\star}\}\leq1$. Secondly, $\mathrm{rank}\{\mathbf{Q}_{\mathbf{v}}^{\star}\}=0$ implies $\mathbf{Q}_{\mathbf{v}}^{\star}=\mathbf{0}$ which contradicts with the positive secrecy rate requirement. Therefore, we claim that $\mathrm{rank}\{\mathbf{Q}_{\mathbf{v}}^{\star}\}=1$. And optimal solutions to the optimization problem in (14)(15) are always rank-one, which completes the proof.

REFERENCES

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

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

[3] Y. Yang, Q. Li, and W.-K. Ma, "Cooperative secure beamforming for AF relay networks with multiple eavesdroppers," *IEEE Signal Processing Letters*, vol. 20, no. 1, pp. 35–38, Jan. 2013.

[4] H.-M. Wang, M. Luo, and X.-G. Xia, "Joint cooperative beamforming and jamming to secure AF relay systems with individual power constraint and no eavesdropper's CSI," *IEEE Signal Processing Letters*, vol. 20, no. 1, pp. 39–42, Jan. 2013.

[5] X. Wang, K. Wang, and X.-D. Zhang, "Secure relay beamforming with imperfect channel side information," *IEEE Transactions on Vehicular Technology*, vol. 62, no. 5, pp. 2140–2155, Jun. 2013.

[6] S. Vishwakarma and A. Chockalingam, "Amplify-and-forward relay beamforming for secrecy with cooperative jamming and imperfect CSI," in *IEEE International Conference on Communications (ICC)*, Budapest,Hungary, Jun. 2013, pp. 1640–1645.

[7] R. Negi and S. Goel, "Secret communication using artificial noise," in *IEEE 62nd Vehicular Technology Conference (VTC-2005-Fall)*, Texas, USA, 2005, pp. 1906–1910.

[8] Q. Li and W.-K. Ma, "A robust artificial noise aided transmit design for MISO secrecy," in *IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, Prague Congress Center, Prague, Czech Republic, May 2011, pp. 3436–3439.

[9] J. Huang and A. L. Swindlehurst, "Robust secure transmission in MISO channels based on worst-case optimization," *IEEE Transactions on Signal Processing*, vol. 60, no. 4, pp. 1696–1707, 2012.

[10] H.-T. Chiang and J. S. Lehnert, "Optimal cooperative jamming for security," in *IEEE Military Communications Conference (MILCOM)*, Baltimore, MD, Nov. 2011, pp. 125–130.

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

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