

Linear Precoding for Cognitive Multiple Access Wiretap Channel with Finite-Alphabet Inputs

Juening Jin*, Chengshan Xiao[†], Meixia Tao* and Wen Chen*

*Department of Electronic Engineering, Shanghai Jiao Tong University

Shanghai, 200240, China, Email: jueningjin@gmail.com, {mxtao, wenchen}@sjtu.edu.cn

[†]Department of Electrical and Computer Engineering, Missouri University of Science and Technology

Rolla, MO 65409, USA, Email: xiaoc@mst.edu

Abstract—This paper investigates the linear precoder design for cognitive multiple-access wiretap channel (CMAC-WT), where two secondary-user transmitters (STs) communicate with one secondary-user receiver (SR) in the presence of an eavesdropper and subject to interference threshold constraints at primary-user receivers (PRs). It designs linear precoders to maximize the ergodic secrecy sum rate for multiple-input multiple-output (MIMO) CMAC-WT under finite-alphabet inputs and statistical channel state information (CSI). For this non-convex problem, a two-layer algorithm is proposed by embedding the convex-concave procedure into an outer approximation framework. The key idea of this algorithm is to reformulate the approximated ergodic secrecy sum rate as a difference of convex (DC) functions, and then generate a sequence of simpler relaxed sets to approach the non-convex feasible set. In this way, near optimal precoding matrices are obtained by maximizing the approximated ergodic secrecy sum rate over a sequence of relaxed sets. Numerical results show that the proposed precoder design provides a significant performance gain over the Gaussian precoding method in the medium and high SNR regimes.

I. INTRODUCTION

Due to the broadcast nature of radio propagation, the message transmitted from a wireless node can be overheard by any nearby device. Therefore, security is a critical issue in wireless networks. This paper concerns the physical layer security to prevent eavesdropping in a spectrum sharing cognitive radio network, where the unlicensed secondary users can coexist concurrently with the licensed primary users by restricting the interference power at primary-user receivers to be below the interference thresholds [1].

Physical-layer security or information-theoretic security originates from Shannon's notion of perfect secrecy [2]. It is first studied in wiretap channel by Wyner [3] and later in broadcast channel with confidential message by Csiszár and Körner in [4]. The study of physical-layer security then is extended to various kinds of multiuser communication scenarios [5]–[7]. However, most existing works on physical-layer security rely on the assumption of Gaussian inputs. Although Gaussian inputs are capacity achieving in a variety of Gaussian channels, practical signals in wireless systems are drawn from finite constellation sets, such as phase shift keying (PSK) modulation or quadrature amplitude modulation (QAM). In fact, the common approach that designs linear precoder in a MIMO system under Gaussian inputs and then applies it to the practical system may lead to significant performance loss [8],

[9]. Therefore, The precoder design with finite-alphabet inputs has drawn great research interests in recent years [10]–[20].

As illustrated in Fig. 1, we consider the underlay cognitive multiple-access wiretap channel, in which two secondary-user transmitters (STs) communicate with one secondary-user receiver (SR) in the presence of an eavesdropper (ED) and subject to interference threshold constraints at multiple primary-user receivers (PRs). Each node in the system has multiple antennas. We design linear precoders at the STs to achieve the maximum ergodic secrecy sum rate under statistical CSI and finite-alphabet inputs. This problem is extremely difficult to solve due to its non-concavity and non-deterministic polynomial-time (NP)-hardness. In this paper, We first utilize an accurate approximation of the ergodic secrecy sum rate to reduce the computational effort, and then propose a two-layer algorithm by combining the outer approximation framework with the convex-concave procedure. The idea behind this algorithm is to rewrite the approximated ergodic secrecy sum rate as a difference of convex functions, and then approximate the non-convex feasible set by a sequence of relaxed sets. Each relaxed set can be represented explicitly as the union of convex sets. Subsequently, the convex-concave procedure is applied to maximize the approximated ergodic secrecy sum rate over these convex sets. Numerical results show that when considering finite-alphabet inputs, our proposed linear precoding algorithm significantly outperforms the conventional Gaussian precoding method in the medium and high signal-to-noise ratio (SNR) regimes.

Notations: boldface lowercase letters, boldface uppercase letters, and calligraphic letters are used to denote vectors, matrices and sets, respectively. The superscripts $(\cdot)^T$ and $(\cdot)^H$ represent transpose and Hermitian operations, respectively. $\text{diag}(\cdot)$ represents a block diagonal matrix whose diagonal elements are matrices. $\text{tr}(\cdot)$ is the trace of a matrix. $\text{vec}(\cdot)$ is a column vector formed by stacking the columns of a matrix; $\|\cdot\|$ denotes the Euclidean norm of a vector. $\mathbf{A} \otimes \mathbf{B}$ is the Kronecker product of two matrices \mathbf{A} and \mathbf{B} . $E(\cdot)$ represents the statistical expectation. $\Re(\cdot)$ and $\Im(\cdot)$ denote the real and imaginary parts of a complex vector or matrix. \mathbf{I} and $\mathbf{0}$ denote an identity matrix and a zero matrix, respectively, with appropriate dimensions. $\mathbf{A} \succeq \mathbf{0}$ denotes the positive semidefiniteness of \mathbf{A} . $\log(\cdot)$ and $\ln(\cdot)$ are used for the base two logarithm and natural logarithm, respectively.

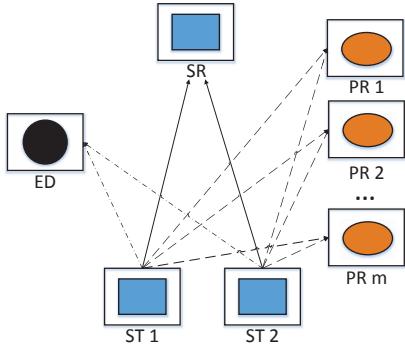


Fig. 1: System model of cognitive multiple-access wiretap channel.

II. PROBLEM FORMULATION

We consider the cognitive multiple-access wiretap channel depicted in Fig. 1. The i -th ST has N_{T_i} antennas, $i = 1, 2$, the SR has N_R antennas, the j -th PR has N_{P_j} antennas, $\forall j$, and the ED has N_E antennas. The channel output at the SR, ED and PRs are, respectively, represented as

$$\begin{aligned} \mathbf{y}_R &= \mathbf{H}_1 \mathbf{P}_1 \mathbf{s}_1 + \mathbf{H}_2 \mathbf{P}_2 \mathbf{s}_2 + \mathbf{n}_R \\ \mathbf{z}_E &= \mathbf{G}_1 \mathbf{P}_1 \mathbf{s}_1 + \mathbf{G}_2 \mathbf{P}_2 \mathbf{s}_2 + \mathbf{n}_E, \\ \mathbf{w}_j &= \mathbf{F}_{1,j} \mathbf{P}_1 \mathbf{s}_1 + \mathbf{F}_{2,j} \mathbf{P}_2 \mathbf{s}_2 + \mathbf{n}_{P_j}, \quad j = 1, 2, \dots, m \end{aligned} \quad (1)$$

where \mathbf{s}_i is the transmit data vector at the i -th ST with zero-mean and covariance matrix $E[\mathbf{s}_i \mathbf{s}_i^H] = \mathbf{I}$, $i = 1, 2$; \mathbf{P}_i is the linear precoding matrix at the i -th ST, $i = 1, 2$; \mathbf{n}_E and \mathbf{n}_{P_j} are independent and identically distributed (i.i.d.) complex Gaussian noises with zero-mean and covariance $\sigma_R^2 \mathbf{I}$, $\sigma_E^2 \mathbf{I}$ and $\sigma_{P_j}^2 \mathbf{I}$, respectively; \mathbf{H}_i , \mathbf{G}_i and $\mathbf{F}_{i,j}$ are complex channel matrices from the i -th ST to the SR, the ED, and the j -th PR, respectively.

We assume double correlated fading channels, where the channel matrices are modeled as [21]

$$\begin{aligned} \mathbf{H}_i &= \Phi_h^{\frac{1}{2}} \mathbf{H}_{w_i} \Psi_{h_i}^{\frac{1}{2}}, \quad i = 1, 2 \\ \mathbf{G}_i &= \Phi_g^{\frac{1}{2}} \mathbf{G}_{w_i} \Psi_{g_i}^{\frac{1}{2}}, \quad i = 1, 2 \\ \mathbf{F}_{i,j} &= \Phi_{f_j}^{\frac{1}{2}} \mathbf{F}_{w_{i,j}} \Psi_{f_{i,j}}^{\frac{1}{2}}, \quad \forall (i, j) \end{aligned} \quad (2)$$

Here Φ_h , Φ_g and Φ_{f_j} are receive correlation matrices of \mathbf{H}_i , \mathbf{G}_i and $\mathbf{F}_{i,j}$, respectively; Ψ_{h_i} , Ψ_{g_i} and $\Psi_{f_{i,j}}$ are transmit correlation matrices of \mathbf{H}_i , \mathbf{G}_i and $\mathbf{F}_{i,j}$, respectively; \mathbf{H}_{w_i} , \mathbf{G}_{w_i} and $\mathbf{F}_{w_{i,j}}$ are random matrices with i.i.d. zero-mean unit variance complex Gaussian entries. We assume that STs only have the knowledge of statistical CSI, i.e., the transmit and receive correlation matrices of \mathbf{H}_i , \mathbf{G}_i and $\mathbf{F}_{i,j}$.

The precoders at STs should satisfy the average power constraint β_i

$$E_{\mathbf{s}_i} \left\{ \text{tr}(\mathbf{P}_i \mathbf{s}_i \mathbf{s}_i^H \mathbf{P}_i^H) \right\} = \text{tr}(\mathbf{P}_i^H \mathbf{P}_i) \leq \beta_i, \quad i = 1, 2 \quad (3)$$

while meeting all the interference threshold constraints γ_j at PRs due to the assumption of underlay cognitive systems

$$\begin{aligned} \sum_{i=1}^2 E_{\mathbf{F}_{i,j}, \mathbf{s}_i} \left\{ \text{tr}(\mathbf{F}_{i,j} \mathbf{P}_i \mathbf{s}_i \mathbf{s}_i^H \mathbf{P}_i^H \mathbf{F}_{i,j}^H) \right\} \\ = \phi_j \cdot \sum_{i=1}^2 \text{tr}(\mathbf{P}_i^H \mathbf{\Psi}_{f_{i,j}} \mathbf{P}_i) \leq \gamma_j, \quad j = 1, 2, \dots, m \end{aligned} \quad (4)$$

where $\phi_j = \text{tr}(\Phi_{f_j})$. The equality in (4) holds because each element of $\mathbf{F}_{w_{i,j}}$ is i.i.d. complex Gaussian variable with zero-mean and unit variance, and $\mathbf{F}_{w_{i,j}}$ is independent to \mathbf{s}_i .

We design linear precoders that maximize the ergodic secrecy sum rate under finite-alphabet inputs. Let each symbol of the transmit data vector \mathbf{s}_i draw independently from an equiprobable discrete constellation with cardinality M_i , $i = 1, 2$. According to [6], the following ergodic secrecy sum rate is achievable

$$R_{\text{erg}} = [\bar{\mathcal{I}}(\mathbf{s}_1, \mathbf{s}_2; \mathbf{y}_R) - \bar{\mathcal{I}}(\mathbf{s}_1, \mathbf{s}_2; \mathbf{z}_E)]^+ \quad (5)$$

where $[x]^+ = \max(x, 0)$, and the ergodic mutual information $\bar{\mathcal{I}}(\mathbf{s}_1, \mathbf{s}_2; \mathbf{y}_R)$ and $\bar{\mathcal{I}}(\mathbf{s}_1, \mathbf{s}_2; \mathbf{z}_E)$ are given by [12]

$$\bar{\mathcal{I}}(\mathbf{s}_1, \mathbf{s}_2; \mathbf{y}_R) = \log N - \frac{1}{N} \sum_{m=1}^N E_{\mathbf{H}_1, \mathbf{H}_2, \mathbf{n}_R} [a_m] \quad (6)$$

$$\bar{\mathcal{I}}(\mathbf{s}_1, \mathbf{s}_2; \mathbf{z}_E) = \log N - \frac{1}{N} \sum_{m=1}^N E_{\mathbf{G}_1, \mathbf{G}_2, \mathbf{n}_E} [b_m] \quad (7)$$

with

$$\begin{aligned} a_m &= \log \sum_{k=1}^N \exp \left\{ \frac{-\|\sum_{i=1}^2 \mathbf{H}_i \mathbf{P}_i \mathbf{e}_{mk,i} + \mathbf{n}_R\|^2 + \|\mathbf{n}_R\|^2}{\sigma_R^2} \right\} \\ b_m &= \log \sum_{k=1}^N \exp \left\{ \frac{-\|\sum_{i=1}^2 \mathbf{G}_i \mathbf{P}_i \mathbf{e}_{mk,i} + \mathbf{n}_E\|^2 + \|\mathbf{n}_E\|^2}{\sigma_E^2} \right\}. \end{aligned}$$

Here $\mathbf{e}_{mk,i}$ is the difference between $\mathbf{d}_{m,i}$ and $\mathbf{d}_{k,i}$, with $\mathbf{d}_{m,i}$ and $\mathbf{d}_{k,i}$ representing two possible distinct signal vectors from \mathbf{s}_i ; N is a constant, equals to $M_1^{N_{T_1}} M_2^{N_{T_2}}$.

The evaluation of the above ergodic mutual information is difficult since there are no closed-form expressions for the expectations in (6) and (7). Although we can use Monte Carlo method to estimate these expectations, the computational complexity is prohibitively high. In order to mitigate this difficulty, we employ an accurate approximation of the ergodic mutual information. According to [14], $\bar{\mathcal{I}}(\mathbf{s}_1, \mathbf{s}_2; \mathbf{y}_R)$ and $\bar{\mathcal{I}}(\mathbf{s}_1, \mathbf{s}_2; \mathbf{z}_E)$ can be approximated respectively as

$$\mathcal{I}_A(\mathbf{s}_1, \mathbf{s}_2; \mathbf{y}_R) = \log N - \frac{1}{N} \sum_{m=1}^N \log \sum_{k=1}^N \exp(-c_{mk}) \quad (8)$$

$$\mathcal{I}_A(\mathbf{s}_1, \mathbf{s}_2; \mathbf{z}_E) = \log N - \frac{1}{N} \sum_{m=1}^N \log \sum_{k=1}^N \exp(-d_{mk}) \quad (9)$$

with

$$c_{mk} = \sum_q \ln \left(1 + \frac{h_q}{2\sigma_R^2} \sum_{i=1}^2 \mathbf{e}_{mk,i}^H \mathbf{P}_i^H \Psi_{h_i} \mathbf{P}_i \mathbf{e}_{mk,i} \right) \quad (10)$$

$$d_{mk} = \sum_q \ln \left(1 + \frac{g_q}{2\sigma_E^2} \sum_{i=1}^2 \mathbf{e}_{mk,i}^H \mathbf{P}_i^H \Psi_{g_i} \mathbf{P}_i \mathbf{e}_{mk,i} \right) \quad (11)$$

where h_q and g_q represent the q -th eigenvalue of Φ_h and Φ_g , respectively. This approximation is very accurate for arbitrary precoders, and the computational complexity is several orders of magnitude lower than that of the original ergodic mutual information [14].

By replacing the ergodic mutual information functions in (5) with the approximated mutual information $\mathcal{I}_A(\mathbf{s}_1, \mathbf{s}_2; \mathbf{y}_R)$ and $\mathcal{I}_A(\mathbf{s}_1, \mathbf{s}_2; \mathbf{z}_E)$, the precoding problem is formulated as

$$\begin{aligned} & \text{maximize}_{\mathbf{P}_1, \mathbf{P}_2} [\mathcal{I}_A(\mathbf{s}_1, \mathbf{s}_2; \mathbf{y}_R) - \mathcal{I}_A(\mathbf{s}_1, \mathbf{s}_2; \mathbf{z}_E)]^+ \\ & \text{subject to} \quad \text{tr}(\mathbf{P}_i^H \mathbf{P}_i) \leq \beta_i, \quad i = 1, 2 \\ & \quad \sum_{i=1}^2 \text{tr}(\mathbf{P}_i^H \Psi_{f_{i,j}} \mathbf{P}_i) \leq \gamma_j / \phi_j, \quad j = 1, 2, \dots, m. \end{aligned} \quad (12)$$

III. ALGORITHM DESIGN

A. Precoder vectorization

Note that $\text{tr}(\mathbf{ABCD}) = \text{vec}(\mathbf{A}^T)^T \cdot (\mathbf{D}^T \otimes \mathbf{B}) \cdot \text{vec}(\mathbf{C})$, c_{mk} in (10) can be rewritten as

$$c_{mk} = \sum_q \ln \left(1 + h_q \cdot \hat{\mathbf{p}}^H \hat{\mathbf{A}}_{mk} \hat{\mathbf{p}} \right) \quad (13)$$

where

$$\hat{\mathbf{p}} = \begin{bmatrix} \text{vec}(\mathbf{P}_1) \\ \text{vec}(\mathbf{P}_2) \end{bmatrix} \quad (14)$$

and

$$\hat{\mathbf{A}}_{mk} = \frac{1}{2\sigma_R^2} \cdot \text{diag}(\mathbf{E}_{mk,1} \otimes \Psi_{h_1}, \mathbf{E}_{mk,2} \otimes \Psi_{h_2}) \quad (15)$$

with $\mathbf{E}_{mk,i} = (\mathbf{e}_{mk,i} \mathbf{e}_{mk,i}^H)^T$, $i = 1, 2$. According to [22], (13) can be further rewritten as

$$c_{mk} = \sum_q \ln \left(1 + h_q \cdot \mathbf{p}^T \mathbf{A}_{mk} \mathbf{p} \right) \quad (16)$$

where

$$\mathbf{p} = \begin{bmatrix} \Re\{\hat{\mathbf{p}}\} \\ \Im\{\hat{\mathbf{p}}\} \end{bmatrix} \quad (17)$$

and

$$\mathbf{A}_{mk} = \begin{bmatrix} \Re\{\hat{\mathbf{A}}_{mk}\} & -\Im\{\hat{\mathbf{A}}_{mk}\} \\ \Im\{\hat{\mathbf{A}}_{mk}\} & \Re\{\hat{\mathbf{A}}_{mk}\} \end{bmatrix} \succeq \mathbf{0}. \quad (18)$$

Similarly, we define $\hat{\mathbf{B}}_{mk}$ and \mathbf{B}_{mk} as

$$\hat{\mathbf{B}}_{mk} = \frac{1}{2\sigma_E^2} \cdot \text{diag}(\mathbf{E}_{mk,1} \otimes \Psi_{g_1}, \mathbf{E}_{mk,2} \otimes \Psi_{g_2}) \quad (19)$$

$$\mathbf{B}_{mk} = \begin{bmatrix} \Re\{\hat{\mathbf{B}}_{mk}\} & -\Im\{\hat{\mathbf{B}}_{mk}\} \\ \Im\{\hat{\mathbf{B}}_{mk}\} & \Re\{\hat{\mathbf{B}}_{mk}\} \end{bmatrix} \succeq \mathbf{0}, \quad (20)$$

$\hat{\mathbf{C}}_i$ and \mathbf{C}_i as

$$\hat{\mathbf{C}}_i = \text{diag}(\mathbf{I} \otimes (2-i)\mathbf{I}, \mathbf{I} \otimes (i-1)\mathbf{I}), \quad i = 1, 2 \quad (21)$$

$$\mathbf{C}_i = \begin{bmatrix} \Re\{\hat{\mathbf{C}}_i\} & -\Im\{\hat{\mathbf{C}}_i\} \\ \Im\{\hat{\mathbf{C}}_i\} & \Re\{\hat{\mathbf{C}}_i\} \end{bmatrix} \succeq \mathbf{0}, \quad (22)$$

$\hat{\mathbf{D}}_j$ and \mathbf{D}_j as

$$\hat{\mathbf{D}}_j = \phi_j \cdot \text{diag}(\mathbf{I} \otimes \Psi_{f_{1,j}}, \mathbf{I} \otimes \Psi_{f_{2,j}}), \quad \forall j \quad (23)$$

$$\mathbf{D}_j = \begin{bmatrix} \Re\{\hat{\mathbf{D}}_j\} & -\Im\{\hat{\mathbf{D}}_j\} \\ \Im\{\hat{\mathbf{D}}_j\} & \Re\{\hat{\mathbf{D}}_j\} \end{bmatrix} \succeq \mathbf{0}. \quad (24)$$

Then problem (12) is converted into a vectorized form

$$\begin{aligned} & \underset{\mathbf{p}}{\text{maximize}} \quad f(\mathbf{p}) - g(\mathbf{p}) \\ & \text{subject to} \quad \mathbf{p}^T \mathbf{C}_i \mathbf{p} \leq \beta_i, \quad i = 1, 2 \\ & \quad \mathbf{p}^T \mathbf{D}_j \mathbf{p} \leq \gamma_j, \quad j = 1, 2, \dots, m \end{aligned} \quad (25)$$

where $f(\mathbf{p})$ and $g(\mathbf{p})$ are given below

$$\begin{aligned} f(\mathbf{p}) &= \frac{1}{N} \sum_{m=1}^N \log \sum_{k=1}^N \exp \left\{ -\sum_q \ln(1 + g_q \cdot \mathbf{p}^T \mathbf{B}_{mk} \mathbf{p}) \right\} \\ g(\mathbf{p}) &= \frac{1}{N} \sum_{m=1}^N \log \sum_{k=1}^N \exp \left\{ -\sum_q \ln(1 + h_q \cdot \mathbf{p}^T \mathbf{A}_{mk} \mathbf{p}) \right\}. \end{aligned}$$

Here the positive operator $[\cdot]^+$ has been removed from the objective function because $\mathbf{p} = \mathbf{0}$ always belongs to the feasible set. Since the objective function in (25) is neither convex nor concave, it is extremely difficult to solve (25) globally. Actually, it has been shown in [13] that problem (25) is an NP-hard problem.

The sequel presents a numerical algorithm to solve (25). The algorithm can be divided into two layers: outer layer and inner layer. The outer layer is done by generating a sequence of relaxed sets to approximate the non-convex feasible set. The inner layer is to reformulate the ergodic secrecy sum rate as a difference of convex function, and then maximize it over the relaxed sets by using the convex-concave procedure.

B. Outer Approximation of the Feasible Set

We first rewrite (25) with an additional hyperrectangle $\mathcal{B}_{\text{init}}$

$$\begin{aligned} & \underset{\mathbf{p}}{\text{maximize}} \quad f(\mathbf{p}) - g(\mathbf{p}) \\ & \text{subject to} \quad \mathbf{p}^T \mathbf{C}_i \mathbf{p} \leq \beta_i, \quad i = 1, 2, \\ & \quad \mathbf{p}^T \mathbf{D}_j \mathbf{p} \leq \gamma_j, \quad j = 1, 2, \dots, m \\ & \quad \mathbf{p} \in \mathcal{B}_{\text{init}} \end{aligned} \quad (26)$$

in which the hyperrectangle $\mathcal{B}_{\text{init}}$ is given by

$$\mathcal{B}_{\text{init}} = \left\{ \mathbf{p} \mid \mathbf{l}(\mathcal{B}_{\text{init}}) \leq \mathbf{p} \leq \mathbf{u}(\mathcal{B}_{\text{init}}) \right\}. \quad (27)$$

To ensure that problem (26) and (25) are equivalent, $\mathbf{l}(\mathcal{B}_{\text{init}})$ and $\mathbf{u}(\mathcal{B}_{\text{init}})$ can be set as

$$\mathbf{l}(\mathcal{B}_{\text{init}}) = \begin{bmatrix} -\sqrt{\beta_1} \cdot \mathbf{1} \\ -\sqrt{\beta_2} \cdot \mathbf{1} \end{bmatrix}, \quad \mathbf{u}(\mathcal{B}_{\text{init}}) = \begin{bmatrix} \sqrt{\beta_1} \cdot \mathbf{1} \\ \sqrt{\beta_2} \cdot \mathbf{1} \end{bmatrix}. \quad (28)$$

where $\mathbf{1}$ represents the vector with all entries one.

By introducing a new variable $\mathbf{Q} = \mathbf{p}\mathbf{p}^T$, we define a function $\varphi(\mathcal{F})$ as the optimal value of the following optimization problem

$$\begin{aligned}\varphi(\mathcal{F}) &\triangleq \underset{\mathbf{Q}, \mathbf{p}}{\text{maximize}} \quad F(\mathbf{Q}) - G(\mathbf{Q}) \\ &\text{subject to} \quad (\mathbf{Q}, \mathbf{p}) \in \mathcal{F}\end{aligned}\quad (29)$$

where $F(\mathbf{Q})$ and $G(\mathbf{Q})$ are given below

$$F(\mathbf{Q}) = \frac{1}{N} \sum_{m=1}^N \log \sum_{k=1}^N \exp(-\bar{c}_{mk}(\mathbf{Q})) \quad (30)$$

$$G(\mathbf{Q}) = \frac{1}{N} \sum_{m=1}^N \log \sum_{k=1}^N \exp(-\bar{d}_{mk}(\mathbf{Q})) \quad (31)$$

with

$$\bar{c}_{mk}(\mathbf{Q}) = \sum_q \ln(1 + g_q \cdot \text{tr}(\mathbf{B}_{mk}\mathbf{Q})) \quad (32)$$

$$\bar{d}_{mk}(\mathbf{Q}) = \sum_q \ln(1 + h_q \cdot \text{tr}(\mathbf{A}_{mk}\mathbf{Q})). \quad (33)$$

Both $F(\mathbf{Q})$ and $G(\mathbf{Q})$ are convex functions thus $F(\mathbf{Q}) - G(\mathbf{Q})$ is a DC function [23]. Furthermore, when $\mathcal{F}_{\text{init}}$, given by

$$\mathcal{F}_{\text{init}} = \left\{ (\mathbf{Q}, \mathbf{p}) \middle| \begin{array}{l} \mathbf{Q} = \mathbf{p}\mathbf{p}^T, \text{tr}(\mathbf{C}_i\mathbf{Q}) \leq \beta_i, i = 1, 2, \\ \mathbf{p} \in \mathcal{B}_{\text{init}}, \text{tr}(\mathbf{D}_j\mathbf{Q}) \leq \gamma_j, \forall j \end{array} \right\} \quad (34)$$

is equivalent to the feasible set of problem (26), $\varphi(\mathcal{F}_{\text{init}})$ serves as the optimal value of (26). However, it is very difficult to obtain $\varphi(\mathcal{F}_{\text{init}})$ directly because $\mathcal{F}_{\text{init}}$ is a non-convex set. In order to overcome this difficulty, we generate a sequence of relaxed sets $\{\mathcal{F}_k\}$ to approach $\mathcal{F}_{\text{init}}$, and then the optimal value $\varphi(\mathcal{F}_{\text{init}})$ can be approached iteratively from above by solving a sequence of optimization problems to obtain $\{\varphi(\mathcal{F}_k)\}$. The sequence $\{\mathcal{F}_k\}$ should satisfy the following properties:

$$\begin{aligned}\mathcal{F}_1 &\supseteq \mathcal{F}_2 \supseteq \dots \supseteq \mathcal{F}_{\text{init}} \\ \lim_{k \rightarrow \infty} \varphi(\mathcal{F}_k) &= \varphi(\mathcal{F}_{\text{init}}) \\ \mathcal{F}_k &= \bigcup_{i=1}^k \mathcal{C}(\mathcal{B}_i), \forall k\end{aligned}\quad (35)$$

where $\mathcal{C}(\mathcal{B}_i)$ is a convex set to be defined in (36). The first property implies that $\{\varphi(\mathcal{F}_k)\}$ is a monotonically decreasing sequence bounded below by $\varphi(\mathcal{F}_{\text{init}})$, and the second property guarantees that $\varphi(\mathcal{F}_{\text{init}})$ is the greatest lower bounds of $\{\varphi(\mathcal{F}_k)\}$. The last property provides a trackable way to compute $\{\varphi(\mathcal{F}_k)\}$, that is,

$$\varphi(\mathcal{F}_k) = \max \left\{ \varphi(\mathcal{C}(\mathcal{B}_1)), \varphi(\mathcal{C}(\mathcal{B}_2)), \dots, \varphi(\mathcal{C}(\mathcal{B}_k)) \right\}, \forall k.$$

We also generate a sequence of lower bounds for $\varphi(\mathcal{F}_{\text{init}})$. Denote the optimal solution for $\varphi(\mathcal{F}_k)$ at the k -th iteration as $(\mathbf{Q}_k^{\text{opt}}, \mathbf{p}_k^{\text{opt}})$. We extract a feasible solution of problem (26) from $\mathbf{Q}_k^{\text{opt}}$, and the corresponding objective value of (26) serves as the lower bound of $\varphi(\mathcal{F}_{\text{init}})$. We denote this lower bound as $\varphi_L(\mathcal{F}_k)$.

In the remaining part of this section, we construct $\{\mathcal{F}_k\}$ explicitly as the union of convex sets $\{\mathcal{C}(\mathcal{B}_i)\}$. The ergodic

secrecy sum rate maximization algorithm over $\mathcal{C}(\mathcal{B}_i)$ and an efficient method to generate the lower bound $\varphi_L(\mathcal{F}_k)$ are investigated in the next subsection.

For convenience, we first define two convex sets $\mathcal{S}(\mathcal{B})$ and $\mathcal{C}(\mathcal{B})$ as

$$\begin{aligned}\mathcal{S}(\mathcal{B}) &\triangleq \left\{ (\mathbf{Q}, \mathbf{p}) \middle| \begin{array}{l} \mathbf{Q} - \mathbf{L}_P(\mathcal{B}) - \mathbf{L}_P(\mathcal{B})^T + \mathbf{l}(\mathcal{B}) \cdot \mathbf{l}(\mathcal{B})^T \geq \mathbf{0}, \\ \mathbf{Q} - \mathbf{U}_P(\mathcal{B}) - \mathbf{U}_P(\mathcal{B})^T + \mathbf{u}(\mathcal{B}) \cdot \mathbf{u}(\mathcal{B})^T \geq \mathbf{0}, \\ \mathbf{Q} - \mathbf{L}_P(\mathcal{B}) - \mathbf{U}_P(\mathcal{B})^T + \mathbf{l}(\mathcal{B}) \cdot \mathbf{u}(\mathcal{B})^T \geq \mathbf{0}, \\ \mathbf{l}(\mathcal{B}) \leq \mathbf{p} \leq \mathbf{u}(\mathcal{B}) \end{array} \right\} \\ \mathcal{C}(\mathcal{B}) &\triangleq \left\{ (\mathbf{Q}, \mathbf{p}) \middle| \begin{array}{l} \mathbf{Q} \succeq \mathbf{p}\mathbf{p}^T, \text{tr}(\mathbf{C}_i\mathbf{Q}) \leq \beta_i, i = 1, 2, \\ (\mathbf{Q}, \mathbf{p}) \in \mathcal{S}(\mathcal{B}), \text{tr}(\mathbf{D}_j\mathbf{Q}) \leq \gamma_j, \forall j \end{array} \right\}\end{aligned}\quad (36)$$

where $\mathbf{L}_P(\mathcal{B}) = \mathbf{l}(\mathcal{B}) \cdot \mathbf{p}^T$ and $\mathbf{U}_P(\mathcal{B}) = \mathbf{u}(\mathcal{B}) \cdot \mathbf{p}^T$. The following two propositions are the foundation for constructing $\{\mathcal{F}_k\}$.

Proposition 1: If we split the initial hyperrectangle $\mathcal{B}_{\text{init}}$ into K smaller hyperrectangles such that $\mathcal{B}_{\text{init}} = \mathcal{B}_1 \cup \dots \cup \mathcal{B}_K$, then $\mathcal{F}_{\text{init}} \subseteq \mathcal{C}(\mathcal{B}_1) \cup \dots \cup \mathcal{C}(\mathcal{B}_K)$.

Proof: We rewrite $\mathcal{F}_{\text{init}}$ as the union of K subsets

$$\mathcal{F}_{\text{init}} = \bigcup_{i=1}^K \bar{\mathcal{F}}_i \quad (37)$$

where $\bar{\mathcal{F}}_i$ are given by

$$\bar{\mathcal{F}}_i = \{(\mathbf{Q}, \mathbf{p}) | (\mathbf{Q}, \mathbf{p}) \in \mathcal{F}_{\text{init}}, \mathbf{p} \in \mathcal{B}_i\}. \quad (38)$$

For any $(\mathbf{Q}, \mathbf{p}) \in \bar{\mathcal{F}}_i$, the following inequalities hold

$$(\mathbf{p} - \mathbf{l}(\mathcal{B}_i)) \cdot (\mathbf{p} - \mathbf{l}(\mathcal{B}_i))^T \geq \mathbf{0} \quad (39)$$

$$(\mathbf{p} - \mathbf{u}(\mathcal{B}_i)) \cdot (\mathbf{p} - \mathbf{u}(\mathcal{B}_i))^T \geq \mathbf{0} \quad (40)$$

$$(\mathbf{p} - \mathbf{l}(\mathcal{B}_i)) \cdot (\mathbf{p} - \mathbf{u}(\mathcal{B}_i))^T \leq \mathbf{0} \quad (41)$$

$$\mathbf{Q} = \mathbf{p} \cdot \mathbf{p}^T, \mathbf{l}(\mathcal{B}_i) \leq \mathbf{p} \leq \mathbf{u}(\mathcal{B}_i). \quad (42)$$

Thus, $\bar{\mathcal{F}}_i$ can be rewritten as

$$\bar{\mathcal{F}}_i = \{(\mathbf{Q}, \mathbf{p}) | (\mathbf{Q}, \mathbf{p}) \in \mathcal{F}_{\text{init}}, \mathbf{p} \in \mathcal{B}_i\} \cap \mathcal{S}(\mathcal{B}_i). \quad (43)$$

By relaxing $\mathbf{Q} = \mathbf{p}\mathbf{p}^T$ in $\bar{\mathcal{F}}_i$ into $\mathbf{Q} \succeq \mathbf{p}\mathbf{p}^T$, one can easily obtain the following

$$\bar{\mathcal{F}}_i \subseteq \mathcal{C}(\mathcal{B}_i), \forall i. \quad (44)$$

Therefore, $\mathcal{F}_{\text{init}} \subseteq \mathcal{C}(\mathcal{B}_1) \cup \dots \cup \mathcal{C}(\mathcal{B}_K)$ and the result follows. \blacksquare

Proposition 2: If we split a hyperrectangle \mathcal{B} into two smaller hyperrectangles \mathcal{B}_1 and \mathcal{B}_2 such that $\mathcal{B} = \mathcal{B}_1 \cup \mathcal{B}_2$ and $\mathcal{B}_1 \cap \mathcal{B}_2 = \emptyset$, then $\mathcal{C}(\mathcal{B}_1) \cup \mathcal{C}(\mathcal{B}_2) \subseteq \mathcal{C}(\mathcal{B})$.

Proof: The proof is omitted here due to space limitations. \blacksquare

With the help of Proposition 1, the first relaxed set \mathcal{F}_1 is obtained

$$\mathcal{F}_1 = \mathcal{C}(\mathcal{B}_{\text{init}}). \quad (45)$$

Similarly, in the second iteration, we can generate \mathcal{F}_2 by partitioning the initial hyperrectangle $\mathcal{B}_{\text{init}}$ into two non-intersection hyperrectangles \mathcal{B}_1 and \mathcal{B}_2

$$\mathcal{F}_2 = \mathcal{C}(\mathcal{B}_1) \cup \mathcal{C}(\mathcal{B}_2) \subseteq \mathcal{F}_1. \quad (46)$$

We continue this process to generate a sequence of asymptotically tight sets $\{\mathcal{F}_k\}$. At the k -th iteration, $\mathcal{B}_{\text{init}}$ is split into k non-intersection hyperrectangles $\mathcal{B}_1, \mathcal{B}_2, \dots, \mathcal{B}_k$ such that

$$\mathcal{F}_k = \mathcal{C}(\mathcal{B}_1) \cup \dots \cup \mathcal{C}(\mathcal{B}_k). \quad (47)$$

The proposed algorithm is summarized as follows.

Algorithm 1 : The outer approximation algorithm

- 1) Initialization: given the maximum number of iterations K_{\max} . Set $k = 1$, $\mathbb{B} = \{\mathcal{B}_{\text{init}}\}$, $U_1 = \varphi(\mathcal{C}(\mathcal{B}_{\text{init}}))$ and $L_1 = \varphi_L(\mathcal{C}(\mathcal{B}_{\text{init}}))$.
- 2) Stopping criterion: if $k \leq K_{\max}$ go to step (3), otherwise STOP.
- 3) Partition criterion:
 - a) select $\mathcal{B}_g = \arg \max_{\mathcal{B} \in \mathbb{B}} \{\varphi(\mathcal{C}(\mathcal{B}))\}$.
 - b) split \mathcal{B}_g along any of its longest edge into two small hyperrectangles, \mathcal{B}_I and \mathcal{B}_{II} , with equal volume.
 - c) remove \mathcal{B}_g from \mathbb{B} , and add \mathcal{B}_I and \mathcal{B}_{II} into \mathbb{B} .
 - d) compute the upper and lower bound of $\varphi(\mathcal{F}_{\text{init}})$

$$U_{k+1} = \max_{\mathcal{B} \in \mathbb{B}} \{\varphi(\mathcal{C}(\mathcal{B}))\}$$

$$L_{k+1} = \min_{\mathcal{B} \in \mathbb{B}} \{\varphi_L(\mathcal{C}(\mathcal{B}))\}.$$

- 4) Set $k := k + 1$ and go to step (2).
-

The convergence of Algorithm 1 is presented by the following proposition.

Proposition 3: The sequence $\{\varphi(\mathcal{F}_k)\}$ converges in a finite number of iterations to a value which is arbitrary close to $\varphi(\mathcal{F}_{\text{init}})$, i.e., $\forall \varepsilon > 0, \exists K > 0$, such that $k > K$ implies $\varphi(\mathcal{F}_{\text{init}}) < \varphi(\mathcal{F}_k) < \varphi(\mathcal{F}_{\text{init}}) + \varepsilon$.

Proof: The proof is omitted here due to space limitations. \blacksquare

C. DC Optimization Over the Convex Set

In this subsection, we employ the convex-concave procedure to maximize the ergodic sum rate over the convex set $\mathcal{C}(\mathcal{B})$. The optimization problem is given below

$$\begin{aligned} \varphi(\mathcal{C}(\mathcal{B})) &= \underset{\mathbf{Q}, \mathbf{p}}{\text{maximize}} \quad F(\mathbf{Q}) - G(\mathbf{Q}) \\ &\text{subject to} \quad (\mathbf{Q}, \mathbf{p}) \in \mathcal{C}(\mathcal{B}). \end{aligned} \quad (48)$$

Since $F(\mathbf{Q}) - G(\mathbf{Q})$ is a DC function, the convex part $F(\mathbf{Q})$ can be lower estimated by its tangent at any point $\mathbf{Q}_c \succeq 0$

$$F(\mathbf{Q}) \geq F(\mathbf{Q}_c) + \text{tr}\left\{\nabla F(\mathbf{Q}_c)^T(\mathbf{Q} - \mathbf{Q}_c)\right\}. \quad (49)$$

Therefore, by replacing the objective function in (48) with a concave approximation

$$\hat{F}(\mathbf{Q}; \mathbf{Q}_c) = F(\mathbf{Q}_c) + \text{tr}\left\{\nabla F(\mathbf{Q}_c)^T(\mathbf{Q} - \mathbf{Q}_c)\right\} - G(\mathbf{Q}),$$

we obtain the following concave maximization problem

$$\begin{aligned} &\underset{\mathbf{Q}, \mathbf{p}}{\text{maximize}} \quad \hat{F}(\mathbf{Q}; \mathbf{Q}_c) \\ &\text{subject to} \quad (\mathbf{Q}, \mathbf{p}) \in \mathcal{C}(\mathcal{B}). \end{aligned} \quad (50)$$

The convex-concave procedure obtains a local maxima of (48) by solving a sequence of concave maximization problems (50) with different \mathbf{Q}_c . Once the optimal solution of (50) in the first iteration is found at some initial \mathbf{Q}_c , denoted as \mathbf{Q}_1^* , the algorithm replaces \mathbf{Q}_c with \mathbf{Q}_1^* and then solve (50) again. At the n -th iteration, the optimal solution of (50) is obtained by replacing \mathbf{Q}_c with \mathbf{Q}_{n-1}^* , which is the optimal solution at the $(n-1)$ -th iteration. The convex-concave procedure can be found in [24].

By embedding the convex-concave procedure into Algorithm 1, we can obtain a near optimal solution $\mathbf{Q}_k^{\text{opt}}$ at the k -th iteration of Algorithm 1. After that, we need to extract a feasible solution of (25) from $\mathbf{Q}_k^{\text{opt}}$, and the ergodic secrecy sum rate under this feasible solution serves as the lower bound $\varphi_L(\mathcal{F}_k)$. Then feasible precoders $(\mathbf{P}_1, \mathbf{P}_2)$ can be recovered from this feasible solution based on (14) and (17). There are several rank one approximation methods to do this, and we adopt the Gaussian randomization procedure proposed in [25].

IV. NUMERICAL RESULTS

In this section, we provide an example to demonstrate the performance of the proposed algorithm. We consider a secure cognitive radio system that has two STs, one SR, one ED, and one PR. Each node in the system is equipped with two antennas. The maximum transmit power is constrained by $\beta_1 = \beta_2 = \beta = 2$. The interference threshold is set as $\gamma_1 = 0.2$. All STs adopt QPSK modulation, and the noise variance $\sigma_R^2 = \sigma_E^2 = \sigma^2$. Then the SNR can be defined as $\text{SNR} = \beta/\sigma^2$. The channel correlation matrices are given by

$$\begin{aligned} \mathbf{H} &= \mathbf{C}(0.25), \mathbf{\Psi}_{h_1} = \mathbf{C}(0.95), \mathbf{\Psi}_{h_2} = \mathbf{C}(0.9) \\ \mathbf{\Phi}_g &= \mathbf{C}(0.75), \mathbf{\Psi}_{g_1} = \mathbf{C}(0.5), \mathbf{\Psi}_{g_2} = \mathbf{C}(0.3) \\ \mathbf{\Phi}_f &= \mathbf{C}(0.5), \mathbf{\Psi}_{f_1} = \mathbf{C}(0.8), \mathbf{\Psi}_{f_2} = \mathbf{C}(0.5) \end{aligned} \quad (51)$$

where $\mathbf{C}(\rho)$ is the exponential correlation model:

$$[\mathbf{C}(\rho)]_{i,j} = \rho^{|i-j|}, \quad \forall (i, j), \rho \in [0, 1]. \quad (52)$$

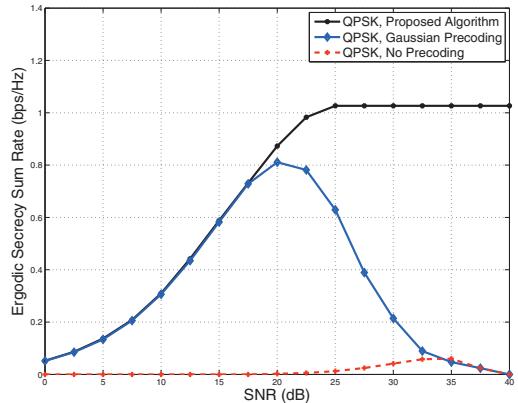


Fig. 2: The interference threshold at the PR is 10 dB less than the transmit power ($\gamma_1 = 0.2$).

In Fig. 2, we compare our proposed algorithm with the Gaussian precoding method and no precoding case. The Gaussian precoding method aims to maximize the ergodic secrecy sum rate under Gaussian signaling

$$\begin{aligned} & \underset{\mathbf{Q}_1, \mathbf{Q}_2}{\text{maximize}} \quad E_{\mathbf{H}, \mathbf{G}} \left\{ f(\mathbf{Q}_1, \mathbf{Q}_2) - g(\mathbf{Q}_1, \mathbf{Q}_2) \right\} \\ & \text{subject to} \quad \text{tr}(\mathbf{Q}_i) \leq \beta_i, \quad i = 1, 2 \\ & \quad \text{tr}(\mathbf{Q}_1 \Psi_{f_{1,j}} + \mathbf{Q}_2 \Psi_{f_{2,j}}) \leq \gamma_j / \phi_j, \quad \forall j \end{aligned} \quad (53)$$

where $f(\mathbf{Q}_1, \mathbf{Q}_2) = \log \det(\mathbf{I} + 1/\sigma_R^2 \cdot \sum_{i=1}^2 \mathbf{H}_i \mathbf{Q}_i \mathbf{H}_i^H)$ and $g(\mathbf{Q}_1, \mathbf{Q}_2) = \log \det(\mathbf{I} + 1/\sigma_E^2 \cdot \sum_{i=1}^2 \mathbf{G}_i \mathbf{Q}_i \mathbf{G}_i^H)$; \mathbf{Q}_i is the transmit covariance matrix of the i -th ST, $i = 1, 2$. Problem (53) is a DC optimization problem and thus can be solved by DC algorithms. After obtaining the optimal transmit covariance matrices $(\bar{\mathbf{Q}}_1, \bar{\mathbf{Q}}_2)$, the ergodic secrecy sum rate can be evaluated under the corresponding precoders $(\bar{\mathbf{Q}}_1^{1/2}, \bar{\mathbf{Q}}_2^{1/2})$ and QPSK inputs. No precoding case sets the precoders as $(\mathbf{P}_1, \mathbf{P}_2) = (\mathbf{I}, \mathbf{I})$, and then scales down its power to meet all the average interference constraints.

Results in Fig. 2 indicate that in the low SNR regime, our proposed algorithm and the Gaussian precoding method have the same performance. This is because the low SNR expansion of the mutual information is irrelevant to the input distribution [10]. In the medium and high SNR regimes, our proposed algorithm offers much higher sum rate than the Gaussian precoding method. The normalized precoders $(\frac{1}{\sigma} \mathbf{P}_1, \frac{1}{\sigma} \mathbf{P}_2)$ obtained by our algorithm remain unchanged in the high SNR regime, thus the ergodic secrecy sum rate remains unchanged. In contrast, both $\bar{I}(\mathbf{s}_1, \mathbf{s}_2; \mathbf{y}_R)$ and $\bar{I}(\mathbf{s}_1, \mathbf{s}_2; \mathbf{z}_E)$ approach 6 bps/Hz under precoders designed by the Gaussian precoding method in the high SNR regime, thus the corresponding ergodic secrecy sum rate approaches zero. No precoding case has the worst performance because it does not exploit any statistical CSI.

V. CONCLUSION

This paper has investigated the precoder design for CMAC-WT under finite-alphabet inputs and statistical CSI. We have presented a two-layer precoding algorithm to maximize the ergodic secrecy sum rate. The work has expanded the existing study on the Gaussian multiple-access wiretap channel in the following three aspects: 1) The practical finite-alphabet signaling and statistical CSI are taken into consideration. 2) The more general scenario of multiple PRs are incorporated into the system model. 3) Each node in the system has multiple antennas. Numerical result has shown that our proposed algorithm outperforms the Gaussian precoding method and no precoding case.

ACKNOWLEDGMENT

The work of C. Xiao was supported in part by US National Science Foundation under grants ECCS-1231848 and ECCS-1539316. The work of M. Tao was supported by the National Science Foundation of China under grant 61322102. This work has been carried out while Mr. Juening Jin is visiting Missouri University of Science and Technology.

REFERENCES

- [1] J. Mitola, "Cognitive radio: An integrated agent architecture for software defined radio," Ph.D. dissertation, KTH, Stockholm, Sweden, 2000.
- [2] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, no. 4, pp. 656–715, 1949.
- [3] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, 1975.
- [4] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, 1978.
- [5] E. Tekin and A. Yener, "The general Gaussian multiple-access and two-way wiretap channels: Achievable rates and cooperative jamming," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2735–2751, 2008.
- [6] R. Bassily and S. Ulukus, "Ergodic secret alignment," *IEEE Trans. Inf. Theory*, vol. 58, no. 3, pp. 1594–1611, 2012.
- [7] J. Zhu, J. Mo, and M. Tao, "Cooperative secret communication with artificial noise in symmetric interference channel," *IEEE Commun. Lett.*, vol. 14, no. 10, pp. 885–887, 2010.
- [8] A. Lozano, A. M. Tulino, and S. Verdú, "Optimum power allocation for parallel Gaussian channels with arbitrary input distributions," *IEEE Trans. Inf. Theory*, vol. 52, no. 7, pp. 3033–3051, 2006.
- [9] C. Xiao and Y. R. Zheng, "On the mutual information and power allocation for vector Gaussian channels with finite discrete inputs," in *Proc. IEEE Globecom*, 2008, pp. 1–5.
- [10] F. Pérez-Cruz, M. R. Rodrigues, and S. Verdú, "MIMO Gaussian channels with arbitrary inputs: Optimal precoding and power allocation," *IEEE Trans. Inf. Theory*, vol. 56, no. 3, pp. 1070–1084, 2010.
- [11] C. Xiao, Y. R. Zheng, and Z. Ding, "Globally optimal linear precoders for finite alphabet signals over complex vector Gaussian channels," *IEEE Trans. Signal Process.*, vol. 59, no. 7, pp. 3301–3314, 2011.
- [12] M. Wang, W. Zeng, and C. Xiao, "Linear precoding for MIMO multiple access channels with finite discrete inputs," *IEEE Trans. Wireless Commun.*, vol. 10, no. 11, pp. 3934–3942, 2011.
- [13] W. Zeng, C. Xiao, J. Lu, and K. B. Letaief, "Globally optimal precoder design with finite-alphabet inputs for cognitive radio networks," *IEEE J. Sel. Areas Commun.*, vol. 30, no. 10, pp. 1861–1874, 2012.
- [14] W. Zeng, C. Xiao, M. Wang, and J. Lu, "Linear precoding for finite-alphabet inputs over MIMO fading channels with statistical CSI," *IEEE Trans. Signal Process.*, vol. 60, no. 6, pp. 3134–3148, 2012.
- [15] S. Bashar, Z. Ding, and C. Xiao, "On secrecy rate analysis of MIMO wiretap channels driven by finite-alphabet input," *IEEE Trans. Commun.*, vol. 60, no. 12, pp. 3816–3825, 2012.
- [16] Y. Wu, C. Xiao, Z. Ding, X. Gao, and S. Jin, "Linear precoding for finite-alphabet signaling over MIMOME wiretap channels," *IEEE Trans. Veh. Technol.*, vol. 61, no. 6, pp. 2599–2612, 2012.
- [17] J. Harshan and B. S. Rajan, "A novel power allocation scheme for two-user GMAC with finite input constellations," *IEEE Trans. Wireless Commun.*, vol. 12, no. 2, pp. 818–827, 2013.
- [18] S. Vishwakarma and A. Chockalingam, "Decode-and-forward relay beamforming for secrecy with finite-alphabet input," *IEEE Commun. Lett.*, vol. 17, no. 5, pp. 912–915, 2013.
- [19] ———, "Power allocation in MIMO wiretap channel with statistical CSI and finite-alphabet input," in *Proc. National Conf. Commun.*, 2014, pp. 1–6.
- [20] M. Girnyk, M. Vehkapera, L. K. Rasmussen *et al.*, "Large-system analysis of correlated MIMO multiple access channels with arbitrary signaling in the presence of interference," *IEEE Trans. Wireless Commun.*, vol. 13, no. 4, pp. 2060–2073, 2014.
- [21] C. Xiao, J. Wu, S.-Y. Leong, Y. R. Zheng, and K. Letaief, "A discrete-time model for triply selective MIMO Rayleigh fading channels," *IEEE Trans. Wireless Commun.*, vol. 3, no. 5, pp. 1678–1688, 2004.
- [22] E. Telatar, "Capacity of multi-antenna Gaussian channels," *Eur. Trans. Telecommun.*, vol. 10, no. 6, pp. 585–595, 1999.
- [23] S. Boyd and L. Vandenberghe, *Convex optimization*. Cambridge university press, 2004.
- [24] A. Khabbazibasmenj, F. Roemer, S. A. Vorobyov, and M. Haardt, "Sum-rate maximization in two-way AF MIMO relaying: Polynomial time solutions to a class of DC programming problems," *IEEE Trans. Signal Process.*, vol. 60, no. 10, pp. 5478–5493, 2012.
- [25] Z.-Q. Luo, W.-K. Ma, A.-C. So, Y. Ye, and S. Zhang, "Semidefinite relaxation of quadratic optimization problems," *IEEE Signal Process. Mag.*, vol. 27, no. 3, pp. 20–34, 2010.