SECRECY RATE MAXIMIZATION FOR MIMO GAUSSIAN WIRETAP CHANNELS WITH MULTIPLE EAVESDROPPERS VIA ALTERNATING MATRIX POTDC

Jens Steinwandt [1], *Sergiy A. Vorobyov* [2,3], *and Martin Haardt* [1]

[1] Communications Research Laboratory, Ilmenau University of Technology, P.O. Box 100565, 98684 Ilmenau, Germany
[2] Department of Signal Processing and Acoustics, Aalto University, P.O. Box 13000, FI-0076 Aalto, Finland
[3] Department of Electrical and Computer Engineering, University of Alberta, Edmonton, AB, T6G 2V4, Canada
Emails: {jens.steinwandt, martin.haardt}@tu-ilmenau.de, svor@ieee.org, Web: www.tu-ilmenau.de/crl

ABSTRACT

In this paper, we consider the problem of optimizing the transmit covariance matrix for a multiple-input multiple-output (MIMO) Gaussian wiretap channel. The scenario of interest consists of a transmitter, a legitimate receiver, and multiple non-cooperating eavesdroppers that are all equipped with multiple antennas. Specifically, we design the transmit covariance matrix by maximizing the secrecy rate under a total power constraint, which is a non-convex difference of convex functions (DC) programming problem. We develop an algorithm, termed alternating matrix POTDC algorithm, based on alternating optimization of the eigenvalues and the eigenvectors of the transmit covariance matrix. The proposed alternating matrix POTDC method provides insights into the non-convex nature of the problem and is very general, i.e., additional constraints on the covariance matrix can easily be incorporated. The secrecy rate performance of the proposed algorithm is demonstrated by simulations.

Index Terms— Secrecy rate maximization, MIMO wiretap channel, alternating optimization, difference of convex functions.

1. INTRODUCTION

Wireless physical layer security, where the physical characteristics of the wireless channel are exploited to enhance the security of communication systems, has recently attracted considerable attention. This information theoretic concept aims at providing a legitimate receiver with confidential information while preventing eavesdroppers from overhearing the communication channel. The first model to capture the physical layer security problem, termed the wiretap channel, was introduced in [1]. Therein, the secrecy rate was introduced as a performance metric to reflect the amount of reliably transmitted information to a receiver, provided that no information is leaked to illegitimate parties. Strictly positive secrecy rates usually require the legitimate receivers' channel statistics to be better than those of the eavesdroppers. To mitigate the dependence on the channel conditions, multiple-input multiple-output (MIMO) techniques [2]-[5] have been of recent focus to enhance the secrecy rate through the additional degrees of freedom provided by multiple antennas.

The maximization of the secrecy rate by designing the transmit covariance matrix under a total power constraint is an intricate task. This is due to the non-convex nature of the optimization problem, which is a difference of convex functions (DC) programming problem. Thus, in the case of both single and multiple eavesdroppers, there is so far no efficient and tractable solution for general channel configurations. Closed-form solutions for the single eavesdropper case have been derived for the special cases of a single antenna receiver/eavesdropper [6], a positive semidefinite power-covariance constraint [7], and channel matrices with certain rank properties [8]. However, for single and multiple eavesdropper scenarios in the generalized case, suboptimal designs have been proposed in [9]-[14].

For the single eavesdropper case, a fixed-point iterative design based on the Karush-Kuhn-Tucker (KKT) optimality conditions was presented in [9]. In [10], a beamforming method based on the generalized singular value decomposition (GSVD) was proposed. Moreover, a zero-forcing strategy and a method relying on the maximization of the signal-to-leakage-plus-noise ratio (SLNR) were derived in [11]. The authors of [12] proposed an alternating optimization approach under per-antenna power constraints. Therein, the original problem is decomposed into two separable convex problems that are solved in an alternating manner. Recently, a new method that optimizes the eigenvalues and eigenvectors of the transmit covariance matrix separately in an alternating fashion was presented in [14]. It relies on the polynomial time DC (POTDC) method [15], which was originally designed for the DC programming problem of optimizing the amplification matrix for a two-way amplify-and-forward relay network. In [16], the POTDC algorithm was applied to robust adaptive beamforming for general-rank signal models and proven to achieve global optimality under the condition that the presumed norm of the covariance matrix mismatch is sufficiently small.

In the case of multiple eavesdroppers, however, only the method in [13] has recently been proposed as an extension of [12]. As a drawback of the scheme in [13], no insights into the non-convex problem structure are revealed and a new derivation of the algorithm procedure is required when incorporating new constraints on the transmit covariance matrix [13]. Here, we take a more general approach and extend [14] to the multiple eavesdropper case, which is not straightforward due to the arising maxmin-type DC programming problem.

In this paper, we develop the alternating matrix POTDC algorithm to optimize the transmit covariance matrix that maximizes the secrecy rate of a MIMO Gaussian wiretap channel with multiple non-cooperating eavesdroppers. We assume that perfect channel state information (CSI) is available at the transmitter. The proposed algorithm is based on a reformulation of the original non-convex problem, which enables an alternating optimization of the eigenvalues and eigenvectors of the transmit covariance matrix under a total power constraint. However, the presented method can easily be generalized by incorporating additional constraints on the covariance matrix, such as per-antenna power constraints, without the need to redesign the algorithm. Furthermore, it provides insights into the non-convex nature of the problem. The secrecy rate performance of the proposed alternating matrix POTDC algorithm is demonstrated by simulations.

978-1-4799-2893-4/14/$31.00 ©2014 IEEE

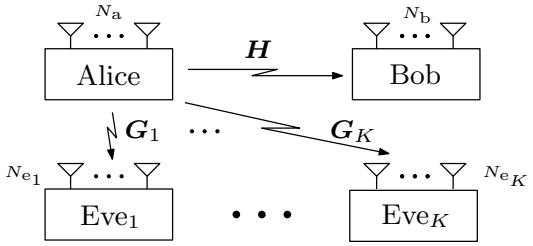

Fig. 1. MIMO Gaussian wiretap channel with K eavesdroppers.

2. SYSTEM MODEL AND PROBLEM STATEMENT

Consider the MIMO Gaussian wiretap channel scenario depicted in Fig. 1, where a transmitter (Alice) with N_{a} antennas sends information to a legitimate receiver (Bob) with N_{b} antennas in the presence of K eavesdroppers (Eves) each with N_{e_k} antennas, where $k = 1, \ldots, K$. The received signals at Bob and the Eves are respectively given by

$$\boldsymbol{y}_{\mathrm{b}} = \boldsymbol{H}^H \boldsymbol{x} + \boldsymbol{n}_{\mathrm{b}} \ \in \mathbb{C}^{N_{\mathrm{b}} \times 1} \tag{1a}$$

$$\boldsymbol{y}_{\mathrm{e}_k} = \boldsymbol{G}_k^H \boldsymbol{x} + \boldsymbol{n}_{\mathrm{e}_k} \ \in \mathbb{C}^{N_{\mathrm{e}_k} \times 1}, \ k = 1, \ldots, K, \tag{1b}$$

where $\boldsymbol{H} \in \mathbb{C}^{N_{\mathrm{a}} \times N_{\mathrm{b}}}$ and $\boldsymbol{G}_k \in \mathbb{C}^{N_{\mathrm{a}} \times N_{\mathrm{e}_k}}$ represent the respective MIMO flat-fading channels from Alice to Bob and from Alice to the k-th Eve, $\boldsymbol{x} \in \mathbb{C}^{N_{\mathrm{a}} \times 1}$ with $\boldsymbol{x} \sim \mathcal{CN}(\boldsymbol{0}_{N_{\mathrm{a}}}, \boldsymbol{P})$ contains the transmit symbols intended for Bob, and $\boldsymbol{n}_{\mathrm{b}} \in \mathbb{C}^{N_{\mathrm{b}} \times 1} \sim \mathcal{CN}(\boldsymbol{0}_{N_{\mathrm{b}}}, \boldsymbol{I}_{N_{\mathrm{b}}})$ and $\boldsymbol{n}_{\mathrm{e}_k} \in \mathbb{C}^{N_{\mathrm{e}_k} \times 1} \sim \mathcal{CN}(\boldsymbol{0}_{N_{\mathrm{e}_k}}, \boldsymbol{I}_{N_{\mathrm{e}_k}})$ are the additive white Gaussian noise vectors at Bob and the k-th Eve. Furthermore, the total power constraint $\mathrm{Tr}\{\boldsymbol{P}\} \leq P$ with $P > 0$ is employed at Alice.

Based on the assumption that perfect channel state information (CSI) is available at the transmitter, we can maximize the achievable secrecy rate by designing the transmit covariance matrix $\boldsymbol{P} \triangleq \mathbb{E}\{\boldsymbol{x}\boldsymbol{x}^H\}$. The secrecy rate for the transmission from Alice to Bob, where the k-th Eve is taken into account has been shown to be [2]

$$R_{\mathrm{s}_k}(\boldsymbol{P}) = \ln|\boldsymbol{I}_{N_{\mathrm{b}}} + \boldsymbol{H}^H \boldsymbol{P} \boldsymbol{H}| - \ln|\boldsymbol{I}_{N_{\mathrm{e}_k}} + \boldsymbol{G}_k^H \boldsymbol{P} \boldsymbol{G}_k|,$$

which is the difference between the mutual information of the Alice-to-Bob and the Alice-to-k-th-Eve channels. Note that $R_{\mathrm{s}_k} > 0$ if $\boldsymbol{H}\boldsymbol{H}^H \succeq \boldsymbol{G}_k \boldsymbol{G}_k^H$ holds [9]. The secrecy rate maximization problem can be formulated as

$$R_{\mathrm{s}}^{\star} = \max_{\boldsymbol{P}} \quad \min_{k=1,\ldots,K} R_{\mathrm{s}_k}(\boldsymbol{P}) \tag{2a}$$

$$\text{s.t.} \quad \mathrm{Tr}\{\boldsymbol{P}\} \leq P, \ \ \boldsymbol{P} \succeq \boldsymbol{0}_{N_{\mathrm{a}}}, \tag{2b}$$

where the goal is to maximize the worst secrecy rate among the Eves.

The objective function in (2a) contains a difference of concave functions. Thus, problem (2) belongs to the class of DC programming problems, which are generally nonconvex. The authors of [12], [13] have recently proposed an alternating optimization approach, in which by introducing a new optimization variable the original problem is decomposed into two separable convex problems that are solved in an alternating manner. Moreover, a proof of the convergence to a KKT point is given. We, however, propose a more general approach that provides further insights and reveals the nonconvexity type of the underlying problem. It is an extension of the method in [14] to the case of multiple Eves and termed alternating matrix POTDC algorithm.

3. PROPOSED ALTERNATING MATRIX POTDC ALGORITHM FOR SECRECY RATE MAXIMIZATION

In this section, we present the alternating matrix POTDC approach to address the MIMO secrecy problem above. We start our development by introducing the auxiliary variable τ [17] to rewrite (2) into its epigraph form

$$\max_{\boldsymbol{P}, \tau} \quad \tau \tag{3a}$$

$$\text{s.t.} \quad R_{\mathrm{s}_k}(\boldsymbol{P}) \geq \tau, \ \ k = 1, \ldots, K \tag{3b}$$

$$\mathrm{Tr}\{\boldsymbol{P}\} \leq P, \ \ \boldsymbol{P} \succeq \boldsymbol{0}_{N_{\mathrm{a}}}. \tag{3c}$$

The eigendecomposition of $\boldsymbol{P}$ is given by $\boldsymbol{P} = \boldsymbol{U}\boldsymbol{\Lambda}\boldsymbol{U}^H$, where the columns of the unitary matrix $\boldsymbol{U} \in \mathbb{C}^{N_{\mathrm{a}} \times N_{\mathrm{a}}}$ represent the eigenvectors and the diagonal matrix $\boldsymbol{\Lambda} \in \mathbb{R}^{N_{\mathrm{a}} \times N_{\mathrm{a}}}$ contains the non-negative eigenvalues $\lambda_i, i = 1, \ldots, N_{\mathrm{a}}$, of $\boldsymbol{P}$ on its diagonal. Thus, problem (3) turns into

$$\max_{\boldsymbol{U}, \boldsymbol{\Lambda}, \tau} \quad \tau \tag{4a}$$

$$\text{s.t.} \quad \ln|\boldsymbol{I}_{N_{\mathrm{b}}} + \boldsymbol{H}^H \boldsymbol{U}\boldsymbol{\Lambda}\boldsymbol{U}^H \boldsymbol{H}| \tag{4b}$$

$$- \ln|\boldsymbol{I}_{N_{\mathrm{e}_k}} + \boldsymbol{G}_k^H \boldsymbol{U}\boldsymbol{\Lambda}\boldsymbol{U}^H \boldsymbol{G}_k| \geq \tau, \ \ \forall k$$

$$\boldsymbol{U}^H\boldsymbol{U} = \boldsymbol{I}_{N_{\mathrm{a}}}, \ \ \mathrm{Tr}\{\boldsymbol{\Lambda}\} \leq P, \ \ \lambda_i \geq 0, \ \ \forall i. \tag{4c}$$

Next, we apply Sylvester's determinant theorem, which states that the equality [18]

$$|\boldsymbol{I}_M + \boldsymbol{A}\boldsymbol{B}| = |\boldsymbol{I}_N + \boldsymbol{B}\boldsymbol{A}| \tag{5}$$

holds for arbitrary matrices $\boldsymbol{A} \in \mathbb{C}^{M \times N}$ and $\boldsymbol{B} \in \mathbb{C}^{N \times M}$. Consequently, we obtain an equivalent formulation of (4) as

$$\max_{\boldsymbol{U}, \boldsymbol{\Lambda}, \tau} \quad \tau \tag{6a}$$

$$\text{s.t.} \quad \ln|\boldsymbol{I}_{N_{\mathrm{b}}} + \boldsymbol{H}^H \boldsymbol{U}\boldsymbol{\Lambda}\boldsymbol{U}^H \boldsymbol{H}| \tag{6b}$$

$$- \ln|\boldsymbol{I}_{N_{\mathrm{a}}} + \boldsymbol{D}_k(\boldsymbol{U})\boldsymbol{\Lambda}| \geq \tau, \ \ \forall k$$

$$\boldsymbol{U}^H\boldsymbol{U} = \boldsymbol{I}_{N_{\mathrm{a}}}, \ \ \mathrm{Tr}\{\boldsymbol{\Lambda}\} \leq P, \ \ \lambda_i \geq 0, \ \ \forall i, \tag{6c}$$

where we have defined $\boldsymbol{D}_k(\boldsymbol{U}) \triangleq \boldsymbol{U}^H \boldsymbol{G}_k \boldsymbol{G}_k^H \boldsymbol{U}$ for notational convenience. While problem (6) is still a nonconvex DC programming problem in both $\boldsymbol{U}$ and $\boldsymbol{\Lambda}$, it is separable in these variables and can be addressed by fixing either $\boldsymbol{U}$ or $\boldsymbol{\Lambda}$ and optimizing for the other variable. This gives rise to an alternating optimization of (6), where we first optimize with respect to $\boldsymbol{\Lambda}$ for a fixed value of $\boldsymbol{U}$ adopting an extended version of the POTDC algorithm [15]. Then, in the second step, we fix the obtained value of $\boldsymbol{\Lambda}$ and further optimize with respect to $\boldsymbol{U}$. Note that the latter is the optimization under the unitary matrix constraint, which is a well-studied class of optimization problems [20], [21].

In more details, we alternatingly solve the following two optimization problems to obtain $\boldsymbol{\Lambda}^{(n)}$ and $\boldsymbol{U}^{(n)}$ at the n-th iteration, $n = 1, 2, \ldots$, until convergence:

$$\boldsymbol{\Lambda}^{(n)} = \arg\max_{\boldsymbol{\Lambda}, \tau} \quad \tau \tag{7}$$

$$\text{s.t.} \quad \ln\left|\boldsymbol{I}_{N_{\mathrm{b}}} + \boldsymbol{H}^H \boldsymbol{U}^{(n-1)} \boldsymbol{\Lambda} \boldsymbol{U}^{(n-1)^H} \boldsymbol{H}\right|$$

$$- \ln\left|\boldsymbol{I}_{N_{\mathrm{a}}} + \boldsymbol{D}_k(\boldsymbol{U}^{(n-1)})\boldsymbol{\Lambda}\right| \geq \tau, \ \ \forall k$$

$$\mathrm{Tr}\{\boldsymbol{\Lambda}\} \leq P, \ \ \lambda_i \geq 0, \ \ \forall i,$$

$$\boldsymbol{U}^{(n)} = \arg\max_{\boldsymbol{U}} \quad \min_{k=1,\ldots,K} \ln \frac{|\boldsymbol{I}_{N_\mathrm{b}} + \boldsymbol{H}^H \boldsymbol{U}\boldsymbol{\Lambda}^{(n)}\boldsymbol{U}^H\boldsymbol{H}|}{|\boldsymbol{I}_{N_{\mathrm{e}_k}} + \boldsymbol{G}_k^H \boldsymbol{U}\boldsymbol{\Lambda}^{(n)}\boldsymbol{U}^H\boldsymbol{G}_k|} \quad (8)$$
$$\text{s.t.} \quad \boldsymbol{U}^H\boldsymbol{U} = \boldsymbol{I}_{N_\mathrm{a}}.$$

In the first step, we address problem (7) via the POTDC algorithm [15], which is designed for DC problems with functions of a single scalar optimization variable in the non-concave term. However, the non-concave term in the objective function of (7) contains the optimization with respect to the matrix $\boldsymbol{\Lambda}$. Thus, we first modify (7) in order for the POTDC algorithm to be applicable. To this end, we utilize Hadamard's inequality, which states that the determinant of a matrix $\boldsymbol{A} \succeq \boldsymbol{0}_M$ is less than or equal to the product of its diagonal entries [22], i.e.,

$$|\boldsymbol{A}| \leq \prod_{m=1}^{M} a_{ii}. \quad (9)$$

Applying inequality (9) to (7), we obtain

$$\max_{\boldsymbol{\Lambda},\tau} \quad \tau \quad (10a)$$
$$\text{s.t.} \quad \ln\left|\boldsymbol{I}_{N_\mathrm{b}} + \boldsymbol{H}^H\boldsymbol{U}\boldsymbol{\Lambda}\boldsymbol{U}\boldsymbol{H}\right| \quad (10b)$$
$$- \sum_{i=1}^{N_\mathrm{a}} \ln(1 + [\boldsymbol{D}_k(\boldsymbol{U})]_{ii}\lambda_i) \geq \tau, \ \forall k$$
$$\mathrm{Tr}\{\boldsymbol{\Lambda}\} \leq P, \ \lambda_i \geq 0, \ \forall i, \quad (10c)$$

where in (10b), we maximize the lower bounds on the actual secrecy rates of the K Eves in problem (7). All the terms in (10) are concave or linear in $\boldsymbol{\Lambda}$, except for the Eve-induced terms $-\ln(1 + [\boldsymbol{D}_k(\boldsymbol{U})]_{ii}\lambda_i), i = 1,\ldots,N_\mathrm{a}$, which are convex and each of which now depends only on a single variable. Hence, we apply the POTDC algorithm [15] and iteratively handle these convex constraints in terms of their linear approximation around suitably selected points. The linear approximation of the convex part of (10b) around the point $\lambda_{i,c} \in [0, P]$ such that $\sum_{i=1}^{N_\mathrm{a}} \lambda_{i,c} = P$ is given by

$$\ln(1 + [\boldsymbol{D}_k(\boldsymbol{U})]_{ii}\lambda_i) \approx \ln(1 + [\boldsymbol{D}_k(\boldsymbol{U})]_{ii}\lambda_{i,c}) \quad (11)$$
$$+ \frac{(\lambda_i - \lambda_{i,c})[\boldsymbol{D}_k(\boldsymbol{U})]_{ii}}{1 + [\boldsymbol{D}_k(\boldsymbol{U})]_{ii}\lambda_{i,c}}.$$

In order to solve (10), we use (11) and perform iterations using interior-point methods [19] over the following problem:

$$\max_{\boldsymbol{\Lambda},\tau} \quad \tau \quad (12a)$$
$$\text{s.t.} \quad \ln\left|\boldsymbol{I}_{N_\mathrm{b}} + \boldsymbol{H}^H\boldsymbol{U}\boldsymbol{\Lambda}\boldsymbol{U}\boldsymbol{H}\right| \quad (12b)$$
$$- \sum_{i=1}^{N_\mathrm{a}} \frac{(\lambda_i - \lambda_{i,c})[\boldsymbol{D}_k(\boldsymbol{U})]_{ii}}{1 + [\boldsymbol{D}_k(\boldsymbol{U})]_{ii}\lambda_{i,c}} \geq \tau, \ \forall k$$
$$\mathrm{Tr}\{\boldsymbol{\Lambda}\} \leq P, \ \lambda_i \geq 0, \ \forall i. \quad (12c)$$

In (12b), we have omitted the first term of the approximation (11), which is a constant if $\sum_{i=1}^{N_\mathrm{a}} \lambda_{i,c} = P$ holds with $\lambda_{i,c} \in [0, P]$. Note that for the initial values $\lambda_{i,c}$ in the first iteration, we choose the maximum available power such that the power constraint $\mathrm{Tr}\{\boldsymbol{\Lambda}_c\} \leq P$ holds with equality. The presented POTDC algorithm guarantees the convergence to a KKT point of the problem (10). Furthermore, the POTDC iterations ensure a non-decreasing sequence of the constraint values over the iterations [15].

In the second step, we address problem (8), which is the optimization over the complex-valued matrix $\boldsymbol{U}$ under the constraint that $\boldsymbol{U}$ is a unitary matrix. To solve this problem, we consider the Riemannian conjugate gradient algorithm on the Lie group of unitary matrices proposed in [21] that is shown to move towards the optimal point along the locally shortest paths over several iterations. This algorithm presumes a differentiable objective function for the required calculation of its gradient with respect to $\boldsymbol{U}$. However, the cost function of (8) is a piecewise function and thus non-differentiable. Nevertheless, the objective function to be maximized in (8) is the minimum of a set of logarithms. It can then be shown that the minimum of the logarithmic functions in (2) also provides the steepest descent in the set of gradients of the objective function. Mathematically expressed, we have

$$\min_{k=1,\ldots,K} R_{\mathrm{s}_k}(\boldsymbol{U}) \Longleftrightarrow \min_{k=1,\ldots,K} \nabla_{\boldsymbol{U}}(R_{\mathrm{s}_k}(\boldsymbol{U})), \quad (13)$$

where $\nabla_{\boldsymbol{U}}(\cdot)$ denotes the gradient of $R_{\mathrm{s}_k}(\boldsymbol{U})$ for the k-th Eve with respect to $\boldsymbol{U}$, which can be derived as [23]

$$\nabla_{\boldsymbol{U}}(R_{\mathrm{s}_k}(\boldsymbol{U})) = \nabla_{\boldsymbol{U}} \ln \frac{|\boldsymbol{I}_{N_\mathrm{b}} + \boldsymbol{H}^H\boldsymbol{U}\boldsymbol{\Lambda}^{(n)}\boldsymbol{U}^H\boldsymbol{H}|}{|\boldsymbol{I}_{N_{\mathrm{e}_k}} + \boldsymbol{G}_k^H\boldsymbol{U}\boldsymbol{\Lambda}^{(n)}\boldsymbol{U}^H\boldsymbol{G}_k|} \quad (14)$$
$$= \boldsymbol{\Lambda}^{(n)}\boldsymbol{U}^H\boldsymbol{H}(\boldsymbol{I}_{N_\mathrm{b}} + \boldsymbol{H}^H\boldsymbol{U}\boldsymbol{\Lambda}^{(n)}\boldsymbol{U}^H\boldsymbol{H})^{-1}\boldsymbol{H}^H \quad (15)$$
$$- \boldsymbol{\Lambda}^{(n)}\boldsymbol{U}^H\boldsymbol{G}_k(\boldsymbol{I}_{N_{\mathrm{e}_k}} + \boldsymbol{G}_k^H\boldsymbol{U}\boldsymbol{\Lambda}^{(n)}\boldsymbol{U}^H\boldsymbol{G}_k)^{-1}\boldsymbol{G}_k^H.$$

Therefore, combining (13) and (15), the Riemannian conjugate gradient algorithm [21] is still applicable to solve problem (8). It should be noted that the accuracy of the solution obtained by this algorithm for a given scenario depends on the adjustment of several performance related parameters such as the chosen line search method and preconditioning.

We summarize the above-developed alternating matrix POTDC optimization procedure for solving the MIMO secrecy maximization problem with multiple eavesdroppers (2) in Algorithm 1. Both optimization steps in Algorithm 1 result in non-decreasing objective values. A more detailed convergence and optimality analysis is the concern of future work.

It should be mentioned that in some applications per-antenna power constraints need to be incorporated into the secrecy maximization problem [12]. This is due to the fact that each antenna may have its own power amplifier, which should only operate in the linear range. Such set of constraints can be written as $[\boldsymbol{P}]_{ii} \leq P_i, \ i =$

Algorithm 1: The alternating matrix POTDC algorithm for solving the secrecy maximization problem (2)

Initialize $n = 1$, $\epsilon_1 > 0$, $\epsilon_2 > 0$,
$\boldsymbol{P}^{(0)} = \boldsymbol{U}^{(0)}\boldsymbol{\Lambda}_c^{(0)}\boldsymbol{U}^{(0)^H} \succeq \boldsymbol{0}_{N_\mathrm{a}}$ such that $\mathrm{Tr}\{\boldsymbol{P}^{(0)}\} = P$;
while $|R_\mathrm{s}^{(n)} - R_\mathrm{s}^{(n-1)}| > \epsilon_1$ **do**
  Set $l = 1$;
  while $|\tau^{(n,l)} - \tau^{(n,l-1)}| > \epsilon_2$ **do**
    Solve (12) to obtain $\boldsymbol{\Lambda}^{(n,l)}$;
    $\boldsymbol{\Lambda}_c^{(n,l)} = \boldsymbol{\Lambda}^{(n,l)}$;
    $l = l + 1$;
  end while
  $\boldsymbol{\Lambda}^{(n)} = \boldsymbol{\Lambda}^{(n,l)}$;
  Solve (8) to obtain $\boldsymbol{U}^{(n)}$;
  $n = n + 1$;
end while
Output: $\boldsymbol{P}^{(n)} = \boldsymbol{U}^{(n)}\boldsymbol{\Lambda}^{(n)}\boldsymbol{U}^{(n)^H}$.

$1, \ldots, N_{\mathrm{a}}$, where $P_i > 0$ is the per-antenna power limit. In this respect, the advantage of the proposed method is that these constraints can be straightforwardly included into (7) and (12) without affecting the alternating optimization procedure in contrast to the algorithms proposed in [12] and [13], which essentially have to be rederived after adding the per-antenna power constraints.

4. SIMULATION RESULTS

In this section, we provide simulation results that demonstrate the performance of the presented alternating matrix POTDC algorithm "AM-POTDC" to solve the MIMO secrecy rate maximization problem with multiple eavesdroppers. For comparison purposes, we include the two recently proposed methods "AO-CVX" and "AO-PG" from [13] into our evaluation. Moreover, we also consider the conventional waterfilling algorithm based on the singular value decomposition (SVD) that only allocates power across Bob's channel irrespectively of the eavesdroppers. In our simulations, the channels $\boldsymbol{H}$ and $\boldsymbol{G}_k$, $k = 1, \ldots, K$, are randomly generated and drawn from an i.i.d. complex Gaussian distribution with zero mean and unit variance. The results are obtained by averaging over 1000 independent Monte Carlo trials. For the proposed algorithm, the initialization point $\boldsymbol{P}^{(0)}$ is chosen randomly according to line 1 of Algorithm 1 and the thresholds ϵ_1 and ϵ_2 are both set to 10^{-5}. Furthermore, we plot the worst secrecy rate achieved among all Eves.

In the first scenario, we have $K = 3$ eavesdroppers and the number of antennas at Alice, Bob, and the Eves are $N_{\mathrm{a}} = 6$, $N_{\mathrm{b}} = 6$, and $N_{\mathrm{e}_1} = \ldots = N_{\mathrm{e}_K} = 2$, respectively. Fig. 2 shows the secrecy rate of the various methods as a function of the transmit power P. Generally, the achieved secrecy rate increases with the transmit power. It can be seen that the performances of the proposed alternating optimization approach and the "AO-CVX" method are identical over the whole range of powers, while the "AO-PG" scheme performs slightly worse. Moreover, all three schemes significantly outperform the waterfilling algorithm.

In the second scenario, we vary the number of Eves for an antenna configuration of $N_{\mathrm{a}} = 6$, $N_{\mathrm{b}} = 6$, and $N_{\mathrm{e}_1} = \ldots = N_{\mathrm{e}_K} = 2$. The maximum transmit power is fixed at $P = 3$ dB. In Fig. 3, we illustrate the secrecy rates as a function of the number of Eves K. As expected, the secrecy rates decrease as K increases. It is apparent that the proposed method and the "AO-CVX" approach again achieve the same secrecy rate over the range of K. They still provide a secrecy rate of 6.2 bits/channel use even with $K = 6$ Eves. Once more, the performance of the "AO-PG" scheme is slightly worse, whereas the waterfilling method that ignores the eavesdroppers yields the worst secrecy rate.

5. CONCLUSION

In this paper, we have considered the non-convex secrecy rate maximization problem for a MIMO wiretap channel with multiple non-cooperating eavesdroppers. All the involved terminals are equipped with multiple antennas and perfect channel state information is assumed at the transmitter. We have developed the alternating matrix POTDC algorithm, which is based on alternating optimization of the eigenvalues and the eigenvectors of the transmit covariance matrix under a total power constraint. The proposed method provides insights into the optimization process and reveals the non-convex nature of the underlying problem. As another advantage, it is a general approach in the sense that additional constraints on the covariance matrix, such as per-antenna power constraints, can easily be incorporated into the optimization procedure. Simulation results

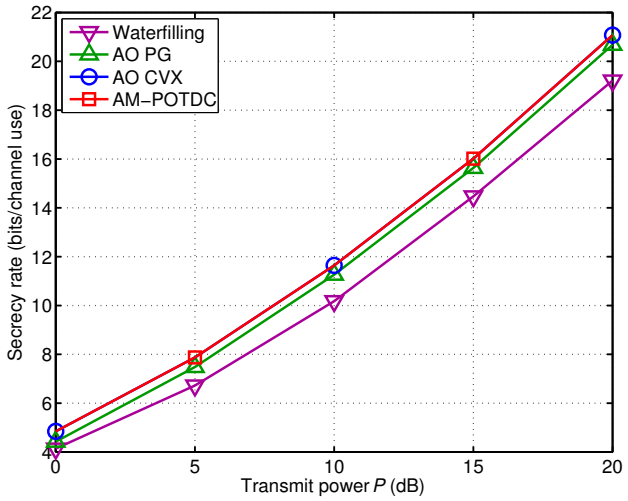

Fig. 2. Secrecy rate versus the total transmit power P for $K = 3$, $N_{\mathrm{a}} = N_{\mathrm{b}} = 6$, and $N_{\mathrm{e}_1} = \ldots = N_{\mathrm{e}_K} = 2$.

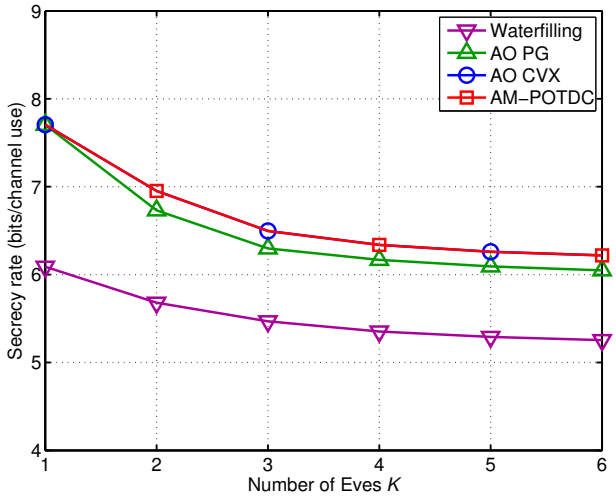

Fig. 3. Secrecy rate versus the number of Eves K for $N_{\mathrm{a}} = N_{\mathrm{b}} = 6$, $N_{\mathrm{e}_1} = \ldots = N_{\mathrm{e}_K} = 2$, and $P = 3$ dB.

have demonstrated the performance of the proposed alternating matrix POTDC algorithm.

6. ACKNOWLEDGMENT

This work was supported by the International Graduate School on Mobile Communications (MOBICOM), Ilmenau, Germany. Moreover, the authors would like to thank Prof. Wing-Kin Ma and his colleagues for providing the codes for [13].

7. REFERENCES

[1] A. D. Wyner, "The wire-tap channel," *The Bell System Technical J.*, vol. 54, pp. 1355-1387, Oct. 1975.

[2] Y. Liang, H. V. Poor, and S. Shamai (Shitz), "Information theoretic security," *Foundations and Trends in Communications and Information Theory*, vol. 5, no. 4-5, pp. 355-580, 2008.

[3] T. Liu and S. Shamai, "A note on the secrecy capacity of the multiple-antenna wiretap channel," *IEEE Transactions on Information Theory*, vol. 55, no. 6, pp. 2547–2553, Jun. 2009.

[4] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas II: The MIMOME wiretap channel," *IEEE Transactions on Information Theory*, vol. 56, no. 11, pp. 5515-5532, Nov. 2010.

[5] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *IEEE Transactions on Information Theory*, vol. 57, no. 8, pp. 4961-4972, Aug. 2011.

[6] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas I: The MISOME wiretap channel," *IEEE Transactions on Information Theory*, vol. 56, no. 7, pp. 3088-3104, July 2010.

[7] R. Bustin, R. Liu, H. V. Poor, and S. Shamai (Shitz), "An MMSE approach to the secrecy capacity of the MIMO Gaussian wiretap channel," *EURASIP J. Wireless Communications and Networking*, 2009.

[8] S. Fakoorian and A. L. Swindlehurst, "Full rank solutions for the MIMO Gaussian wiretap channel with an average power constraint," available online at http://arxiv.org/abs/1210.4795, Oct. 2012.

[9] J. Li and A. P. Petropulu, "Transmitter optimization for achieving secrecy capacity in Gaussian MIMO wiretap channels," available online at http://arxiv.org/abs/0909.2622, Sep. 2009.

[10] S. Fakoorian and A. L. Swindlehurst, "Optimal power allocation for GSVD-based beamforming in the MIMO wiretap channel," in *Proc. IEEE Int. Symposium on Information Theory (ISIT)*, Cambridge, MA, July 2012.

[11] K. Wang, X. Wang, and X. Zhang, "SLNR-based transmit beamforming for MIMO wiretap channel," *Wireless Pers. Commun.*, pp. 1–13, 2012.

[12] Q. Li, M. Hong, H.-T. Wai, W.-K. Ma, Y.-F. Liu and Z.-Q. Luo, "An alternating optimization algorithm for the MIMO secrecy capacity problem under sum power and per-antenna power constraints," in *Proc. IEEE Int. Conference on Acoustics, Speech, and Signal Processing (ICASSP)*, Vancouver, Canada, May 2013.

[13] Q. Li, M. Hong, H.-T. Wai, Y.-F. Liu, W.-K. Ma, and Z.-Q. Luo, "Transmit solutions for MIMO wiretap channels using alternating optimization," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 9, pp. 1714-1727, Sep. 2013.

[14] A. Khabbazibasmenj, M. A. Girnyk, S. A. Vorobyov, M. Vehkaper, and L. K. Rasmussen, "On the optimal precoding for MIMO Gaussian wire-tap Channels," in *Proc. 10-th Int. Symposium on Wireless Communications Systems (ISWCS)*, Ilmenau, Germany, Aug. 2013.

[15] 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 Transactions on Signal Processing*, vol. 60, no. 10, pp. 5478-5493, Oct. 2012.

[16] A. Khabbazibasmenj and S. A. Vorobyov, "Robust adaptive beamforming for general-rank signal model with positive semi-definite constraint via POTDC," *IEEE Transactions on Signal Processing*, vol. 61, no. 23, pp. 6103–6117, Dec. 2013.

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

[18] A. G. Akritas, E. K. Akritas, and G. I. Malaschonok, "Various proofs of Sylvesters (determinant) identity," *Mathematics and Computers in Simulation*, vol. 42, no. 4, pp. 585–593, 1996.

[19] M. Grant and S. Boyd, "CVX: Matlab software for disciplined convex programming," Apr. 2011, http://cvxr.com/cvx.

[20] J. H. Manton, "Optimization algorithms exploiting unitary constraints," *IEEE Transactions on Signal Processing*, vol. 50, no. 3, pp. 635-650, Mar. 2002.

[21] T. Abrudan, J. Eriksson, V. Koivunen, "Conjugate Gradient Algorithm for Optimization Under Unitary Matrix Constraint," *Signal Processing*, vol. 89, no. 9, pp. 1704-1714, Sep. 2009.

[22] R. A. Horn and C. R. Johnson, *Matrix Analysis*, New York: Cambridge University Press, 1988.

[23] J. Dattorro, *Convex Optimization and Euclidean Distance Geometry*, New York: Meboo, 2005.