Worst Case SINR Guarantees for Secrecy using Relay Beamforming with Imperfect CSI

Agepati Sujana, Sanjay Vishwakarma, and A. Chockalingam
Department of ECE, Indian Institute of Science, Bangalore 560012

Abstract—**In this paper, we study beamforming techniques for secrecy with worst case signal-to-interference-plus-noise ratio (SINR) guarantees in cooperative communications with imperfect channel state information (CSI). The worst case SINRs are the minimum SINR at the intended destination and the maximum SINR at the eavesdroppers. We consider a norm bounded CSI error model. With the available imperfect channel estimates, we design beamformers such that the minimum SINR receivable by the intended destination is above a certain threshold, while the maximum value of SINRs receivable at the eavesdroppers are below another lower threshold. We consider amplify-and-forward (AF) and decode-and-forward (DF) relaying schemes. The relays do the worst case transmit beamforming and injection of artificial noise (AN). We jointly optimize the beamformers and the AN for the AF and DF schemes subject to the worst case SINR constraints at the destination and the eavesdroppers. We solve the corresponding optimization problems as semi-definite programming (SDP) problems by rank relaxation and S-procedure. Numerical results show that AN injection at the relays significantly reduces the average total transmit power required to meet the worst case SINR constraints, and improves the solution feasibility of the optimization problems.**

Keywords – *Physical layer security, cooperative communication, artificial noise, imperfect CSI, semi-definite programming, S-procedure.*

I. Introduction

Because of their broadcast nature, wireless channels are vulnerable to eavesdropping. Secure wireless communication in the presence of eavesdroppers is a topic of current interest [1], [2], [3]. In physical layer security, secrecy guarantees can be achieved by exploiting the characteristics of the physical layer. Secrecy in wireless communication can be improved using multiple antennas [4]. Techniques used for secrecy with multiple antennas include beamforming and injection of artificial noise (AN). In the AN technique, a portion of the transmit power is used to artificially generate noise which is injected into the channel. The injected noise can interfere at the eavesdroppers, and hence can potentially increase the secrecy rate [5].

The signal-to-noise ratio (SNR) at the receiver determines the bit error rate (BER) performance of communication links. So, for secret communication, we need certain SNR targets at the destination and at the eavesdroppers. Beamforming can be used to guarantee these SNRs at the destination and the eavesdroppers. Secrecy can be improved by using AN injection, which essentially act as interference at the eavesdroppers [5].

This work was supported in part by a gift from the Cisco University Research Program, a corporate advised fund of Silicon Valley Community Foundation.

978-1-4799-3083-8/14/$31.00 © 2014 IEEE

In scenarios with AN injection, it would be appropriate to use signal-to-interference-plus-noise (SINR) targets instead of SNR targets, e.g., maintain good SINR at the destination and poor SINRs at the eavesdroppers.

In this paper, we focus on the design of beamformers and AN in cooperative communications *with imperfect channel state information (CSI)*. We ensure that the minimum SINR at the destination to be above a certain threshold (γ_D) and the maximum SINR at the eavesdroppers is below another lower threshold (γ_E). In [6], robust beamforming strategies for multiple-input single-output (MISO) system is studied with imperfect knowledge of eavesdroppers CSI. Having multiple antennas at the source may not be feasible always due to space constraints of accommodating them. Relays can be used to aid communication in such cases. Relay communication for secrecy has been investigated in [7] and [8]. In this work, we study beamformer design and AN injection at the relays with minimum total transmit power, subject to worst case SINR constraints at the destination and the eavesdroppers in amplify-and-forward (AF) and decode-and-forward (DF) relaying protocols with imperfect CSI on all links, where the CSI error vectors are norm-bounded by a known value.

The considered beamformer designs with minimal total transmit power are non-convex optimization problems. By rank relaxation and S-procedure they are converted to semi-definite optimization problems and solved by semi-definite programming (SDP) tools. The performance of the beamformers with and without AN are compared. Numerical results show that injection of AN at the relays significantly reduces the average total transmit power required to meet the SINR constraints, and also improves the solution feasibility of the optimization problems for AF and DF relaying schemes.

Notations: Vectors and matrices are denoted by boldface lowercase letters and boldface uppercase letters, respectively. $[.]^T$, $[.]^*$, $[.]^\dagger$ denote the transpose, conjugate, hermitian operations, respectively. $\mathbb{E}[.]$ denotes expectation, $\|.\|$ is euclidean norm, tr(.) is the trace operator, $diag(\mathbf{y})$ denotes a diagonal matrix with the elements of vector $\mathbf{y}$ along its diagonal, $diag(\mathbf{A})$ denotes a vector formed with the diagonal elements of $\mathbf{A}$, and $\mathbf{I}_n$ denotes $n \times n$ identity matrix.

II. System model

We consider one source and one destination communicating with the help of multiple relays in the presence of multiple eavesdroppers. The system model is as shown in Fig.

1. The model consists of a source S, a destination D, N relay nodes $\{\mathrm{R}_i\}_{i=1}^{N}$, and M eavesdroppers $\{\mathrm{E}_m\}_{m=1}^{M}$. All nodes are assumed to be half-duplex with one antenna each. All channels are assumed to be flat fading. Let $\mathbf{h}_{SR}^* = [h_{SR_1}^*, h_{SR_2}^*, \cdots, h_{SR_N}^*]^T$ denote the $N \times 1$ channel gain vector from source to relays, h_{SD}^* denote the channel gain from source to destination, $\mathbf{h}_{SE}^* = [h_{SE_1}^*, h_{SE_2}^*, \cdots, h_{SE_M}^*]^T$ denote the $M \times 1$ channel gain vector from source to eavesdroppers, $\mathbf{h}_{RD}^* = [h_{R_1D}^*, h_{R_2D}^*, \cdots, h_{R_ND}^*]^T$ denote the $N \times 1$ channel gain vector from relays to the destination, and $\mathbf{H}_{RE}^*$ denotes the $N \times M$ channel matrix between relays and eavesdroppers given by $\mathbf{H}_{RE}^* = [\mathbf{h}_{RE_1}^* \ \mathbf{h}_{RE_2}^* \ \cdots \ \mathbf{h}_{RE_M}^*]$, where $\mathbf{h}_{RE_m}^* = [h_{R_1E_m}^*, h_{R_2E_m}^*, \cdots, h_{R_NE_m}^*]^T$, $m = 1, 2, \cdots, M$. In

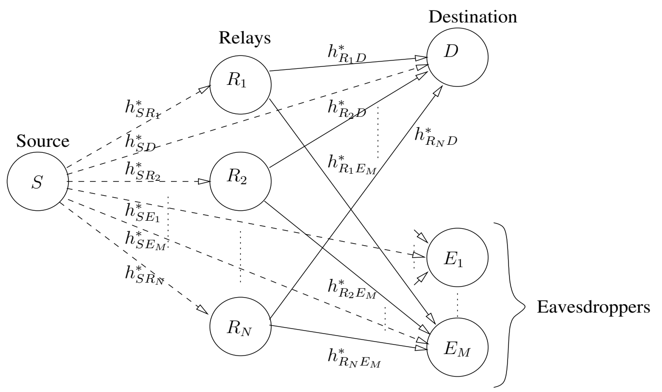

Fig. 1. System model of relay beamforming with multiple eavesdroppers.

both AF and DF schemes, communication between source and destination takes place in two time slots. In the first slot, source transmits the data symbol, which is received by the relays, destination and eavesdroppers. In the next slot, the relays transmit to the destination which is received at the eavesdroppers too. The signal received by the relays during the first slot is given by

$$\mathbf{y}_R = \sqrt{P_s}\mathbf{h}_{SR}^* x + \mathbf{n}_R, \tag{1}$$

where P_s is the source power, x is the source data with unit variance, $\mathbf{y}_R$ is the $N \times 1$ vector with received signals at N relays, $\mathbf{n}_R$ is the thermal noise vector at the relays, i.e., $\mathbf{n}_R \sim \mathcal{CN}(0, \sigma_R^2 \mathbf{I}_N)$. The received signals at the destination and at the mth eavesdropper during first slot are given by

$$y_{1D} = \sqrt{P_s} h_{SD}^* x + n_{1D}, \tag{2}$$

$$y_{1E_m} = \sqrt{P_s} h_{SE_m}^* x + n_{1E_m}. \tag{3}$$

A. Amplify-and-forward scheme

In the AF relaying scheme, during the second time slot, the relays transmit the weighted version of the received signal and add artificial noise (AN). The transmit signal of the relays, denoted by $\mathbf{s}$, is given by

$$\mathbf{s} = diag(\mathbf{y}_R)\mathbf{w} + \mathbf{n}_{AN}, \tag{4}$$

where $\mathbf{n}_{AN} = [n_{AN_1}, n_{AN_2}, \cdots, n_{AN_N}]^T$, and n_{AN_i} is the artificial noise injected by the ith relay. $\mathbf{n}_{AN}$ is $N \times 1$ complex Gaussian vector with zero mean and covariance matrix $\mathbf{\Omega}$, i.e., $\mathbf{n}_{AN} \sim \mathcal{CN}(0, \mathbf{\Omega})$. The received signal at the destination in the second time slot is given by

$$y_{2D} = \sqrt{P_s}\mathbf{h}^\dagger \mathbf{w} x + \mathbf{n}_R^T diag(\mathbf{h}_{RD}^*)\mathbf{w} + \mathbf{h}_{RD}^\dagger \mathbf{n}_{AN} + n_{2D}, \tag{5}$$

where $\mathbf{h} \triangleq diag(\mathbf{h}_{SR})\mathbf{h}_{RD}$. Similarly, the received signal at the mth eavesdropper is given by

$$y_{2E_m} = \sqrt{P_s}\mathbf{h}_m^\dagger \mathbf{w} x + \mathbf{n}_R^T diag(\mathbf{h}_{RE_m}^*)\mathbf{w} + \mathbf{h}_{RE_m}^\dagger \mathbf{n}_{AN} + n_{2E_m}, \tag{6}$$

where $\mathbf{h}_m \triangleq diag(\mathbf{h}_{SR})\mathbf{h}_{RE_m}$. The thermal noise components at the destination and the mth eavesdropper, are assumed to be i.i.d; $n_{iD} \sim \mathcal{CN}(0, \sigma_D^2)$ and $n_{iE_m} \sim \mathcal{CN}(0, \sigma_{E_m}^2)$ for i = 1, 2. Using (4), the total transmit power in AF scheme is given by

$$P_T = P_s + \mathbf{w}^\dagger (P_s diag(\mathbf{h}_{SR}^*) diag(\mathbf{h}_{SR}) + \sigma_R^2 \mathbf{I}_n)\mathbf{w} + tr(\mathbf{\Omega}). \tag{7}$$

B. Decode-and-forward scheme

In the DF scheme, a relay selection scheme is considered where k out of N relays $(1 \leq k \leq N)$ decode the data from the received signal (1) in the first slot, and transmit the decoded data along with AN in the second slot. Relay R_i is chosen to participate in the DF relaying if its minimum receivable SNR in the first slot is above a threshold γ_R. The transmit signal from k selected DF relays is

$$\mathbf{s} = diag(\mathbf{x})\mathbf{w} + \mathbf{n}_{AN}, \tag{8}$$

where $\mathbf{x} = [x_1, x_2, \cdots, x_k]^T$, $x_i (= x)$ is the decoded symbol with unit variance at the ith relay for $(1 \leq i \leq k)$, $\mathbf{w}$ is the beamforming vector for the k selected relays, and $\mathbf{n}_{AN}$ is the AN vector injected by the k relays. In this DF scheme with relay selection, $\mathbf{h}_{RD}^*$ is a $k \times 1$ vector with channel gains from the selected relays to the destination. Likewise, $\mathbf{h}_{RE_m}^*$ is a $k \times 1$ vector with channel gains from k relays to the mth eavesdropper. The received signal at the destination during second slot is given by

$$y_{2D} = \mathbf{h}_{RD}^\dagger diag(\mathbf{x})\mathbf{w} + \mathbf{h}_{RD}^\dagger \mathbf{n}_{AN} + n_{2D}. \tag{9}$$

Similarly, the received signal at the mth eavesdropper during second slot is given by

$$y_{2E_m} = \mathbf{h}_{RE_m}^\dagger diag(\mathbf{x})\mathbf{w} + \mathbf{h}_{RE_m}^\dagger \mathbf{n}_{AN} + n_{2E_m}. \tag{10}$$

The total transmit power in DF scheme using (8) is given by

$$\mathrm{P}_T = P_s + \|\mathbf{w}\|^2 + tr(\mathbf{\Omega}). \tag{11}$$

In DF, for minimum transmit power, we have to solve the optimization problem over all possible relay combinations (i.e., $2^N - 1$ combinations) and choose the subset of relays which results in the lowest transmit power. Beamforming has to be done over these selected best relays and AN has to be injected.

III. SINR EXPRESSIONS WITH IMPERFECT CSI

We assume that channel state information (CSI) knowledge is imperfect. Only the channel estimates are available. Let the channel error vectors be defined as follows: $e_{SD} = h_{SD} - \hat{h}_{SD}$, $e_{SE_m} = h_{SE_m} - \hat{h}_{SE_m}$, $e_{SR_i} = h_{SR_i} - \hat{h}_{SR_i}$, for $i = 1, 2, \cdots, N$, $\mathbf{e}_{RD} = \mathbf{h}_{RD} - \hat{\mathbf{h}}_{RD}$, $\mathbf{e}_{RE_m} = \mathbf{h}_{RE_m} - \hat{\mathbf{h}}_{RE_m}$, for $m = 1, 2, \cdots, M$, where e_{SD}, e_{SE_m}, e_{SR_i}, $\mathbf{e}_{RD}$, $\mathbf{e}_{RE_m}$ are the error components and $\hat{h}_{SD}$, $\hat{h}_{SE_m}$, $\hat{h}_{SR_i}$, $\hat{\mathbf{h}}_{RD}$, $\hat{\mathbf{h}}_{RE_m}$ are the available CSI estimates. The error vectors are assumed to be norm bounded, i.e., $|e_{SD}|^2 \leq \epsilon_{SD}^2$, $|e_{SE_m}|^2 \leq \epsilon_{SE}^2$ $|e_{SR_i}|^2 \leq \epsilon_{SR}^2$, $i = 1, 2, \cdots, N$, $\|\mathbf{e}_{RD}\|^2 \leq \epsilon_{RD}^2$ and $\|\mathbf{e}_{RE_m}\|^2 \leq \epsilon_{RE}^2$, for $m = 1, 2, \cdots, M$, where $\epsilon_{SD}^2, \epsilon_{SE}^2, \epsilon_{SR}^2, \epsilon_{RD}^2$ and ϵ_{RE}^2 are known. In case of AF, we assume that the estimates of $\mathbf{h}$ and $\mathbf{h}_m$ are available and the corresponding error vectors are as follows: $\mathbf{e} = \mathbf{h} - \hat{\mathbf{h}}$ and $\mathbf{e}_m = \mathbf{h}_m - \hat{\mathbf{h}}_m$, for $m = 1, 2, \cdots, M$. The error vectors are norm bounded, i.e., $\|\mathbf{e}\|^2 \leq \epsilon^2$ and $\|\mathbf{e}_m\|^2 \leq \epsilon_m^2$, for $m = 1, 2, \cdots, M$, where ϵ^2, ϵ_m^2 are known.

Our aim is to find optimal source power P_s, relay weights $\mathbf{w}$, and AN co-variance matrix $\mathbf{\Omega}$, subject to the worst case SINR constraints at the destination and eavesdroppers, i.e., we have to ensure that

$$\min(SINR_D) \geq \gamma_D \text{ and}$$
$$\max(SINR_{E_m}) \leq \gamma_{E_m} \text{ for } m = 1, 2, \cdots, M.$$

Define $\mathbf{\Phi} \triangleq \mathbf{w}\mathbf{w}^\dagger$. $\mathbf{\Phi}$ is an $N \times N$ complex hermitian positive semi-definite matrix (denoted by $\succeq 0$).

A. Amplify-and-forward scheme

Using (2),(3),(5),(6), the SINR expressions at the destination and the mth eavesdropper in terms of channel estimates and error vectors are

$$SINR_D = \frac{P_s|\hat{h}_{SD} + e_{SD}|^2}{\sigma_D^2} + \frac{tr(\mathbf{\Phi} P_s(\hat{\mathbf{h}} + \mathbf{e})(\hat{\mathbf{h}} + \mathbf{e})^\dagger)}{\sigma_R^2 tr(\mathbf{\Phi}\mathbf{U}) + \sigma_D^2 + tr(\mathbf{\Omega}\mathbf{B})},$$
$$SINR_{E_m} = \frac{P_s|\hat{h}_{SE_m} + e_{SE_m}|^2}{\sigma_{E_m}^2} + \frac{tr(\mathbf{\Phi} P_s(\hat{\mathbf{h}}_m + \mathbf{e}_m)(\hat{\mathbf{h}}_m + \mathbf{e}_m)^\dagger)}{\sigma_R^2 tr(\mathbf{\Phi}\mathbf{U}_m) + \sigma_{E_m}^2 + tr(\mathbf{\Omega}\mathbf{B}_m)}.$$

B. Decode-and-forward scheme

Using (1),(2),(3),(9),(10), the SNR expression at ith relay, the SINR expressions at the destination and the mth eavesdropper in terms of channel estimates and error vectors are

$$SNR_{R_i} = \frac{P_s|\hat{h}_{SR_i} + e_{SR_i}|^2}{\sigma_R^2},$$
$$SINR_D = \frac{P_s|\hat{h}_{SD} + e_{SD}|^2}{\sigma_D^2} + \frac{tr(\mathbf{\Phi}\mathbf{B})}{\sigma_D^2 + tr(\mathbf{\Omega}\mathbf{B})},$$
$$SINR_{E_m} = \frac{P_s|\hat{h}_{SE_m} + e_{SE_m}|^2}{\sigma_{E_m}^2} + \frac{tr(\mathbf{\Phi}\mathbf{B}_m)}{\sigma_{E_m}^2 + tr(\mathbf{\Omega}\mathbf{B}_m)}.$$

where $\mathbf{U} = diag(\hat{\mathbf{h}}_{RD} + \mathbf{e}_{RD})^* diag(\hat{\mathbf{h}}_{RD} + \mathbf{e}_{RD}), \mathbf{U}_m = diag(\hat{\mathbf{h}}_{RE_m} + \mathbf{e}_{RE_m})^* diag(\hat{\mathbf{h}}_{RE_m} + \mathbf{e}_{RE_m}), \mathbf{B} = (\hat{\mathbf{h}}_{RD} + \mathbf{e}_{RD})(\hat{\mathbf{h}}_{RD} + \mathbf{e}_{RD})^\dagger$ and $\mathbf{B}_m = (\hat{\mathbf{h}}_{RE_m} + \mathbf{e}_{RE_m})(\hat{\mathbf{h}}_{RE_m} + \mathbf{e}_{RE_m})^\dagger$.

IV. Beamforming and AN with SINR constraints

In this section, we present the beamformer design with minimum total transmit power subject to the worst case SINR constraints at the destination and eavesdroppers. By rank relaxation and using S-procedure, the optimization problems are solved using SDP tools.

A. Amplify-and-forward scheme

Here, we will find P_s, relay weights and AN required in the AF scheme to guarantee the worst case SINRs at the destination and eavesdroppers to be above and below certain set thresholds, respectively. The SINR thresholds at the destination and the mth eavesdropper are denoted by γ_D and γ_{E_m}, respectively. Without loss of generality, assume $\{\gamma_{E_m}\}_{m=1}^M = \gamma_E$. We write the worst case SINR constraints as follows:

$$\min_{e_{SD}} \frac{P_s|\hat{h}_{SD} + e_{SD}|^2}{\sigma_D^2} + \min_{\mathbf{e},\ \mathbf{e}_{RD}} \frac{tr(\mathbf{\Phi} P_s(\hat{\mathbf{h}} + \mathbf{e})(\hat{\mathbf{h}} + \mathbf{e})^\dagger)}{\sigma_R^2 tr(\mathbf{\Phi}\mathbf{U}) + \sigma_D^2 + tr(\mathbf{\Omega}\mathbf{B})} \geq \gamma_D,$$
$$\text{s.t } |e_{SD}|^2 \leq \epsilon_{SD}^2,\ \|\mathbf{e}\|^2 \leq \epsilon^2,\ \|\mathbf{e}_{RD}\|^2 \leq \epsilon_{RD}^2, \tag{12}$$

$$\max_{e_{SE_m}} \frac{P_s|\hat{h}_{SE_m} + e_{SE_m}|^2}{\sigma_E^2} + \max_{\mathbf{e}_m,\ \mathbf{e}_{RE_m}} \frac{tr(\mathbf{\Phi} P_s(\hat{\mathbf{h}}_m + \mathbf{e}_m)(\hat{\mathbf{h}}_m + \mathbf{e}_m)^\dagger)}{\sigma_R^2 tr(\mathbf{\Phi}\mathbf{U}_m) + \sigma_E^2 + tr(\mathbf{\Omega}\mathbf{B}_m)} \leq \gamma_E,$$
$$\text{s.t } |e_{SE_m}|^2 \leq \epsilon_{SE}^2,\ \|\mathbf{e}_m\|^2 \leq \epsilon_m^2,\ \|\mathbf{e}_{RE_m}\|^2 \leq \epsilon_{RE}^2. \tag{13}$$

First, we minimize the direct link SNR at the destination in (12), which is

$$\alpha = \min_{e_{SD}} \frac{P_s|\hat{h}_{SD} + e_{SD}|^2}{\sigma_D^2}\ ;\ \text{s.t } |e_{SD}|^2 \leq \epsilon_{SD}^2, \tag{14}$$
$$= \frac{P_s||\hat{h}_{SD}| - \epsilon_{SD}|^2}{\sigma_D^2}. \tag{15}$$

Having obtained α as mentioned above, we rewrite (12) in terms of α in the following form:

$$\min_{\mathbf{e},\ \mathbf{e}_{RD}} \frac{tr(\mathbf{\Phi} P_s(\hat{\mathbf{h}} + \mathbf{e})(\hat{\mathbf{h}} + \mathbf{e})^\dagger)}{\sigma_R^2 tr(\mathbf{\Phi}\mathbf{U}) + \sigma_D^2 + tr(\mathbf{\Omega}\mathbf{B})}) \geq (\gamma_D - \alpha),$$
$$\text{s.t } \|\mathbf{e}\|^2 \leq \epsilon^2,\ \|\mathbf{e}_{RD}\|^2 \leq \epsilon_{RD}^2,$$

which can be transformed as

$$\frac{s}{t} \geq (\gamma_D - \alpha), \tag{16}$$
$$\forall e \text{ s.t } \|\mathbf{e}\|^2 \leq \epsilon^2 \implies$$
$$tr(\mathbf{\Phi} P_s(\hat{\mathbf{h}} + \mathbf{e})(\hat{\mathbf{h}} + \mathbf{e})^\dagger) \geq s \geq 0, \tag{17}$$
$$\forall \mathbf{e}_{RD} \text{ s.t } \|\mathbf{e}_{RD}\|^2 \leq \epsilon_{RD}^2 \implies$$
$$\sigma_R^2 tr(\mathbf{\Phi}\mathbf{U}) + \sigma_D^2 + tr(\mathbf{\Omega}\mathbf{B}) \leq t. \tag{18}$$

Using S-procedure [10], we rewrite (17) and (18) in the following equivalent LMI's (Linear Matrix Inequality) form:

$$s \geq 0, \quad \lambda_D \geq 0,$$
$$\mathbf{J}_1 \triangleq \begin{bmatrix} \lambda_D I + P_s\mathbf{\Phi} & P_s\mathbf{\Phi}\hat{\mathbf{h}} \\ P_s\hat{\mathbf{h}}^\dagger\mathbf{\Phi} & -\lambda_D\epsilon^2 + \hat{\mathbf{h}}^\dagger\mathbf{\Phi} P_s\hat{\mathbf{h}} - s \end{bmatrix} \succeq 0, \tag{19}$$
$$\mu_D \geq 0, \quad \mathbf{J}_2 \triangleq$$
$$\begin{bmatrix} \mu_D I - \mathbf{A} & -\mathbf{A}\hat{\mathbf{h}}_{RD} \\ -\hat{\mathbf{h}}_{RD}^\dagger\mathbf{A} & -\mu_D\epsilon_{RD}^2 - \hat{\mathbf{h}}_{RD}^\dagger\mathbf{A}\hat{\mathbf{h}}_{RD} - \sigma_D^2 + t \end{bmatrix} \succeq 0, \tag{20}$$

where $\mathbf{A} = \sigma_R^2 diag(diag(\mathbf{\Phi})) + \mathbf{\Omega}$. We now maximize the direct link SNR at the mth eavesdropper in (13)

$$\beta_m = \max_{e_{SE_m}} \frac{P_s|\hat{h}_{SE_m} + e_{SE_m}|^2}{\sigma_{E_m}^2}\ ;\ \text{s.t } |e_{SE_m}|^2 \leq \epsilon_{SE}^2, \tag{21}$$
$$= \frac{P_s||\hat{h}_{SE_m}| + \epsilon_{SE}|^2}{\sigma_{E_m}^2}. \tag{22}$$

We rewrite (13) in terms of β_m as follows:

$$\max_{\mathbf{e}_m, \mathbf{e}_{RE_m}} \frac{tr(\mathbf{\Phi} P_s(\hat{\mathbf{h}}_m + \mathbf{e}_m)(\hat{\mathbf{h}}_m + \mathbf{e}_m)^\dagger)}{\sigma_R^2 tr(\mathbf{\Phi}\mathbf{U}_m) + \sigma_E^2 + tr(\mathbf{\Omega}\mathbf{B}_m)} \leq (\gamma_E - \beta_m),$$
$$\text{s.t } \|\mathbf{e}_m\|^2 \leq \epsilon_m^2,\ \|\mathbf{e}_{RE_m}\|^2 \leq \epsilon_{RE}^2,$$

which can be transformed as

$$\frac{s_m}{t_m} \leq (\gamma_E - \beta_m) \text{ for } m = 1, 2, ..M, \quad (23)$$

$$\forall \mathbf{e}_m \text{ s.t } \|\mathbf{e}_m\|^2 \leq \epsilon_m^2 \implies$$

$$tr(\mathbf{\Phi} P_s(\hat{\mathbf{h}}_m + \mathbf{e}_m)(\hat{\mathbf{h}}_m + \mathbf{e}_m)^\dagger) \leq s_m, \quad (24)$$

$$\forall \mathbf{e}_{RE_m} \text{ s.t } \|\mathbf{e}_{RE_m}\|^2 \leq \epsilon_{RE}^2 \implies$$

$$\sigma_R^2 tr(\mathbf{\Phi}\mathbf{U}_m) + \sigma_E^2 + tr(\mathbf{\Omega}\mathbf{B}_m) \geq t_m \geq 0. \quad (25)$$

Using S-procedure, we rewrite (24) and (25) in the following equivalent LMI's form, as

$$\lambda_{E_m} \geq 0, \quad \mathbf{L}_1^m \triangleq$$

$$\begin{bmatrix} \lambda_{E_m}\mathbf{I} - P_s\mathbf{\Phi} & -P_s\mathbf{\Phi}\hat{\mathbf{h}}_m \\ -P_s\hat{\mathbf{h}}_m^\dagger\mathbf{\Phi} & -\lambda_{E_m}\epsilon_m^2 - \hat{\mathbf{h}}_m^\dagger\mathbf{\Phi}P_s\hat{\mathbf{h}}_m + s_m \end{bmatrix} \succeq 0, \quad (26)$$

$$t_m \geq 0, \quad \mu_{E_m} \geq 0, \quad \mathbf{L}_2^m \triangleq$$

$$\begin{bmatrix} \mu_{E_m}\mathbf{I} + \mathbf{A} & \mathbf{A}\hat{\mathbf{h}}_{RE_m} \\ \hat{\mathbf{h}}_{RE_m}^\dagger\mathbf{A} & -\mu_{E_m}\epsilon_{RE}^2 + \hat{\mathbf{h}}_{RE_m}^\dagger\mathbf{A}\hat{\mathbf{h}}_{RE_m} + \sigma_E^2 - t_m \end{bmatrix} \succeq 0. \quad (27)$$

From (7), the required worst case minimum power would be

$$\min_{\mathbf{\Phi},\, \mathbf{\Omega}} \max_{\mathbf{e}_{SR}} (tr(\mathbf{\Phi}(P_s diag(\hat{\mathbf{h}}_{SR} + \mathbf{e}_{SR}) diag(\hat{\mathbf{h}}_{SR} + \mathbf{e}_{SR})^* + \sigma_R^2\mathbf{I}_n)) + P_s + tr(\mathbf{\Omega})).$$

By doing the inner most maximization w.r.t e_{SR_i}, the worst case total power can be written as

$$\min_{\mathbf{\Phi},\, \mathbf{\Omega}} P_s + tr(\mathbf{\Phi}(P_s diag(\mathbf{v})) + \sigma_R^2\mathbf{I}_n)) + tr(\mathbf{\Omega}), \quad (28)$$

where $\mathbf{v} = [v_1, v_2, \cdots, v_N]^T$ and for $i = 1, 2, \cdots, N$,

$$v_i = \max_{e_{SR_i}} |\hat{h}_{SR_i} + e_{SR_i}|^2; \text{ s.t } |e_{SR_i}|^2 \leq \epsilon_{SR}^2, \quad = ||\hat{h}_{SR_i}| + \epsilon_{SR}|^2.$$

Using (16), (19), (20), (23), (26), (27) as constraints and (28) as the objective function, the optimization problem for minimizing AF total transmit power is

$$\begin{aligned} \min_{\substack{P_s,\, \mathbf{\Phi},\, \mathbf{\Omega},\, \lambda_D,\, \mu_D, \\ s,\, t,\, \lambda_{E_m},\, \mu_{E_m}, \\ s_m,\, t_m}} \quad & P_s + tr(\mathbf{\Phi}(P_s diag(\mathbf{v})) + \sigma_R^2\mathbf{I}_n)) + tr(\mathbf{\Omega}) \\ \text{s.t } & \mathbf{J}_1,\ \mathbf{J}_2 \succeq 0,\ s \geq 0, \lambda_D \geq 0, \mu_D \geq 0, \\ & s \geq t(\gamma_D - \alpha), \\ & \text{for } m = 1, 2, ..M,\ s_m \leq t_m(\gamma_E - \beta_m), \\ & \mathbf{L}_1^m,\ \mathbf{L}_2^m \succeq 0,\ t_m \geq 0,\ \lambda_{E_m} \geq 0,\ \mu_{E_m} \geq 0, \\ & P_s \geq 0,\ \mathbf{\Phi} \succeq 0,\ rank(\mathbf{\Phi}) = 1,\ \mathbf{\Omega} \succeq 0. \end{aligned} \quad (29)$$

This is a non-convex optimization problem. To make this problem a convex SDP, we

1) relax the non-convex rank constraint, i.e., rank($\mathbf{\Phi}$) = 1, and
2) fix P_s and solve the above problem. Choose different P_s varied with a chosen step size for the considered source power constraint $P_s \leq P_o$. Pick the solution with least total power solved over different P_s.

Our goal is to find the beamforming vector $\mathbf{w}$ and the AN covariance matrix $\mathbf{\Omega}$. The optimum solution of the SDP relaxation problems are matrices, denoted by $\mathbf{\Phi}'$, $\mathbf{\Omega}'$. Numerically $\mathbf{\Phi}'$ is seen to be a rank-1 matrix. We choose $\mathbf{w}$ along the principal eigen vector of $\mathbf{\Phi}'$. The beamformer design with minimum transmit power without AN is a special case of (29) with $\mathbf{\Omega} = 0$. This completes the beamformer design for the AF scheme.

B. Decode-and-forward scheme

Here, we present the design to find the relay weights, source power and AN required in the DF scheme which minimizes the worst case total transmit power. The required worst case SNR constraint at ith relay, worst case SINR constraints at the destination and mth eavesdropper are

$$\min_{e_{SR_i}} \frac{P_s|\hat{h}_{SR_i} + e_{SR_i}|^2}{\sigma_R^2} \geq \gamma_R, \text{ s.t } |\mathbf{e}_{SR_i}|^2 \leq \epsilon_{SR}^2, \quad (30)$$

$$\implies \frac{P_s||\hat{h}_{SR_i}| - \epsilon_{SR}|^2}{\sigma_R^2} \geq \gamma_R, \quad (31)$$

$$\min_{e_{SD}} \frac{P_s|\hat{h}_{SD} + e_{SD}|^2}{\sigma_D^2} + \min_{\mathbf{e}_{RD}} \frac{tr(\mathbf{\Phi}\mathbf{B})}{\sigma_D^2 + tr(\mathbf{\Omega}\mathbf{B})} \geq \gamma_D,$$

$$\text{s.t } |e_{SD}|^2 \leq \epsilon_{SD}^2, \|\mathbf{e}_{RD}\|^2 \leq \epsilon_{RD}^2, \quad (32)$$

$$\max_{e_{SE_m}} \frac{P_s|\hat{h}_{SE_m} + e_{SE_m}|^2}{\sigma_{E_m}^2} + \max_{\mathbf{e}_{RE_m}} \frac{tr(\mathbf{\Phi}\mathbf{B}_m)}{\sigma_{E_m}^2 + tr(\mathbf{\Omega}\mathbf{B}_m)}$$

$$\leq \gamma_E, \quad \text{s.t } |e_{SE_m}|^2 \leq \epsilon_{SE}^2, \|\mathbf{e}_{RE}\|^2 \leq \epsilon_{RE}^2. \quad (33)$$

Using (15), we rewrite (32) in terms of α as

$$\min_{\mathbf{e}_{RD}} \frac{tr(\mathbf{\Phi}\mathbf{B})}{\sigma_D^2 + tr(\mathbf{\Omega}\mathbf{B})} \geq (\gamma_D - \alpha), \text{ s.t } \|\mathbf{e}_{RD}\|^2 \leq \epsilon_{RD}^2,$$

which can be transformed as

$$\frac{s}{t} \geq (\gamma_D - \alpha), \quad (34)$$

$$\forall \mathbf{e}_{RD} \text{ s.t } \|\mathbf{e}_{RD}\|^2 \leq \epsilon_{RD}^2 \implies$$

$$(\hat{\mathbf{h}}_{RD} + \mathbf{e}_{RD})^\dagger\mathbf{\Phi}(\hat{\mathbf{h}}_{RD} + \mathbf{e}_{RD}) \geq s \geq 0, \quad (35)$$

$$\forall \mathbf{e}_{RD} \text{ s.t } \|\mathbf{e}_{RD}\|^2 \leq \epsilon_{RD}^2 \implies$$

$$\sigma_D^2 + (\hat{\mathbf{h}}_{RD} + \mathbf{e}_{RD})^\dagger\mathbf{\Omega}(\hat{\mathbf{h}}_{RD} + \mathbf{e}_{RD}) \leq t. \quad (36)$$

Using S-procedure, we rewrite (35) and (36) in the following equivalent LMI's:

$$s \geq 0, \quad \lambda_D \geq 0,$$

$$\mathbf{J}_1 \triangleq \begin{bmatrix} \lambda_D\mathbf{I} + \mathbf{\Phi} & \mathbf{\Phi}\hat{\mathbf{h}}_{RD} \\ \hat{\mathbf{h}}_{RD}^\dagger\mathbf{\Phi} & -\lambda_D\epsilon_{RD}^2 + \hat{\mathbf{h}}_{RD}^\dagger\mathbf{\Phi}\hat{\mathbf{h}}_{RD} - s \end{bmatrix} \succeq 0, \quad (37)$$

$$\mu_D \geq 0, \quad \mathbf{J}_2 \triangleq$$

$$\begin{bmatrix} \mu_D\mathbf{I} - \mathbf{\Omega} & -\mathbf{\Omega}\hat{\mathbf{h}}_{RD} \\ -\hat{\mathbf{h}}_{RD}^\dagger\mathbf{\Omega} & -\mu_D\epsilon_{RD}^2 - \hat{\mathbf{h}}_{RD}^\dagger\mathbf{\Omega}\hat{\mathbf{h}}_{RD} - \sigma_D^2 + t \end{bmatrix} \succeq 0. \quad (38)$$

Using (22), we rewrite (33) as

$$\max_{\mathbf{e}_{RE_m}} \frac{tr(\mathbf{\Phi}\mathbf{B}_m)}{\sigma_{E_m}^2 + tr(\mathbf{\Omega}\mathbf{B}_m)} \leq (\gamma_E - \beta_m), \text{ s.t } \|\mathbf{e}_{RE}\|^2 \leq \epsilon_{RE}^2,$$

which can be transformed as

$$\frac{s_m}{t_m} \leq (\gamma_E - \beta_m) \text{ for } m = 1, 2, ..M, \quad (39)$$

$$\forall \mathbf{e}_{RE_m} \text{ s.t } \|\mathbf{e}_{RE_m}\|^2 \leq \epsilon_{RE}^2 \implies$$

$$(\hat{\mathbf{h}}_{RE_m} + \mathbf{e}_{RE_m})^\dagger\mathbf{\Phi}(\hat{\mathbf{h}}_{RE_m} + \mathbf{e}_{RE_m}) \leq s_m, \quad (40)$$

$$\forall \mathbf{e}_{RE_m} \text{ s.t } \|\mathbf{e}_{RE_m}\|^2 \leq \epsilon_{RE}^2 \implies$$

$$\sigma_{E_m}^2 + (\hat{\mathbf{h}}_{RE_m} + \mathbf{e}_{RE_m})^\dagger\mathbf{\Omega}(\hat{\mathbf{h}}_{RE_m} + \mathbf{e}_{RE_m}) \geq t_m \geq 0. \quad (41)$$

Using S-procedure, we rewrite (40) and (41) in the following equivalent LMI's form:

$$\lambda_{E_m} \geq 0, \quad \mathbf{L}_1^m \triangleq \begin{bmatrix} \lambda_{E_m}\mathbf{I} - \mathbf{\Phi} & -\mathbf{\Phi}\hat{\mathbf{h}}_{RE_m} \\ -\hat{\mathbf{h}}_{RE_m}^{\dagger}\mathbf{\Phi} & -\lambda_{E_m}\epsilon_{RE}^2 - \hat{\mathbf{h}}_{RE_m}^{\dagger}\mathbf{\Phi}\hat{\mathbf{h}}_{RE_m} + s_m \end{bmatrix} \succeq 0, \qquad (42)$$

$$t_m \geq 0, \quad \mu_{E_m} \geq 0, \quad \mathbf{L}_2^m \triangleq \begin{bmatrix} \mu_{E_m}\mathbf{I} + \mathbf{\Omega} & \mathbf{\Omega}\hat{\mathbf{h}}_{RE_m} \\ \hat{\mathbf{h}}_{RE_m}^{\dagger}\mathbf{\Omega} & -\mu_{E_m}\epsilon_{RE_m}^2 + \hat{\mathbf{h}}_{RE_m}^{\dagger}\mathbf{\Omega}\hat{\mathbf{h}}_{RE_m} + \sigma_E^2 - t_m \end{bmatrix} \succeq 0. \qquad (43)$$

Using (11) as the objective function, (34), (37), (38), (39), (42), (43) as constraints, the optimization problem for minimizing DF total transmit power is

$$\begin{aligned} \min_{P_s, \mathbf{\Phi}, \mathbf{\Omega}, \lambda_D, \mu_D, s, t, \lambda_{E_m}, \mu_{E_m}, s_m, t_m} \quad & P_s + tr(\mathbf{\Phi}) + tr(\mathbf{\Omega}) \\ \text{s.t} \quad P_s||\hat{h}_{SR_i}| - \epsilon_{SR}|^2 \geq \sigma_R^2\gamma_R, \quad & \text{for} \quad i = 1, 2, ..k, \\ \mathbf{J}_1, \ \mathbf{J}_2 \succeq 0, \ s \geq 0, \lambda_D \geq 0, \ & \mu_D \geq 0, \\ & s \geq t(\gamma_D - \alpha), \\ \text{for} \quad m = 1, 2, ..M, \quad & s_m \leq t_m(\gamma_E - \beta_m), \\ \mathbf{L}_1^m, \ \mathbf{L}_2^m \succeq 0, \ t_m \geq 0, \ \lambda_{E_m} \geq 0, \ & \mu_{E_m} \geq 0, \\ P_s \geq 0, \ \mathbf{\Phi} \succeq 0, \ rank(\mathbf{\Phi}) = 1, \ & \mathbf{\Omega} \succeq 0. \end{aligned} \qquad (44)$$

As in the case of AF, we drop the constraint rank ($\mathbf{\Phi}$) = 1, fix P_s and solve the problem. We choose different P_s varied with a chosen step size for the source power constraint $P_s \leq P_o$ and pick that source power for different P_s used which results in least transmit power, i.e., the objective function. By using semi-definite tool, we find the optimal beamformer vector $\mathbf{w}$, source power P_s, and AN covariance matrix $\mathbf{\Omega}$. The beamformer design without AN is a special case of (44) with $\mathbf{\Omega} = 0$.

V. Results and Discussions

We evaluated the beamforming weights and AN covariance matrices for AF and DF schemes. We obtained the average total powers needed to meet the worst case SINR guarantees with and without AN. We also obtained the feasibility percentage as another performance measure. We compare the numerical results with imperfect CSI with those with perfect CSI. All the channel gains except the direct links are assumed to be $\mathcal{CN}(0, 1)$. The direct link channel gains from source to destination and source to eavesdroppers are assumed to be $\mathcal{CN}(0, 0.01)$. We have considered $N = 3$ relays and $M = 2$ eavesdroppers. Thermal noise variance at all the eavesdroppers is assumed to be same, i.e., $(\sigma_{E_m}^2)_{m=1}^M = \sigma_E^2$. The thermal noise variance at the destination and the relays is considered as $\sigma_D^2 = \sigma_R^2 = 0.1$. We consider the source power constraint $P_s \leq P_o$ = 3 dB. We solved the optimization problem over different fixed P_s varied with a step size of 0.2. The SDP problems in (29) and (44) are solved by using SeDuMi [11].

The average total power versus $\frac{1}{\sigma_E^2}$ performance plots for AF and DF are plotted in Fig. 2 and Fig. 4, respectively. These have been averaged for 100 channel realizations. When only channel estimates are available with norm bounded errors, we don't know the actual error vector. In the case of imperfect CSI, as we design for worst case scenarios, the worst case total transmit power required would be higher compared to the perfect CSI case. We also numerically observe that the average total transmit powers for imperfect CSI in Fig. 2 and Fig. 4 are more than those required in the perfect CSI case. From Fig. 2 and Fig. 4, we observe that the transmit power needed to meet the SINR guarantees with AN is less compared to the transmit power needed without AN for both perfect and imperfect CSI cases.

The solution feasibility percentage versus $\frac{1}{\sigma_E^2}$ plots averaged for 1000 channel realizations for AF and DF are shown in Fig. 3 and Fig. 5, respectively. The considered optimization problems without AN are a subset of optimization problems with AN. So, the solution feasibility with AN will be improved as we have additional freedom of AN. When checked over all possible error vectors within the norm, the solution feasibility with imperfect CSI case is less compared to perfect CSI case since the channel will be discarded even if the optimization problem fails for one possible error vector. Thus the feasibility performance is degraded with imperfect CSI compared to perfect CSI.

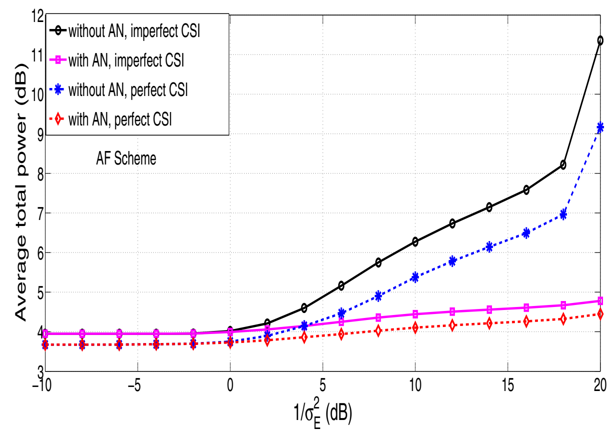

Fig. 2. Average total power in AF scheme with 3 relays, 2 eavesdroppers, $\gamma_D = 10$ dB, and $\gamma_E = 3$ dB.

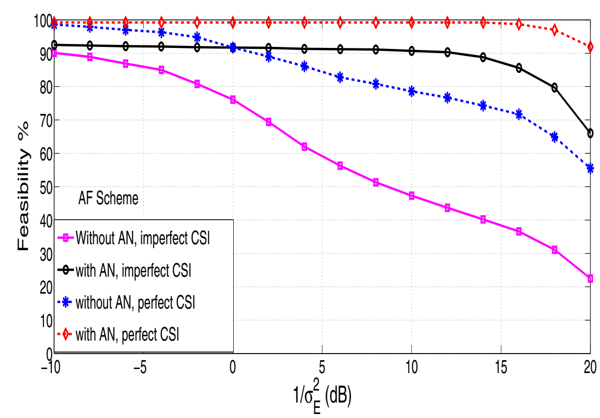

Fig. 3. Feasibility percentage in AF scheme with 3 relays, 2 eavesdroppers, $\gamma_D = 10$ dB, and $\gamma_E = 3$ dB.

A. Discussions on AF performance

The error component parameters used for AF simulations are $\epsilon_{RD}^2 = \epsilon_{RE}^2 = \epsilon_h^2 = \epsilon_{h1}^2 = \epsilon_{h2}^2 = 0.01$, $\epsilon_{SR}^2 = 0.001$ and $\epsilon_{SD}^2 = \epsilon_{SE}^2 = 0.0001$. In Fig. 2, for $\frac{1}{\sigma_E^2} \leq$ -2 dB, the average total power required is flat as the constraint $SINR_E \leq \gamma_E$ becomes insignificant. The meaningful constraint for the optimization problem is only $SINR_D$ constraint and so the transmit power becomes independent of σ_E^2. With AN, power increase for decreasing σ_E^2 is small due to the domination of AN term in the denominator of the SINR expressions. When $\frac{1}{\sigma_E^2}$ becomes $\geq$ 15 dB, direct link SNR contribution increases as σ_E^2 reduces. Due to direct links, the SINR contribution to be done by the relays to guarantee the SINRs reduces. This reflects as beamforming design at relays with reduced SINR thresholds γ_D and γ_E. If γ_E is decreased, the minimization of transmit power becomes a more constrained problem and so the minimum power increases. For $\frac{1}{\sigma_E^2}$= 20 dB with imperfect CSI, we see that the total power with AN is around 6.5 dB less compared to without AN case. In Fig. 3, the solution feasibility with AN is around 92% initially and does not vary much due to AN term dominating the variation of σ_E^2. But when $\frac{1}{\sigma_E^2}$ exceeds 10 dB, feasibility drops to 65% due to direct links contributing considerable SNR at the eavesdroppers. Whereas, without AN, feasibility % reduces from 90% to 22%.

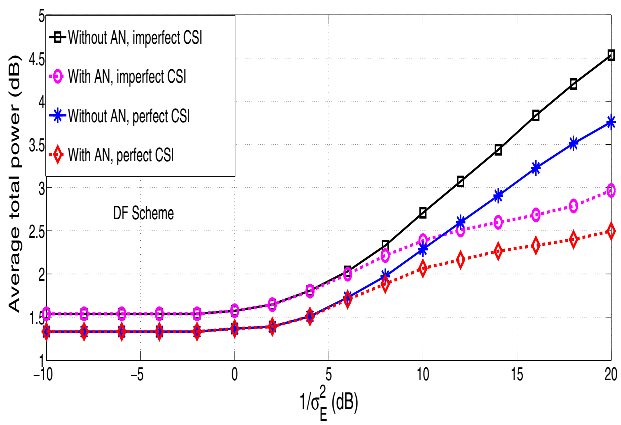

Fig. 4. Average total power in DF scheme with 3 relays, 2 eavesdroppers, $\gamma_R = 10$ dB, $\gamma_D = 10$ dB, and $\gamma_E = 3$ dB.

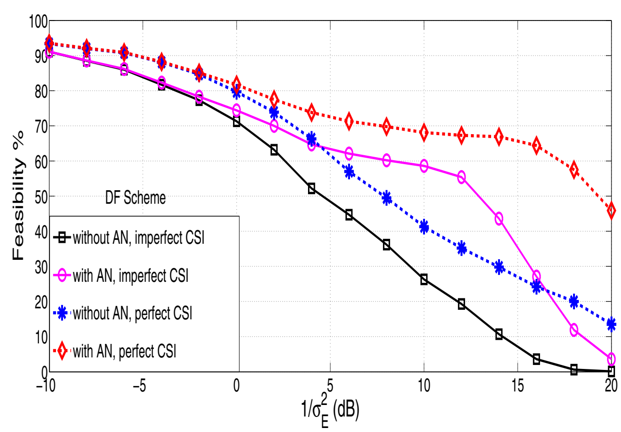

Fig. 5. Feasibility percentage in DF scheme with 3 relays, 2 eavesdroppers, $\gamma_R = 10$ dB, $\gamma_D = 10$ dB, and $\gamma_E = 3$ dB.

B. Discussion on DF performance

For the average total power of DF scheme in Fig. 4, following error component parameters are used: $\epsilon_{RD}^2 = \epsilon_{RE}^2 = \epsilon_{SR}^2 = 0.001$ and $\epsilon_{SD}^2 = \epsilon_{SE}^2 = 0.0001$. Without AN, in the imperfect CSI case, the total power grows from 1.5 dB to around 4.5 dB. When AN is injected, the power plot grows slowly as it is not dominated by the low values of σ_E^2 due to the additional AN term in the denominator of the $SINR_E$ expression. For $\frac{1}{\sigma_E^2} \geq$ 15 dB, σ_E^2 in the denominator of direct link term dominates, and so power increases even when AN is injected. The above explained behavior is seen in the average power plots in Fig. 4. For the solution feasibility plots of Fig. 5, error component parameters are same as in Fig. 4. We see that solution feasibility with AN drops from 90% to 65% and then decreases slowly to 55% due to AN term dominating the variation of σ_E^2, later reduces to 4% due to increase in direct path SNR contribution for decreasing σ_E^2. For $\frac{1}{\sigma_E^2} \geq$= 12 dB, feasibility % drops faster due to imperfect CSI. We can observe this by comparing with the perfect CSI plot. Whereas, the solution feasibility without AN drops from 90% to 1% for decreasing σ_E^2. We see that the feasibility % improves with the addition of AN.

VI. Conclusions

We investigated optimum power allocation to beamformer and artificial noise (AN) for secrecy in AF and DF relaying with imperfect CSI, by considering a norm bounded CSI error model. We designed the beamformers and AN with minimum transmit power subject to worst SINR constraints at the destination and eavesdroppers. The optimization problems were solved as semi-definite programming problems by rank relaxation and S-procedure. Numerical results showed that injection of AN at the relays significantly reduces the average total transmit power required to meet the SINR constraints, and also improves the solution feasibility of the optimization problems. We further note that the proposed problem formulation and solution approach with imperfect CSI and without AN can be relevant in cognitive radio scenarios where interference to users needs to be constrained.

References

[1] A. D. Wyner, "The wiretap channel," *Bell System Tech. Jl.*, vol. 54, no. 8, pp. 1355-1387, Jan. 1975.

[2] S. K. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inform. Theory*, vol. 24, pp. 451-456, Jul. 1978.

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

[4] A. Khisti and G. W. Wornell, "Secure communication with multiple antennas: The MISOME wiretap channel," *IEEE Trans. Inform. Theory*, vol. 56, no. 7, pp. 3088-3104, Jul. 2010.

[5] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, pp. 2180-2189, Jun. 2008.

[6] J. Huang and A. L. Swindlehurst, "Robust secure transmission in MISO channels based on worst-case optimization," *IEEE Trans. Signal Process.*, vol. 60, no. 4, pp. 1696-1707, Apr. 2011.

[7] L. Dong, Z. Han, A. Petropulu, and H. V. Poor, "Secure wireless communications via cooperation," *Proc. Allerton Conf. Commun., Control, Computing*, pp. 1132-1138, Oct. 2008.

[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, J. Li, K.-K. Wong, A. P. Petropulu, and B. Ottersten, "Using simple relays to improve physical-layer security," *Proc. IEEE ICCC'2012: Signal Proc. for Commun.*, pp. 377-381, Aug. 2012.

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

[11] J. Strum, "Using SeDuMi 1.02: A MATLAB toolbox for optimization over symmetric cones," *Opt. Methods and Software*, vol. 11-12, pp. 625-653, 1999.