Low Complexity Precoding for MIMOME Wiretap Channels Based on Cut-off Rate

Sina Rezaei Aghdam   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 a low complexity transmit signal design scheme for achieving information-theoretic secrecy over a MIMO wiretap channel driven by finite-alphabet inputs. We assume that the transmitter has perfect channel state information (CSI) of the main channel and also knows the statistics of the eavesdropper's channel. The proposed transmission scheme relies on jointly optimizing the precoder matrix and the artificial noise so as to maximize the achievable secrecy rates. In order to lower the computational complexity associated with the transmit signal design, we employ a design metric using the cut-off rate instead of the mutual information. We formulate a gradient-descent based optimization algorithm and demonstrate via extensive numerical examples that the proposed signal design scheme can yield an enhanced secrecy performance compared with the existing solutions in spite of its relatively lower computational complexity. The impacts of the modulation order as well as the number of antennas at the transmitter and receiver ends on the achievable secrecy rates are also investigated.**

Index Terms — Physical layer security, MIMO wiretap channel, precoding, finite-alphabet inputs, cut-off rate.

I. Introduction

Due to its open nature, wireless communications are prone to eavesdropping attacks. On the other hand, with the ever-growing demand for the services which rely on data transfer over wireless networks, a challenging issue is the security of the transmitted information. Securing the communications at the physical layer is an alternative to the conventional higher-network-layer solutions, such as encryption, which can resolve the vulnerabilities and the complexities associated with key distribution and management. The basic principle of physical layer security, also known as information-theoretic security, is to exploit the randomness of the communication channels to allow a transmitter to deliver its message to an intended receiver while guaranteeing that a third party cannot infer any information about the transmitted message.

Among the studies in the area of physical layer security, the multiple-input multiple-output multiple-antenna eavesdropper (MIMOME) wiretap channels have been of particular interest [1]. While exploiting multiple antennas for transmission is, in general, an effective means to combat fading in wireless communications and to increase capacity or robustness, it does not give rise to an unconditional improvement from a physical layer security perspective. This is due to the fact that the unintended receiver is also capable of attaining an improved reception performance. Therefore, so as to achieve an increased secrecy using multiple-antennas, one needs to design a suitable transmission scheme which adopts an appropriate preprocessing algorithm so as to prevent the unintended receiver from benefiting fully from the MIMO performance gains.

An example of such a scheme is artificial noise (AN)-aided beamforming for which information is transmitted along the directions in which the legitimate receiver can experience a gain and on the contrary synthetic noise is sent along the directions which have the least effect on the reception performance of the intended receiver. Beamforming and precoding schemes are other examples of techniques which can be employed so as to transmit signals in directions which result in maximal signal quality difference at the legitimate receiver and the eavesdropper. With the assumption that the channel input is Gaussian, it has been shown in [2] and [3] that MIMOME channel can be decomposed into independent subchannels corresponding to the generalized eigenvectors, and the transmitter uses the subchannels over which the legitimate receiver has an advantage with respect to the eavesdropper.

While most of the studies in the literature are based on Gaussian source signals, more practical studies of the MIMOME channel, e.g., [4] and [5], have characterized the achievable secrecy rates of multiple-antenna wiretap channels with finite-alphabet inputs. In [4], a generalized singular value decomposition (GSVD) aided precoding has been proposed which decomposes the MIMOME channel into a bank of parallel subchannels and accordingly a power allocation is carried out. After proving that the proposed strategy in [4] is suboptimal, authors in [5] formulate the optimal transmit precoding scheme with the aid of the perfect channel state information (CSI) corresponding to the main channel and the evesdropper's channel.

While the algorithm proposed in [5] is optimal for the perfect CSI case, its solution for the cases without the perfect eavesdropper's CSI (ECSI) is suboptimal. This is due to the fact that, in the adopted transmit signal design approach, the power is assigned to the artificial noise only in the cases where excess power is available. In other words, no optimization is carried out over the power assigned to the artificial noise. To resolve this issue, in this paper, we propose a joint precoder

This work is supported by the Scientific and Technical Research Council of Turkey (TUBITAK) under the grant #113E223.

and artificial noise optimization scheme. Through numerical examples, we show that by jointly optimizing the precoder and the artificial noise, higher secrecy rates can be achieved compared to the case of optimization of the precoder matrix only, as done in [5].

We also introduce a low complexity alternative to directly maximizing the ergodic secrecy rates, as it possesses a high complexity due to the need for several evaluations of the mutual information expression which lacks a closed-form and can only be estimated using Monte Carlo methods. We formulate a cut-off rate based approximation for the ergodic secrecy rates and demonstrate that maximizing this approximate expression requires considerably lower computational effort. Moreover, we study the impact of the number of antennas as well as the modulation order on the secrecy rates attained with the proposed signalling method.

The paper is organized as follows. Section II describes the system model under consideration. In Section III, we formulate the joint signal and artificial noise design. Section IV presents several numerical examples which demonstrate the efficacy of the proposed transmit signal design scheme, and Section V concludes the paper.

Throughout the paper, vectors and matrices are denoted with the lowercase and uppercase bold letters. The expectation of a random variable X is represented by $\mathbb{E}_X\{.\}$ and $(.)^H$, $(.)^T$ and $\|\,.\,\|_F$ denote Hermitian, transpose and Frobenius norm operations.

II. System Model

Consider a general MIMOME wiretap channel. The transmitter, Alice, the legitimate receiver, Bob, and the eavesdropper, Eve, are assumed to be equipped with N_t, N_{r_b} and N_{r_e} antennas, respectively.

The received vectors at Bob and Eve can be written as:

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

$$\mathbf{z} = \mathbf{H}_e\mathbf{x} + \mathbf{n}_z, \tag{2}$$

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's channel and the eavesdropper's channel, respectively. The elements of the channel matrix $\mathbf{H}_b$ are independent and identically distributed (i.i.d.) with distribution $\mathcal{CN}(0, 1)$. We model the eavesdropper's channel as a doubly correlated fading MIMO channel, namely,

$$\mathbf{H}_e = \mathbf{\Psi}_r^{1/2}\hat{\mathbf{H}}_e\mathbf{\Psi}_t^{1/2}, \tag{3}$$

where $\mathbf{\Psi}_r$ and $\mathbf{\Psi}_t$ are the transmit and receive correlation matrices. $\hat{\mathbf{H}}_e$ is a complex matrix with i.i.d. zero mean unit variance Gaussian entries. $\mathbf{n}_y$ and $\mathbf{n}_z$ are 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. Furthermore, $\mathbf{H}_b$, $\mathbf{H}_e$, $\mathbf{n}_y$ and $\mathbf{n}_z$ are independent. It is assumed that the fading process is ergodic. The legitimate receiver and the eavesdropper know their own channels perfectly. The transmitter knows the instantaneous channel of the legitimate receiver and only the statistics of the eavesdropper's CSI. In other words, the transmitter knows the correlation matrices $\mathbf{\Psi}_r$ and $\mathbf{\Psi}_t$ and the noise variance at the eavesdropper. One example of the scenarios where transmitter can acquire such information is in cellular networks where eavesdropper is also a valid user of the network, long-term channel statistics of whom can be estimated by the transmitter.

With the assumption that $N_t > N_{r_b}$, the objective is to construct a precoded signal as

$$\mathbf{s} = \mathbf{Ps} + \alpha_{AN}\frac{\mathbf{V}_b}{\sqrt{N_t - N_{r_b}}}\mathbf{u}, \tag{4}$$

where $\mathbf{P} \in \mathbb{C}^{N_t \times N_t}$ is the precoding matrix and $\mathbf{s} \in \mathbb{C}^{N_t \times 1}$ is the transmitted signal vector with zero mean and identity covariance matrix. Each element of $\mathbf{s}$ is drawn from a discrete modulation constellation, such as M-QAM or M-PSK. $\mathbf{V}_b \in \mathbb{C}^{N_t \times (N_t - N_{r_b})}$ stands for the orthonormal basis of the null space of $\mathbf{H}_b$ and $\mathbf{u}$ denotes the artificial noise which follows $\mathcal{CN}(0, \mathbf{I}_{N_t - N_{r_b}})$. The portion of the power assigned to the artificial noise is determined by the coefficient α_{AN}.

We consider two channel models corresponding to the legitimate receiver as follows.

1) *Constant Main Channel*: For this scenario similar to [5] - [6], the ergodic secrecy rate can be calculated as

$$R_s = (I(\mathbf{s}; \mathbf{y}|\mathbf{H}_b) - \mathbb{E}_{\mathbf{H}_e} I(\mathbf{s}; \mathbf{z}|\mathbf{H}_e))^+. \tag{5}$$

2) *Fading Main Channel*: In this case, we assume that the channel gains are fixed during each coherence interval whereas they change independently from one coherence interval to the next. Furthermore, each coherence interval is large enough so that random coding arguments can be invoked. In this scenario, the secrecy rate is calculated using [7]

$$R_s = \mathbb{E}_{\mathbf{H}_b, \mathbf{H}_e}\big(I(\mathbf{s}; \mathbf{y}|\mathbf{H}_b) - I(\mathbf{s}; \mathbf{z}|\mathbf{H}_e)\big)^+. \tag{6}$$

III. Joint Precoder and Artificial Noise Design

With the aid of the instantaneous knowledge of the main channel and the statistical knowledge of the eavesdropper's channel, we seek to find the optimal $\mathbf{P}$ and α_{AN} which maximize the ergodic secrecy rate, R_s. This optimization problem is given as

$$\max_{\mathbf{P},\ \alpha_{AN}} \ R_s \tag{7}$$

$$\text{s.t.} \quad \text{tr}(\mathbf{PP}^H) + \alpha^2_{AN} \leq N_t. \tag{8}$$

A. Direct Maximization of R_s

Due to the nonconvexity of the problem in (7)-(8), obtaining a closed-form globally optimal solution is intractable. However, it is possible to implement numerical algorithms which iteratively search for local maxima of the objective function. First, we formulate the optimization over $\mathbf{P}$ with a fixed α_{AN}. In this case, the optimization problem can be formulated as

$$\max_{\mathbf{P}} \ (I(\mathbf{s}; \mathbf{y}|\mathbf{H}_b) - \mathbb{E}_{\mathbf{H}_e} I(\mathbf{s}; \mathbf{z}|\mathbf{H}_e))^+ \tag{9}$$

$$\text{s.t.} \quad \text{tr}(\mathbf{PP}^H) \leq N_t - \alpha^2_{AN}, \tag{10}$$

Algorithm 1 Gradient Descent for Maximizing R_s

```
**Consider different values for** $\alpha_{AN} \in [0\ \sqrt{N_t}]$ **and for each value of** $\alpha_{AN}$**, repeat**:
    **Step 1**: Initialize $\mathbf{P}_1$ with constraint $\mathrm{tr}(\mathbf{P}_1\mathbf{P}_1^H) \leq N_t - \alpha_{AN}^2$. Set step size $u$ and min. tolerance $u_{min}$
    **Step 2**: Set $k = 1$, compute $R_{s_1} = R_s(\mathbf{P}_1)$
    **Step 3**: Compute $\nabla_{P_1} R_s(\mathbf{P})$
    **Step 4**: If $u \geq u_{min}$ goto Step 5, otherwise Stop algorithm and return $\mathbf{P}_k$
    **Step 5**: Calculate $\hat{\mathbf{P}}_k = \mathbf{P}_k + u\nabla_{\mathbf{P}_k} R_s(\mathbf{P})$ and if $\mathrm{tr}(\hat{\mathbf{P}}_k\hat{\mathbf{P}}_k^H) > N_t - \alpha_{AN}^2$, normalize as $\hat{\mathbf{P}}_k := \sqrt{\frac{N_t-\alpha_{AN}^2}{\mathrm{tr}(\hat{\mathbf{P}}_k\hat{\mathbf{P}}_k^H)}}\hat{\mathbf{P}}_k$
    **Step 6**: Compute $\hat{R}_s = R_s(\hat{\mathbf{P}}_k)$; If $\hat{R}_s \geq R_{s_k}$ update $R_{s_{k+1}} = \hat{R}_s$ and $\mathbf{P}_{k+1} = \hat{\mathbf{P}}_k$ & goto Step 8, O/W let $u = 0.5u$ and goto Step 4
    **Step 7**: $k = k + 1$ goto Step 3
**Select** $\alpha_{AN}$ **and the corresponding optimal P which result in the maximum** $R_s$:
```

where the instantaneous mutual information over the main channel is given by [8]

$$I(\mathbf{s};\mathbf{y}|\mathbf{H}_b) = N_t \log M$$
$$-\frac{1}{M^{N_t}} \sum_{m=1}^{M^{N_t}} \mathbb{E}_{\mathbf{n}_y} \log \sum_{k=1}^{M^{N_t}} \exp\left(-\frac{\|\mathbf{H}_b\mathbf{P}\mathbf{d}_{mk} + \mathbf{n}_y\|^2 - \|\mathbf{n}_y\|^2}{\sigma_{\mathbf{n}_y}^2}\right), \tag{11}$$

where $\mathbf{d}_{mk} = \mathbf{s}_m - \mathbf{s}_k$ and M is the modulation order. Mutual information over the eavesdropper's channel, i.e., $I(\mathbf{s};\mathbf{z}|\mathbf{H}_e)$, can be calculated similarly.

In order to solve this optimization problem, a gradient descent algorithm [9] can be employed. In order to obtain the optimal $(\alpha_{AN}, \mathbf{P})$, we repeat this gradient descent algorithm for different values of α_{AN} and select the best $(\alpha_{AN}, \mathbf{P})$ as described in Algorithm 1. For each value of α_{AN}, the algorithm should be repeated with multiple initializations of $\mathbf{P}$ to increase the likelihood for the gradient descent algorithm to converge to the globally optimal solution.

Gradient of R_s can be calculated as

$$\nabla R_s(\mathbf{P}) = \frac{\log_2 e}{\sigma_{\mathbf{n}_y}^2}\left(\mathbf{H}_b^H\mathbf{H}_b\mathbf{P}\boldsymbol{\Sigma}_b(\mathbf{P})\right)$$
$$- \mathbb{E}_{\mathbf{H}_e}\left\{\frac{\log_2 e}{\sigma_{\mathbf{n}_z}^2}\left(\mathbf{H}_e^H\mathbf{H}_e\mathbf{P}\boldsymbol{\Sigma}_b(\mathbf{P})\right)\right\}, \tag{12}$$

where $\boldsymbol{\Sigma}_b(\mathbf{P})$ and $\boldsymbol{\Sigma}_e(\mathbf{P})$ are the receive minimum mean square error (MMSE) matrices at the legitimate receiver and the eavesdropper, respectively, and are given by [10]

$$\boldsymbol{\Sigma}_b(\mathbf{P}) = \mathbb{E}\{(\mathbf{s} - \mathbb{E}\{\mathbf{s}|\mathbf{y}\})(\mathbf{s} - \mathbb{E}\{\mathbf{s}|\mathbf{y}\})^H\}, \tag{13}$$
$$\boldsymbol{\Sigma}_e(\mathbf{P}) = \mathbb{E}\{(\mathbf{s} - \mathbb{E}\{\mathbf{s}|\mathbf{z}\})(\mathbf{s} - \mathbb{E}\{\mathbf{s}|\mathbf{z}\})^H\}. \tag{14}$$

B. Cut-off Rate Based Approximation for R_s

The instantaneous and average mutual information terms in (5) lack closed-form expressions and involve multiple integrals. To estimate $I(\mathbf{s};\mathbf{y}|\mathbf{H}_b)$ and $\mathbb{E}_{\mathbf{H}_e} I(\mathbf{s};\mathbf{z}|\mathbf{H}_e)$, one can take advantage of Monte Carlo methods, which require averaging over sufficiently large number of noise and channel samples. Accordingly, finding the optimal $\mathbf{P}$ and α_{AN} which maximize R_s in (5) is a computationally complex task. A gradient descent type solution for maximization of R_s, similar to the ones proposed in [5] and [11], requires several evaluations of the mutual information expression as well as the gradient of the mutual information, which also lacks a closed-form. Hence, employing a closed-form approximation of R_s and maximizing this approximation can significantly reduce the computational complexity associated with the transmit signal design.

We define a cut-off rate based metric as

$$R_s' = R_0^{(B)} - \bar{R_0}^{(E)}, \tag{15}$$

where R_s' is an approximation of the instantaneous secrecy rate, with $R_0^{(B)}$ being the instantaneous cut-off rate for Bob, which is a valid lower bound on the mutual information, given by [12, Eq. (4.3.34)]

$$R_0^{(B)} =$$
$$- \log \sum_{i}^{M^{N_t}} \sum_{j}^{M^{N_t}} \frac{1}{M^{2N_t}} \int p(y|\mathbf{s}_i, \mathbf{H}_b)^{1/2} p(y|\mathbf{s}_j, \mathbf{H}_b)^{1/2} dy$$
$$= 2N_t \log M - \log \sum_{i}^{M^{N_t}} \sum_{j}^{M^{N_t}} \exp\left(-\frac{\mathbf{d}_{ij}^H\mathbf{P}^H\mathbf{H}_b^H\mathbf{H}_b\mathbf{P}\mathbf{d}_{ij}}{4\sigma_{\mathbf{n}_y}^2}\right), \tag{16}$$

and $\bar{R_0}^{(E)}$ is the average cut-off rate over the eavesdropper's channel. If either $N_{r_e} = 1$ or $N_t - N_{r_b} = 1$, the expression for $\bar{R_0}^{(E)}$ is obtained as

$$\bar{R_0}^{(E)} = 2N_t \log M$$
$$- \log \sum_{i}^{M^{N_t}} \sum_{j}^{M^{N_t}} \mathbb{E}_{\mathbf{H}_e} \exp\left(-\frac{\mathbf{d}_{ij}^H\mathbf{P}^H\mathbf{H}_e^H\mathbf{H}_e\mathbf{P}\mathbf{d}_{ij}}{4(\sigma_{\mathbf{n}_z}^2 + \alpha_{AN}^2\|\mathbf{W}\|^2)}\right), \tag{17}$$

where $\mathbf{W} = \frac{\mathbf{H}_e\mathbf{V}_b}{\sqrt{N_t - N_{r_b}}}$. The expression in (17) is derived in the following manner. The received vector at the eavesdropper can be written as

$$\mathbf{z} = \mathbf{H}_e\mathbf{P}\mathbf{s} + \alpha_{AN}\mathbf{W}\mathbf{u} + \mathbf{n}_z. \tag{18}$$

If either $N_{r_e} = 1$ or $N_t - N_{r_b} = 1$, the summation of the artificial noise and the additive white Gaussian noise, i.e., $\mathbf{n}_z' = \alpha_{AN}\mathbf{W}\mathbf{u} + \mathbf{n}_z$, is a zero-mean white Gaussian vector with covariance $(\sigma_{\mathbf{n}_z}^2 + \alpha_{AN}^2\|\mathbf{W}\|^2)\mathbf{I}_{N_{r_e}}$. However, in the cases with $N_{r_e} > 1$ and $N_t - N_{r_b} \neq 1$, the vector $\mathbf{n}_z'$ would be a zero-mean colored Gaussian vector. In such cases, the cut-off rate expression in (17) as well as the mutual information over the eavesdropper's channel can be obtained after whitening $\mathbf{n}_z'$ (see, e.g., Lemma 3.1 in [13]).

In order to demonstrate that employing the closed-form design metric in (15) instead of directly maximizing (5) can significantly reduce the computational complexity, we compare the matrix multiplication steps required for evaluation of R_s and R_s' in Table I. We assume that N_{samp} is the number of sample points required for an accurate estimation of the expectation operators, $\mathbb{E}_n$ and $\mathbb{E}_{\mathbf{H}_e}$. For instance, it can be observed through numerical experiments that a sufficiently accurate estimation of the average mutual information $\mathbb{E}_{\mathbf{H}_e} I(\mathbf{s};\mathbf{z}|\mathbf{H}_e)$ requires an averaging over at least $N_{\text{samp}} = 500$ realizations of noise and channel coefficients. Accordingly, Table I reveals that the computational complexity associated with calculation of R'_s is considerably smaller than that of R_s.

TABLE I: Number of matrix multiplication steps

$I(\mathbf{s};\mathbf{y}|\mathbf{H}_b)$	$R_0^{(B)}$	$\mathbb{E}_{\mathbf{H}_e} I(\mathbf{s};\mathbf{z}|\mathbf{H}_e)$	$\bar{R_0}^{(E)}$
$12M^{2N_t}N_{\text{samp}}$	$5M^{2N_t}$	$12M^{2N_t}N_{\text{samp}}^2$	$8M^{2N_t}N_{\text{samp}}$

Our extensive numerical evaluations demonstrate that R'_s serves as a valid approximation of R_s even though its evaluation requires significantly reduced computational complexity. Hence, maximization of R'_s is a reasonable alternative. In order to maximize R'_s, we jointly optimize $\mathbf{P}$ and α_{AN} using Algorithm 1 and by replacing R_s with R'_s. We apply the matrix differentiation technique in [14] to derive the gradient of R'_s as shown on top of the next page in (19).

C. Search Region for the Optimal α_{AN}

Since an exhaustive search is performed over the values of α_{AN} to obtain the optimal pair $(\alpha_{AN}, \mathbf{P})$, defining a criterion for such a search is mandatory for keeping the computational complexity at a reasonable level. In the scenarios with finite-alphabet inputs and with equal SNR values at the legitimate receiver and the eavesdropper, lower fractions of the power should be allocated to data transmission at higher SNRs [6]. This is due to the fact that, under finite-alphabet input constraints, transmission at full power for high SNRs allows the eavesdropper to acquire the maximum number of bits per channel use which results in zero secrecy. With this key point in mind, for a fixed main channel given as

$$\mathbf{H}_b = \begin{bmatrix} 0.5128 - 0.3239i & -0.8903 - 0.0318i \end{bmatrix}, \qquad (20)$$

we compare the ergodic secrecy rates with precoding versus the fractions of power allocated to artificial noise for different SNR values. It is clear from Fig. 1 that the optimal α_{AN} depends on the SNR value, and that the higher the SNR, the higher is the fraction of power allocated to the artificial noise. More specifically, it is desirable to allocate 0, 8 and 33 percentages of the total power to the artificial noise at the SNR values of $-5dB$, $5dB$ and $15dB$, respectively, for this example. Basically, it is possible to limit the searching space of the optimization in Algorithm 1 to reduce the computational costs.

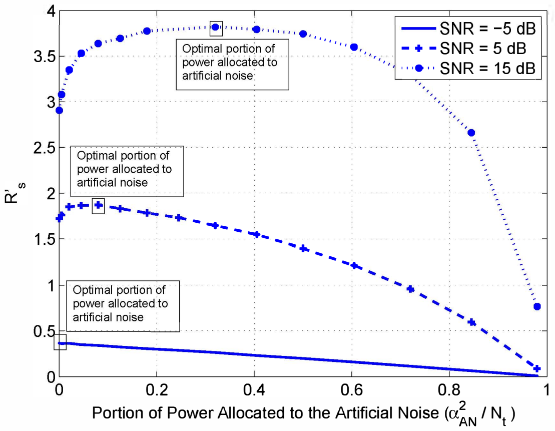

Fig. 1: R'_s with precoding for the main channel given in (20) and with no correlation over the eavesdropper's channel versus fractions of power allocated to artificial noise.

IV. Numerical Examples

In order to demonstrate the efficacy of the proposed signal design schemes, we provide several numerical examples. Throughout the simulations, equal noise levels are assumed at the legitimate receiver and the eavesdropper. The numerical results are provided for the scenarios with constant and fading main channels.

A. Constant Main Channel

In this scenario, the secrecy rate is calculated using (5). More than 500 realizations of $\mathbf{H}_e$ are considered for evaluation of the average mutual information for the eavesdropper. Figure 2 compares the ergodic secrecy rates for three different transmit signal design algorithms. A fixed main channel has been considered as given in (20). The eavesdropper's channel is assumed to be correlated according to (3) where $\mathbf{\Psi}_t$ and $\mathbf{\Psi}_r$ have exponential entries, i.e.,

$$[\mathbf{\Psi}_t]_{ij} = \rho_t^{|i-j|}, \quad \text{and} \quad [\mathbf{\Psi}_r]_{ij} = \rho_r^{|i-j|}, \qquad (21)$$

with $\rho_t = 0.9$ and $\rho_r = 1$.

Figure 2 indicates the suboptimality of the transmit signal design scheme in [5], as it can be observed that maximization of R_s with jointly optimizing the precoder matrix and the power allocated to the artificial noise, i.e., employing Algorithm 1, can yield higher secrecy rates. Furthermore, it can be inferred from Fig. 2 that, the maximization of the cut-off rate based design metric R'_s using Algorithm 1 yields a relatively small loss with respect to the scheme proposed in [5] in low and moderate SNR values. The proposed algorithm can also outperform the algorithm in [5] in high SNRs due to the further optimization carried out over the power assigned to the artificial noise.

B. Fading Main Channel

In this scenario, Algorithm 1 is applied for each realization of $\mathbf{H}_b$ and the secrecy rate is averaged over 500 realizations of $\mathbf{H}_b$ and $\mathbf{H}_e$ according to (6). In this experiment, the eavesdropper's channel is assumed to be correlated as in (3) where the transmit and receive correlations are calculated according to (21) with $\rho_t = 0.8$ and $\rho_r = 0.8$.

Figure 3 compares the secrecy rates achieved by different transmissions with different number of transmit antennas and for different channel inputs. Figure 3 reveals an important difference between the secrecy behavior of the Gaussian source and that of practical inputs picked from a discrete

$$\nabla R_s'(\mathbf{P}) = \frac{\sum\limits_{i=1}^{M^{N_t}} \sum\limits_{j=1}^{M^{N_t}} (\mathbf{d}_{ij}^H \mathbf{P}^H \mathbf{H}_b^H \mathbf{H}_b \mathbf{P} \mathbf{d}_{ij})^T \exp(-\mathbf{d}_{ij}^H \mathbf{P}^H \mathbf{H}_b^H \mathbf{H}_b \mathbf{P} \mathbf{d}_{ij} / 4\sigma_{\mathbf{n}_y}^2)}{4\sigma_{\mathbf{n}_y}^2 \sum\limits_{i'=1}^{M^{N_t}} \sum\limits_{j'=1}^{M^{N_t}} \exp(-\mathbf{d}_{i'j'}^H \mathbf{P}^H \mathbf{H}_b^H \mathbf{H}_b \mathbf{P} \mathbf{d}_{i'j'} / 4\sigma_{\mathbf{n}_y}^2)} - \sum_{m=1}^{M^{N_t}} \sum_{k=1}^{M^{N_t}} \mathbb{E}_{\mathbf{H}_e} \frac{(\mathbf{d}_{mk}^H \mathbf{P}^H \mathbf{H}_e^H \mathbf{H}_e \mathbf{P} \mathbf{d}_{mk})^T \exp(-\mathbf{d}_{mk}^H \mathbf{P}^H \mathbf{H}_e^H \mathbf{H}_e \mathbf{P} \mathbf{d}_{ij} / 4\sigma_{\mathbf{n}_z'}^2)}{4\sigma_{\mathbf{n}_z'}^2 \sum\limits_{m'=1}^{M^{N_t}} \sum\limits_{k'=1}^{M^{N_t}} \exp(-\mathbf{d}_{m'k'}^H \mathbf{P}^H \mathbf{H}_e^H \mathbf{H}_e \mathbf{P} \mathbf{d}_{m'k'} / 4\sigma_{\mathbf{n}_z'}^2)} \tag{19}$$

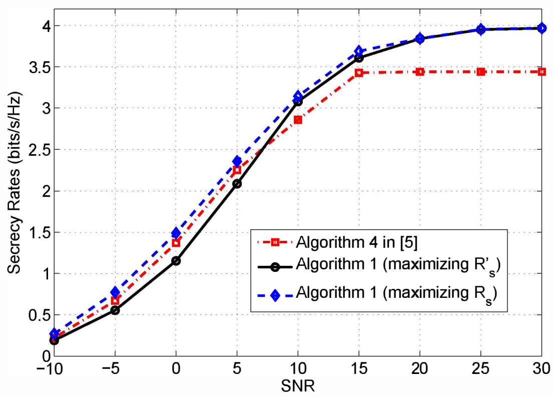

Fig. 2: Secrecy rates with QPSK input for the main channel given in (20) and the eavesdropper channels with $\rho_t = 0.9$ and $\rho_r = 1$.

constellation. While the achievable secrecy rates with Gaussian inputs increase monotonically with increasing SNR, it saturates for the finite-alphabet input scenarios. According to Fig. 3, when the SNR is sufficiently high, the proposed transmit signal design scheme provides achievable secrecy rates close to $N_t \log M$, i.e., the maximum rate which can be attained by the legitimate receiver in the context of finite-alphabet constraints. Also, it reveals that, with a fixed number of receive antennas, the achievable secrecy rates increase by increasing N_t and M. Thanks to the joint optimization of the precoder matrix and the artificial noise, the proposed transmit signal design scheme is capable of providing positive secrecy rates even for the cases where the eavesdropper is equipped with a higher number of antennas compared to the legitimate receiver.

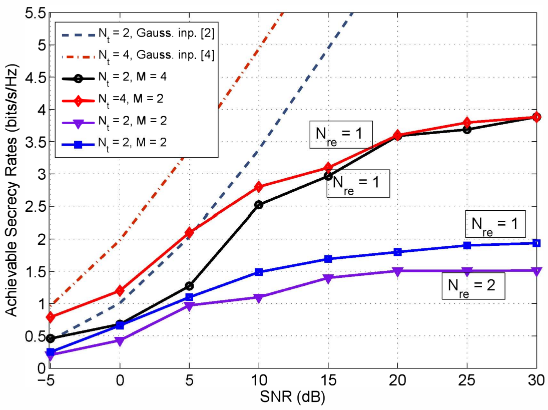

Fig. 3: Achievable secrecy rates for fading main channel, with different values of M and N_t and N_{r_e}, where $N_{r_b} = 1$.

V. Conclusions

In this paper, with the assumption of statistical knowledge on the eavesdropper's channel, we derived a cut-off rate based approximation for the ergodic secrecy rates of a MIMO wiretap channel for finite-alphabet inputs. An iterative joint precoder and artificial noise design scheme is proposed which maximizes this approximation. Extensive numerical results demonstrate that the proposed transmit signal design method provides positive secrecy rates in a variety of scenarios and yields an enhanced secrecy performance compared to the existing solutions in spite of its significantly lower computational complexity.

References

[1] 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.

[2] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas - Part I: The MISOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 7, pp. 3088–3104, Jul. 2009.

[3] F. Oggier, B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *IEEE Trans. Inf. Theory*, vol. 57, no. 8, pp. 4961–4972, 2011.

[4] 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, Dec. 2012

[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. Bashar, Z. Ding, and C. Xiao, "On the secrecy rate of multi-antenna wiretap channel under finite-alphabet input," *IEEE Commun. Lett.*, vol. 15, no. 5, pp. 527-529, May 2011.

[7] P. Gopala, L. Lai and H. El Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inf. Theory* , vol. 54, pp. 4687–4698, Oct. 2008.

[8] C. Xiao and Y. R. Zheng, "On the mutual information and power allocation for vector Gaussian channels with finite discrete inputs," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, LA, 2008.

[9] S. Boyd and L. Vandenberghe, *Convex Optimization*. New York: Cambridge Univ. Press, 2004.

[10] 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.

[11] S. Rezaei Aghdam and T. M. Duman, "Physical layer security for space shift keying transmission with precoding," *IEEE Wireless Commun. Lett.*, vol. 5, no. 2, pp. 180-183, Apr. 2016.

[12] S. G. Wilson, *Digital Modulation and Coding*. Englewood Cliffs, NJ: Prentice-Hall, 1995.

[13] P. Parada and R. Blahut, "Secrecy capacity of SIMO and slow fading channels," in Proc. *IEEE Int. Symp. Information Theory (ISIT)*, Adelaide, Australia, Sep. 2005, pp. 2152–2155.

[14] A. Hjorunges, *Complex-Valued Matrix Derivatives*. New York: Cambridge Univ. Press, 2011.