Transmit Signal Design for MIMO Wiretap Channels with Statistical CSI and Arbitrary Inputs

Sina Rezaei Aghdam and Tolga M. Duman

Dept. of Electrical and Electronics Engineering
Bilkent University, Ankara, Turkey, TR 06800
Emails: {aghdam, duman}@ee.bilkent.edu.tr

***Abstract*—We propose transmit optimization techniques for multi-input multi-output (MIMO) wiretap channels with statistical channel state information (CSI) at the transmitter. We consider doubly correlated channels towards the legitimate receiver and the eavesdropper. The aim is to maximize the secrecy rates using the knowledge of the channel correlation matrices. We develop gradient-descent based optimization algorithms for obtaining the optimal transmit signals for both Gaussian and finite-alphabet inputs. Furthermore, we introduce a joint precoder and artificial noise (AN) design scheme. We demonstrate the efficacy of the proposed schemes via numerical examples.**

I. Introduction

Securing wireless communications at the physical layer serves as an appealing approach to replace the conventional key-based solutions, especially in decentralized networks where key management is expensive. The idea in physical layer security is to exploit the inherent randomness of the channel to allow a transmitter to deliver its messages to a legitimate receiver while making them unintelligible at an eavesdropper [1].

Establishing the fundamental limits for secure transmission rates has been one of the most important objectives of the studies in the area of physical layer security, and a variety of channel models with different assumptions on the transmitter's knowledge of the channel state information (CSI) have been investigated (see [2] for a survey). A common assumption in many of these studies is that the transmitter is capable of estimating at least the instantaneous main channel coefficient. However, in fast fading scenarios, the transmitter may not be able to track the rapidly varying channel. An initial study on the secrecy capacity of the fast faded multi-antenna wiretap channel has been reported in [3] where it has been shown that when both the main and the eavesdropper's channels have independent identically distributed (i.i.d.) complex Gaussian entries with zero-mean and unit variance, the secrecy capacity achieving input is Gaussian without prefixing. The authors in [4] have studied MIMO wiretap channels with statistical CSI in semi-correlated scenarios with correlation at the transmitter side only. So as to maximize the ergodic secrecy rates, they have proposed transmit precoding schemes which rely on statistical waterfilling and generalized singular value decomposition (GSVD)-based beamforming.

978-1-5386-3531-5/17/$31.00 © 2017 IEEE

In this paper, we focus on fast Rayleigh faded doubly correlated channels towards the legitimate receiver and the eavesdropper, and assume that the transmitter only knows the transmit and receive correlation matrices corresponding to both channels. First, with the assumption that the transmitter employs Gaussian signaling, we propose an input covariance matrix optimization algorithm which relies on gradient-based updating. We demonstrate via numerical examples that this scheme achieves higher ergodic secrecy rates with respect to the solutions in [4]. Furthermore, we introduce a signal design algorithm for a more practical scenario where the channel inputs are drawn from a finite-alphabet. Transmit signal design for secrecy rate maximization over MIMO wiretap channels under finite-alphabet inputs with perfect and partial CSI at the transmitter have been addressed in [5] and [6], respectively. In [6], a joint precoder and AN design algorithm is proposed with the aid of the instantaneous CSI of the main channel along with the statistical CSI of the eavesdropper. Similar to [7], it was assumed that AN is injected along the null-space of the main channel and hence, no degradation occurs in the reception of the legitimate receiver. On the other hand, injection of AN along the null-space of the main channel is not possible when the transmitter only knows the statistics of the channels. Hence, we propose a joint precoder and AN design algorithm in which the AN can be injected in all directions spanned by the main channel. In the proposed scheme, the data and the AN precoder matrices are optimized in a manner that the ergodic secrecy rate is maximized.

The remainder of this paper is organized as follows. In the next section, we describe the system model under consideration. In Sections III and IV, we propose transmit signal design algorithms with Gaussian signaling and finite-alphabet inputs, respectively. Section V presents numerical examples, and finally, Section VI concludes the paper.

Notation: Vectors and matrices are denoted by lowercase and uppercase bold letters, respectively. The expectation of a random variable A is represented by $\mathbb{E}_A\{.\}$. $(.)^H$ and $\| \, . \, \|$ denote the Hermitian and Frobenius norm operations, respectively.

II. System Model

Consider a general multiple-input-multiple-output-multiple-antenna eavesdropper (MIMOME) wiretap channel. The number of antennas at the transmitter (Alice), the legitimate receiver (Bob) and the eavesdropper (Eve) are N_t, N_{r_b} and N_{r_e}, respectively. The received vectors at Bob and Eve are given by

$$\mathbf{y} = \mathbf{H}_b\mathbf{x} + \mathbf{n}_y, \quad \mathbf{z} = \mathbf{H}_e\mathbf{x} + \mathbf{n}_z, \tag{1}$$

where $\mathbf{H}_b$ and $\mathbf{H}_e$ are the $N_{r_b} \times N_t$ and $N_{r_e} \times N_t$ channel matrices corresponding to the legitimate receiver and the eavesdropper, respectively. Both channels are assumed to be doubly correlated. The receive correlation matrices corresponding to the main channel and the eavesdropper's channel are denoted by $\mathbf{\Psi}_{rb} \in \mathbb{C}^{N_{r_b} \times N_{r_b}}$ and $\mathbf{\Psi}_{re} \in \mathbb{C}^{N_{r_e} \times N_{r_e}}$, respectively, whereas the transmit correlation matrices are $\mathbf{\Psi}_{tb} \in \mathbb{C}^{N_t \times N_t}$ and $\mathbf{\Psi}_{te} \in \mathbb{C}^{N_t \times N_t}$. The channel matrices are as follows

$$\mathbf{H}_b = \mathbf{\Psi}_{rb}^{1/2}\hat{\mathbf{H}}_b\mathbf{\Psi}_{tb}^{1/2}, \quad \mathbf{H}_e = \mathbf{\Psi}_{re}^{1/2}\hat{\mathbf{H}}_e\mathbf{\Psi}_{te}^{1/2}, \tag{2}$$

where $\hat{\mathbf{H}}_b$ and $\hat{\mathbf{H}}_e$ are complex matrices with i.i.d. zero mean unit variance circularly symmetric complex Gaussian entries. $\mathbf{n}_y$ and $\mathbf{n}_z$ denote i.i.d. additive white Gaussian noise terms. The elements of noise vectors follow circularly symmetric complex Gaussian distributions, $\mathcal{CN}(0, \sigma^2_{\mathbf{n}_y})$ and $\mathcal{CN}(0, \sigma^2_{\mathbf{n}_z})$, respectively. Moreover, $\hat{\mathbf{H}}_b$, $\hat{\mathbf{H}}_e$, $\mathbf{n}_y$ and $\mathbf{n}_z$ are independent. The fading process is assumed to be ergodic. The legitimate receiver and the eavesdropper know their own channels perfectly. However, the transmitter does not know the realizations of the channels and it is only capable of acquiring the long-term statistics. In other words, the transmitter knows the correlation matrices $\mathbf{\Psi}_{tb}$, $\mathbf{\Psi}_{te}$, $\mathbf{\Psi}_{rb}$, $\mathbf{\Psi}_{re}$ and the noise variances at the receivers.

Regarding the channel input, we make different assumptions in different sections of the paper. In Section III, we consider zero-mean Gaussian distributed inputs the covariance matrix of which ($\mathbf{Q}_x = \mathbb{E}(\mathbf{x}\mathbf{x}^H)$) is subject to optimization. In Section IV, however, we consider a more practical scenario where the channel input is selected equiprobably from a discrete signal constellation. Under the assumption that Alice does not know the instantaneous $\mathbf{H}_b$ and $\mathbf{H}_e$, while Bob knows $\mathbf{H}_b$ and Eve knows both $\mathbf{H}_b$ and $\mathbf{H}_e$ perfectly, the secrecy capacity is given by [8, Eq. (3)]

$$C_s = \max_{p(x|w),p(w)} I(w; \mathbf{y}|\mathbf{H}_b) - I(w; \mathbf{z}|\mathbf{H}_e), \tag{3}$$

where w is an auxiliary random variable which satisfies the Markov chain $w \to \mathbf{x} \to \mathbf{y}, \mathbf{z}$. Determining the optimal joint distribution of $(w, \mathbf{x})$ and the resulting exact secrecy capacity is an open problem. Throughout this paper, we quantify secrecy using an achievable ergodic secrecy rate (a lower-bound on (3)) as

$$R_s = \left[I(\mathbf{x}; \mathbf{y}|\mathbf{H}_b) - I(\mathbf{x}; \mathbf{z}|\mathbf{H}_e)\right]^+. \tag{4}$$

III. Input Covariance Matrix Optimization

In this section, we assume that Alice employs Gaussian signaling and we tackle the ergodic secrecy rate maximization problem via optimizing the input covariance matrix using an iterative approach.

A. Optimization of Input Covariance

Our objective is to obtain a covariance matrix $\mathbf{Q}_x$ that is the optimizer of the following problem:

$$\begin{aligned} \max_{\mathbf{Q}_x} f(\mathbf{Q}_x) = \mathbb{E}_{\hat{\mathbf{H}}_b} \log\det\left(\mathbf{I}_{N_{r_b}} + \frac{1}{\sigma^2_{\mathbf{n}_y}}\mathbf{H}_b\mathbf{Q}_x\mathbf{H}_b^H\right) \\ - \mathbb{E}_{\hat{\mathbf{H}}_e} \log\det\left(\mathbf{I}_{N_{r_e}} + \frac{1}{\sigma^2_{\mathbf{n}_z}}\mathbf{H}_e\mathbf{Q}_x\mathbf{H}_e^H\right), \end{aligned} \tag{5}$$

$$\text{s.t.} \quad \text{tr}(\mathbf{Q}_x) = 1, \quad \mathbf{Q}_x \succeq 0. \tag{6}$$

The objective function $f(\mathbf{Q}_x)$ is a lower-bound on the achievable ergodic secrecy rate in (4). In order to solve the non-convex optimization problem in (5)-(6), we propose a numerical algorithm which iteratively searches for local maxima of $f(\mathbf{Q}_x)$ using a gradient-based update rule. In order to implement this algorithm, we obtain the gradient of the objective function with respect to $\mathbf{Q}_x$ as [9, Eq. (12)]

$$\begin{aligned} \nabla f(\mathbf{Q}_x) =& \mathbb{E}_{\hat{\mathbf{H}}_b}\left\{\mathbf{H}_b^H\left(\mathbf{I}_{N_{r_b}} + \frac{1}{\sigma^2_{\mathbf{n}_y}}\mathbf{H}_b\mathbf{Q}_x\mathbf{H}_b^H\right)^{-1}\mathbf{H}_b\right\} \\ &- \mathbb{E}_{\hat{\mathbf{H}}_e}\left\{\mathbf{H}_e^H\left(\mathbf{I}_{N_{r_e}} + \frac{1}{\sigma^2_{\mathbf{n}_z}}\mathbf{H}_e\mathbf{Q}_x\mathbf{H}_e^H\right)^{-1}\mathbf{H}_e\right\}. \end{aligned} \tag{7}$$

The iterative procedure for this optimization is given in Alg. 1. Once the covariance is updated using the gradient in (7), the power constraint, i.e., tr$(\mathbf{Q}_x) = 1$, and the positive semi-definiteness of the updated covariance matrix, i.e., $\mathbf{Q}_x \succeq 0$, need to be established. While the former is addressed using a normalization, the latter is handled heuristically. Particularly, without taking into account the positive semi-definiteness constraint, we run Alg. 1 with different initializations and we ignore those which produce non-positive semidefinite $\mathbf{Q}_x$'s. It is verified through numerical experiments that suitable starting points (e.g., solutions of [4]) lead to feasible solutions with a high probability.

IV. Precoder Design for Finite-Alphabet Inputs

Although Gaussian signals are secrecy capacity achieving in a variety of scenarios, the transmit signal design under Gaussian input assumption can be quite sub-optimal when applied to the practical signals drawn

```
Algorithm 1 Grad. Desc. for Maximizing $f(\mathbf{Q}_x)$ (or $g(\mathbf{P}_D)$)
Step 1: Initialize $\mathbf{Q}_1$ (or $\mathbf{P}_{D_1}$) with constraint tr$(\mathbf{Q}_x) = 1$ (or tr$(\mathbf{P}_D\mathbf{P}_D^H) \leq N_t$). Set step size $u$ and min. tolerance $u_{min}$
Step 2: Set $k = 1$, compute $f_1 = f(\mathbf{Q}_1)$ (or $g_1 = g(\mathbf{P}_{D_1})$)
Step 3: Compute $\nabla_{Q_1} f(\mathbf{Q}_1)$ using (7) (or $\nabla_{\mathbf{P}_D} g(\mathbf{P}_D)$ using (13) )
Step 4: If $u \geq u_{min}$ goto Step 5, otherwise Stop algorithm and return $\mathbf{Q}_k$ (or $\mathbf{P}_D$)
Step 5: Calculate $\hat{\mathbf{Q}}_k = \mathbf{Q}_k + u\nabla_{\mathbf{Q}_k} f(\mathbf{Q})$ (or $\mathbf{P}_{D_k}$ using (12)).
Step 6: Compute $\hat{f} = f(\hat{\mathbf{Q}}_k)$ (or $\hat{g} = g(\hat{\mathbf{P}}_{D_k})$) If $\hat{f} \geq f_k$ (or $\hat{g} \geq g_k$) update $f_{k+1} = \hat{f}$ (or $g_{k+1} = \hat{g}$ ) and $\mathbf{Q}_{k+1} = \hat{\mathbf{Q}}_k$ (or $\mathbf{P}_{D_{k+1}} = \hat{\mathbf{P}}_{D_k}$) and goto Step 7, O/W let $u = 0.5u$ and goto Step 4
Step 7: $k = k + 1$ goto Step 3
```

from discrete constellations. With this motivation, in this section, we propose transmit signal design algorithms for practical finite-alphabet inputs.

A. Precoder Optimization

In this section, we assume that Alice transmits a precoded signal as

$$\mathbf{x} = \mathbf{P}_D \mathbf{s}, \tag{8}$$

where $\mathbf{s} \in \mathbb{C}^{N_t \times 1}$ is the channel input which is drawn from an equiprobable discrete constellation set such as quadrature amplitude modulation (QAM) or phase shift keying (PSK) with modulation order M and identity covariance ($\mathbb{E}\{\mathbf{s}\mathbf{s}^H\} = \mathbf{I}$). $\mathbf{P}_D \in \mathbb{C}^{N_t \times N_t}$ is the precoding matrix which is subject to optimization. In evaluation of (4), the mutual information expression corresponding to the main channel is calculated as [10]

$$I(\mathbf{s};\mathbf{y}|\mathbf{H}_b) = N_t \log M - \frac{1}{M^{N_t}} \times$$
$$\sum_{i=1}^{M^{N_t}} \mathbb{E}_{\hat{\mathbf{H}}_b,\mathbf{n}_y} \log \sum_{j=1}^{M^{N_t}} \exp\left(-\frac{\|\mathbf{H}_b\mathbf{P}_D\mathbf{d}_{ij} + \mathbf{n}_y\|^2 - \|\mathbf{n}_y\|^2}{\sigma^2_{\mathbf{n}_y}}\right),$$

where $\mathbf{d}_{ij} = \mathbf{s}_i - \mathbf{s}_j$. Each vector $\mathbf{s}_i$ contains N_t symbols which are independently taken from the M-ary signal constellation. The mutual information expression corresponding to the eavesdropper's channel is calculated similarly.

With the assumption that the transmitter knows the correlation matrices $\mathbf{\Psi}_{tb}$, $\mathbf{\Psi}_{te}$, $\mathbf{\Psi}_{rb}$ and $\mathbf{\Psi}_{re}$ as well as the signal-to-noise ratio (SNR) values at the receivers, the objective is to obtain the optimal precoder matrix $\mathbf{P}_D$ which maximizes the ergodic secrecy rate in (4). To formulate this optimization problem, we consider a lower-bound on C_s given by

$$g(\mathbf{P}_D) = I(\mathbf{s};\mathbf{y}|\mathbf{H}_b) - I(\mathbf{s};\mathbf{z}|\mathbf{H}_e), \tag{9}$$

and define the relevant optimization problem as

$$\max_{\mathbf{P}_D} g(\mathbf{P}_D) \tag{10}$$

$$\text{s.t.} \quad \text{tr}(\mathbf{P}_D\mathbf{P}_D^H) \leq N_t. \tag{11}$$

Due to the nonconvexity of the problem in (10)-(11), we implement a numerical algorithm which iteratively search for local maxima of the objective function. This procedure is explained in Alg. 1. In this scheme, the precoder is updated as

$$\mathbf{P}_{D_{k+1}} = \left[\mathbf{P}_{D_k} + u\nabla_{\mathbf{P}_D} g(\mathbf{P}_{D_k})\right]^{\dagger}_{\text{tr}(\mathbf{P}_D\mathbf{P}_D^H) \leq N_t}, \tag{12}$$

where k and u are the iteration index and the step-size of the update, respectively, and $[.]^{\dagger}_{\text{tr}(\mathbf{P}_D\mathbf{P}_D^H) \leq N_t}$ stands for the normalization which guarantees the feasibility of the solution at each step. More specifically, for cases where the updated precoder matrix $\hat{\mathbf{P}}_{D_k}$ does not satisfy the constraint in (11), similar to [11], we adopt a normalization as $\hat{\mathbf{P}}_{D_k} = \sqrt{N_t/\text{tr}(\hat{\mathbf{P}}_{D_k}\hat{\mathbf{P}}^H_{D_k}})\hat{\mathbf{P}}_{D_k}$, which projects the solution onto the feasible set. In order to evaluate the gradient of $g(\mathbf{P}_D)$, we use the results in [11] to obtain

$$\nabla_{\mathbf{P}_D} g(\mathbf{P}_D) = \mathbb{E}_{\hat{\mathbf{H}}_b}\left\{\frac{\log_2 e}{\sigma^2_{\mathbf{n}_y}}\left(\mathbf{H}_b^H\mathbf{H}_b\mathbf{P}_D\mathbf{\Delta}_b(\mathbf{P}_D)\right)\right\}$$
$$- \mathbb{E}_{\hat{\mathbf{H}}_e}\left\{\frac{\log_2 e}{\sigma^2_{\mathbf{n}'_z}}\left(\mathbf{H}_e^H\mathbf{H}_e\mathbf{P}_D\mathbf{\Delta}_e(\mathbf{P}_D)\right)\right\}, \tag{13}$$

where $\mathbf{\Delta}_b(\mathbf{P}_D)$ and $\mathbf{\Delta}_e(\mathbf{P}_D)$ are the minimum mean square error matrices corresponding to estimation of $\mathbf{s}$ upon the observations at the legitimate receiver and the eavesdropper which are calculated using [11, Eq. (12)].

B. Joint Precoder and AN Optimization

In this section, we introduce a joint precoder and AN optimization scheme based on statistical CSI. Since the instantaneous CSI of the main channel is not known at the transmitter, it is not possible to inject AN in the null-space of $\mathbf{H}_b$. Therefore, we consider injection of a generalized AN which is allowed to be transmitted in all directions spanned by $\mathbf{H}_b$ [12] and we develop an optimization algorithm to obtain the optimal pair of data and AN precoders, which maximize the ergodic secrecy rate. Particularly, we assume that Alice transmits a signal as

$$\mathbf{x} = \mathbf{P}_D\mathbf{s} + \mathbf{P}_{AN}\mathbf{v}, \tag{14}$$

where $\mathbf{s}$ is the data signal and $\mathbf{v}$ stands for the AN signal that follows $\mathcal{CN}(0, \mathbf{I}_{N_t})$. $\mathbf{P}_D$ and $\mathbf{P}_{AN}$ are the precoder matrices for the data and the artificial noise signals, respectively. Although this AN degrades the reception both at the legitimate receiver and the eavesdropper, it is possible to optimize $\mathbf{P}_{AN}$ in a manner that the achievable rate at the eavesdropper is highly suppressed while the mutual information over the main channel undergoes less degradation.

The received vectors at the legitimate receiver and the eavesdropper are given as

$$\mathbf{y} = \mathbf{H}_b\mathbf{P}_D\mathbf{s} + \mathbf{H}_b\mathbf{P}_{AN}\mathbf{v} + \mathbf{n}_y, \tag{15}$$

$$\mathbf{z} = \mathbf{H}_e\mathbf{P}_D\mathbf{s} + \mathbf{H}_e\mathbf{P}_{AN}\mathbf{v} + \mathbf{n}_z. \tag{16}$$

The objective is to obtain the optimal $\mathbf{P}_D$ and $\mathbf{P}_{AN}$ by solving the following optimization problem

$$\max_{\mathbf{P}_D,\ \mathbf{P}_{AN}} g(\mathbf{P}_D, \mathbf{P}_{AN}) \tag{17}$$

$$\text{s.t.} \quad \text{tr}(\mathbf{P}_D\mathbf{P}_D^H) + \text{tr}(\mathbf{P}_{AN}\mathbf{P}_{AN}^H) \leq N_t, \tag{18}$$

Algorithm 2 Alternating Optimization for Maximizing $R_{s,l}$

```
Initialize $\lambda_h > \lambda_l = 0$, $\mathbf{P}_D$, $\mathbf{P}_{AN}$ and converg. criteria $\epsilon_L$ and $\epsilon_\lambda$:
Step 1: update $\lambda = \frac{1}{2}(\lambda_l + \lambda_h)$
Step 2: repeat:
    obtain optimal $\mathbf{P}_D$ with fixed $\mathbf{P}_{AN}$ similar to Alg. 1
    obtain optimal $\mathbf{P}_{AN}$ with fixed $\mathbf{P}_D$ similar to Alg. 1
until: consecutive values of $L(\mathbf{P}_D, \mathbf{P}_{AN}, \lambda)$ differ by less than $\epsilon_L$
Step 3: If $\text{tr}(\mathbf{P}_D\mathbf{P}_D^H) + \text{tr}(\mathbf{P}_{AN}\mathbf{P}_{AN}^H) < N_t$ then update $\lambda_h = \lambda$
If $\text{tr}(\mathbf{P}_D\mathbf{P}_D^H) + \text{tr}(\mathbf{P}_{AN}\mathbf{P}_{AN}^H) > N_t$ then update $\lambda_l = \lambda$
until: two consecutive values of $\lambda$ differ by less than $\epsilon_\lambda$.
```

where $g(\mathbf{P}_D, \mathbf{P}_{AN})$ is equal to the right hand side of (9). Since $\mathbf{n}'_y = \mathbf{H}_b\mathbf{P}_{AN}\mathbf{v} + \mathbf{n}_y$ is colored with covariance $\mathbf{K}_{\mathbf{n}'_y} = \mathbf{H}_b\mathbf{P}_{AN}\mathbf{P}_{AN}^H\mathbf{H}_b^H + \sigma^2_{\mathbf{n}_y}\mathbf{I}_{N_{r_b}}$, the mutual information over the main channel can be calculated after whitening the noise by pre-multiplying (15) with $\mathbf{K}_{\mathbf{n}'_y}^{-\frac{1}{2}}$ as

$$\mathbf{y}'' = \mathbf{K}_{\mathbf{n}'_y}^{-\frac{1}{2}}\mathbf{H}_b\mathbf{P}_D\mathbf{s} + \mathbf{n}''_y, \tag{19}$$

where $\mathbf{n}''_y$ is a zero-mean additive white Gaussian noise with unit variance. Therefore, we have

$$I(\mathbf{s};\mathbf{y}''|\mathbf{H}_b) = N_t \log M - \frac{1}{M^{N_t}} \times$$
$$\sum_{i=1}^{M^{N_t}} \mathbb{E}_{\hat{\mathbf{H}}_b,\mathbf{n}''_y} \log \sum_{j=1}^{M^{N_t}} \exp\left(-\|\mathbf{K}_{\mathbf{n}'_y}^{-\frac{1}{2}}\mathbf{H}_b\mathbf{P}_D\mathbf{d}_{ij} + \mathbf{n}''_y\|^2 + \|\mathbf{n}''_y\|^2\right).$$

The expression for $I(\mathbf{s};\mathbf{z}|\mathbf{H}_e)$ can be calculated by taking similar steps. Instead of directly tackling the non-convex optimization in (17)-(18), we solve a Lagrange dual optimization problem. The Lagrangian associated with (17)-(18) is given by

$$L(\mathbf{P}_D, \mathbf{P}_{AN}, \lambda) = g(\mathbf{P}_D, \mathbf{P}_{AN}) + \lambda(N_t - \text{tr}(\mathbf{P}_D\mathbf{P}_D^H) - \text{tr}(\mathbf{P}_{AN}\mathbf{P}_{AN}^H)), \tag{20}$$

where λ is the Lagrange dual variable. We define the Lagrange dual optimization problem as

$$\min_{\lambda > 0} D(\lambda), \tag{21}$$

where $D(\lambda)$ denotes the Lagrange dual function, which is given by

$$D(\lambda) = \max_{\mathbf{P}_D,\ \mathbf{P}_{AN}} L(\mathbf{P}_D, \mathbf{P}_{AN}, \lambda). \tag{22}$$

It can be seen that $D(\lambda)$ is a convex function in λ. To solve the problem in (21), similar to [13], we employ a bisection method as described in Alg. 2. In this scheme, when the subgradient $\nabla D(\lambda) = N_t - \text{tr}(\mathbf{P}_D\mathbf{P}_D^H) - \text{tr}(\mathbf{P}_{AN}\mathbf{P}_{AN}^H)$ is positive, λ is decreased and otherwise, it is increased.

In order to maximize the Lagrangian for a fixed λ, we update $\mathbf{P}_D$ and $\mathbf{P}_{AN}$ in an alternating fashion. To obtain the optimal $\mathbf{P}_D$ with a fixed $\mathbf{P}_{AN}$, and conversely, to obtain the optimal $\mathbf{P}_{AN}$ with a fixed $\mathbf{P}_D$, we employ gradient descent type algorithms similar to Alg. 1. Once the optimal λ is obtained, the corresponding $\mathbf{P}_D$ and $\mathbf{P}_{AN}$ become the desired precoder matrices, which serve as suboptimal solutions for the optimization in (17)-(18).

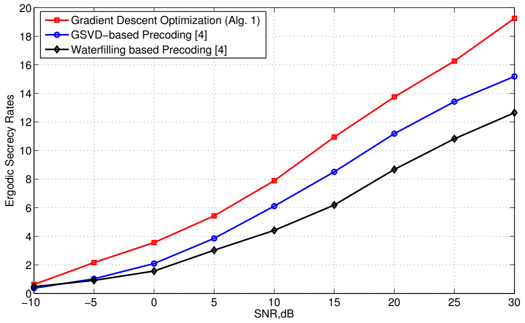

Fig. 1: Ergodic secrecy rates for Gaussian signaling.

V. Numerical Examples

In order to illustrate the performance of the proposed signal design schemes, we provide numerical examples for Gaussian inputs as well as inputs drawn from discrete constellations. We consider a MIMOME setup with $N_t = 4$, $N_{r_b} = 4$ and $N_{r_e} = 2$. Throughout the simulations, equal noise variances are assumed at the legitimate receiver and the eavesdropper. In order to evaluate ergodic secrecy rates, the average mutual information terms in (4) are evaluated using 500 realizations of $\hat{\mathbf{H}}_b$ and $\hat{\mathbf{H}}_e$.

A. Examples with Gaussian Signaling

In this subsection, we compare the secrecy performance of the proposed input covariance optimization approach with those of the existing suboptimal solution (statistical waterfilling based on $\mathbf{\Psi}_{tb}$, and GSVD-based precoding [4]). We assume that the legitimate receiver and the eavesdropper experience indoor-to-indoor and indoor-to-outdoor environments which correspond to highly correlated and partially decorrelated cases, respectively. To model these scenarios, we employ the experimentally validated model in [14]. We assume that $\mathbf{\Psi}_{tb}$ and $\mathbf{\Psi}_{rb}$ are as [14, Eq. (12)] and we consider $\mathbf{\Psi}_{te}$ and $\mathbf{\Psi}_{re}$ as given at the bottom of the page.

Fig. 1 depicts the ergodic secrecy rates for different transmission schemes. It is clear that the proposed input covariance optimization outperforms statistical waterfilling and GSVD-based precoding. One reason for this enhanced performance is that unlike the precoding schemes in [4], the proposed transmit signal design scheme is carried out by taking into account the transmit and receive correlation matrices corresponding to both channels. Furthermore, since in Alg. 1, the secrecy rate

$$\mathbf{\Psi}_{te} = \begin{bmatrix} 1 & -0.61+0.77i & 0.14-0.94i & 0.24+0.89i \\ -0.61-0.77i & 1 & -0.85+0.50i & 0.57-0.78i \\ 0.14+0.94i & -0.85-0.50i & 1 & -0.91+0.4i \\ 0.24-0.89i & 0.57+0.78i & -0.91-0.4i & 1 \end{bmatrix} \qquad \mathbf{\Psi}_{re} = \begin{bmatrix} 1 & -0.12-0.18i \\ -0.12+0.18i & 1 \end{bmatrix}$$

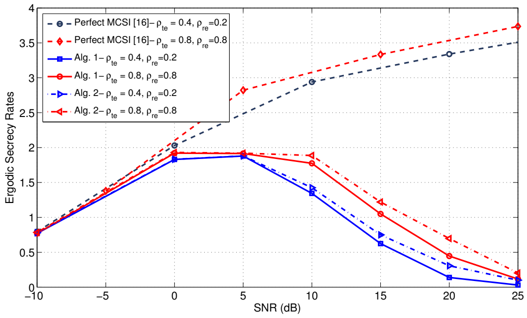

Fig. 2: Ergodic secrecy rates for BPSK input ($\rho_{tb} = 0.9$ and $\rho_{rb} = 0.6$).

increases from one iteration to the next, by initializing the proposed numerical algorithm with the covariance matrices corresponding to the ones obtained in [4], equal or higher secrecy rates are guaranteed to be attained.

B. Examples with Finite-Alphabet Inputs

In this subsection, we provide ergodic secrecy rates for the scenarios where the channel is driven by finite-alphabet inputs. We consider correlation matrices with exponentially decaying entries as $[\mathbf{\Psi}(\rho)]_{ij} = \rho^{|i-j|}$.

Fig. 2 depicts the ergodic secrecy rates with BPSK inputs. The proposed algorithms are shown to achieve positive ergodic secrecy rates at low and moderate SNRs. However, at high SNRs, under the finite-alphabet input constraint, secrecy rate drops to zero. This is in contrast to the scenarios with Gaussian signaling where achievable secrecy rates increase monotonically by increasing SNR (with $N_{rb} > N_{re}$, e.g., the results in Fig. 1).

We also observe that injection of AN provides slight improvements in moderate to high SNR regions. This behavior is different from the cases with uncorrelated channels where injection of AN with statistical CSI is a waste of power [15]. Fig. 2 also underlines the importance of availability of the main channel CSI at the transmitter. By jointly optimizing the precoder and the AN using the knowledge of instantaneous CSI of the main channel [16], considerably higher secrecy rates are attained with respect to the transmit signal design with statistical CSI only. More specifically, in the presence of instantaneous CSI of the main channel, the transmitter is capable of injecting AN in a more efficient manner where the noise leakage at the legitimate receiver is minimal (or zero when AN is injected along null-space of the main channel). Therefore, at high SNRs, the transmitter allocates a considerable portion of the total power to AN which efficiently suppresses the reception at the eavesdropper. However, when the instantaneous CSI of the main channel is not available, due to the leakage of AN at the legitimate receiver, allocating a large portion of the total power to AN does not help, and since at high SNRs the mutual information over both channels approach the saturation value of $N_t \log M$, ergodic secrecy rate drops to zero.

VI. Conclusions

We have provided transmit signal design algorithms for MIMO wiretap channels where the transmit and receive correlation matrices are the only CSI available at the transmitter. We have considered both Gaussian and finite-alphabet inputs. With Gaussian signaling, the proposed gradient-based input covariance matrix optimization outperforms the existing solutions. Under the finite-alphabet input assumption, we have shown that injecting AN with statistical CSI provides some improvements in the secrecy rate. However, it does not prevent secrecy rate from dropping to zero at high SNRs.

References

[1] A. D. Wyner, “The wire-tap channel,” *Bell Sys. Tech. J.*, vol. 54, pp. 1355–1387, 1975.

[2] A. Mukherjee, S. A. A. Fakoorian, J. Huang and A. L. Swindlehurst, “Principles of physical layer security in multiuser wireless networks: A survey,” *IEEE Commun. Surv. Tutorials*, vol. 16, no. 3, pp. 1550–1573, Third Quarter 2014.

[3] S.-C. Lin and C.-L. Lin, “On secrecy capacity of fast fading MIMOME wiretap channels with statistical CSIT,” *IEEE Trans. Wireless Commun.*, vol. 13, no. 6, pp. 3293–3306, 2014.

[4] M. A. Girnyk, F. Gabry, M. Vehkapera, L. K. Rasmussen, and M. Skoglund, “On the transmit beamforming for MIMO wiretap channels: Large-system analysis,” in *Proc. Int. Conf. Inf. Theoretic Secur. (ICITS)*, Singapore, Nov. 2013, pp. 90–102.

[5] 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, Jul. 2012.

[6] S. Rezaei Aghdam and T. M. Duman, “Low complexity precoding for MIMOME wiretap channels based on cut-off rate,” *IEEE Int. Symp. Inf. Theory (ISIT 2016)*, Barcelona, Jul. 2016, pp. 2988–2992.

[7] S. Goel and R. Negi, “Guaranteeing secrecy using artificial noise,” *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, June 2008.

[8] P.-H. Lin and E. Jorswieck, “On the fast fading gaussian wiretap channel with statistical channel state information at the transmitter,” *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 1, pp. 46–58, Jan. 2016.

[9] C.-K. Wen, J.-C. Chen, and P. Ting, “Robust transmitter design for amplify-and-forward MIMO relay systems exploiting only channel statistics,” *IEEE Trans. Wireless Commun.*, vol. 11, no. 2, pp. 668-682, Feb. 2012.

[10] 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*, LA, 2008.

[11] D. P. Palomar and S. Verdu, “Gradient of mutual information in linear vector Gaussian channels,” *IEEE Trans. Inf. Theory*, vol. 52, no. 1, pp. 141–154, Jan. 2006.

[12] P.-H. Lin S.-H. Lai, S.-C. Lin, and H.-J. Su, “On secrecy rate of the generalized artificial-noise assisted secure beamforming for wiretap channels,” *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1728–1740, Sep. 2013.

[13] H. Qin et al., “Power allocation and time-domain artificial noise design for wiretap OFDM with discrete inputs,” in *IEEE Trans. Wireless Commun.*, vol. 12, no. 6, pp. 2717–2729, June 2013.

[14] J. Kermoal, L. Schumacher, K. Pedersen, P. Mogensen, and F. Frederiksen, “A stochastic MIMO radio channel model with experimental validation,” *IEEE J. Sel. Areas Commun.*, vol. 20, no. 6, pp. 1211–1226, Jun. 2002.

[15] A. Zappone, P. H. Lin and E. Jorswieck, “Energy efficiency of confidential multi-antenna systems with artificial noise and statistical CSI,” in *IEEE J. Sel. Topics Signal Process.*, vol. 10, no. 8, pp. 1462–1477, Dec. 2016.

[16] S. Rezaei Aghdam, T. M. Duman, “Joint precoder and artificial noise design for MIMO wiretap channels with finite-alphabet inputs based on the cut-off rate,” *IEEE Trans. Wireless Commun.*, vol. 16, no. 6, pp. 3913–3923, Jun. 2017.