A Safe Approximation Approach to Secrecy Outage Design for MIMO Wiretap Channels

Qiang Li, *Member, IEEE,* Wing-Kin Ma, *Senior Member, IEEE,* and Anthony Man-Cho So, *Member, IEEE*

***Abstract*—Consider a multi-input multi-output (MIMO) channel wiretapped by multiple multi-antenna eavesdroppers. Assuming imperfect eavesdroppers' channel state information (CSI) at the transmitter, an outage-constrained secrecy rate maximization (OC-SRM) problem is considered. Specifically, we aim to design the transmit covariance matrix such that the outage secrecy rate is maximized for a given outage probability. The OC-SRM problem is challenging, and as a compromise, we resort to a recently developed Bernstein-type inequality approach to obtain a safe (conservative) approximate solution for OC-SRM. The merit of the proposed safe design lies in its tractability. In particular, a safe solution can be efficiently computed by alternately solving two convex conic optimization problems. The efficacy of the proposed design is demonstrated by simulations.**

***Index Terms*—MIMO wiretap channel, Outage secrecy rate, Bernstein-type inequality, Physical-layer security.**

I. Introduction

Physical-layer secrecy has emerged as a promising new approach to the information security problem. In contrast to the widely used cryptographic approach, the idea of physical-layer secrecy is to exploit the channel capacity difference between the legitimate receiver and the eavesdroppers to securely convey the confidential information to the intended receiver [1]. Recently, with the success of multi-input multi-output (MIMO) communications, there has been increasing interest in using the MIMO degrees of freedom (d.o.f.) to enhance physical-layer security [2]–[9]. To fully exploit the MIMO d.o.f., perfect channel state information (CSI) of the links is desired at the transmitter. However, in practice the perfect CSI assumption may be too stringent, especially for the eavesdroppers' channels. As such, there have been a number of works that investigate physical-layer secrecy under imperfect CSI, e.g., the deterministically bounded CSI error model [3], [4] and the random CSI error model [5]–[8], [10]. Here, we focus on the latter.

In this letter, we consider a robust transmit design for an outage-constrained secrecy-rate maximization (OC-SRM) problem under the assumption of Gaussian CSI errors for the eavesdroppers' channels. Specifically, we aim to optimize the covariance matrix of the transmit signal such that the outage secrecy rate is maximized while satisfying a given outage probability requirement. We should mention that apart from the outage-based design formulation, alternatively one can optimize the average (or ergodic) secrecy rate by taking expectation over all possible channel realizations; see, e.g., [11]. In contrast to the average-based design, the outage-based design caters for the delay-critical scenario and provides a probabilistic guarantee for secrecy performance. The OC-SRM problem has been studied in the previous works, e.g., [5]–[8], where both the legitimate receiver and the eavesdropper have a single antenna, i.e., multi-input single-output (MISO) wiretap channel. In particular, the work [5] proposed an approximate solution to the OC-SRM problem for MISO wiretap channels, but the approach developed in [5] is not applicable for the MIMO case. In [6], the authors considered an artificial noise (AN)-aided secrecy outage design and analyzed the optimal power allocation for fixed transmit directions. In [7], [8], the authors characterized the optimal transmit covariance structure and derived a closed-form secrecy outage expression for the case of one MISO eavesdropper. Here we consider a more general scenario—multiple eavesdroppers are present, and both the legitimate receiver and the eavesdroppers have multiple antennas, i.e., MIMO wiretap channels. The considered MIMO OC-SRM problem is more challenging than its SISO/MISO counterparts, owing to the nonconvex and nonsmooth secrecy rate function and the more complicated probabilistic constraint, which generally has no closed-form expression. To tackle these challenges, we adopt an approximation technique to extract a safe (conservative) solution[1] for OC-SRM. Unlike [6]–[8], the proposed approach does not require explicitly calculating the outage probability. The key to this is to employ a Bernstein-type inequality [12] and a conjugate reformulation of the secrecy rate function [13] (see also [9]). The former circumvents the difficulty of the outage probability calculation, while the latter renders a tractable solution for the safe approximation by alternately solving two convex optimization problems.

Notations: $\mathrm{vec}(\mathbf{A})$ denotes the vectorization of matrix $\mathbf{A}$ by stacking its columns; $\mathbf{A} \succeq \mathbf{0}$ means that $\mathbf{A}$ is a Hermitian positive semidefinite matrix; $\mathbb{H}^n(\mathbb{H}^n_+)$ denotes the set of n-by-n Hermitian (positive semidefinite) matrices; $\otimes$ denotes the Kronecker product.

This work is supported by a Direct Grant of the Chinese University of Hong Kong (Project ID: 2050489) and the Hong Kong Research Grants Council (RGC) General Research Fund (GRF) (Project ID: CUHK 416012).

Q. Li is with the School of Communication and Information Engineering, University of Electronic Science and Technology of China, Chengdu, China. E-mail: lq@uestc.edu.cn.

W.-K. Ma is with the Department of Electronic Engineering, The Chinese University of Hong Kong, Shatin, Hong Kong S.A.R., China. E-mail: wkma@ieee.org.

A. M.-C. So is with the Department of Systems Engineering and Engineering Management, The Chinese University of Hong Kong, Shatin, Hong Kong S.A.R., China. E-mail: manchoso@se.cuhk.edu.hk.

[1] By "safe solution" we mean that a solution, which is obtained from solving a conservative approximation of OC-SRM, always fulfills the secrecy outage probabilistic constraint.

II. System Model and Problem Formulation

Consider an MIMO wiretap channel, where a source node intends to transmit confidential information to a legitimate receiver in the presence of multiple eavesdroppers. For ease of exposition, we call the source, the legitimate receiver and the eavesdropper as *Alice*, *Bob* and *Eve*, respectively. We assume that all nodes have multiple antennas, and denote by $\mathbf{H} \in \mathbb{C}^{N_t \times N_b}$ and $\mathbf{G}_k \in \mathbb{C}^{N_t \times N_{e,k}}$ the channel matrices from Alice to Bob, and to the kth Eve respectively, with N_t, N_b and $N_{e,k}$ being the number of transmit antennas, Bob's receive antennas and kth Eve's receive antennas, respectively. Then, the received signals at Bob and Eves may be written as

$$\mathbf{y}_b(t) = \mathbf{H}^H \mathbf{x}(t) + \mathbf{n}_b(t), \tag{1a}$$

$$\mathbf{y}_{e,k}(t) = \mathbf{G}_k^H \mathbf{x}(t) + \mathbf{n}_{e,k}(t), \quad k = 1, \ldots, K, \tag{1b}$$

where K is the number of Eves; $\mathbf{n}_b(t) \sim \mathcal{CN}(\mathbf{0}, \mathbf{I})$ and $\mathbf{n}_{e,k}(t) \sim \mathcal{CN}(\mathbf{0}, \mathbf{I})$, $\forall k$ are i.i.d. standard complex Gaussian noise; $\mathbf{x}(t) \in \mathbb{C}^{N_t}$ is the coded confidential signal, whose distribution follows $\mathcal{CN}(\mathbf{0}, \mathbf{W})$ with $\mathbf{W} \succeq \mathbf{0}$ being the covariance matrix of the transmitted signal. Given $\mathbf{W}$, an achievable secrecy rate of the MIMO Gaussian wiretap channel is given by [1]

$$R_s = \min_{k=1,\ldots,K} f_k(\mathbf{W}), \tag{2}$$

where $f_k(\mathbf{W}) \triangleq C_b(\mathbf{W}) - C_{e,k}(\mathbf{W})$, $C_b(\mathbf{W}) \triangleq \ln|\mathbf{I} + \mathbf{H}^H\mathbf{W}\mathbf{H}|$ and $C_{e,k}(\mathbf{W}) \triangleq \ln|\mathbf{I} + \mathbf{G}_k^H\mathbf{W}\mathbf{G}_k|$. Physically, the rate R_s represents the information rate at which Bob can correctly decode the confidential information, while Eves can retrieve almost no information from their observations [1].

In this work, we assume that Alice has perfect knowledge of Bob's CSI $\mathbf{H}$ and imperfect knowledge of Eves' CSIs $\mathbf{G}_k, \forall k$. The latter is modeled by a random Gaussian model:

$$\mathrm{vec}(\mathbf{G}_k) \sim \mathcal{CN}(\bar{\mathbf{g}}_k, \mathbf{C}_k), \quad k = 1, \ldots, K, \tag{3}$$

where $\bar{\mathbf{g}}_k = \mathrm{vec}(\bar{\mathbf{G}}_k)$ is Alice's estimate of the kth-Eve channel $\mathbf{G}_k$, and $\mathbf{C}_k \in \mathbb{H}_+^{N_t N_{e,k}}$ is the associated channel uncertainty covariance. In addition, $\mathbf{G}_k$ is assumed to be independent of $\mathbf{G}_l$ for any $k \neq l$. Under the above setting, the outage-constrained secrecy rate maximization (OC-SRM) problem may be formulated as follows [7], [8], [10]:

$$\max_{\mathbf{W}, R} \; R \tag{4a}$$

$$\text{s.t. } \Pr_{\{\mathbf{G}_k\}_{k=1}^K}\big\{ \min_{k=1,\ldots,K} f_k(\mathbf{W}) \geq R\big\} \geq 1 - \rho, \tag{4b}$$

$$\mathrm{Tr}(\mathbf{W}) \leq P, \; \mathbf{W} \succeq \mathbf{0}, \tag{4c}$$

where the constant $P > 0$ represents the transmit power budget, and $0 < \rho < 0.5$ is a given parameter specifying the secrecy outage probability—the chance of the achievable secrecy rate falling below the target rate R in the presence of random CSI uncertainty.

The difficulty of solving the OC-SRM problem (4) lies in the probabilistic constraint (4b), which generally has no closed-form expression. Even if it has, the resulting OC-SRM problem is likely to be intractable. In the sequel, we will propose a safe solution for problem (4) by employing recent advances in chance-constrained optimization.

III. A Bernstein-type Inequality-Based Safe Approximation of the OC-SRM Problem

The development of the safe OC-SRM approximation is based on the following observation: If we can find an easy-to-handle function $\varphi(\mathbf{W}, R)$ such that $\varphi(\mathbf{W}, R) \leq 0 \Longrightarrow$ (4b) holds for all $\mathbf{W}$ and R, then any $(\mathbf{W}, R)$ satisfying $\varphi(\mathbf{W}, R) \leq 0$ fulfills the probabilistic constraint (4b), and thus is a safe solution to problem (4).

A. A Safe Approximation of OC-SRM (4)

The development of the safe approximation consists of the following three steps:

Step 1: Decouple the probabilistic constraint: To begin, by noting the independence between $\mathbf{G}_k$ and $\mathbf{G}_l$, $\forall k \neq l$, we have

$$\text{(4b)} \iff \textstyle\prod_{k=1}^K \Pr_{\mathbf{G}_k}\{f_k(\mathbf{W}) \geq R\} \geq 1 - \rho \tag{5a}$$

$$\impliedby \Pr_{\mathbf{G}_k}\{f_k(\mathbf{W}) \geq R\} \geq 1 - \bar{\rho}, \forall k, \tag{5b}$$

where $\bar{\rho} = 1 - (1-\rho)^{1/K}$. Physically, (5b) can be seen as a per-Eve secrecy outage probability. The per-Eve outage probability constraint (5b) is still not convenient to process, owing to the log-det function in f_k. Our next step is to turn f_k into a more convenient form.

Step 2: A convenient approximation of f_k: We need the following lemma:

Lemma 1 The following implication holds true:

$$\exists\, \mathbf{S}_k \in \mathbb{H}_+^{N_{e,k}} \textit{ such that}$$

$$\Pr_{\mathbf{G}_k}\Big\{\mathrm{Tr}\left(\mathbf{G}_k^H\mathbf{W}\mathbf{G}_k\mathbf{S}_k\right) \leq t_k\Big\} \geq 1 - \bar{\rho} \tag{6a}$$

$$\implies \Pr_{\mathbf{G}_k}\{f_k(\mathbf{W}) \geq R\} \geq 1 - \bar{\rho}, \tag{6b}$$

where $t_k = C_b(\mathbf{W}) - R - \mathrm{Tr}(\mathbf{S}_k) + \ln|\mathbf{S}_k| + N_{e,k}$.

The proof of Lemma 1 is relegated to Appendix A. With the implication (6), our challenge now turns to the probabilistic constraint (6a). By letting $\mathbf{g}_k = \mathrm{vec}(\mathbf{G}_k)$ and invoking the identity $\mathrm{Tr}(\mathbf{A}^H\mathbf{B}\mathbf{C}\mathbf{D}) = \mathrm{vec}(\mathbf{A})^H(\mathbf{D}^T \otimes \mathbf{B})\mathrm{vec}(\mathbf{C})$, we have

$$\mathrm{Tr}\left(\mathbf{G}_k^H\mathbf{W}\mathbf{G}_k\mathbf{S}_k\right) = \mathbf{g}_k^H(\mathbf{S}_k^T \otimes \mathbf{W})\mathbf{g}_k. \tag{7}$$

Since $\mathbf{g}_k \sim \mathcal{CN}(\bar{\mathbf{g}}_k, \mathbf{C}_k)$, we can apply the following change of variable

$$\mathbf{g}_k = \bar{\mathbf{g}}_k + \mathbf{C}_k^{1/2}\mathbf{v}_k \tag{8}$$

with $\mathbf{v}_k \sim \mathcal{CN}(\mathbf{0}, \mathbf{I}_{N_t N_{e,k}})$. Now, substituting (7) and (8) into (6a) yields

$$\text{(6a)} \iff \Pr_{\mathbf{v}_k}\left\{\mathbf{v}_k^H\mathbf{A}_k\mathbf{v}_k + 2\mathcal{R}e\{\mathbf{v}_k^H\mathbf{u}_k\} + c_k \geq 0\right\} \geq 1 - \bar{\rho}, \tag{9}$$

where $\mathbf{A}_k = -\mathbf{C}_k^{\frac{1}{2}}\left(\mathbf{S}_k^T \otimes \mathbf{W}\right)\mathbf{C}_k^{\frac{1}{2}}$, $\mathbf{u}_k = -\mathbf{C}_k^{\frac{1}{2}}\left(\mathbf{S}_k^T \otimes \mathbf{W}\right)\bar{\mathbf{g}}_k$ and $c_k = t_k - \bar{\mathbf{g}}_k^H\left(\mathbf{S}_k^T \otimes \mathbf{W}\right)\bar{\mathbf{g}}_k$.

Step 3: A Bernstein-type inequality-based safe approximation: The equivalence in (9) implies that the outage probability in (6a) can be characterized by the quadratic inequality $\mathbf{v}_k^H\mathbf{A}_k\mathbf{v}_k + 2\mathcal{R}e\{\mathbf{v}_k^H\mathbf{u}_k\} + c_k \geq 0$ with respect to (w.r.t.) the Gaussian random vector $\mathbf{v}_k$. Such a chance constraint can be safely approximated using the following Bernstein-type inequality [12]:

Lemma 2 ([12]) For any $(\mathbf{A}, \mathbf{u}, c) \in \mathbb{H}^n \times \mathbb{C}^n \times \mathbb{R}$, $\mathbf{v} \sim \mathcal{CN}(\mathbf{0}, \mathbf{I}_n)$ *and* $\rho \in (0, 1]$, *the following implication holds:*

$$\begin{aligned} &\left\{ \begin{array}{l} \mathrm{Tr}(\mathbf{A}) - \sqrt{-2\ln(\rho)} \cdot x + \ln(\rho) \cdot y + c \geq 0, \\ \left\| \begin{bmatrix} \mathrm{vec}(\mathbf{A}) \\ \sqrt{2}\mathbf{u} \end{bmatrix} \right\|_2 \leq x, \\ y\mathbf{I}_n + \mathbf{A} \succeq \mathbf{0}, \quad y \geq 0 \end{array} \right. \\ &\Longrightarrow \Pr_{\mathbf{v}} \left\{ \mathbf{v}^H \mathbf{A} \mathbf{v} + 2\mathcal{R}e\{\mathbf{v}^H \mathbf{u}\} + c \geq 0 \right\} \geq 1 - \rho, \end{aligned} \tag{10}$$

where x *and* y *are slack variables. Moreover, the system* (10) *is convex in* $(\mathbf{A}, \mathbf{u}, c, x, y)$.

Now, by replacing the hard probabilistic constraint (4b) with the implication (5b), and then by invoking Lemmas 1 and 2, we arrive at the desired safe approximation of OC-SRM, which is shown in (11). From the above development, it can be verified that any feasible solution of (11) must satisfy (6b), owing to the implications in Lemmas 1 and 2. Moreover, it follows from (5) that such a feasible solution also satisfies the probabilistic constraint (4b).

$$\begin{aligned} \max_{\mathbf{W}, R, \{\mathbf{S}_k, x_k, y_k\}_{k=1}^K} \quad & R \\ \text{s.t. } & \mathrm{Tr}(\mathbf{C}_k^{\frac{1}{2}}(\mathbf{S}_k^T \otimes \mathbf{W})\mathbf{C}_k^{\frac{1}{2}}) + \sqrt{-2\ln\bar{\rho}} \cdot x_k - \ln\bar{\rho} \cdot y_k \\ & + R - \ln|\mathbf{I} + \mathbf{H}^H \mathbf{W} \mathbf{H}| + \mathrm{Tr}(\mathbf{S}_k) - \ln|\mathbf{S}_k| \\ & + \bar{\mathbf{g}}_k^H (\mathbf{S}_k^T \otimes \mathbf{W}) \bar{\mathbf{g}}_k \leq N_{e,k}, \quad k = 1, \ldots, K, \\ & \left\| \begin{bmatrix} \mathrm{vec}(\mathbf{C}_k^{\frac{1}{2}}(\mathbf{S}_k^T \otimes \mathbf{W})\mathbf{C}_k^{\frac{1}{2}}) \\ \sqrt{2}\mathbf{C}_k^{\frac{1}{2}}(\mathbf{S}_k^T \otimes \mathbf{W})\bar{\mathbf{g}}_k \end{bmatrix} \right\|_2 \leq x_k, \quad k = 1, \ldots, K, \\ & y_k \mathbf{I}_{N_t N_{e,k}} - \mathbf{C}_k^{\frac{1}{2}}(\mathbf{S}_k^T \otimes \mathbf{W})\mathbf{C}_k^{\frac{1}{2}} \succeq \mathbf{0}, \quad k = 1, \ldots, K, \\ & y_k \geq 0, \quad \mathbf{S}_k \succeq \mathbf{0}, \quad k = 1, \ldots, K, \\ & \mathrm{Tr}(\mathbf{W}) \leq P, \quad \mathbf{W} \succeq \mathbf{0}. \end{aligned} \tag{11}$$

B. An Alternating Optimization Approach to (11)

A merit of the safe approximation (11) is that it has all its constraints explicitly expressed, which facilitates the numerical optimization of $\mathbf{W}$. In particular, one can verify that when fixing either $\mathbf{W}$ or $\{\mathbf{S}_k\}_{k=1}^K$, problem (11) becomes convex w.r.t. the remaining variables. It should however be noted that problem (11) is nonconvex w.r.t. all the variables jointly. For this reason, we employ alternating optimization (AO) to handle problem (11). The AO algorithm for problem (11) is summarized in Algorithm 1. Notice that in lines 3 and 4 of Algorithm 1, the two convex subproblems can be efficiently solved using a general-purpose conic optimization solver, e.g., `SeDuMi` [14]. Moreover, as a basic property of AO, one can check that the $(n-1)$st iterate $(\mathbf{W}^{n-1}, \{\mathbf{S}_k^{n-1}, x_k^{n-1}, y_k^{n-1}\}_{k=1}^K, R^{n-1})$ (cf. line 3) is a feasible solution for the subproblem solved in the nth iteration (cf. line 4). Hence the AO algorithm yields a nondecreasing sequence of the outage secrecy rate, i.e., $R^n \geq \cdots \geq R^0$.

Remark 1 The complexity of the AO algorithm can be roughly estimated through the complexity of solving the AO subproblems times the total number of AO iterations. The latter relies heavily on the stopping criterion, namely the tolerance ϵ (cf. Algorithm 1). In general, the smaller ϵ is, the more AO iterations are needed. According to our numerical experience in Sec. IV, around ten AO iterations are enough to deliver a reasonably good transmit solution.

Algorithm 1 AO Algorithm for the Safe Approximation (11)

1: Initialize $n = 1$, $\epsilon > 0$ and $\mathbf{S}_k^0 = \mathbf{I}$, $k = 1, \ldots, K$;
2: **repeat**
3: Fix $\mathbf{S}_k = \mathbf{S}_k^{n-1}, \forall k$ and solve problem (11) to get $(\mathbf{W}^{n-1}, \{x_k^{n-1}, y_k^{n-1}\}_{k=1}^K, R^{n-1})$;
4: Fix $\mathbf{W} = \mathbf{W}^{n-1}$ and solve problem (11) to get $(\{\mathbf{S}_k^n, x_k^n, y_k^n\}_{k=1}^K, R^n)$;
5: $n = n + 1$;
6: **until** $|R^n - R^{n-1}| < \epsilon$
7: Output $(\mathbf{W}^n, R^n)$.

IV. Simulation Results and Conclusions

In this section, we demonstrate the performance gains of the proposed safe design by comparing it with the plain SVD [3] and the projected SVD [15]. Plain SVD maximizes Bob's channel capacity without considering Eves' receptions; i.e., transmitting over the eigenmodes of $\mathbf{H}$ with powers on each eigenmode determined by water-filling, whereas projected SVD aims to completely null out Eves' receptions by first projecting the transmit signal onto the nullspace of Eves' estimated concatenated channels $\bar{\mathbf{G}} \triangleq [\bar{\mathbf{G}}_1 \ldots, \bar{\mathbf{G}}_K]$ and then performing plain SVD. The simulation settings are as follows unless otherwise specified: $N_t = 5$, $N_b = N_{e,k} = 2$, $\forall k$, $K = 2$, $\rho = 0.01$, $P = 10$dB, $\epsilon = 0.01$, $\mathbf{C}_k = \sigma^2 \mathbf{I}$, $\forall k$ and $\sigma^2 = 0.002$; each entry of $\mathbf{H}$ and $\bar{\mathbf{G}}_k$ is randomly generated following $\mathcal{CN}(0, 1)$. All results were averaged over 100 independent channel trials.

Fig. 1 plots the outage secrecy rates against the average transmit power P. In the legend, 'Bernstein computable lower bound' represents the R^n returned by Algorithm 1, which is a theoretically guaranteed outage secrecy rate when the transmit solution $\mathbf{W}^n$ is used; 'AO with perfect CSI' represents the result of the AO algorithm in [9], where perfect CSI is assumed at the transmitter. Here, we include the result of AO with perfect CSI as a benchmark to evaluate the secrecy rate loss induced by imperfect CSI. The remaining three curves were obtained by substituting the corresponding transmit solutions $\mathbf{W}$ into (4b) to find an R such that

$$R = \sup_{\hat{R}} \{\hat{R} \mid \Pr\{\min_{k=1,\ldots,K} f_k(\mathbf{W}) \geq \hat{R}\} \geq 1 - \rho\}. \tag{12}$$

In general, the supremum in (12) has no closed-form expression, and thus we resort to Monte-Carlo (MC) simulations to evaluate R. From the figure, we see that the proposed safe design outperforms plain SVD and projected SVD. In particular, there is at least 1 bit per channel use secrecy rate gap between the proposed design and the two SVD-based designs. It should however be noted that the two SVD-based designs admit semi-closed-form solution and thus have much lower complexities than the proposed AO design. In addition, we see from Fig. 1 that when the power is small, the Bernstein computable lower bound almost coincides with its MC result, which implies that the proposed safe approximation can achieve a good approximation accuracy for small powers.

Fig. 2 shows the relationship between the outage secrecy rate and Eves' channel uncertainty level σ^2 for various methods. As expected, with the increase of σ^2, the outage secrecy rates of all methods decrease. Moreover, the proposed safe design always achieves a higher outage secrecy rate than the other two SVD-based designs.

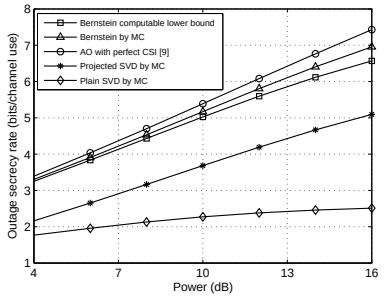

Fig. 1. The outage secrecy rate versus the average transmit power with $\sigma^2 = 0.002$.

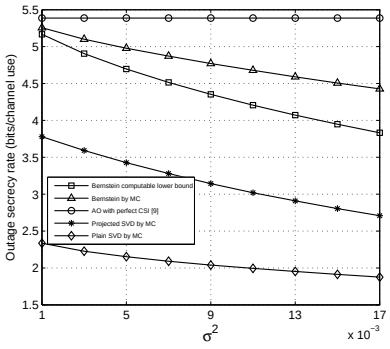

Fig. 2. The outage secrecy rate versus σ^2 with $P = 10$dB.

To conclude, we have considered an outage-constrained secrecy rate maximization (OC-SRM) problem for an MIMO channel overheard by multiple MIMO Eves. To handle the OC-SRM problem, we resort to a Bernstein-type inequality approach to obtain a safe approximate solution. We show that a safe solution can be computed by alternately solving two convex optimization problems. Simulation results demonstrated that the proposed safe design outperforms some existing methods and can achieve good approximation accuracies for small transmit powers or low channel uncertainty levels.

APPENDIX

A. Proof of Lemma 1

We need the following lemma:

Lemma 3 ([13]) Let $\mathbf{E} \in \mathbb{C}^{N\times N}$ *be any matrix such that* $\mathbf{E} \succ \mathbf{0}$. *Consider the function* $\nu(\mathbf{S}, \mathbf{E}) = -\mathrm{Tr}(\mathbf{SE}) + \ln|\mathbf{S}| + N$. *Then,*

$$\ln|\mathbf{E}^{-1}| = \max_{\mathbf{S}\in\mathbb{C}^{N\times N}, \mathbf{S}\succeq\mathbf{0}} \nu(\mathbf{S}, \mathbf{E}). \tag{13}$$

By invoking Lemma 3, we can re-express $C_{e,k}(\mathbf{W})$ as

$$\begin{aligned} C_{e,k}(\mathbf{W}) &= -\ln|(\mathbf{I} + \mathbf{G}_k^H\mathbf{W}\mathbf{G}_k)^{-1}| \\ &= -\max_{\mathbf{S}_k\succeq\mathbf{0}} \nu(\mathbf{S}_k, \mathbf{I} + \mathbf{G}_k^H\mathbf{W}\mathbf{G}_k) \\ &= \min_{\mathbf{S}_k\succeq\mathbf{0}} -\nu(\mathbf{S}_k, \mathbf{I} + \mathbf{G}_k^H\mathbf{W}\mathbf{G}_k) \triangleq \varphi_{e,k}(\mathbf{W}, \mathbf{S}_k), \end{aligned} \tag{14}$$

where $\varphi_{e,k}(\mathbf{W}, \mathbf{S}_k) \triangleq -\nu(\mathbf{S}_k, \mathbf{I} + \mathbf{G}_k^H\mathbf{W}\mathbf{G}_k) = \mathrm{Tr}((\mathbf{I} + \mathbf{G}_k^H\mathbf{W}\mathbf{G}_k)\mathbf{S}_k) - \ln|\mathbf{S}_k| - N_{e,k}$. By substituting (14) into (5b), we have

$$\begin{aligned} & \Pr_{\mathbf{G}_k}\{f_k(\mathbf{W}) \geq R\} \geq 1-\bar{\rho} \\ \Longleftrightarrow\ & \Pr_{\mathbf{G}_k}\Big\{\min_{\mathbf{S}_k\succeq\mathbf{0}} \varphi_{e,k}(\mathbf{W}, \mathbf{S}_k) \leq C_b(\mathbf{W}) - R\Big\} \geq 1-\bar{\rho} \\ \Longleftarrow\ & \Pr_{\mathbf{G}_k}\{\varphi_{e,k}(\mathbf{W}, \mathbf{S}_k) \leq C_b(\mathbf{W}) - R\} \geq 1-\bar{\rho} \\ & \text{for some } \mathbf{S}_k \succeq \mathbf{0} \\ \Longleftrightarrow\ & \Pr_{\mathbf{G}_k}\Big\{\mathrm{Tr}\left(\mathbf{G}_k^H\mathbf{W}\mathbf{G}_k\mathbf{S}_k\right) \leq t_k\Big\} \geq 1-\bar{\rho} \\ & \text{for some } \mathbf{S}_k \succeq \mathbf{0}, \end{aligned}$$

where $t_k = C_b(\mathbf{W}) - R - \mathrm{Tr}(\mathbf{S}_k) + \ln|\mathbf{S}_k| + N_{e,k}$. This completes the proof of Lemma 1.

REFERENCES

[1] 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.

[2] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas I: The MISOME wiretap channel," *IEEE Trans. Inform. Theory*, vol. 56, no. 7, pp. 3088–3104, July 2010.

[3] Q. Li and W.-K. Ma, "Optimal and robust transmit designs for MISO channel secrecy by semidefinite programming," *IEEE Trans. Signal Process.*, vol. 59, no. 8, pp. 3799–3812, Aug. 2011.

[4] J. Huang and A. L. Swindlehurst, "Robust secure transmission in MISO channels based on worst-case optimization," *IEEE Trans. Signal Process.*, vol. 60, no. 4, pp. 1696–1707, Apr. 2012.

[5] Q. Li, W.-K. Ma, and A. M.-C. So, "Safe convex approximation to outage-based MISO secrecy rate optimization under imperfect CSI and with artificial noise," in *Proc. 45th Annual Asilomar Conference on Signals, Systems, and Computers*, Nov. 3-6, 2011, Pacific Grove, California, pp. 207–211.

[6] N. Romero-Zurita, M. Ghogho, and D. McLernon, "Outage probability based power distribution between data and artificial noise for physical layer security," *IEEE Signal Process. Letters*, vol. 19, no. 2, pp. 71–74, Feb. 2012.

[7] S. Gerbracht, C. Scheunert, and E. A. Jorswieck, "Secrecy outage in MISO systems with partial channel information," *IEEE Trans. Information Forensics and Security*, vol. 7, no. 2, pp. 704–716, April 2012.

[8] S. Luo, J. Li, and A. P. Petropulu, "Outage constrained secrecy rate maximization using cooperative jamming," in *IEEE Statistical Sig. Process. Workshop (SSP)*, Aug. 2012, Ann Arbor, USA, pp. 389–392.

[9] 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 J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1714–1727, Sept. 2013.

[10] M. Bloch, J. Barros, M. R. S. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inform. Theory*, vol. 54, no. 6, pp. 2515–2534, June 2008.

[11] P. K. Gopala, L. Lai, and H. E. Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4687–4698, Oct. 2008.

[12] K.-Y. Wang, A. M.-C. So, T.-H. Chang, W.-K. Ma, and C.-Y. Chi, "Outage constrained robust transmit optimization for multiuser MISO downlinks: Tractable approximations by conic optimization," available online at `http://arxiv.org/abs/1108.0982`.

[13] J. Jose, N. Prasad, M. Khojastepour, and S. Rangarajan, "On robust weighted-sum rate maximization in MIMO interference networks," in *Proc. IEEE Int. Conf. Communications (ICC)*, June 5-9, 2011, Kyoto, Japan, pp. 1–6.

[14] J. Sturm, "Using SeDuMi 1.02, a MATLAB toolbox for optimization over symmetric cones," *Optim. Methods Softw.*, vol. 11, pp. 625–653, 1999, (webpage and software) http://sedumi.ie.lehigh.edu/.

[15] L. Zhang, R. Zhang, Y.-C. Liang, Y. Xin, and S. Cui, "On the relationship between the multi-antenna secrecy communications and cognitive radio communications," *IEEE Trans. Commun.*, vol. 58, no. 6, pp. 1877–1886, Jun. 2010.