Cooperative Precoding and Artificial Noise Design for Security Over Interference Channels

Ayça Özçelikkale and Tolga M. Duman

***Abstract*—We focus on linear precoding strategies as a physical layer technique for providing security in Gaussian interference channels. We consider an artificial noise aided scheme where transmitters may broadcast noise in addition to data in order to confuse eavesdroppers. We formulate the problem of minimizing the total mean-square error at the legitimate receivers while keeping the error values at the eavesdroppers above target levels. This set-up leads to a non-convex problem formulation. Hence, we propose a coordinate block descent technique based on a tight semi-definite relaxation and design linear precoders as well as spatial distribution of the artificial noise. Our results illustrate that artificial noise can provide significant performance gains especially when the secrecy levels required at the eavesdroppers are demanding.**

***Index Terms*—Beamforming, multi-user, secrecy.**

I. Introduction

SECURE transmission in the presence of eavesdroppers is a problem of central importance in wireless communications. In recent years, physical layer techniques which typically exploit the channel conditions to provide secrecy have become increasing popular. Here, we focus on Gaussian interference channels, which form a particularly important and relevant setting in wireless media [1]–[4].

Various aspects of secure communications over interference channels have been studied from a rate perspective [1]–[5]. Although rate as a performance metric provides important insights into fundamental limits for secure communications, it should be complemented with low-complexity approaches in order to obtain practical secure systems. With this motivation, quality-of-service (QoS) framework which adopts signal-to-noise ratio (SNR) or mean-square error based metrics as performance criteria has recently been used to improve the security performance of communication systems [6]–[13].

In this regard, we adopt a minimum mean-square error (MMSE) based framework similar to [8]–[13]. Characterization of optimal precoders are provided for a point-to-point (P2P) setting for parallel degraded Gaussian channels in [8] and for general degraded Gaussian channels in [9]. General case of Gaussian multiple-input multiple-output (MIMO) P2P channels where the legitimate receiver uses a linear zero-forcing (ZF) filter is considered in [10]. An artificial noise (AN) aided MMSE scheme without explicit performance constraints for eavesdroppers is investigated in [11]. Design of artificial noise that lies in the null space of legitimate receivers' channels is considered for multi-user settings in [12], [13].

We consider the Gaussian interference channel scenario, and formulate the problem of minimizing the total weighted MMSE at the legitimate receivers while keeping the MMSE at the eavesdroppers above target levels. Transmitters also utilize artificial noise transmission in addition to linear precoding. We focus on the scenario with MIMO legitimate receiver channels and multiple-input single-output (MISO) eavesdropper channels. This set-up, in general, leads to a non-convex problem formulation. Utilizing a semi-definite relaxation, we propose a block coordinate descent approach with a convergence guarantee. Our results illustrate that adopting an artificial noise aided scheme is particularly important when the secrecy levels desired at the eavesdroppers are demanding.

The rest of the letter is organized as follows. The system model is given in Section II. The linear precoder and artificial noise design problem is formulated in Section III. In Section IV, the proposed approaches are presented. The performance of the proposed solutions are illustrated in Section V. We conclude the letter in Section VI.

Notation: Uppercase and lowercase letters denote matrices, and column/row vectors respectively. The complex conjugate transpose of a matrix $\mathbf{A}$ is denoted by $\mathbf{A}^\dagger$. The ith row, jth column element of a matrix $\mathbf{A}$ is denoted as $[\mathbf{A}]_{ij}$. Positive semi-definite ordering is denoted by $\succeq$. An optimal value of an optimization variable $\mathbf{A}$ is denoted by $\mathbf{A}^*$.

II. System Model

A. Interference Channel

The multi-antenna transmitter $i(\mathrm{T}_i)$ sends information to the multi-antenna legitimate receiver $i(\mathrm{LR}_i)$, $i = 1, 2$. This communication is eavesdropped through a MISO channel by the eavesdropper receivers (ERs) whose aim is to reconstruct the message of T_i's. The signals received by LR_i and ER_i can be represented as follows:

$$\mathbf{y}_i^L = \mathbf{H}_{i1}^L \mathbf{x}_1 + \mathbf{H}_{i2}^L \mathbf{x}_2 + \mathbf{w}_i^L, \quad (1)$$

$$y_i^E = \mathbf{h}_{i1}^E \mathbf{x}_1 + \mathbf{h}_{i2}^E \mathbf{x}_2 + w_i^E, \quad (2)$$

where $\mathbf{H}_{ik}^L \in \mathbb{C}^{n_r \times n_t}$ and $\mathbf{h}_{ik}^E \in \mathbb{C}^{1 \times n_t}$ represent the channel gains from the transmitter k to the LR_i and to the ER_i, respectively $i, k = 1, 2$. All channel gains are fixed throughout the transmission. Zero-mean complex proper Gaussian $\mathbf{w}_i^L \in$

Manuscript received July 15, 2015; accepted August 10, 2015. Date of publication August 24, 2015; date of current version September 01, 2015. This work was supported in part by TUBITAK 1001 Project 113E223. A. Özçelikkale acknowledges the support of EU Marie Skłodowska-Curie Fellowship. The associate editor coordinating the review of this manuscript and approving it for publication was Prof. Jiaheng Wang.

A. Özçelikkale is with the Department of Signals and Systems, Chalmers University of Technology, SE-41296 Gothenburg, Sweden (e-mail: ayca.ozcelikkale@chalmers.se).

T. M. Duman is with the Department of Electrical and Electronics Engineering, Bilkent University, TR-06800 Ankara, Turkey (e-mail: duman@ee.bilkent.edu.tr).

Digital Object Identifier 10.1109/LSP.2015.2472275

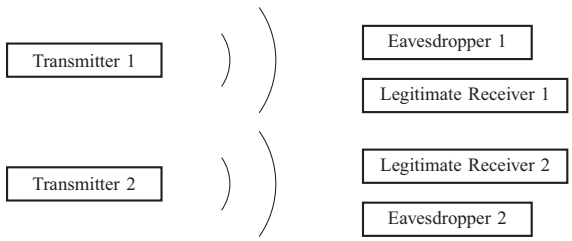

Fig. 1. Interference channel with eavesdroppers.

$\mathbb{C}^{n_r\times 1} \sim \mathcal{CN}(\mathbf{0}, \mathbf{K}_{\mathbf{w}_i^L})$, $\mathbf{K}_{\mathbf{w}_i^L} = E[\mathbf{w}_i^L \mathbf{w}_i^{L\dagger}] = \sigma^2_{w,L,i}\mathbf{I}$, $\sigma^2_{w,L,i} > 0$ and $w_i^E \in \mathbb{C}^{1\times 1} \sim \mathcal{CN}(0, \sigma^2_{w,E,i})$, denote the noise at LRs' and ERs' channels, respectively.

The channel inputs $\mathbf{x}_i$'s are formed as follows

$$\mathbf{x}_i = \mathbf{A}_i\mathbf{s}_i + \mathbf{v}_i, \tag{3}$$

where the zero-mean complex proper Gaussian $\mathbf{s}_i \in \mathbb{C}^n$, $\mathbf{s}_i \sim \mathcal{CN}(\mathbf{0}, \mathbf{I})$, denotes the data and $\mathbf{A}_i \in \mathbb{C}^{n_t\times n}$ denotes the precoding matrix at the ith transmitter. The zero-mean complex proper Gaussian $\mathbf{v}_i \in \mathbb{C}^{n_t}$, $\mathbf{v}_i \sim \mathcal{CN}(\mathbf{0}, \mathbf{K}_{\mathbf{v}_i})$ with $\mathbf{K}_{\mathbf{v}_i} = \mathrm{E}[\mathbf{v}_i\mathbf{v}_i^\dagger]$ denotes the artificial noise transmitter i broadcasts with the aim of obtaining better secrecy levels (higher error values) at the eavesdroppers. All signals, $\mathbf{s}_i$, $\mathbf{v}_i$, $\mathbf{w}_i^L$ and w_i^E, $i = 1, 2$, are assumed to be statistically independent. Hence we have $\mathbf{K}_{\mathbf{x}_i} = \mathrm{E}[\mathbf{x}_i\mathbf{x}_i^\dagger] = \mathbf{A}_i\mathbf{A}_i^\dagger + \mathbf{K}_{\mathbf{v}_i}$.

We adopt the following short-hand notations: $\bar{\mathbf{A}} = (\mathbf{A}_1, \mathbf{A}_2)$, $\bar{\mathbf{K}}_{\mathbf{v}} = (\mathbf{K}_{\mathbf{v}_1}, \mathbf{K}_{\mathbf{v}_2})$. The conditions $\mathbf{K}_{\mathbf{v}_1} \succeq 0, \mathbf{K}_{\mathbf{v}_2} \succeq 0$ are denoted by $\bar{\mathbf{K}}_{\mathbf{v}} \succeq 0$.

B. MMSE Estimation at the Legitimate Receivers

The designated legitimate receiver for transmitter i is denoted by LR_i. Hence upon receiving $\mathbf{y}_i^L$, LR_i forms the MMSE estimate of $\mathbf{s}_i$ as follows [14, ch. 2],

$$\mathrm{E}[\mathbf{s}_i|\mathbf{y}_i^L] = \mathbf{K}_{\mathbf{s}_i\mathbf{y}_i^L}\mathbf{K}^{-1}_{\mathbf{y}_i^L}\mathbf{y}_i^L, \tag{4}$$

where $\mathbf{K}_{\mathbf{s}_i\mathbf{y}_i^L} = \mathrm{E}[\mathbf{s}_i\mathbf{y}_i^{L\dagger}] = \mathbf{K}_{\mathbf{s}_i}\mathbf{A}_i^\dagger\mathbf{H}_{ii}^{L\dagger}$ and

$$\mathbf{K}_{\mathbf{y}_i^L} = \mathrm{E}[\mathbf{y}_i^L\mathbf{y}_i^{L\dagger}] = \mathbf{H}_{ii}^L\mathbf{K}_{\mathbf{x}_i}\mathbf{H}_{ii}^{L\dagger} + \mathbf{H}_{ij}^L\mathbf{K}_{\mathbf{x}_j}\mathbf{H}_{ij}^{L\dagger} + \sigma^2_{w,L,i}\mathbf{I},$$

where $i, j = 1, 2$, $i \neq j$. Here $\mathbf{K}_{y_i}^{-1}$ exists, since $\mathbf{K}_{y_i} \succ 0$ with $\sigma^2_{w,L,i}\mathbf{I} \succ 0$. The MMSE at LR_i can be expressed as follows

$$\begin{aligned}\varepsilon_{LR_i}(\bar{\mathbf{A}}, \bar{\mathbf{K}}_{\mathbf{v}}) &= \mathrm{E}[\|\mathbf{s}_i - \mathrm{E}[\mathbf{s}_i|\mathbf{y}_i^L]\|^2] \\ &= \mathrm{tr}[\mathbf{K}_{\mathbf{s}_i} - \mathbf{K}_{\mathbf{s}_i\mathbf{y}_i^L}\mathbf{K}^{-1}_{\mathbf{y}_i^L}\mathbf{K}^\dagger_{\mathbf{s}_i\mathbf{y}_i^L}] \\ &= n - \mathrm{tr}[\mathbf{A}_i^\dagger\mathbf{H}_{ii}^{L\dagger}\mathbf{K}^{-1}_{\mathbf{y}_i^L}\mathbf{H}_{ii}^L\mathbf{A}_i]. \end{aligned} \tag{5}$$

C. Secrecy Constraints at the Eavesdroppers

Eavesdroppers are interested in the data transmitted by both transmitters. They employ MMSE estimation, hence the estimate of $\mathbf{s}_i$ at ER_k can be expressed as

$$\mathrm{E}[\mathbf{s}_i|y_k^E] = \mathbf{K}_{\mathbf{s}_i y_k^E}K^{-1}_{y_k^E}y_k^E, \tag{6}$$

where $K_{y_k^E} = \sigma^2_{y_k^E} = \mathrm{E}[y_k^E y_k^{E\dagger}]$. Under the Gaussian signalling assumptions, MMSE estimation is the optimum strategy that can be adopted by the ERs for the mean-square error performance criterion. We also note that the mean-square error based filters provide a reasonably accurate alternative to maximum likelihood (ML) decoding for preprocessing of coded data symbols [15]. Since it is difficult to provide a comprehensive analysis of practical bit error performance in security scenarios, here we adopt mean-square error estimation as a practical measure. Similar SNR or MMSE based approaches have been adopted for a number of security scenarios; see, for instance, [6]–[13].

The mean-square error at ER_k for estimating $\mathbf{s}_i$ can be expressed as follows

$$\begin{aligned}\varepsilon^i_{ER_k}(\bar{\mathbf{A}}, \bar{\mathbf{K}}_{\mathbf{v}}) &= \mathrm{E}[\|\mathbf{s}_i - \mathrm{E}[\mathbf{s}_i|y_k^E]\|^2] \\ &= n - \frac{\mathbf{h}_{ki}^E\mathbf{A}_i\mathbf{A}_i^\dagger\mathbf{h}_{ki}^{E\dagger}}{\mathbf{h}_{ki}^E\mathbf{K}_{\mathbf{x}_i}\mathbf{h}_{ki}^{E\dagger} + \mathbf{h}_{kj}^E\mathbf{K}_{\mathbf{x}_j}\mathbf{h}_{kj}^{E\dagger} + \sigma^2_{w,E,i}},\end{aligned}$$

where $i, j, k = 1, 2$, $i \neq j$.

We consider the following secrecy (security) requirements that aim to keep the MMSE at the ERs above given levels

$$\varepsilon^i_{ER_k}(\bar{\mathbf{A}}, \bar{\mathbf{K}}_{\mathbf{v}}) \geq \gamma_{ki}, \quad i, k = 1, 2. \tag{7}$$

We note that the region of interest for γ_{ki} is $\gamma_{ki} \in [n-1, n]$ where $[n-1, n]$ is the range of admissible values for the MMSE over a MISO channel. (The lower bound $n-1$ is found by considering the case without the interference and the noise; and the upper bound $n = \mathrm{tr}[\mathbf{K}_{\mathbf{s}_i}]$ is the total uncertainty in the unknown signal $\mathbf{s}_i$.) When $\gamma_{ki} > n$, the secrecy constraints cannot be satisfied. The secrecy constraints can be written more explicitly as follows

$$\begin{aligned}&\mathbf{h}_{ki}^E\mathbf{K}_{\mathbf{v}_i}\mathbf{h}_{ki}^{E\dagger} + \mathbf{h}_{kj}^E\mathbf{K}_{\mathbf{x}_j}\mathbf{h}_{kj}^{E\dagger} + \sigma^2_{w,E,i} \\ &\quad - \bar{\gamma}_{ki}(\mathbf{h}_{ki}^E\mathbf{A}_i\mathbf{A}_i^\dagger\mathbf{h}_{ki}^{E\dagger}) \geq 0,\end{aligned} \tag{8}$$

where $i \neq j$, $\bar{\gamma}_{ki} = (n - \gamma_{ki})^{-1} - 1$, $\bar{\gamma}_{ki} \in [0, \infty]$, $\gamma_{ki} < n$.

III. Joint Linear Precoder and Artificial Noise Design

We consider the following collaborative transmission strategies design problem which seeks the optimal linear precoders and the artificial noise covariances in order to minimize the sum of the weighted MMSE's at the legitimate receivers while satisfying the secrecy requirements at the eavesdroppers:

$$(P1) \quad \min_{\substack{\bar{\mathbf{A}} \\ \bar{\mathbf{K}}_{\mathbf{v}}\succeq 0}} \quad \alpha_1\varepsilon_{LR_1}(\bar{\mathbf{A}}, \bar{\mathbf{K}}_{\mathbf{v}}) + \alpha_2\varepsilon_{LR_2}(\bar{\mathbf{A}}, \bar{\mathbf{K}}_{\mathbf{v}}) \tag{9a}$$

$$\text{s.t.} \quad \varepsilon^i_{ER_k}(\bar{\mathbf{A}}, \bar{\mathbf{K}}_{\mathbf{v}}) \geq \gamma_{ki}, \quad i, k = 1, 2, \tag{9b}$$

$$\mathrm{tr}[\mathbf{A}_i{\mathbf{A}_i}^\dagger] + \mathrm{tr}[\mathbf{K}_{\mathbf{v}_i}] \leq P_i, \ i = 1, 2, \tag{9c}$$

where (9(c)) represents the power constraints at the transmitters. The noise covariance matrices $\mathbf{K}_{\mathbf{v}_i}$'s determine the spatial distribution of the artificial noise. Hence this formulation optimizes the spatial distribution of the noise together with the linear precoders.

In this set-up, transmitters can exchange information about channel state information and determine the optimal strategies cooperatively, for instance, through the usage of a secure land line [7], [16]. Such approaches are particularly relevant when the eavesdroppers' channel information is available at the transmitter side, for instance, in broadcasting with confidential messages [7], [16]–[18]. In such scenarios, the eavesdroppers are

registered users of the network but they are only allowed to access to a particular set of content.

We note that the formulation in Problem P1 is not convex. The objective function is not a convex function of $(\bar{\mathbf{A}}, \bar{\mathbf{K}}_{\mathbf{v}})$. Moreover, in general the security constraints are not convex. In particular, left-hand side of (8) is the sum of a convex quadratic function and a concave quadratic function in terms of $\mathbf{A}_i$'s. In general, lower bounding such a function does not form a convex constraint. Although it is possible to write the problem using new variables $\mathbf{R}_i = \mathbf{A}_i\mathbf{A}_i^\dagger \succeq 0$ instead of $\mathbf{A}_i$'s so that security constraints are linear constraints, this new formulation will have rank-constraints, i.e., $\mathrm{rank}(\mathbf{R}_i) \leq n$, which, in general, do not form convex constraints.

IV. Transmission Strategies for Linear Precoding and Artificial Noise Broadcast

We first study the scenario where fixed receiver filters are adopted at the legitimate receivers in Section IV-A. In Section IV-B, we utilize this formulation to provide designs for the general case.

A. Fixed Estimators at Legitimate Receivers

In this case, the estimation filters at the LRs are fixed while the eavesdroppers employ the MMSE estimation.

Let $\mathbf{B}_i^L$ be the estimator adopted at the LR_i. Hence the mean-square error at LR_i can be expressed as follows:

$$\begin{aligned}
&\varepsilon_{LR_i}^F(\bar{\mathbf{A}}, \bar{\mathbf{K}}_{\mathbf{v}}) \\
&= \mathrm{E}[\|\mathbf{s}_i - \mathbf{B}_i^L\mathbf{y}_i^L\|^2], \\
&= \mathrm{tr}[\mathbf{K}_{\mathbf{s}_i}] - \mathrm{tr}[\mathbf{K}_{\mathbf{s}_i\mathbf{y}_i^L}{\mathbf{B}_i^L}^\dagger] - \mathrm{tr}[\mathbf{B}_i^L\mathbf{K}_{\mathbf{s}_i\mathbf{y}_i^L}^\dagger] \\
&\quad + \mathrm{tr}[\mathbf{B}_i^L\mathbf{K}_{\mathbf{y}_i^L}{\mathbf{B}_i^L}^\dagger], \\
&= n - \mathrm{tr}[\mathbf{A}_i^\dagger{\mathbf{H}_{ii}^L}^\dagger{\mathbf{B}_i^L}^\dagger] - \mathrm{tr}[\mathbf{B}_i^L\mathbf{H}_{ii}^L\mathbf{A}_i] \\
&\quad + \mathrm{tr}[\mathbf{B}_i^L\mathbf{H}_{ii}(\mathbf{A}_i{\mathbf{A}_i}^\dagger + \mathbf{K}_{\mathbf{v}_i}){\mathbf{H}_{ii}}^\dagger{\mathbf{B}_i^L}^\dagger] \\
&\quad + \mathrm{tr}[\mathbf{B}_i^L\mathbf{H}_{ij}(\mathbf{A}_j{\mathbf{A}_j}^\dagger + \mathbf{K}_{\mathbf{v}_j}){\mathbf{H}_{ij}}^\dagger{\mathbf{B}_i^L}^\dagger] \\
&\quad + \sigma_{w,L,i}^2\mathrm{tr}[\mathbf{B}_i^L{\mathbf{B}_i^L}^\dagger],
\end{aligned}$$

where $i, j = 1, 2, i \neq j$. Hence, for fixed $\mathbf{B}_i^L$'s, the problem of finding the optimal $(\bar{\mathbf{A}}, \bar{\mathbf{K}}_{\mathbf{v}})$ in order to minimize the weighted sum of the estimation errors at the LRs while satisfying the secrecy constraints can be formulated as follows:

$$(P2) \quad \min_{\bar{\mathbf{A}}, \bar{\mathbf{K}}_{\mathbf{v}}} \quad \alpha_1\varepsilon_{LR_1}^F(\bar{\mathbf{A}}, \bar{\mathbf{K}}_{\mathbf{v}}) + \alpha_2\varepsilon_{LR_2}^F(\bar{\mathbf{A}}, \bar{\mathbf{K}}_{\mathbf{v}}) \quad \text{s.t.} \quad (9b), (9c). \tag{10}$$

In this formulation, the objective function is a convex quadratic function in $\mathbf{A}_i\mathbf{A}_i^\dagger$ and linear in $\mathbf{K}_{\mathbf{v}_i}$. Hence it is convex in $(\bar{\mathbf{A}}, \bar{\mathbf{K}}_{\mathbf{v}})$. Nevertheless, the eavesdropper error constraints are, in general, still not convex in $(\mathbf{A}_1, \mathbf{A}_2)$. Hence we introduce $\mathbf{Z}_i = \mathbf{A}_i\mathbf{A}_i^\dagger$, $i = 1, 2$ with $\bar{\mathbf{Z}} = (\mathbf{Z}_1, \mathbf{Z}_2)$. The part of the error that depends on the optimization variables $(\bar{\mathbf{A}}, \bar{\mathbf{K}}_{\mathbf{v}}, \bar{\mathbf{Z}})$

$$\begin{aligned}
\varepsilon_{LR_i}^Z(\bar{\mathbf{A}}, \bar{\mathbf{K}}_{\mathbf{v}}, \bar{\mathbf{Z}}) &= \mathrm{tr}[\mathbf{B}_i^L\mathbf{H}_{ii}^L(\mathbf{Z}_i + \mathbf{K}_{\mathbf{v}_i}){\mathbf{H}_{ii}^L}^\dagger{\mathbf{B}_i^L}^\dagger] \\
&\quad + \mathrm{tr}[\mathbf{B}_i^L{\mathbf{H}_{ij}}^L(\mathbf{Z}_j + \mathbf{K}_{\mathbf{v}_j}){\mathbf{H}_{ij}}^{L\dagger}{\mathbf{B}_i^L}^\dagger] \\
&\quad - 2\mathrm{Re}(\mathrm{tr}[\mathbf{A}_i^\dagger{\mathbf{H}_{ii}^L}^\dagger{\mathbf{B}_i^L}^\dagger]),
\end{aligned}$$

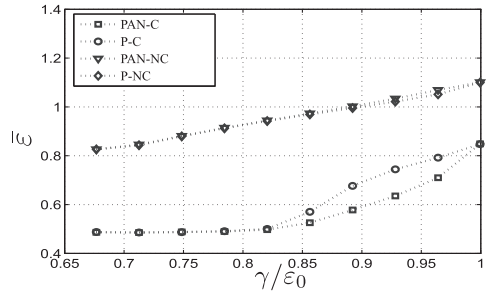

Fig. 2. MMSE versus secrecy requirements, $n_t = 5$.

where $\mathrm{Re}[z]$ denotes the real part of $z \in \mathbb{C}$. The error at ER_k for estimating $\mathbf{s}_i$ can be written in terms $\mathbf{Z}_j$'s as follows

$$\varepsilon_{ER_k}^{iZ}(\bar{\mathbf{K}}_{\mathbf{v}}, \bar{\mathbf{Z}}) = n - \frac{\mathbf{h}_{ki}^E\mathbf{Z}_i{\mathbf{h}_{ki}^E}^\dagger}{\mathbf{h}_{ki}^E(\mathbf{Z}_i + \mathbf{K}_{\mathbf{v}_i}){\mathbf{h}_{ki}^E}^\dagger + \mathbf{h}_{kj}^E(\mathbf{Z}_j + \mathbf{K}_{\mathbf{v}_j}){\mathbf{h}_{kj}^E}^\dagger + \sigma_{w,E,k}^2}$$

where $i, j, k = 1, 2$, $i \neq j$. Hence the problem in (10) can be reformulated as follows:

$$\min_{\bar{\mathbf{A}}, \bar{\mathbf{K}}_{\mathbf{v}}, \bar{\mathbf{Z}}} \quad \alpha_1\varepsilon_{LR_1}^Z(\bar{\mathbf{A}}, \bar{\mathbf{K}}_{\mathbf{v}}, \bar{\mathbf{Z}}) + \alpha_2\varepsilon_{LR_2}^Z(\bar{\mathbf{A}}, \bar{\mathbf{K}}_{\mathbf{v}}, \bar{\mathbf{Z}}) \tag{11a}$$

$$\text{s.t.} \quad \varepsilon_{ER_k}^{iZ}(\bar{\mathbf{K}}_{\mathbf{v}}, \bar{\mathbf{Z}}) \geq \gamma_{ik}, \quad i, k = 1, 2, \tag{11b}$$

$$\mathrm{tr}[\mathbf{Z}_i + \mathbf{K}_{\mathbf{v}_i}] \leq P_i, \quad i = 1, 2, \tag{11c}$$

$$\mathbf{Z}_i = \mathbf{A}_i\mathbf{A}_i^\dagger, \quad i = 1, 2. \tag{11d}$$

We note that (11(b)) form convex constraints, since they can be written as linear functions of $(\bar{\mathbf{K}}_{\mathbf{v}}, \bar{\mathbf{Z}})$ similar to (8). The constraints in (11(d)) represent equality constraints involving convex functions of $\mathbf{A}_i$'s, hence they are not convex. We relax the constraints in (11(d)) as follows:

$$\mathbf{Z}_1 \succeq \mathbf{A}_1{\mathbf{A}_1}^\dagger, \quad \mathbf{Z}_2 \succeq \mathbf{A}_2{\mathbf{A}_2}^\dagger. \tag{12}$$

Hence a relaxation of (11) is obtained, i.e.,

$$\min_{\bar{\mathbf{A}}, \bar{\mathbf{K}}_{\mathbf{v}}, \bar{\mathbf{Z}}} \quad \alpha_1\varepsilon_{LR_1}^Z(\bar{\mathbf{A}}, \bar{\mathbf{K}}_{\mathbf{v}}, \bar{\mathbf{Z}}) + \alpha_2\varepsilon_{LR_2}^Z(\bar{\mathbf{A}}, \bar{\mathbf{K}}_{\mathbf{v}}, \bar{\mathbf{Z}}) \quad \text{s.t.} \quad (11b), (11c), (12). \tag{13}$$

We note that $\varepsilon_{LR_i}^Z(\bar{\mathbf{A}}, \bar{\mathbf{K}}_{\mathbf{v}}, \bar{\mathbf{Z}})$ still depends on $\mathbf{A}_i$. This relaxation is tight as shown in Thm. 4.1:

Theorem 4.1: Let $n \geq 3$. Let (13) be solvable. Then the optimum error values for the relaxed problem in (13) and the problem in (10) are equal and can be attained. Moreover, an optimal solution for (10) can be constructed from an optimal solution of (13).

The proof is given in Appendix A. Since (13) is convex, optimal solutions can be found by efficient numerical techniques using tools such as SeDuMi, SDPT3 and CVX [20]–[22]. Although (10) is non-convex, Thm. 4.1 guarantees that it can be efficiently solved using the convex problem in (13).

B. MMSE Estimators at All Receivers

We now consider Problem P1 where the MMSE estimators are employed also at the legitimate receivers. We propose a block coordinate descent method where we take turns in fixing $(\bar{\mathbf{A}}, \bar{\mathbf{K}}_{\mathbf{v}})$ and fixing the estimators $\mathbf{B}_i^L, i = 1, 2$. For fixed $(\bar{\mathbf{A}}, \bar{\mathbf{K}}_{\mathbf{v}})$ the optimal $\mathbf{B}_i^L$'s are given by (4). By Theorem 4.1, at fixed $(\mathbf{B}_1^L, \mathbf{B}_2^L)$ step, Problem P2 can be optimally solved using

(13). An optimal rank constrained solution from the solution of (13) is generated using the procedure given in Appendix A. The proposed method is summarized in Algorithm 1. Here the objective function of Problem P1 is guaranteed to decrease under each iteration. Since the error is bounded from below, Algorithm 1 is guaranteed to converge.

Algorithm 1 Algorithm for Problem P1

Initialize:

Set $\varepsilon_{LR_i}^0 = \mathrm{tr}[\mathbf{K}_{\mathbf{s}_i}]$, $i = 1, 2$.
Set $(\mathbf{B}_1^L, \mathbf{B}_2^L)^0 = (\mathbf{I}, \mathbf{I})$.
Let $t = 1$.

repeat

Using $(\mathbf{B}_1^L, \mathbf{B}_2^L)^{t-1}$, solve (13) for $(\bar{\mathbf{A}}, \bar{\mathbf{K}}_{\mathbf{v}}, \bar{\mathbf{Z}})^t$.
if (11(d)) is not satisfied **then**
Generate $(\bar{\mathbf{A}}, \bar{\mathbf{K}}_{\mathbf{v}})^t$ using [19, Algorithm RED].
end if
Using $(\bar{\mathbf{A}}, \bar{\mathbf{K}}_{\mathbf{v}})^t$, solve (4) for $(\mathbf{B}_1^L, \mathbf{B}_2^L)^t$.
Using $(\bar{\mathbf{A}}, \bar{\mathbf{K}}_{\mathbf{v}})^t$ and (5) determine $\varepsilon_{LR_1}^t$, $\varepsilon_{LR_2}^t$.

until $(\alpha_1 \varepsilon_{LR_1}^{t-1} + \alpha_2 \varepsilon_{LR_2}^{t-1} - (\alpha_1 \varepsilon_{LR_1}^t + \alpha_2 \varepsilon_{LR_2}^t) \leq \epsilon)$
// *The stopping criterion is met.*
Output: $(\bar{\mathbf{A}}, \bar{\mathbf{K}}_{\mathbf{v}})^t$, $\varepsilon_{LR_1}^t$, $\varepsilon_{LR_2}^t$.

V. Numerical Results

We now illustrate the performance of our designs. The error performance of the legitimate receivers is reported as follows: $\bar{\varepsilon} = (\alpha_1 \varepsilon_1 + \alpha_2 \varepsilon_2)/\varepsilon_0$, where $\varepsilon_0 = \mathrm{tr}[\mathbf{K}_{\mathbf{s}_1}] = \mathrm{tr}[\mathbf{K}_{\mathbf{s}_2}] = n$. The channel matrices for LRs and ERs are generated independently with independent and identically distributed complex proper zero-mean Gaussian elements with variance $\sigma_H^2 = 1$. The average results for 100 channel realizations are reported. We set $\sigma_{w,L,i}^2 = \sigma_{w,E,i}^2 = \sigma_w^2 = 1$, $i = 1, 2$; $n = 3$, $n_r = 3$; $\gamma_{ik} = \gamma, i, k = 1, 2$; $\alpha_1 = \alpha_2 = 1$; $P_1 = P_2 = P$; SNR $= P/\sigma_w^2 = 10$ dB, $\epsilon = 10^{-5}$.

The trade-offs between the error and the security constraints γ are shown in Fig. 2 and Fig. 3 for $n_t = 5$ and $n_t = 3$, respectively. Here PAN-C denotes the proposed design for Problem P1 (precoding + artificial noise) found by using the cooperative optimization approach in Section IV. P-C denotes the proposed design when there is no artificial noise broadcast, i.e., $\mathrm{tr}[\mathbf{K}_{\mathbf{v}_i}] = 0$. Similarly, PAN-NC (precoding + artificial noise) and P-NC (precoding only) denote the designs for the scenario when the transmitters do not corporate while designing the strategies.

In all scenarios PAN-C shows the best performance as expected. In general, there is a substantial gap between the performance of cooperative and non-cooperative schemes. This gap gets smaller as secrecy constraints become more demanding. Comparing PAN-C and P-C, we observe that for low values of γ, these designs show similar performance illustrating that linear precoding is sufficient to satisfy security demands. On the other hand for relatively high values of γ, a prominent performance difference is observed.

We observe that PAN-NC performs worse than or the same as P-NC. Hence when there is no cooperation, additional noise transmission may degrade the performance on average. When there is no cooperation, each transmitter assumes that the channel will be used only by itself. As a result, it is inclined to use artificial noise with relatively high power in order to satisfy the security constraints. When these designs are used in the interference setting, they may degrade the performance substantially as seen in Fig. 3; where the number of transmit antennas is relatively small, hence transmitters are more likely to adopt noise aided scheme to satisfy the security constraints.

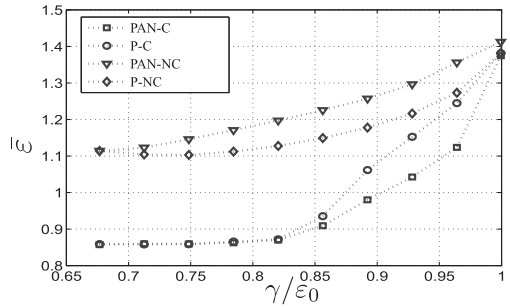

Fig. 3. MMSE versus secrecy requirements, $n_t = 3$.

VI. Conclusions

We have considered the problem of joint design of linear precoder and artificial noise in Gaussian interference channels with secrecy constraints. We have illustrated that broadcasting artificial noise provides significant improvements especially when the secrecy levels required at the eavesdroppers are demanding. Our results also show that artificial noise aided scheme can introduce substantial performance degradation when the transmitters cannot cooperate. This suggests that artificial noise should be used with caution in multiuser environments if joint design is not possible.

We have focused on scenarios where eavesdroppers are registered users of the network and full CSI is available at the transmitters. Extensions to partial CSI scenarios are considered as an important future research direction.

Appendix A
Proof of Theorem 4.1

Let $\mathbf{S}_i = \begin{bmatrix} \mathbf{I} & \mathbf{A}_i^\dagger \\ \mathbf{A}_i & \mathbf{Z}_i \end{bmatrix}$, $i = 1, 2$. Using Schur complement [23, A.5.5], the positive semi-definite ordering constraints in (12) can be written as positive semi-definiteness conditions as $\mathbf{S}_i \succeq 0$, $i = 1, 2$. Let $\bar{\mathbf{S}} = (\mathbf{S}_1, \mathbf{S}_2)$. Now the formulation in (13) can be equivalently written in terms of $(\bar{\mathbf{S}}, \bar{\mathbf{K}}_{\mathbf{v}})$ instead of $(\bar{\mathbf{Z}}, \bar{\mathbf{A}}, \bar{\mathbf{K}}_{\mathbf{v}})$ (with the additional constraints $[\mathbf{S}_i]_{kl} = [\mathbf{I}]_{kl}, \quad k, l = 1, \ldots, n$). Let us refer to this equivalent formulation as Problem 2-S. Since the formulation in (13) is assumed to be solvable, Problem 2-S is also solvable and there exist optimum values $(\mathbf{S}_1^*, \mathbf{S}_2^*, \mathbf{K}_{\mathbf{v}_1}^*, \mathbf{K}_{\mathbf{v}_2}^*)$. Considering Problem 2-S with $\mathbf{S}_i$'s as optimization variables under these fixed optimum values of $(\mathbf{K}_{\mathbf{v}_1}^*, \mathbf{K}_{\mathbf{v}_2}^*)$ and invoking [19, Thm 2.1] reveals that for $n \geq 3$, there exist optimum solutions with $\mathrm{rank}(\mathbf{S}_i) \leq n$. Hence Problem 2-S, or equivalently (13), has the same optimum values with (10). Optimal $\mathbf{S}_i$'s for Problem 2-S with rank n can be constructed from an optimal solution $\mathbf{S}_i^*$ with arbitrary rank using [19, Algorithm RED]. Optimal $\mathbf{A}_i$'s for (10) can be found by taking the lower left $n_t \times n$ matrix of these rank-constrained $\mathbf{S}_i$'s [19, Lemma~2.1]. □

REFERENCES

[1] Y. Liang, A. Somekh-Baruch, H. V. Poor, S. Shamai (Shitz), and S. Verdu, "Capacity of cognitive interference channels with and without secrecy," *IEEE Trans. Inf. Theory*, vol. 55, pp. 604–619, Feb. 2009.

[2] X. He and A. Yener, "K-user interference channels: Achievable secrecy rate and degrees of freedom," in *IEEE Information Theory Workshop on Networking and Information Theory (ITW), 2009*, 2009, pp. 336–340.

[3] O. O. Koyluoglu, H. El Gamal, L. Lai, and H. V. Poor, "Interference alignment for secrecy," *IEEE Trans. Inf. Theory*, vol. 57, pp. 3323–3332, Jun. 2011.

[4] J. Zhu, J. Mo, and M. Tao, "Cooperative secret communication with artificial noise in symmetric interference channel," *IEEE Commun. Lett.*, vol. 14, pp. 885–887, Oct. 2010.

[5] J. Yang, I.-M. Kim, and D. I. Kim, "Joint design of optimal cooperative jamming and power allocation for linear precoding," *IEEE Trans. Commun.*, vol. 62, pp. 3285–3298, Sep. 2014.

[6] N. Romero-Zurita, M. Ghogho, and D. McLernon, "Outage probability based power distribution between data and artificial noise for physical layer security," *IEEE Signal Process. Lett.*, vol. 19, pp. 71–74, Feb. 2012.

[7] 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, pp. 1202–1216, Mar. 2011.

[8] M. R. Rodrigues and P. D. Almeida, "Filter design with secrecy constraints: The degraded parallel gaussian wiretap channel," in *IEEE Global Telecommunications Conf. (GLOBECOM) 2008*, 2008, pp. 1–5.

[9] H. Reboredo, M. Ara, M. R. D. Rodrigues, and J. Xavier, "Filter design with secrecy constraints: The degraded multiple-input multiple-output gaussian wiretap channel," in *2011 IEEE Vehicular Technology Conf. (VTC Spring)*, 2011, pp. 1–5.

[10] H. Reboredo, J. Xavier, and M. Rodrigues, "Filter design with secrecy constraints: The MIMO gaussian wiretap channel," *IEEE Trans. Signal Process.*, vol. 61, no. 15, pp. 3799–3814, 2013.

[11] M. Pei, J. Wei, K.-K. Wong, and X. Wang, "Masked beamforming for multiuser MIMO wiretap channels with imperfect CSI," *IEEE Trans. Wireless Commun.*, vol. 11, pp. 544–549, Feb. 2012.

[12] J. Yang, I.-M. Kim, and D. I. Kim, "Optimal cooperative jamming for multiuser broadcast channel with multiple eavesdroppers," *IEEE Trans. Wireless Commun.*, vol. 12, pp. 2840–2852, Jun. 2013.

[13] J. Yang, I.-M. Kim, and D. I. Kim, "Power-constrained optimal cooperative jamming for multiuser broadcast channel," *IEEE Wireless Commun. Lett.*, vol. 2, pp. 411–414, Aug. 2013.

[14] B. D. O. Anderson and J. B. Moore, *Optimal filtering*. : Prentice-Hall, 1979.

[15] M. Rupf, F. Tarkoy, and J. Massey, "User-separating demodulation for code-division multiple-access systems," *IEEE J. Sel. Areas Commun.*, vol. 12, pp. 786–795, Jun. 1994.

[16] Q. Li and W.-K. Ma, "Spatially selective artificial-noise aided transmit optimization for MISO multi-eves secrecy rate maximization," *IEEE Trans. Signal Process.*, vol. 61, pp. 2704–2717, May 2013.

[17] E. Ekrem and S. Ulukus, "Capacity region of gaussian MIMO broadcast channels with common and confidential messages," *IEEE Trans. Inf. Theory*, vol. 58, pp. 5669–5680, Sep. 2012.

[18] R. Liu, T. Liu, H. Poor, and S. Shamai, "New results on multiple-input multiple-output broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 59, pp. 1346–1359, Mar. 2013.

[19] A. Beck, "Convexity properties associated with nonconvex quadratic matrix functions and applications to quadratic programming," *J. Optim. Theory Applicat.*, vol. 142, no. 1, pp. 1–29, 2009.

[20] J. F. Sturm, "Using SeDuMi 1.02, a matlab toolbox for optimization over symmetric cones," *Optim. Meth. Softw.*, vol. 11, no. 1–4, pp. 625–653, 1999.

[21] R. H. Tütüncü, K. C. Toh, and M. J. Todd, "Solving semidefinite-quadratic-linear programs using SDPT3," *Math. Programm.*, vol. 95, no. 2, pp. 189–217, 2003.

[22] CVX Research Inc., "CVX: Matlab software for disciplined convex programming 2.0," [Online]. Available: http://cvxr.com/cvx 2012

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