SAFE CONVEX APPROXIMATION TO OUTAGE-BASED MISO SECRECY RATE OPTIMIZATION UNDER IMPERFECT CSI AND WITH ARTIFICIAL NOISE

Qiang Li, Wing-Kin Ma

Dept. Electronic Engineering
The Chinese University of Hong Kong
E-mail: qli@ee.cuhk.edu.hk, wkma@ieee.org

Anthony Man-Cho So

Dept. of System Eng. & Eng. Management
The Chinese University of Hong Kong
E-mail: manchoso@se.cuhk.edu.hk

ABSTRACT

Consider a scenario in which an MISO channel is overheard by multiple single-antenna eavesdroppers. The transmitter has perfect channel state information (CSI) with the legitimate channel, but has imperfect CSI with the eavesdroppers' channels. The CSI uncertainties are assumed stochastic. We formulate an artificial-noise (AN)-aided secrecy-rate maximization problem where the CSI uncertainties are handled using an outage-based formulation. Our aim is to find, for this problem, tractable designs for the transmit and AN covariances. Unfortunately, outage-based optimization problems are generally difficult to solve. The main contribution here is to derive a safe, convex optimization-based, approximation to the considered problem. The advantages of the method are shown by simulations.

***Index Terms*—** Secrecy capacity, Convex optimization, Bernstein-type inequality, Transmit beamforming

1. INTRODUCTION

Information security is one of the fundamental problems in communications, and this problem is usually tackled by cryptographic approaches. Recently, we have seen flourishing interest in delivering information security from a physical-layer perspective, which is known as *physical-layer secrecy* or *information-theoretic security* [1]. The merit of physical-layer secrecy lies in its provable security, even when we assume that the eavesdropper possesses unlimited computational power. To achieve this, the transmitter need to encode the message into a sequence of random symbols such that the legitimate receiver can correctly decode it, while the eavesdropper retrieve almost no information from its observation [2]. Intuitively, and roughly speaking, this coding-based approach can be regarded as a way of discriminating the legitimate receiver and the eavesdropper in time domain. We can also provide security in space domain. For example, consider a transmitter having multiple antennas. Zero-forcing beamforming may be employed at the transmitter to completely null out the eavesdropper, thereby achieving perfectly secure transmission. In fact, there has been a growing interest in exploiting the spatial degree of freedom to enhance the system security in recent studies [3–9]. Among those works, the artificial noise (AN)-aided approach is promising and has received much attention.

The idea of AN is to send artificially generated noise to interfere the eavesdropper deliberately, without affecting the legitimate receiver too much [5]. This selective interfering process is possible only when the transmitter has multiple antennas. Depending on how accurate the eavesdropper's channel state information (CSI) is known at the transmitter, there are different ways to generate AN: 1) No CSI: a widely used strategy in this case is *isotropic AN* [5], which places AN uniformly in the nullspace of the legitimate channel. 2) Perfect CSI: We can block the eavesdropper much more effectively by aligning AN with the eavesdropper's direction, instead of keeping AN isotropic; see, e.g., [6]. Note that the perfect CSI case may arise from scenarios where the eavesdropper is also a user of the system, and the transmitter wants to provide different services for different types of users. 3) Imperfect CSI: This case may be regarded as being more general than the no CSI and perfect CSI cases, but also more challenging. Some endeavors have recently emerged to address the imperfect CSI case; e.g., the worst-case robust formulation [8].

This paper focuses on the imperfect CSI case. Specifically, we consider the scenario in which an MISO channel is overheard by multiple single-antenna eavesdroppers, and deal with an outage-based robust formulation for AN-aided transmit design optimization under Gaussian CSI uncertainties. Unlike most existing AN designs, we do not impose any orthogonal restrictions on AN. Instead, we attempt to maximize the secrecy rate by jointly optimizing the information and the AN covariances. However, it is challenging to do so, owing to the difficult outage constraint, which has no closed form in general. We handle this problem by developing a safe (conservative) approximation—the method is based on a concurrently developed chance constrained optimization technique, known as Bernstein-type inequality [10, 11]. The merit of the proposed approximation lies in its tractability. In particular, the proposed safe approximation can be reformulated as a one-dimensional line search problem, whose optimal solution can be efficiently computed by solving a sequence of convex optimization problems. By investigating the optimality conditions of the safe approximation under an independent and identically distributed (i.i.d.) isotropic Gaussian CSI error model, we found that the optimal information and AN covariances are closely related to the isotropic AN design, thereby explaining in part the validity of the isotropic AN from an outage perspective.

This paper is organized as follows. Problem formulation is given in Section 2. Section 3 develops a Bernstein-type inequality-based safe approximation to the outage-based transmit optimization problem. Simulation results comparing the proposed design and isotropic AN design are illustrated in Section 4. Section 5 concludes the paper.

Notations: vec($\mathbf{A}$) denotes the vectorization of matrix $\mathbf{A}$ by stacking its columns; $\mathbf{A} \succeq \mathbf{0}$ ($\mathbf{A} \succ \mathbf{0}$) means that $\mathbf{A}$ is a Hermitian positive semidefinite (definite) matrix; $\mathbb{H}^N$ and $\mathbb{H}^N_+$ denote the set of all N-by-N Hermitian matrices and Hermitian positive semidefinite matrices, respectively; $\mathbf{A} \perp \mathbf{B}$ signifies that $\mathbf{A}$ is orthogonal to $\mathbf{B}$, i.e., $\mathbf{A}^H\mathbf{B} = \mathbf{0}$; $\mathbf{x} \sim \mathcal{CN}(\boldsymbol{\mu}, \boldsymbol{\Omega})$ means that $\mathbf{x} - \boldsymbol{\mu}$ is a random vector following a circular symmetric complex Gaussian distribution

This work was supported by a Direct Grant awarded by the Chinese University of Hong Kong (Project Code 2050489).

with covariance $\mathbf{\Omega}$.

2. PROBLEM FORMULATION

2.1. Background

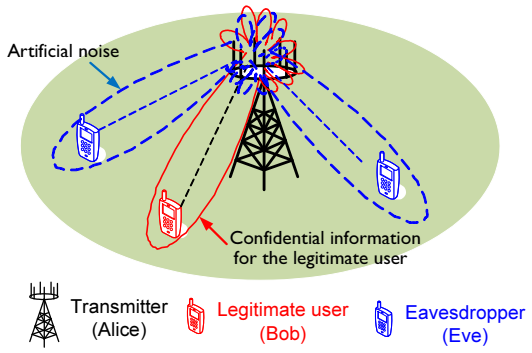

Fig. 1. System model.

Consider the wireless scenario shown in Fig. 1, where a multi-antenna transmitter communicates with a single-antenna receiver in the presence of a number of single-antenna eavesdroppers. The eavesdroppers are assumed to be non-colluding. The task of the transmitter is, intuitively speaking, to manipulate its multi-antenna degree of freedom in accordance with its knowledge about the CSI of the receivers, both legitimate and eavesdropping, so that good information security can be achieved. To make this process more effective, the transmitter would also use a fraction of its transmit power to send artificially generated noise to interfere the eavesdroppers.

The signal model is as follows. For ease of exposition, we will refer to the transmitter, legitimate receiver and eavesdropper as *Alice*, *Bob* and *Eve*, respectively. Assuming slow frequency-flat fading channels for all the communication links, the received signals at Alice and Eves are respectively modeled as

$$y_b(t) = \mathbf{h}^H \mathbf{x}(t) + n_b(t), \tag{1a}$$

$$y_{e,k}(t) = \mathbf{g}_k^H \mathbf{x}(t) + n_{e,k}(t), \quad k = 1, \ldots, K, \tag{1b}$$

where $\mathbf{h} \in \mathbb{C}^{N_t}$ is the channel vector from Alice to Bob; $\mathbf{g}_k \in \mathbb{C}^{N_t}$ is the channel vector from Alice to the kth Eve; K is the number of Eves; N_t is the number of transmit antennas employed by Alice; $n_b(t)$ and $n_{e,k}(t)$, $k = 1, \ldots, K$ are i.i.d. complex Gaussian noise with zero mean and unit variance; $\mathbf{x}(t) \in \mathbb{C}^{N_t}$ is the transmitted signal vector by Bob. The transmitted signal consists of two components:

$$\mathbf{x}(t) = \mathbf{s}(t) + \mathbf{z}(t),$$

where $\mathbf{s}(t)$ is the encoded confidential information signal intended for Bob; $\mathbf{z}(t)$ is the artificial noise for interfering Eves' reception. We assume $\mathbf{s}(t) \sim \mathcal{CN}(\mathbf{0}, \mathbf{W})$ (i.e., vector Gaussian codebook), where $\mathbf{W}$ is the transmit covariance. The AN $\mathbf{z}(t)$ is assumed to be independent of $\mathbf{s}(t)$, and follow a distribution $\mathbf{z}(t) \sim \mathcal{CN}(\mathbf{0}, \mathbf{\Sigma})$ where $\mathbf{\Sigma}$ is the AN covariance.

This work considers the design of the transmit covariance $\mathbf{W}$ and AN covariance $\mathbf{\Sigma}$ under an achievable secrecy rate maximization formulation. Given $(\mathbf{W}, \mathbf{\Sigma})$, the achievable secrecy rate is given by [12]

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

where $f_k(\mathbf{W}, \mathbf{\Sigma})$ is the mutual information difference of Bob and the kth Eve:

$$f_k(\mathbf{W}, \mathbf{\Sigma}) = C_b(\mathbf{W}, \mathbf{\Sigma}) - C_{e,k}(\mathbf{W}, \mathbf{\Sigma}),$$

$$C_b(\mathbf{W}, \mathbf{\Sigma}) = \log_2 \left(1 + \frac{\mathbf{h}^H \mathbf{W} \mathbf{h}}{1 + \mathbf{h}^H \mathbf{\Sigma} \mathbf{h}}\right),$$

$$C_{e,k}(\mathbf{W}, \mathbf{\Sigma}) = \log_2 \left(1 + \frac{\mathbf{g}_k^H \mathbf{W} \mathbf{g}_k}{1 + \mathbf{g}_k^H \mathbf{\Sigma} \mathbf{g}_k}\right).$$

Note that (2) is a rate at which perfect secrecy is possible; i.e., Bob can correctly decode the confidential information at R bits per channel use, while Eves can retrieve almost nothing [2]. Suppose that Alice has perfect CSI of Bob and Eves, or full information of $\mathbf{h}$ and $\{\mathbf{g}_k\}_{k=1}^K$. The secrecy-rate maximization (SRM) formulation for designing $(\mathbf{W}, \mathbf{\Sigma})$ is as follows:

$$\begin{aligned} \max_{\mathbf{W} \succeq \mathbf{0}, \mathbf{\Sigma} \succeq \mathbf{0}} \quad & \min_{k=1,\ldots,K} f_k(\mathbf{W}, \mathbf{\Sigma}) \\ \text{s.t.} \quad & \mathrm{Tr}(\mathbf{W} + \mathbf{\Sigma}) \leq P, \end{aligned} \tag{3}$$

where $P > 0$ denotes a (given) average transmit power limit. We should point out that while (3) is optimal in providing the best achievable secrecy rate, it is a challenging problem involving joint optimization of $\mathbf{W}, \mathbf{\Sigma}$. In our previous work [8], we have developed a tractable solution to (3) by using convex optimization machinery. More precisely, the work [8] solved a worst-case robust extension of (3) where Eves' CSI is assumed to be imperfectly known.

2.2. Outage Constrained Secrecy-Rate Maximization

Our interest in the present paper lies in an outage constrained SRM (OC-SRM) formulation. In this formulation, we assume that Alice has perfect knowledge of Bob's CSI, but imperfect knowledge of Eves' CSI. The latter is modeled by a random Gaussian model (see, e.g., [9]), in which the CSI of the kth Eve is modeled as

$$\mathbf{g}_k \sim \mathcal{CN}(\bar{\mathbf{g}}_k, \mathbf{C}_k), \quad k = 1, \ldots, K, \tag{4}$$

where $\bar{\mathbf{g}}_k$ is Alice's estimate of the kth-Eve channel $\mathbf{g}_k$, and $\mathbf{C}_k \in \mathbb{H}_+^{N_t}$ is the associated channel uncertainty covariance. In addition, $\mathbf{g}_k$ is assumed independent of $\mathbf{g}_l$, for any $k \neq l$.

The OC-SRM problem is formulated as follows:

$$\max_{\mathbf{W} \succeq \mathbf{0}, \mathbf{\Sigma} \succeq \mathbf{0}, R} \quad R \tag{5a}$$

$$\text{s.t.} \quad \Pr_{\{\mathbf{g}_k\}_{k=1}^K} \left\{ \min_{k=1,\ldots,K} f_k(\mathbf{W}, \mathbf{\Sigma}) \geq R \right\} \geq 1 - \rho, \tag{5b}$$

$$\mathrm{Tr}(\mathbf{W} + \mathbf{\Sigma}) \leq P, \tag{5c}$$

where $0 < \rho < 0.5$ is a given parameter specifying the maximum tolerable probability of the achievable secrecy rate falling below R, or, simply, secrecy outage probability[1]. In other words, the chance of perfect secrecy, under imperfect CSI, is guaranteed to be at least $1 - \rho$.

The OC-SRM problem (5) is even more challenging to solve than the perfect-CSI SRM problem (3) (as well as its worst-case robust extension). The main difficulty lies in the probability function in (5b), which appears to have no closed-form expression. Hence,

[1]Note that there are other possibilities to define the outage probability (cf. [13]); herein we adopt the definition in [14] for simplicity.

in what follows, we will make a compromise by deriving a safe approximation to OC-SRM. By "safe approximation" we mean that the approximation formulation has its optimal solution always fulfilling the probabilistic constraint (5b). In other words, the safe approximation is a restriction of, or conservation approximation to, the original OC-SRM problem. Moreover, the safe approximation is developed in such a way that its solution can be efficiently computable by available convex optimization tools.

3. A BERNSTEIN-TYPE INEQUALITY-BASED SAFE APPROXIMATION TO THE OC-SRM PROBLEM

We present the proposed safe OC-SRM approximation by dividing the derivations into three steps. Among them, the second step, application of Bernstein-type inequality, is most significant providing us with a tractable handle with the challenging probabilistic constraints.

3.1. Step 1: Decoupling the probabilistic constraint (5b)

In (5b), the probability term is coupled among Eves. Our first step is to decouple (5b) into per-Eve terms. By noting the independence between $\mathbf{g}_k$ and $\mathbf{g}_l$, $\forall k \neq l$, we have the following implication:

$$\text{(5b)} \iff \prod_{k=1}^{K} \Pr_{\mathbf{g}_k}\left\{f_k(\mathbf{W},\mathbf{\Sigma}) \geq R\right\} \geq 1-\rho, \tag{6a}$$

$$\impliedby \Pr_{\mathbf{g}_k}\left\{f_k(\mathbf{W},\mathbf{\Sigma}) \geq R\right\} \geq 1-\bar{\rho}, \forall k. \tag{6b}$$

where $\bar{\rho} = 1-(1-\rho)^{1/K}$. Physically, the implication (6b) means that we constrain the outage probability of each mutual information difference (which can be seen as a per-Eve secrecy rate) to be no greater than $\bar{\rho}$, thereby fulfilling the overall secrecy outage probability constraint (5b).

3.2. Step 2: Application of Bernstein-type inequality to (6b)

Our challenge now turns to the probabilistic constraints $\Pr_{\mathbf{g}_k}\left\{f_k(\mathbf{W},\mathbf{\Sigma}) \geq R\right\} \geq 1-\bar{\rho}$. Since $\mathbf{g}_k \sim \mathcal{CN}(\bar{\mathbf{g}}_k, \mathbf{C}_k)$, we can make a change of variable

$$\mathbf{g}_k = \bar{\mathbf{g}}_k + \mathbf{C}_k^{1/2}\mathbf{v}_k, \tag{7}$$

with $\mathbf{v}_k \sim \mathcal{CN}(\mathbf{0}, \mathbf{I}_{N_t})$. By substituting (7) into $f_k(\mathbf{W},\mathbf{\Sigma})$, and through some careful derivations, one can obtain

$$f_k(\mathbf{W},\mathbf{\Sigma}) \geq R \iff \mathbf{v}_k^H\mathbf{A}_k\mathbf{v}_k + 2\mathcal{R}e\{\mathbf{v}_k^H\mathbf{u}_k\} + c_k \geq 0, \tag{8}$$

where

$$\begin{aligned}
\beta &= 1+\frac{\mathbf{h}^H\mathbf{W}\mathbf{h}}{1+\mathbf{h}^H\mathbf{\Sigma}\mathbf{h}},\\
\mathbf{A}_k &= \mathbf{C}_k^{1/2}\left((2^{-R}\beta-1)\mathbf{\Sigma}-\mathbf{W}\right)\mathbf{C}_k^{1/2},\\
\mathbf{u}_k &= \mathbf{C}_k^{1/2}\left((2^{-R}\beta-1)\mathbf{\Sigma}-\mathbf{W}\right)\bar{\mathbf{g}}_k,\\
c_k &= \bar{\mathbf{g}}_k^H\left((2^{-R}\beta-1)\mathbf{\Sigma}-\mathbf{W}\right)\bar{\mathbf{g}}_k + 2^{-R}\beta - 1.
\end{aligned}$$

In particular, (8) shows that the inequality $f_k(\mathbf{W},\mathbf{\Sigma}) \geq R$ can be expressed as a quadratic inequality with respect to the complex Gaussian vector $\mathbf{v}_k$. This means that in the implication in (6b), we are dealing with *chance quadratic constraints*.

Chance quadratic constraints generally do not have closed-form expressions, and, in fact, are unlikely to be tractable. What further adds to the difficulty is that the matrices $\mathbf{A}_k$ are generally indefinite, and as a result the quadratic inequalities in (8) are indefinite. However, there exist safe tractable approximations to general chance quadratic constraints. One is the Bernstein-type inequality by Bechar [11], which is very recently converted by us to provide safe approximation to a different transmit optimization problem [10]. The result is summarized as follows:

Lemma 1. *([10]) 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 true:*

$$\begin{aligned}
&\Pr_{\mathbf{v}}\left\{\mathbf{v}^H\mathbf{A}\mathbf{v} + 2\mathcal{R}e\{\mathbf{v}^H\mathbf{u}\} + c \geq 0\right\} \geq 1-\rho\\
\impliedby &\begin{cases}
\mathrm{Tr}(\mathbf{A}) - \sqrt{-2\ln(\rho)}\cdot x + \ln(\rho)\cdot y + c \geq 0,\\
\left\|\begin{bmatrix}\mathrm{vec}(\mathbf{A})\\ \sqrt{2}\mathbf{u}\end{bmatrix}\right\|_2 \leq x,\\
y\mathbf{I}_n + \mathbf{A} \succeq \mathbf{0}, \quad y \geq 0,
\end{cases}
\end{aligned} \tag{9}$$

where x and y are slack variables. Moreover, Eqs. (9) *are convex in $(\mathbf{A},\mathbf{u},c,x,y)$.*

We are now ready to present the safe OC-SRM approximation. By replacing the hard probabilistic constraint (5b) with the implication (6b), and then by applying Lemma 1 to (6b) (note (8)), we obtain the following safe approximation to OC-SRM:

$$R^\star = \max_{\substack{\mathbf{W},\mathbf{\Sigma},R,\beta\\ \{x_k\}_{k=1}^K,\{y_k\}_{k=1}^K}} \quad R \tag{10a}$$

$$\text{s.t. } \mathrm{Tr}(\mathbf{A}_k) - \sqrt{-2\ln(\bar{\rho})}\cdot x_k + \ln(\bar{\rho})\cdot y_k + c_k \geq 0,\ \forall k \tag{10b}$$

$$\left\|\begin{bmatrix}\mathrm{vec}(\mathbf{A}_k)\\ \sqrt{2}\mathbf{u}_k\end{bmatrix}\right\|_2 \leq x_k,\ \forall k, \tag{10c}$$

$$y_k\mathbf{I}_{N_t} + \mathbf{A}_k \succeq \mathbf{0}, \quad y_k \geq 0,\ \forall k, \tag{10d}$$

$$\frac{\mathbf{h}^H\mathbf{W}\mathbf{h}}{1+\mathbf{h}^H\mathbf{\Sigma}\mathbf{h}} = \beta - 1, \tag{10e}$$

$$\mathrm{Tr}(\mathbf{W}+\mathbf{\Sigma}) \leq P,\ \ \mathbf{W} \succeq \mathbf{0},\ \ \mathbf{\Sigma} \succeq \mathbf{0}. \tag{10f}$$

A significant merit of the safe approximation (10) is that all its constraints have explicit forms. However, by careful inspection, one can see that problem (10) is still nonconvex. We deal with this issue in the next step.

3.3. Step 3: One-variable-parameterized convex reformulation of (10)

While the safe approximation (10) is nonconvex, it can be reformulated to a form where the problem is convex when one particular variable is fixed. Hence, by doing line search over that variable, we can solve (10) optimally.

To describe the reformulation, we note that the left hand side of (10e) is a linear fractional function, which can be simplified by using the Charnes-Cooper transformation [15]. Specifically, by letting

$$\mathbf{Q} = \xi\mathbf{W}, \quad \mathbf{\Gamma} = \xi\mathbf{\Sigma}, \quad \xi > 0, \tag{11}$$

and making a change of variables

$$\nu = 2^{-R}\beta, \quad \eta = 2^R, \tag{12}$$

problem (10) can be transformed to the following equivalent problem:

$$\max_{\substack{\mathbf{Q},\mathbf{\Gamma},\nu,\eta,\xi \\ \{\hat{x}_k\}_{k=1}^K,\{\hat{y}_k\}_{k=1}^K}} \quad \eta \tag{13a}$$

$$\text{s.t.} \quad \mathrm{Tr}(\hat{\mathbf{A}}_k) - \sqrt{-2\ln(\bar{\rho})}\cdot\hat{x}_k + \ln(\bar{\rho})\cdot\hat{y}_k + \hat{c}_k \geq 0,\ \forall k \tag{13b}$$

$$\left\| \begin{bmatrix} \mathrm{vec}(\hat{\mathbf{A}}_k) \\ \sqrt{2}\hat{\mathbf{u}}_k \end{bmatrix} \right\|_2 \leq \hat{x}_k,\ \ \forall k, \tag{13c}$$

$$\hat{y}_k\mathbf{I} + \hat{\mathbf{A}}_k \succeq \mathbf{0}, \quad \hat{y}_k \geq 0,\ \ \forall k, \tag{13d}$$

$$\mathbf{h}^H\mathbf{Q}\mathbf{h} = \nu\eta - 1, \tag{13e}$$

$$\xi + \mathbf{h}^H\mathbf{\Gamma}\mathbf{h} = 1, \tag{13f}$$

$$\mathrm{Tr}(\mathbf{Q}+\mathbf{\Gamma}) \leq P\xi,\ \mathbf{Q}\succeq\mathbf{0},\ \mathbf{\Gamma}\succeq\mathbf{0},\ \xi\geq 0, \tag{13g}$$

where

$$\begin{aligned}
\hat{\mathbf{A}}_k &= \xi\mathbf{A}_k = \mathbf{C}_k^{1/2}\left((\nu-1)\mathbf{\Gamma}-\mathbf{Q}\right)\mathbf{C}_k^{1/2}, \\
\hat{\mathbf{u}}_k &= \xi\mathbf{u}_k = \mathbf{C}_k^{1/2}\left((\nu-1)\mathbf{\Gamma}-\mathbf{Q}\right)\bar{\mathbf{g}}_k, \\
\hat{c}_k &= \xi c_k = \bar{\mathbf{g}}_k^H\left((\nu-1)\mathbf{\Gamma}-\mathbf{Q}\right)\bar{\mathbf{g}}_k + (\nu-1)\xi.
\end{aligned}$$

Note that as a common trick in the Charnes-Cooper transformation, (13f) is introduced to fix the denominator of the linear fraction function in (10e). In (13g), we have replaced $\xi > 0$ by $\xi \geq 0$; this mild relaxation causes no loss, since any feasible ξ of (13) has to be positive, for otherwise (13g) implies that $\mathbf{Q} = \mathbf{\Gamma} = \mathbf{0}$, which violates (13f).

Problem (13) is nonconvex with respect to all the optimization variables, but is convex for a fixed ν. Specifically, problem (13), for a fixed ν, is a conic (and convex) program involving positive semidefinite constraints and second order cone constraints. Hence, we recast (13) as

$$\max_{\nu} \ \varphi(\nu) \tag{14a}$$

$$\text{s.t.}\ \ 1 \leq \nu \leq 1 + P\|\mathbf{h}\|^2, \tag{14b}$$

where

$$\varphi(\nu) = \max_{\substack{\mathbf{Q},\mathbf{\Gamma},\eta,\xi \\ \{\hat{x}_k\}_{k=1}^K,\{\hat{y}_k\}_{k=1}^K}} \quad \eta \quad \text{s.t.}\ \ (13\text{b}) - (13\text{g}). \tag{15}$$

In (14b), the lower bound on ν is due to the feasibility of (6b). To see this, supposing $\nu = 2^{-R}\beta < 1$, then one can check that $\mathbf{v}_k^H\mathbf{A}_k\mathbf{v}_k + 2\mathcal{R}e\{\mathbf{v}_k^H\mathbf{u}_k\} + c_k < 0$ holds for arbitrary $\mathbf{v}_k$, and thus (6b) cannot be satisfied. The upper bound on ν is derived as follows:

$$\nu = 2^{-R}\beta \leq \beta = 1 + \frac{\mathbf{h}^H\mathbf{W}\mathbf{h}}{1+\mathbf{h}^H\mathbf{\Sigma}\mathbf{h}} \leq 1 + \mathbf{h}^H\mathbf{W}\mathbf{h} \leq 1 + P\|\mathbf{h}\|^2$$

where the first inequality is due to the secrecy rate $R \geq 0$; the last inequality follows from $\mathrm{Tr}(\mathbf{W}) \leq P$; and the equality can be achieved with $\mathbf{W} = P\mathbf{h}\mathbf{h}^H/\|\mathbf{h}\|^2$.

Note that (14) is a box-constrained single-variable optimization problem, whose objective value can be evaluated by solving the conic program (15) (say, using available software [16]). Therefore, (14) can be handled by performing one-dimensional line search over ν. There are many derivative-free search algorithms that one can use, e.g., Golden search [17], compass or coordinate search [18], etc. Once (14) has been solved, $\mathbf{W}$ and $\mathbf{\Sigma}$ can be recovered through (12).

Our development of safe OC-SRM approximation is now complete. We have the following remark.

Remark 1: The safe OC-SRM approximation derived above not only provides a tractable way to optimize the transmit solution $(\mathbf{W}, \mathbf{\Sigma})$, it also gives an efficiently computable lower bound on the outage-constrained secrecy rate R. For example, given a transmit solution $(\mathbf{W}, \mathbf{\Sigma})$ of some other methods, what one may desire to do is to evaluate its outage-constrained secrecy rate. The safe approximation method can be used to compute a lower bound on its outage-constrained secrecy rate (by fixing $(\mathbf{W}, \mathbf{\Sigma})$ in the safe approximation problem). While we can also use Monte-Carlo simulations to obtain an accurate evaluation of the outage-constrained secrecy rate, such evaluation can be computationally demanding especially for small outage specification ρ.

Before closing this section, let us see some physical interpretations of the proposed design. For simplicity, consider an i.i.d. isotropic Gaussian CSI model:

$$\mathbf{g}_k \sim \mathcal{CN}(\mathbf{0}, \sigma^2\mathbf{I}),\ k = 1, \ldots, K \tag{16}$$

for some $\sigma > 0$. We can show the following:

Proposition 1. *Suppose that a positive secrecy rate $R^\star$ can be achieved in* (10) *under the i.i.d. isotropic Gaussian CSI model. Then, the optimal $\mathbf{W}^\star$ and $\mathbf{\Sigma}^\star$ in* (10) *must satisfy*

$$\mathbf{W}^\star = \boldsymbol{w}^\star\boldsymbol{w}^{\star H}, \quad \mathbf{\Sigma}^\star \perp (\boldsymbol{w}^\star + \tau^\star\mathbf{h})$$

for some $\boldsymbol{w}^\star \in \mathbb{C}^{N_t} \neq \mathbf{0}$ and $\tau^\star \in \mathbb{C} \neq \mathbf{0}$.

The proof is omitted due to lack of space. From Proposition 1, we can see at least two physical interpretations of the proposed design under the considered scenario: 1) *Transmit beamforming* is an optimal transmit strategy for the proposed design; 2) the AN should be placed orthogonally to a linear combination of the beamforming direction and the legitimate user's channel direction. Actually, by simulation, we found that the optimal beamforming direction $\boldsymbol{w}^\star$ always aligns with $\mathbf{h}$, and $\mathbf{\Sigma}^\star$, if it is nonzero, is orthogonal to $\mathbf{h}$ with its components uniformly distributed on the nullspace of $\mathbf{h}$. This observation in part explains the validity of the popular isotropic-AN design from an outage perspective.

4. SIMULATION RESULTS

In this section, two simulations are presented to demonstrate the efficacy of the proposed safe approximation solution. Unless specified, we set $N_t = 4$, $K = 5$, $\rho = 0.05$, $\sigma = 0.1$, and $P = 10$dB. The i.i.d. isotropic Gaussian CSI model in (16) is adopted. All the simulation results were averages of 500 independent trials. At each trial, $\mathbf{h}$ is randomly generated following $\mathcal{CN}(\mathbf{0}, \mathbf{I})$.

The proposed safe approximation solution is compared with the isotropic AN solution in [19], which is a simple method. Our performance measure is the outage-constrained (OC) secrecy rate; given a transmit solution $(\mathbf{W}, \mathbf{\Sigma})$, either the proposed or the isotropic AN solution, the outage-constrained secrecy rate is defined as

$$R_{MC} = \sup_R\{R \mid \Pr\{\min_{k=1,\ldots,K} f_k(\mathbf{W}, \mathbf{\Sigma}) \geq R\} \geq 1-\rho\} \tag{17}$$

The OC secrecy rate above has no analytical expression, and we have to evaluate it by Monte-Carlo (MC) simulations (hence the subscript 'MC' in (17)).

Fig. 2 plots the OC secrecy rates against the average transmit power P. In the legend, 'AN Bernstein by MC' and 'isotropic AN

by MC' represent MC-evaluated OC secrecy rates R_{MC} of the proposed safe approximation solution and isotropic AN solution, respectively. In addition, 'AN Bernstein computable lower bound' is the rate outputted by the proposed solution, i.e., $R^\star$ in (10). Note that this is a guaranteed OC secrecy rate value obtained by the proposed safe optimization, rather than MC evaluation. We can see from Fig. 2 that the proposed solution outperforms the isotropic AN for $P \leq 20$ dB, and otherwise for $P > 20$ dB. This means that the advantage of the proposed safe approximation lies in lower transmit powers. This is further confirmed when we observe the gaps between 'AN Bernstein by MC' and 'AN Bernstein computable lower bound'—smaller gaps mean better approximation accuracies.

In Fig. 3 we demonstrate how the Eves' CSI uncertainty level σ affects the OC secrecy rates. The proposed safe approximation solution is seen to exhibit better performance for smaller σ.

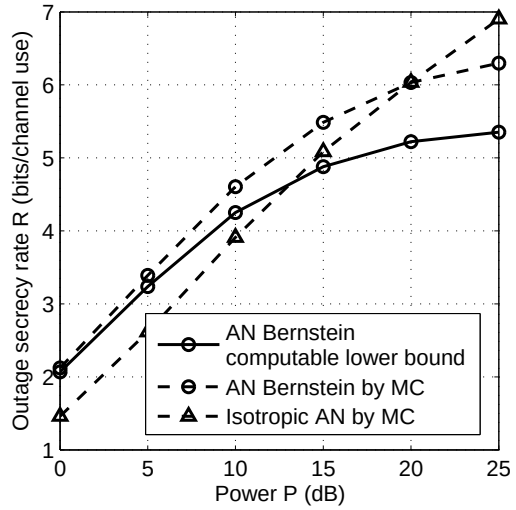

Fig. 2. The outage secrecy rate versus the average transmit power.

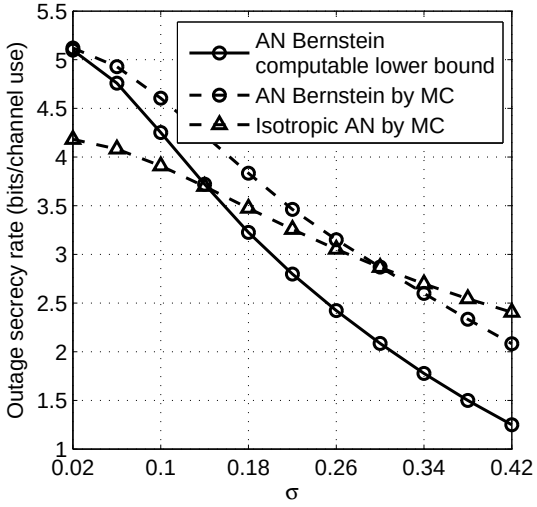

Fig. 3. The outage secrecy rate versus σ.

5. CONCLUSION

To conclude, this paper has considered an outage-constrained secrecy rate maximization problem for an MISO channel overheard by multiple single-antenna Eves. This is a challenging problem, and we have developed a safe approximation method for this problem, using a concurrent chance constrained optimization technique called Bernstein-type inequality. The resulting safe approximation can be efficiently handled by solving a sequence of convex problems. Simulation results demonstrate that the proposed design can give a better performance than the isotropic AN design under some scenarios. As a future work, it is worthwhile to investigate how the approximation quality of the proposed design can be further improved, e.g., by resorting to advanced probability theory.

6. 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. D. Wyner, "The wiretap channel," in *The Bell System Technical Journal*, vol. 54, October 1975, pp. 1355–1387.

[3] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," in *IEEE Int'l Symp. on Info. Theory*, July 2008, pp. 524–528.

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

[5] R. Negi and S. Goel, "Secret communication using artificial noise," in *IEEE Vehicular Technology Conference*, Sept. 2005, pp. 1906–1910.

[6] W.-C. Liao, T.-H. Chang, W.-K. Ma, and C.-Y. Chi, "QoS-based transmit beamforming in the presence of eavesdroppers: An optimized artificial-noise-aided approach," *IEEE Trans. Signal Process.*, vol. 59, no. 3, pp. 1202–1216, Mar. 2011.

[7] A. L. Swindlehurst, "Fixed SINR solution for the MIMO wiretap channel," in *Proc. ICASSP 2009*, April 2009, pp. 2437–2440.

[8] Q. Li and W.-K. Ma, "A robust artificial noise aided transmit design for MISO secrecy," in *ICASSP 2011*, May 2011, pp. 3436 – 3439.

[9] S. Gerbracht, A. Wolf, and E. A. Jorswieck, "Beamforming for fading wiretap channels with partial channel information," in *International ITG Workshop on Smart Antennas, Bremen, Germany*, Feb. 2010.

[10] 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`.

[11] I. Bechar, "A Bernstein-type inequality for stochastic processes of quadratic forms of Gaussian variables," available online at `http://arxiv.org/abs/0909.3595`.

[12] Y. Liang, G. Kramer, H. V. Poor, and S. Shamai (Shitz), "Compound wire-tap channels," in *Proc. 45th Annual Allerton Conf. Commun., Control, and Computing*, Sept. 2007, pp. 136–143.

[13] X. Zhou, M. R. McKay, B. Maham, and A. Hjørungnes, "Rethinking the secrecy outage formulation: A secure transmission design perspective," *IEEE Commun. Lett.*, vol. 15, no. 3, pp. 302–304, Mar. 2011.

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

[15] A. Charnes and W. W. Cooper, "Programming with linear fractional functionals," *Naval Res. Logistics Quarterly*, vol. 9, pp. 181–186, 1962.

[16] M. Grant and S. Boyd, "CVX: Matlab software for disciplined convex programming, version 1.21," http://cvxr.com/cvx, Apr. 2011.

[17] D. Bertsekas, *Nonlinear Programming*. Belmont, MA: Athena Scientific, 1999.

[18] A. R. Conn, K. Scheinberg, and L. N. Vicente, *Introduction to derivative-free optimization*. Philadelphia: MPS-SIAM Series on Optimization, 2009.

[19] X. Zhou and M. R. McKay, "Secure transmission with artificial noise over fading channels: Achievable rate and optimal power allocation," *IEEE Trans. Veh. Tech.*, vol. 59, no. 8, pp. 3831–3842, Oct. 2010.