Spatially Selective Artificial-Noise Aided Transmit Optimization for MISO Multi-Eves Secrecy Rate Maximization

Qiang Li[†] and Wing-Kin Ma[‡]

Abstract

Consider an MISO channel overheard by multiple eavesdroppers. Our goal is to design an artificial noise (AN)-aided transmit strategy, such that the achievable secrecy rate is maximized subject to the sum power constraint. AN-aided secure transmission has recently been found to be a promising approach for blocking eavesdropping attempts. In many existing studies, the confidential information transmit covariance and the AN covariance are not simultaneously optimized. In particular, for design convenience, it is common to prefix the AN covariance as a specific kind of spatially isotropic covariance. This paper considers joint optimization of the transmit and AN covariances for secrecy rate maximization (SRM), with a design flexibility that the AN can take any spatial pattern. Hence, the proposed design has potential in jamming the eavesdroppers more effectively, based upon the channel state information (CSI). We derive an optimization approach to the SRM problem through both analysis and convex conic optimization machinery. We show that the SRM problem can be recast as a single-variable optimization problem, and that resultant problem can be efficiently handled by solving a sequence of semidefinite programs. Our framework deals with a general setup of multiple multi-antenna eavesdroppers, and can cater for additional constraints arising from specific application scenarios, such as interference temperature constraints in interference networks. We also generalize the framework to an imperfect CSI case where a worst-case robust SRM formulation is considered. A suboptimal but safe solution to the outage-constrained robust SRM design is also investigated. Simulation results show that the proposed AN-aided SRM design yields significant secrecy rate gains over an optimal no-AN design and the isotropic AN design, especially when there are more eavesdroppers.

Index terms– Physical-layer security, artificial noise, transmit beamforming, semidefinite program.

EDICS: MSP-CODR (MIMO precoder/decoder design), MSP-APPL (Applications of MIMO communications and signal processing), SAM-BEAM (Applications of sensor and array multichannel processing)

[§] Copyright (c) 2012 IEEE. Personal use of this material is permitted. However, permission to use this material for any other purposes must be obtained from the IEEE by sending a request to pubs-permissions@ieee.org. This work is supported by a Direct Grant awarded by the Chinese University of Hong Kong (Project Code 2050489).

[†]Qiang Li is with Department of Electronic Engineering, The Chinese University of Hong Kong, Shatin, Hong Kong S.A.R., China. E-mail: qli@ee.cuhk.edu.hk.

[‡]Wing-Kin Ma is the corresponding author. Address: Department of Electronic Engineering, The Chinese University of Hong Kong, Shatin, Hong Kong S.A.R., China. E-mail: wkma@ieee.org.

I. Introduction

In the last decade, multi-antenna techniques have been extensively investigated from the perspective of providing high throughput and reliable communications. Recently, there has been growing interest in using multiple antennas to achieve secure communication, which is known as *physical-layer secrecy*. Intuitively speaking, the idea of physical-layer secrecy is to add structured redundancy in the transmit signal such that the legitimate user can correctly decode the confidential information, but the eavesdroppers can retrieve almost nothing from their observations [1], [2]. To make physical-layer secrecy viable, we usually need the legitimate user's channel condition to be better than the eavesdroppers'. However, this may not be always possible in practice. To alleviate the dependence on the channels conditions, recent studies are mainly focused on multi-antenna transmission, since multiple transmit antennas provide spatial degrees of freedom (d.o.f.) to degrade the reception of the eavesdroppers. A possible way to do this is transmit beamforming, which concentrates the transmit signal over the direction of the legitimate user while reducing power leakage to the eavesdroppers at the same time. Apart from this, a more active approach is to send artificially generated noise to interfere the eavesdroppers deliberately.

The notion of using artificial noise (AN) to enhance physical-layer security was first introduced by Negi and Goel in [3], and has received much attention in recent studies; see [3]–[9] and the references therein. The way of generating AN depends on how much the transmitter knows the eavesdroppers' channel state information (CSI). Consider a case where no eavesdropper's CSI is available. A popular design in such a case is *isotropic AN* [3], where AN is uniformly spread on the legitimate channel's nullspace. By doing so, one can guarantee that no interference will be made to the legitimate receiver, while the eavesdroppers' reception may be degraded by AN. A picture is shown in Fig. 1(a) to illustrate how the isotropic AN design works. On the other hand, consider cases where the eavesdroppers' CSI is available. This may arise from scenarios where the eavesdroppers are also users of the system, and the transmitter aims to provide different types of users with different services. Moreover, for an active eavesdropper, the CSI can be estimated from the eavesdropper's transmission. More interestingly, a very recent study has suggested that even for a passive eavesdropper, there is a possibility for one to estimate the CSI through the local oscillator power inadvertently leaked from the eavesdropper's receiver RF frontend [10]. With knowledge of CSI, we can block the eavesdroppers much more effectively by generating spatially selective AN, rather than keeping AN isotropic [11], [12]. Fig. 1(b) shows a picture to illustrate the idea of spatially selective AN. However, perfect CSI may not be always available in practice, and an important issue is how to robustify a secure transmit design in the presence of imperfect CSI, which is a more general and realistic assumption. Tackling imperfect CSI in physical-layer security is presently an emerging subject with several concurrent endeavors; e.g., the worst-case robust design [13]–[15], the outage robust design [16], [17] and the ergodic design [8].

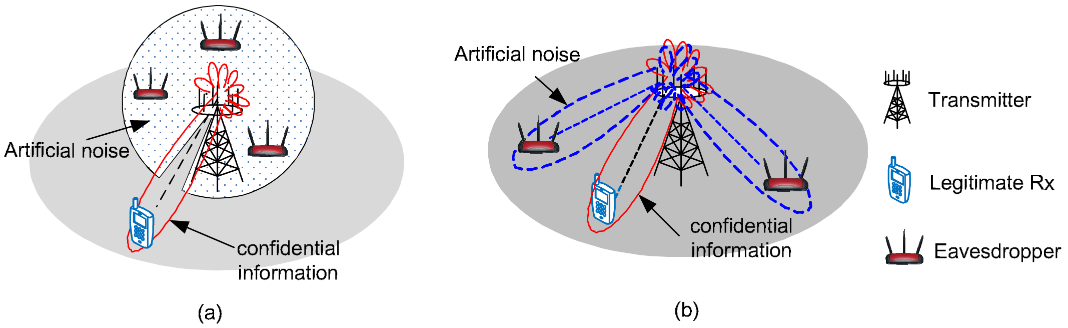


Fig. 1. Secure transmission by (a) isotropic AN; (b) spatially selective AN.

This paper concentrates on the problem of AN-aided secrecy rate maximization (SRM) of a multi-input single-output (MISO) channel overheard by multiple multi-antenna eavesdroppers, with either perfect or imperfect CSI. This problem has been addressed when there is no AN [15] (also [4] for the one eavesdropper case). In the present problem, we consider joint optimization of the confidential information covariance and the AN covariance, and there is a design flexibility for the AN to take any spatial pattern. This AN-aided SRM problem is a challenging optimization problem. The main difficulty lies in the AN covariance, which makes the secrecy rate expression more complicated to optimize. To make the AN-aided SRM problem easier to handle, a vast majority of existing works have to impose additional restrictions on AN, which leads to tractable but SRM suboptimal designs. For example, [3]–[8], [13], [16], [17] restrict AN in the nullspace of the legitimate channel, [11] requires AN to cause no decrease in the legitimate channel's mutual information, and [9], [18], [19] assume that transmit beamforming is employed to generate AN. We should point out that all the above mentioned works consider only one eavesdropper and the sum power constraint. On the other hand, there are works that consider additional design constraints for satisfying some application-specific requirements, e.g., per-antenna power constraints, and the interference temperature constraints for interference networks [20]–[22]. However, AN is not incorporated in those designs and only one single-antenna eavesdropper is assumed. In addition, there are some other AN-aided secure transmit designs, e.g., the SINR-based design [5], [12] and the MSE-based design [23]. However, the goal of those designs is to provide the legitimate receiver with certain QoS, rather than directly maximizing the secrecy rate.

In this paper, we will develop a semidefinite program (SDP)-based optimization approach to handle the

AN-aided SRM problem, with no structural restrictions on the AN. Our problem formulation considers multiple multi-antenna evesdroppers, either perfect or imperfect CSI with the eavesdroppers, and additional design constraints arising from certain application-specific scenarios (such as the aforementioned). Our main contributions are summarized as follows.

1) For the perfect CSI case, we derive an equivalent problem of the SRM problem through analysis. The equivalent problem is less complex than the original SRM. We show that the equivalent problem can be recast as a single-variable optimization problem, and that the latter can be handled by solving a sequence of convex SDPs, for which efficient and reliable solvers are readily available [24], [25].
2) For the imperfect CSI case, we consider a worst-case robust extension of the SRM problem. We show that the worst-case robust SRM (WCR-SRM) problem can be handled in a similar manner as SRM, though the development is more involved and a specific matrix inequality lemma is required. A suboptimal but safe solution to an outage-constrained robust SRM (OCR-SRM) problem is also investigated.
3) Our SRM problem formulation assumes general transmit covariance for the confidential information, and does not fix the transmit strategy as transmit beamforming. Interestingly, in deriving the equivalent SRM problem, we show that *transmit beamforming is an SRM optimal strategy for the confidential information transmission.* This result is meaningful in giving a theoretical justification for using transmit beamforming in the considered scenario. Moreover, the result applies to both the perfect CSI case and worst-case robust imperfect CSI case. We should mention that the optimality of transmit beamforming has been proven in [4], [26] under the assumption of one eavesdropper, no AN and perfect CSI. Our result in comparison is more general.

This paper is organized as follows. A system model description and problem statement is given in Section II. Section III considers the SRM problem for the MISO multi-eavesdropper scenario with perfect CSI, wherein the SDP-based optimization approach is established. Section IV extends the SRM results to the imperfect CSI case. Simulation results comparing the proposed SRM solutions and some other suboptimal secrecy transmit designs are illustrated in Section V. Section VI concludes the paper.

Our notations are as follows. $\mathbf{A}^H$, Tr$(\mathbf{A})$, rank$(\mathbf{A})$ and $\det(\mathbf{A})$ represent the Hermitian (conjugate) transpose, trace, rank and determinant of a matrix $\mathbf{A}$; $\mathbf{I}$ denotes an identity matrix; $\|\cdot\|$ and $\|\cdot\|_F$ represent the ℓ_2 norm and Frobenius norm, respectively; $\mathbf{A} \succeq \mathbf{0}$ $(\mathbf{A} \succ \mathbf{0})$ means that $\mathbf{A}$ is a Hermitian positive semidefinite (definite) matrix; $[\mathbf{A}]_{m,n}$ denotes the (m,n)th element of matrix $\mathbf{A}$; $\mathbb{R}_+$ denotes the set of all nonnegative real numbers; $\mathbb{H}_+^N$ denotes the set of all N-by-N Hermitian positive semidefinite matrices;

$\mathbf{x} \sim \mathcal{CN}(\boldsymbol{\mu}, \boldsymbol{\Omega})$ means that $\mathbf{x}$ is a random vector following a complex circular Gaussian distribution with mean $\boldsymbol{\mu}$ and covariance $\boldsymbol{\Omega}$.

II. System Model and Problem Statement

A. System Model

Consider the scenario shown in Fig. 1(b). A multi-antenna transmitter, called *Alice*, intends to send confidential information to a single-antenna legitimate receiver, called *Bob*, in the presence of a number of multi-antenna eavesdroppers, called *Eves*. All the communication links are assumed to undergo slow frequency-flat fading. The received signals at Bob and Eves may then be modeled as

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

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

respectively, where $\mathcal{K} \triangleq \{1, \ldots, K\}$; $\mathbf{h} \in \mathbb{C}^{N_t}$ is the channel response from Alice to Bob, with N_t being the number of transmit antennas; $\mathbf{G}_k \in \mathbb{C}^{N_t \times N_{e,k}}$ is the channel response from Alice to kth Eve, with $N_{e,k}$ being the number of receive antennas at kth Eve; K is the number of Eves; $n(t) \sim \mathcal{CN}(0,1)$ and $\mathbf{v}_k(t) \sim \mathcal{CN}(\mathbf{0}, \mathbf{I}_{N_{e,k}})$ are standard additive white complex Gaussian noises at Bob and kth Eve, respectively; $\mathbf{x}(t) \in \mathbb{C}^{N_t}$ is the transmit signal vector, which possesses the following form

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

Here, $\{\mathbf{s}(t)\}$ is the coded confidential information intended for Bob, and $\mathbf{z}(t)$ is the noise vector artificially created by Alice to interfere Eves, i.e., the so-called AN. The confidential signal vector $\mathbf{s}(t)$ is assumed to follow a complex Gaussian distribution $\mathcal{CN}(\mathbf{0}, \mathbf{W})$ [2], where $\mathbf{W}$ is the transmit covariance and is to be designed. For the AN, we assume $\mathbf{z}(t) \sim \mathcal{CN}(\mathbf{0}, \boldsymbol{\Sigma})$, where $\boldsymbol{\Sigma}$ is the AN covariance and is again to be designed. Note that if $\mathbf{W}$ is chosen such that $\mathbf{W} = \boldsymbol{w}\boldsymbol{w}^H$ for some $\boldsymbol{w} \in \mathbb{C}^{N_t}$, or equivalently, $\mathrm{rank}(\mathbf{W}) \leq 1$, then the transmit strategy for the confidential information is transmit beamforming; viz., $\mathbf{s}(t) = \boldsymbol{w}s(t)$ where $s(t)$ is a data stream carrying the confidential information.

B. Problem Statement

Our problem is to design the transmit and AN covariances $\mathbf{W}, \boldsymbol{\Sigma}$ such that maximum information secrecy can be achieved. Given $(\mathbf{W}, \boldsymbol{\Sigma})$, an achievable secrecy rate is given by [27]

$$R_s = \min_{k \in \mathcal{K}} \left\{ C_b(\mathbf{W}, \boldsymbol{\Sigma}) - C_{e,k}(\mathbf{W}, \boldsymbol{\Sigma}) \right\}, \tag{2}$$

where $C_b(\mathbf{W}, \mathbf{\Sigma})$ and $C_{e,k}(\mathbf{W}, \mathbf{\Sigma})$ are the mutual information at Bob and Eves, respectively:

$$C_b(\mathbf{W}, \mathbf{\Sigma}) = \log\left(1 + \frac{\mathbf{h}^H \mathbf{W} \mathbf{h}}{1 + \mathbf{h}^H \mathbf{\Sigma} \mathbf{h}}\right), \tag{3a}$$

$$C_{e,k}(\mathbf{W}, \mathbf{\Sigma}) = \log\det(\mathbf{I} + (\mathbf{I} + \mathbf{G}_k^H \mathbf{\Sigma} \mathbf{G}_k)^{-1} \mathbf{G}_k^H \mathbf{W} \mathbf{G}_k). \tag{3b}$$

Note that (2) is a rate at which perfect secrecy is possible; i.e., Bob can correctly decode the confidential information at R_s bits per channel use, while Eves can retrieve almost nothing about the information. Readers are referred to the information theoretic security literature, such as [2], for the detail. Assuming perfect CSI at Alice, the *secrecy-rate maximization (SRM)* design problem is formulated as:

$$R_s^\star = \max_{\mathbf{W} \succeq \mathbf{0}, \mathbf{\Sigma} \succeq \mathbf{0}} \ \min_{k \in \mathcal{K}} \{C_b(\mathbf{W}, \mathbf{\Sigma}) - C_{e,k}(\mathbf{W}, \mathbf{\Sigma})\} \tag{4a}$$

$$\text{s.t. } \operatorname{Tr}(\mathbf{W} + \mathbf{\Sigma}) \leq P, \tag{4b}$$

$$\operatorname{Tr}(\mathbf{\Phi}_l(\mathbf{W} + \mathbf{\Sigma})) \leq \rho_l, \ \forall l \in \mathcal{L}, \tag{4c}$$

where $\mathcal{L} \triangleq \{1, \ldots, L\}$; $P > 0$ specifies the transmit sum power budget, and $\mathbf{\Phi}_l \in \mathbb{H}_+^{N_t}$, $\rho_l \in \mathbb{R}_+, \ \forall l \in \mathcal{L}$, are given design parameters. A standard SRM problem has the sum power constraint (4b), but not (4c). In the following, we describe two application-specific scenarios where (4c) is necessary.

1) *Per-antenna power constraints*: In multi-antenna system implementations, each antenna is often equipped with its own power amplifier (PA). In order to operate within the linear region of each PA, one may want to limit the per-antenna peak power [22], [28]. The per-antenna power constraints can be formulated as

$$[\mathbf{W} + \mathbf{\Sigma}]_{ll} \leq \rho_l, \quad l = 1, \ldots, N_t, \tag{5}$$

where ρ_l is the power limit of the lth antenna. The per-antenna power constraints above can be represented by (4c), by setting $\mathbf{\Phi}_l = \mathbf{e}_l \mathbf{e}_l^H$, $L = N_t$, where $\mathbf{e}_l$ is the lth unit vector (i.e., $[\mathbf{e}_l]_i = 1$ for $i = l$ and $[\mathbf{e}_l]_i = 0$ for all $i \neq l$).

2) *Interference temperature constraints*: Consider an extension of the secure communication problem setup in Section II-A, where the system is operating under an interference network scenario. In such a case, besides the security concern arising from Eves, Alice also needs to cautiously control her transmission such that no excessive interference will be made to other network users. Take the spectrum-sharing cognitive radio (CR) network as an example. Alice and Bob are the secondary transmitter and receiver, respectively. To limit interference to the primary users, the following

interference temperature constraints can be added in the SRM design [20]:

$$\mathrm{Tr}\left(\mathbf{R}_l^H(\mathbf{W}+\mathbf{\Sigma})\mathbf{R}_l\right) \leq \rho_l, \quad l=1,\ldots,L, \tag{6}$$

where $\mathbf{R}_l \in \mathbb{C}^{N_t \times N_{p,l}}$ is the channel response from Alice to lth primary user, with $N_{p,l}$ being the number of receive antennas at the lth primary user; L is the number of primary users; $\rho_l \geq 0$ is the maximal allowable interference level of the lth primary user. The interference temperature constraints (6) can be represented by (4c), by setting $\mathbf{\Phi}_l \triangleq \mathbf{R}_l\mathbf{R}_l^H$, $l=1,\ldots,L$. It is worthwhile to note that apart from CR, the same interference control idea may be applied to multicell interference networks [29].

III. An SDP-based Approach to the SRM Problem

In this section, we derive an SDP-based optimization approach to the SRM problem (4).

A. A Tight Relaxation of the SRM Problem (4)

To start with, we rewrite the SRM problem (4) as

$$R_s^\star = \max_{\mathbf{W}\succeq\mathbf{0},\mathbf{\Sigma}\succeq\mathbf{0},\beta\geq1} C_b(\mathbf{W},\mathbf{\Sigma}) - \log\beta \tag{7a}$$

$$\text{s.t. } C_{e,k}(\mathbf{W},\mathbf{\Sigma}) \leq \log\beta,\ \forall k\in\mathcal{K}, \tag{7b}$$

$$\mathrm{Tr}(\mathbf{W}+\mathbf{\Sigma}) \leq P,\ \mathrm{Tr}(\mathbf{\Phi}_l(\mathbf{W}+\mathbf{\Sigma})) \leq \rho_l,\ \forall l\in\mathcal{L}, \tag{7c}$$

where β is a slack variable introduced to simplify the objective function. Physically, $\log\beta$ can be interpreted as the maximal allowable mutual information of Eves' links. By adjusting β, we can control the level of mutual information between Alice and Eves, and consequently, the secrecy rate. By substituting (3a) and (3b) into (7), we express problem (7) as

$$R_s^\star = \max_{\mathbf{W},\mathbf{\Sigma},\beta} \log\left(1+\frac{\mathbf{h}^H\mathbf{W}\mathbf{h}}{1+\mathbf{h}^H\mathbf{\Sigma}\mathbf{h}}\right) - \log\beta \tag{8a}$$

$$\text{s.t. } \log\det\left(\mathbf{I}+\left(\mathbf{I}+\mathbf{G}_k^H\mathbf{\Sigma}\mathbf{G}_k\right)^{-1}\mathbf{G}_k^H\mathbf{W}\mathbf{G}_k\right) \leq \log\beta,\ \forall k\in\mathcal{K}, \tag{8b}$$

$$\mathbf{W}\succeq\mathbf{0},\ \mathbf{\Sigma}\succeq\mathbf{0},\ \beta\geq1,\ \text{and (7c) satisfied.}$$

Problem (8) is nonconvex. In particular, the most challenging part lies in (8b), which can be verified to be nonconvex and may be difficult to deal with. To circumvent this difficulty, our idea is to derive a relatively easy-to-handle inequality in place of (8b):

Proposition 1. *The following implication holds*

$$\log\det\left(\mathbf{I} + \left(\mathbf{I} + \mathbf{G}^H\mathbf{\Sigma}\mathbf{G}\right)^{-1}\mathbf{G}^H\mathbf{W}\mathbf{G}\right) \leq \log\beta \tag{9a}$$

$$\Longrightarrow\ (\beta-1)(\mathbf{I} + \mathbf{G}^H\mathbf{\Sigma}\mathbf{G}) - \mathbf{G}^H\mathbf{W}\mathbf{G} \succeq \mathbf{0} \tag{9b}$$

for any $\mathbf{G} \in \mathbb{C}^{N\times M}$*,* $\mathbf{W} \in \mathbb{H}_+^N$*, and* $\mathbf{\Sigma} \in \mathbb{H}_+^N$*. Moreover,* (9a) *and* (9b) *are equivalent if* $\operatorname{rank}(\mathbf{W}) \leq 1$.

The proof of Proposition 1 is given in Appendix A. From Proposition 1, we note the following:

Remark 1. The merit of (9b) is that for any fixed β, (9b) is a convex inequality. Specifically, (9b) is a linear matrix inequality w.r.t. $(\mathbf{W}, \mathbf{\Sigma})$. In comparison, in (9a), we are confronted with the troublesome matrix inversion and determinant.

Remark 2. Proposition 1 indicates that any $(\mathbf{W}, \mathbf{\Sigma}, \beta)$ satisfying (9a) also satisfies (9b). In other words, (9b) is a relaxation of (9a) in the sense that replacing (8b) with (9b) yields a larger feasible solution set (or equivalently higher secrecy rate) for the SRM problem (8). In addition, such a replacement makes no difference if $\operatorname{rank}(\mathbf{W}) \leq 1$.

Now, let us replace (8b) with (9b) and consider the subsequent *relaxed SRM problem*, which is formulated as follows:

$$\bar{R}_s^\star = \max_{\mathbf{W},\mathbf{\Sigma},\beta}\ \log\left(\frac{1 + \mathbf{h}^H(\mathbf{W}+\mathbf{\Sigma})\mathbf{h}}{\beta(1+\mathbf{h}^H\mathbf{\Sigma}\mathbf{h})}\right) \tag{10a}$$

$$\text{s.t. } (\beta-1)(\mathbf{I} + \mathbf{G}_k^H\mathbf{\Sigma}\mathbf{G}_k) \succeq \mathbf{G}_k^H\mathbf{W}\mathbf{G}_k,\ \forall k \in \mathcal{K}, \tag{10b}$$

$$\mathbf{W} \succeq \mathbf{0},\ \ \mathbf{\Sigma} \succeq \mathbf{0},\ \ \beta \geq 1,\ \text{(7c) satisfied}, \tag{10c}$$

where $\bar{R}_s^\star$ denotes the optimal objective value of problem (10). As discussed in Remark 2, problem (10) relaxes the feasible solution set of problem (8), and hence has $R_s^\star \leq \bar{R}_s^\star$ in general. Interestingly, we show that $R_s^\star = \bar{R}_s^\star$ always holds for problem (10).

Theorem 1. *Problem* (10) *is a tight relaxation to, or an equivalent form of, the SRM problem* (8)*. In particular, there exists an optimal solution* $(\mathbf{W}^\star, \mathbf{\Sigma}^\star, \beta^\star)$ *of problem* (10)*, for which* $\operatorname{rank}(\mathbf{W}^\star) \leq 1$*; the solution* $(\mathbf{W}^\star, \mathbf{\Sigma}^\star, \beta^\star)$ *is also an optimal solution of problem* (8)*, achieving* $R_s^\star = \bar{R}_s^\star$*.*

Theorem 1 suggests that we can equivalently solve the SRM problem (8) by solving the relaxed (and less difficult) problem (10). The proof of Theorem 1 is relegated to Appendix B. The intuition behind the proof is the equivalence between (10b) and (8b) when $\operatorname{rank}(\mathbf{W}) \leq 1$, cf. Proposition 1. This key observation motivates us to prove the existence of an optimal $\mathbf{W}^\star$ of problem (10) that has $\mathrm{rank}(\mathbf{W}^\star) \leq 1$. We have the following remarks for Theorem 1:

Remark 3. Theorem 1 implies that the SRM problem (8) admits an optimal $\mathbf{W}^\star$ with $\mathrm{rank}(\mathbf{W}^\star) \leq 1$, which holds true irrespective of the number of Eves and the number of antennas of Eves. Physically, it means that transmit beamforming is an optimal strategy for the confidential information transmission.

Remark 4. One should note that the solution correspondence between (8) and (10) holds not only at the optimal $\beta^\star$. In fact, the proof of the theorem reveals that given any feasible β in (8), the corresponding optimal $(\mathbf{W}, \mathbf{\Sigma})$ can be found by solving the relaxation (10) for the same β.

In Theorem 1, our statement is that a rank-one SRM-optimal $\mathbf{W}^\star$ exists for problem (10). In fact, the proof of Theorem 1 reveals that a rank-one SRM-optimal $\mathbf{W}^\star$ can always be constructed algorithmically. Based on the proof, we have the following rank-one solution construction procedure:

Corollary 1. *Suppose that* $(\bar{\mathbf{W}}^\star, \bar{\mathbf{\Sigma}}^\star, \beta^\star)$ *is an optimal solution returned by solving problem* (10). *If* $\mathrm{rank}(\bar{\mathbf{W}}^\star) \leq 1$, *then output* $(\bar{\mathbf{W}}^\star, \bar{\mathbf{\Sigma}}^\star, \beta^\star)$ *as an optimal solution of the SRM problem* (8). *Otherwise, solve the following SDP*

$$\begin{aligned} (\mathbf{W}^\star, \mathbf{\Sigma}^\star) = \arg \min_{\mathbf{W}\succeq \mathbf{0}, \mathbf{\Sigma}\succeq \mathbf{0}} \ & \mathrm{Tr}(\mathbf{W} + \mathbf{\Sigma}) \\ \text{s.t. } & \mathbf{h}^H \left(\mathbf{W} + \mu \mathbf{\Sigma}\right) \mathbf{h} + \mu \geq 0, \\ & (\beta^\star - 1)(\mathbf{I} + \mathbf{G}_k^H \mathbf{\Sigma} \mathbf{G}_k) \succeq \mathbf{G}_k^H \mathbf{W} \mathbf{G}_k, \ \forall k \in \mathcal{K}, \\ & \mathrm{Tr}\left(\mathbf{\Phi}_l(\mathbf{W} + \mathbf{\Sigma})\right) \leq \rho_l, \ \forall l \in \mathcal{L}, \end{aligned} \tag{11}$$

where $\mu = 1 - \beta^\star 2^{\bar{R}_s^\star}$, *and output* $(\mathbf{W}^\star, \mathbf{\Sigma}^\star, \beta^\star)$ *as an optimal solution of the SRM problem* (8). *In particular, it must hold true that* $\mathrm{rank}(\mathbf{W}^\star) \leq 1$.

Corollary 1 is a direct consequence of the proof of Theorem 1; see Appendix B for the details.

B. An SDP-based Line Search Method for Relaxed SRM (10)

We now focus on solving the tight SRM relaxation (10) derived in the last subsection. Problem (10) can be reformulated as a one-variable optimization problem, which can be efficiently handled by solving a sequence of SDPs. To show this, note that

$$\beta \leq 1 + \frac{\mathbf{h}^H \mathbf{W} \mathbf{h}}{1 + \mathbf{h}^H \mathbf{\Sigma} \mathbf{h}} \leq 1 + \mathbf{h}^H \mathbf{W} \mathbf{h} \leq 1 + P \|\mathbf{h}\|^2, \tag{12}$$

where the first inequality is due to (10a) and $R_s^\star \geq 0$, and the third inequality follows from the fact that $\mathbf{h}^H\mathbf{W}\mathbf{h} \leq \mathrm{Tr}(\mathbf{W})\|\mathbf{h}\|^2$ for any $\mathbf{W} \succeq \mathbf{0}$ and $\mathrm{Tr}(\mathbf{W}) \leq P$. Then we rewrite (10) as

$$\begin{aligned} \bar{\gamma}^\star = \max_{\alpha} \quad & \varphi(\alpha) \\ \text{s.t.} \quad & (1 + P\|\mathbf{h}\|^2)^{-1} \leq \alpha \leq 1, \end{aligned} \tag{13}$$

where $\log \bar{\gamma}^\star = \bar{R}_s^\star$, $\alpha = 1/\beta$ and

$$\varphi(\alpha) \triangleq \max_{\mathbf{W},\mathbf{\Sigma}} \frac{1 + \mathbf{h}^H(\mathbf{W} + \mathbf{\Sigma})\mathbf{h}}{\alpha^{-1}(1 + \mathbf{h}^H\mathbf{\Sigma}\mathbf{h})} \tag{14a}$$

$$\text{s.t. } (\alpha^{-1} - 1)(\mathbf{I} + \mathbf{G}_k^H\mathbf{\Sigma}\mathbf{G}_k) \succeq \mathbf{G}_k^H\mathbf{W}\mathbf{G}_k, \ \forall k \in \mathcal{K}, \tag{14b}$$

$$\mathbf{W} \succeq \mathbf{0}, \ \mathbf{\Sigma} \succeq \mathbf{0}, \ \text{and (7c) satisfied.} \tag{14c}$$

The function $\varphi(\alpha)$ does not have a closed form, but is numerically tractable. In particular, (14) can be converted to a convex optimization problem. By applying the Charnes-Cooper transformation [30], where we introduce a change of variables

$$\mathbf{W} = \mathbf{Q}/\xi, \quad \mathbf{\Sigma} = \mathbf{\Gamma}/\xi, \quad \xi > 0, \tag{15}$$

we can equivalently express (14) as

$$\varphi(\alpha) = \max_{\mathbf{Q},\mathbf{\Gamma},\xi} \xi + \mathbf{h}^H(\mathbf{Q} + \mathbf{\Gamma})\mathbf{h} \tag{16a}$$

$$\text{s.t. } \xi + \mathbf{h}^H\mathbf{\Gamma}\mathbf{h} = \alpha, \tag{16b}$$

$$(1 - \alpha)(\xi\mathbf{I} + \mathbf{G}_k^H\mathbf{\Gamma}\mathbf{G}_k) \succeq \alpha\mathbf{G}_k^H\mathbf{Q}\mathbf{G}_k, \ \forall k \in \mathcal{K}, \tag{16c}$$

$$\mathrm{Tr}\left(\mathbf{\Phi}_l(\mathbf{Q} + \mathbf{\Gamma})\right) \leq \rho_l\xi, \ \forall l \in \mathcal{L}, \tag{16d}$$

$$\mathrm{Tr}(\mathbf{Q} + \mathbf{\Gamma}) \leq \xi P, \ \mathbf{Q} \succeq \mathbf{0}, \ \mathbf{\Gamma} \succeq \mathbf{0}. \tag{16e}$$

The motivation of the transformation above is that we want to transform the fractional objective function in (14a), which is quasiconvex but not convex, to the linear (and convex) objective function in (16a). Intuitively, the idea is to fix the denominator of (14a), and that leads to the constraint in (16b). The proof of the solution equivalence of problems (14) and (16) can be easily obtained by following the argument in [15]. The upshot of the transformation above is that problem (16) is a convex SDP, which can be efficiently and conveniently solved in a globally optimal manner by off-the-shelf conic optimization softwares, e.g. `SeDuMi` [24] and `CVX` [25]. Therefore, the SDP (16) provides us with an efficient way to compute $\varphi(\alpha)$ for any fixed α. Since α lies in the interval $[(1 + P\|\mathbf{h}\|^2)^{-1}, \ 1]$, the single-variable optimization problem (13) can be handled by performing a one-dimensional line search over α, and choosing the one that leads to the maximum $\varphi(\alpha)$ as an optimal solution of (13). In the optimization literature, there are many derivative-free search algorithms for solving one-dimensional optimization problems, e.g., compass or coordinate search (cf. [31], [32]). In practice, we use either uniform sampling or the golden search [33] to obtain a satisfactory solution. Once problem (13) is solved, the solution $(\mathbf{Q}^\star, \mathbf{\Gamma}^\star, \xi^\star)$ outputted from the SDP (16) can be used to recover $\mathbf{W}^\star$ and $\mathbf{\Sigma}^\star$ through the relation (15). Note that an additional rank-one solution construction procedure may be needed depending on the rank of $\mathbf{W}^\star$. This can be done by further solving the SDP (11), cf. Corollary 1.

Summarizing the development in this section, we have presented an SDP-based optimization approach to the SRM problem (4). The approach is based on solving problem (10), which is equivalent to problem (4) as our analysis has revealed. To solve problem (10), we have proposed an SDP-based line search formulation in Section III-B. In addition to design optimization, our development has shown that the transmit beamforming strategy is SRM-optimal for the transmission of confidential information.

IV. Extension to Robust SRM

Our next endeavor is to extend the optimization approach developed in the last section to an imperfect CSI case, where Alice has incomplete knowledge of Eves' CSI. Specifically, we consider a worst-case robust SRM (WCR-SRM) formulation under norm-bounded CSI uncertainties, and derive an SDP-based solution approach to the problem. We will also illustrate how the developed WCR-SRM design solution can be used to provide a safe approximation to an even more challenging design, namely, the outage-constrained robust design (OCR-SRM) under Gaussian distributed CSI uncertainties.

A. The Worst-Case Robust SRM Problem

We consider the same problem setup as in Section II, with the additional assumption that Alice has imperfect CSI on Eves' links. To put into context, let

$$\mathbf{G}_k = \bar{\mathbf{G}}_k + \Delta\mathbf{G}_k, \quad k = 1, \ldots, K, \tag{17}$$

where $\mathbf{G}_k$ is the *actual* channel response from Alice to the kth Eve, as before; $\bar{\mathbf{G}}_k$ is Alice's *presumed* value of $\mathbf{G}_k$; $\Delta\mathbf{G}_k$ represents the associated CSI error. In the WCR-SRM formulation, we assume that $\Delta\mathbf{G}_k$ are deterministic and bounded, satisfying [13], [14]

$$\|\Delta\mathbf{G}_k\|_F \le \varepsilon_k, \ k = 1, \ldots, K$$

for some $\varepsilon_k > 0, \ k = 1, \ldots, K$. The WCR-SRM design problem is formulated as

$$\boxed{\begin{aligned} R_s^\star = \max_{\mathbf{W}\succeq\mathbf{0},\boldsymbol{\Sigma}\succeq\mathbf{0}} \min_{k\in\mathcal{K}} \left\{ C_b(\mathbf{W},\boldsymbol{\Sigma}) - C_{e,k}^{\rm worst}(\mathbf{W},\boldsymbol{\Sigma}) \right\} && \text{(18a)} \\ \text{s.t. } {\rm Tr}(\mathbf{W}+\boldsymbol{\Sigma}) \le P, && \text{(18b)} \\ {\rm Tr}\left(\boldsymbol{\Phi}_l(\mathbf{W}+\boldsymbol{\Sigma})\right) \le \rho_l,\ \forall l\in\mathcal{L}, && \text{(18c)} \end{aligned}}$$

where we recall that $C_b(\mathbf{W},\boldsymbol{\Sigma}) = \log\left(1+\frac{\mathbf{h}^H\mathbf{W}\mathbf{h}}{1+\mathbf{h}^H\boldsymbol{\Sigma}\mathbf{h}}\right)$ is Bob's mutual information, and

$$C_{e,k}^{\rm worst}(\mathbf{W},\boldsymbol{\Sigma}) \triangleq \max_{\mathbf{G}_k\in\mathcal{B}_k} \log\det\left(\mathbf{I} + \left(\mathbf{I}+\mathbf{G}_k^H\boldsymbol{\Sigma}\mathbf{G}_k\right)^{-1}\mathbf{G}_k^H\mathbf{W}\mathbf{G}_k\right),$$
$$\mathcal{B}_k \triangleq \left\{\mathbf{G}_k \mid \mathbf{G}_k = \bar{\mathbf{G}}_k + \Delta\mathbf{G}_k,\ \|\Delta\mathbf{G}_k\|_F \le \varepsilon_k\right\},\ \forall k\in\mathcal{K}$$

is the kth-Eve's worst-case, or largest possible, mutual information among the set of all admissible CSIs $\mathcal{B}_k$. Problem (18) is a safe design—under the optimal design $(\mathbf{W},\boldsymbol{\Sigma})$ of problem (18), the actual secrecy rate w.r.t. the true $\mathbf{G}_k$'s, albeit uncertain, must not lie below the optimal worst-case secrecy rate $R_s^\star$.

Our WCR-SRM optimization approach is derived as follows. We rewrite (18) as

$$R_s^\star = \max_{\mathbf{W}\succeq\mathbf{0},\boldsymbol{\Sigma}\succeq\mathbf{0},\beta\ge 1} \log\left(\frac{1+\mathbf{h}^H(\mathbf{W}+\boldsymbol{\Sigma})\mathbf{h}}{1+\mathbf{h}^H\boldsymbol{\Sigma}\mathbf{h}}\right) - \log\beta \tag{19a}$$
$$\text{s.t. } \log\det\left(\mathbf{I} + \left(\mathbf{I}+\mathbf{G}_k^H\boldsymbol{\Sigma}\mathbf{G}_k\right)^{-1}\mathbf{G}_k^H\mathbf{W}\mathbf{G}_k\right) \le \log\beta,\ \forall\,\mathbf{G}_k\in\mathcal{B}_k,\ k\in\mathcal{K}, \tag{19b}$$
$$\text{(18b)} - \text{(18c) satisfied.} \tag{19c}$$

Note that in (19b), there are infinitely many inequalities w.r.t. $\mathbf{G}_k$ to satisfy; this makes the WCR-SRM problem more challenging to solve than the SRM. Let us set aside the infinitely many inequalities issue for the moment. By using Proposition 1, which has played a key role in solving SRM in the last section, we have the following relaxation for (19b):

$$\log\det\left(\mathbf{I} + \left(\mathbf{I}+\mathbf{G}_k^H\boldsymbol{\Sigma}\mathbf{G}_k\right)^{-1}\mathbf{G}_k^H\mathbf{W}\mathbf{G}_k\right) \le \log\beta,\ \forall\,\mathbf{G}_k\in\mathcal{B}_k, \tag{20a}$$
$$\Longrightarrow (\beta-1)(\mathbf{I}+\mathbf{G}_k^H\boldsymbol{\Sigma}\mathbf{G}_k) \succeq \mathbf{G}_k^H\mathbf{W}\mathbf{G}_k,\ \forall\,\mathbf{G}_k\in\mathcal{B}_k, \tag{20b}$$

for $k=1,\ldots,K$. Moreover, (20a) and (20b) become equivalent if ${\rm rank}(\mathbf{W}) \le 1$ (again, by Proposition 1). Eq. (20b) corresponds to an infinite number of quadratic matrix inequalities w.r.t. $\mathbf{G}_k$. While (20b) is less complex than (20a), we still need to find an efficient way to manage the infinitely many inequalities in (20b). It turns out that the latter is possible, by employing an advanced matrix inequality result in the optimization literature.

Lemma 1 (Luo-Sturm-Zhang [34]). *Let* $f(\mathbf{X}) = \mathbf{X}^H\mathbf{A}\mathbf{X}+\mathbf{X}^H\mathbf{B}+\mathbf{B}^H\mathbf{X}+\mathbf{C}$*, and* $\mathbf{D} \succeq \mathbf{0}$*. The following equivalence holds:*

$$\begin{aligned} & f(\mathbf{X}) \succeq \mathbf{0}, \ \forall \ \mathbf{X} \in \{\mathbf{X} \mid \mathrm{Tr}(\mathbf{D}\mathbf{X}\mathbf{X}^H) \leq 1\}, \\ \Longleftrightarrow & \begin{bmatrix} \mathbf{C} & \mathbf{B}^H \\ \mathbf{B} & \mathbf{A} \end{bmatrix} - t \begin{bmatrix} \mathbf{I} & \mathbf{0} \\ \mathbf{0} & -\mathbf{D} \end{bmatrix} \succeq \mathbf{0}, \ \text{for some } t \geq 0. \end{aligned} \tag{21}$$

By applying Lemma 1 to (20b), we establish the following key result:

Proposition 2. *The following implication holds*

$$\log\det\left(\mathbf{I} + \left(\mathbf{I} + \mathbf{G}_k^H\mathbf{\Sigma}\mathbf{G}_k\right)^{-1}\mathbf{G}_k^H\mathbf{W}\mathbf{G}_k\right) \leq \log\beta, \ \forall\, \mathbf{G}_k \in \mathcal{B}_k, \tag{22a}$$

$$\Longrightarrow \mathbf{T}_k(\beta, \mathbf{W}, \mathbf{\Sigma}, t_k) \succeq \mathbf{0}, \ \text{for some } t_k \geq 0, \tag{22b}$$

for any $k \in \mathcal{K}$*, where*

$$\mathbf{T}_k(\beta, \mathbf{W}, \mathbf{\Sigma}, t_k) = \begin{bmatrix} (\beta - 1 - t_k)\mathbf{I} + \bar{\mathbf{G}}_k^H\left((\beta-1)\mathbf{\Sigma} - \mathbf{W}\right)\bar{\mathbf{G}}_k & \bar{\mathbf{G}}_k^H\left((\beta-1)\mathbf{\Sigma} - \mathbf{W}\right) \\ \left((\beta-1)\mathbf{\Sigma} - \mathbf{W}\right)\bar{\mathbf{G}}_k & (\beta-1)\mathbf{\Sigma} - \mathbf{W} + \frac{t_k}{\varepsilon_k^2}\mathbf{I} \end{bmatrix}. \tag{23}$$

Moreover, (22a) *and* (22b) *are equivalent if* $\mathrm{rank}(\mathbf{W}) \leq 1$.

Proof: Following (20), it suffices to show that for each k, (20b) is equivalent to (22b). Eq. (20b) can be represented by the left-hand side of (21). Specifically, we substitute (17) into (20b), and then set $\mathbf{X} = \Delta\mathbf{G}_k$, $\mathbf{A} = (\beta-1)\mathbf{\Sigma} - \mathbf{W}$, $\mathbf{B} = ((\beta-1)\mathbf{\Sigma} - \mathbf{W})\,\bar{\mathbf{G}}_k$, $\mathbf{C} = \bar{\mathbf{G}}_k^H\left((\beta-1)\mathbf{\Sigma} - \mathbf{W}\right)\bar{\mathbf{G}}_k + (\beta-1)\mathbf{I}$ and $\mathbf{D} = \varepsilon_k^{-2}\mathbf{I}$. By the right-hand side of (21), we obtain (22b) as an equivalent form of (20b). ■

The upshot of the implication in Proposition 2 is that fixing β, (22b) is a *single* linear matrix inequality w.r.t. $(\mathbf{W}, \mathbf{\Sigma}, t_k)$ (rather than infinitely many), and can be efficiently handled by convex conic optimization. Therefore, we replace (19b) by (22b) to obtain a relaxation of (19), given as follows:

$$\begin{aligned} \bar{R}_s^\star = \max_{\mathbf{W}\succeq\mathbf{0}, \mathbf{\Sigma}\succeq\mathbf{0}, \{t_k\}, \beta\geq 1} \ & \log\left(\frac{1 + \mathbf{h}^H(\mathbf{W}+\mathbf{\Sigma})\mathbf{h}}{\beta(1+\mathbf{h}^H\mathbf{\Sigma}\mathbf{h})}\right) \\ \text{s.t. } & \mathbf{T}_k(\beta, \mathbf{W}, \mathbf{\Sigma}, t_k) \succeq \mathbf{0}, \ t_k \geq 0, \forall k \in \mathcal{K} \\ & \text{(18b)} - \text{(18c) satisfied,} \end{aligned} \tag{24}$$

where $\bar{R}_s^\star$ is the optimal objective value of (24) and we have $R_s^\star \leq \bar{R}_s^\star$. Now, a crucial question is whether (24) is a tight relaxation of the WCR-SRM problem (19). Remarkably, we prove that the answer is yes.

Theorem 2. *Problem* (24) *is a tight relaxation to, or an equivalent formulation of, the WCR-SRM problem* (19)*. In particular, there exists an optimal solution* $(\mathbf{W}^\star, \mathbf{\Sigma}^\star, \beta^\star)$ *of problem* (24)*, for which* $\mathrm{rank}(\mathbf{W}^\star) \leq 1$*; the solution* $(\mathbf{W}^\star, \mathbf{\Sigma}^\star, \beta^\star)$ *is also an optimal solution of* (19)*, achieving* $R_s^\star = \bar{R}_s^\star$*.*

Corollary 2. *Suppose that* $(\bar{\mathbf{W}}^\star, \bar{\mathbf{\Sigma}}^\star, \beta^\star)$ *is an optimal solution returned by solving* (24). *If* $\operatorname{rank}(\bar{\mathbf{W}}^\star) \leq 1$*, then output* $(\bar{\mathbf{W}}^\star, \bar{\mathbf{\Sigma}}^\star, \beta^\star)$ *as an optimal solution of the WCR-SRM problem* (19). *Otherwise, solve the following SDP*

$$\begin{aligned} (\mathbf{W}^\star, \mathbf{\Sigma}^\star, \{t_k^\star\}) = \arg \min_{\mathbf{W}, \mathbf{\Sigma}, \{t_k\}} \quad & \operatorname{Tr}(\mathbf{W} + \mathbf{\Sigma}) \\ \text{s.t.} \quad & \mathbf{h}^H (\mathbf{W} + \mu \mathbf{\Sigma}) \mathbf{h} + \mu \geq 0, \\ & \mathbf{T}_k(\beta^\star, \mathbf{W}, \mathbf{\Sigma}, t_k) \succeq \mathbf{0}, \ t_k \geq 0, \ \forall k \in \mathcal{K}, \\ & \operatorname{Tr}(\mathbf{\Phi}_l (\mathbf{W} + \mathbf{\Sigma})) \leq \rho_l, \ \forall l \in \mathcal{L}, \\ & \mathbf{W} \succeq \mathbf{0}, \ \mathbf{\Sigma} \succeq \mathbf{0}, \end{aligned} \tag{25}$$

where $\mu = 1 - 2^{\bar{R}_s^\star} \beta^\star$*, and output* $(\mathbf{W}^\star, \mathbf{\Sigma}^\star, \beta^\star)$ *as an optimal solution of the WCR-SRM problem* (19). *In particular, it must hold true that* $\operatorname{rank}(\mathbf{W}^\star) \leq 1$.

Theorem 2 and Corollary 2 can be seen as a generalization of their perfect-CSI counterpart in Theorem 1 and Corollary 1, respectively. The proof of the former is more difficult to obtain than that of the latter, owing to the complicated structure of $\mathbf{T}_k(\beta, \mathbf{W}, \mathbf{\Sigma}, t_k)$ [see (23)]. We relegate the proof to Appendix C.

Since we have identified that (24) is a tight relaxation of the WCR-SRM problem (19), our last step is to solve (24). Problem (24) can be handled by using the same SDP-based line search method developed in the last section. For conciseness, here we only point out several key steps. We reexpress (24) in the form of the one-dimensional problem in (13), where $\varphi(\alpha)$ is now given by

$$\begin{aligned} \varphi(\alpha) = \max_{\mathbf{W} \succeq \mathbf{0}, \mathbf{\Sigma} \succeq \mathbf{0}, \{t_k\}} \quad & \frac{1 + \mathbf{h}^H (\mathbf{W} + \mathbf{\Sigma}) \mathbf{h}}{\alpha^{-1} (1 + \mathbf{h}^H \mathbf{\Sigma} \mathbf{h})} \\ \text{s.t.} \quad & \mathbf{T}_k(\alpha^{-1}, \mathbf{W}, \mathbf{\Sigma}, t_k) \succeq \mathbf{0}, \ t_k \geq 0, \forall k \in \mathcal{K}, \\ & \operatorname{Tr}(\mathbf{W} + \mathbf{\Sigma}) \leq P, \ \operatorname{Tr}\left(\mathbf{\Phi}_l (\mathbf{W} + \mathbf{\Sigma})\right) \leq \rho_l, \forall l \in \mathcal{L}. \end{aligned} \tag{26}$$

By a change of variables $\mathbf{W} = \mathbf{Q}/\xi, \mathbf{\Sigma} = \mathbf{\Gamma}/\xi, t_k = \lambda_k/\xi, \ \xi > 0$, and using the Charnes-Cooper transformation, we show that (26) can be converted to a convex SDP

$$\begin{aligned} \max_{\mathbf{Q} \succeq \mathbf{0}, \mathbf{\Gamma} \succeq \mathbf{0}, \xi, \{\lambda_k\}} \quad & \xi + \mathbf{h}^H (\mathbf{Q} + \mathbf{\Gamma}) \mathbf{h} \\ \text{s.t.} \quad & \xi + \mathbf{h}^H \mathbf{\Gamma} \mathbf{h} = \alpha, \\ & \bar{\mathbf{T}}_k(\mathbf{Q}, \mathbf{\Gamma}, \alpha, \xi, \lambda_k) \succeq \mathbf{0}, \ \lambda_k \geq 0, \ \forall k \in \mathcal{K}, \\ & \operatorname{Tr}(\mathbf{Q} + \mathbf{\Gamma}) \leq P\xi, \ \operatorname{Tr}\left(\mathbf{\Phi}_l (\mathbf{Q} + \mathbf{\Gamma})\right) \leq \rho_l \xi, \ \forall l \in \mathcal{L}, \end{aligned} \tag{27}$$

where

$$\bar{\mathbf{T}}_k(\mathbf{Q}, \mathbf{\Gamma}, \alpha, \xi, \lambda_k) = \begin{bmatrix} (\xi - \alpha\xi - \alpha\lambda_k)\mathbf{I} + \bar{\mathbf{G}}_k^H \left((1-\alpha)\mathbf{\Gamma} - \alpha\mathbf{Q}\right) \bar{\mathbf{G}}_k & \bar{\mathbf{G}}_k^H \left((1-\alpha)\mathbf{\Gamma} - \alpha\mathbf{Q}\right) \\ \left((1-\alpha)\mathbf{\Gamma} - \alpha\mathbf{Q}\right) \bar{\mathbf{G}}_k & (1-\alpha)\mathbf{\Gamma} - \alpha\mathbf{Q} + \frac{\alpha\lambda_k}{\varepsilon_k^2}\mathbf{I} \end{bmatrix}.$$

Hence, for a fixed α, $\varphi(\alpha)$ can be computed by solving the SDP (27). Problem (24) is then handled by applying a line search on $\varphi(\alpha)$ w.r.t. α; the procedure is the same as that described in Section III-B.

Summarizing, in this section we have tackled the WCR-SRM problem (18) by deriving a tight relaxation. The tight WCR-SRM relaxation, given in (24), can be handled by an SDP-based line search procedure. Furthermore, it is worthwhile to mention that by Theorem 2, transmit beamforming is still an optimal confidential information transmission strategy for the WCR-SRM formulation.

Remark 5. One may be curious to know whether the AN-aided WCR-SRM solution method developed above can be extended to the scenario where Bob's channel is also imperfectly known. In fact, this has been considered for the no-AN case [15]. For the AN-aided case here, such an extension is possible; the idea is to follow the same derivations as above and [15]. It can be shown that the problem can once again be handled via one-dimensional line search, but the line search involves solving a sequence of factional SDPs, which is quasiconvex and is computationally more expensive to solve. As a future direction, it will be interesting to study efficient methods for handling this problem.

B. The Outage-Constrained Robust SRM Problem

The WCR-SRM formulation in the previous subsection is an absolutely safe design under bounded CSI uncertainties. In this subsection, we consider an alternative robust formulation where the CSI errors $\Delta\mathbf{G}_k$ are random and follow certain distribution. Specifically, we employ the popular i.i.d. complex Gaussian CSI error model

$$[\Delta\mathbf{G}_k]_{m,n} \sim \mathcal{CN}(0,\sigma_k^2), \quad \forall m,n,\ k=1,\ldots,K. \tag{28}$$

Moreover, $\Delta\mathbf{G}_k$ is assumed to be independent of $\Delta\mathbf{G}_l$ for any $k \neq l$. In this setup, since $\Delta\mathbf{G}_k$ are unbounded, it may not be possible to deliver an absolutely safe design. However, one can adopt a $(1-\delta)\%$ safe design, for some outage probability specification δ [16], [35]. Consider the following outage-constrained robust SRM formulation:

$$\boxed{\begin{aligned}
&\max_{\mathbf{W},\boldsymbol{\Sigma},R_s}\ R_s && \text{(29a)}\\
&\text{s.t. } \Pr_{\{\Delta\mathbf{G}_k\}_{k=1}^K}\Big\{C_b(\mathbf{W},\boldsymbol{\Sigma}) - \max_{k\in\mathcal{K}} C_{e,k}(\mathbf{W},\boldsymbol{\Sigma}) \geq R_s\Big\} \geq 1-\delta, && \text{(29b)}\\
&\qquad \mathrm{Tr}\left(\boldsymbol{\Phi}_l(\mathbf{W}+\boldsymbol{\Sigma})\right) \leq \rho_l,\ \forall l \in \mathcal{L}, && \text{(29c)}\\
&\qquad \mathrm{Tr}(\mathbf{W}+\boldsymbol{\Sigma}) \leq P,\ \mathbf{W}\succeq\mathbf{0},\ \boldsymbol{\Sigma}\succeq\mathbf{0}, && \text{(29d)}
\end{aligned}}$$

where $C_b(\mathbf{W},\mathbf{\Sigma})$ and $C_{e,k}(\mathbf{W},\mathbf{\Sigma})$ have been defined in (3); $0<\delta<0.5$ is a given parameter specifying the maximum tolerable secrecy outage probability, i.e., the probability of the achievable secrecy rate falling below R_s [35]. Therefore, the goal of (29) is to maximize the $\delta\%$-outage secrecy rate.

The OCR-SRM problem (29) is very challenging to solve. The main obstacle lies in the probabilistic constraint (29b), which is unlikely to have a tractable closed-form expression except for some special cases, e.g., when there is only one Eve with a single antenna and AN is restricted to lie on the nullspace of $\mathbf{h}$ [16]. As a compromise, we consider an approximation of (29) based on the previous WCR-SRM design, which we have solved. We summarize our main result in the following proposition:

Proposition 3. *Consider the WCR-SRM problem* (18). *Suppose that the CSI error radii ε_k are chosen as*

$$\varepsilon_k=\sqrt{\frac{\sigma_k^2}{2}F^{-1}_{\chi^2_{2N_tN_{e,k}}}((1-\delta)^{1/K})},\quad k=1,\ldots,K, \tag{30}$$

where $F^{-1}_{\chi^2_{2N_tN_{e,k}}}(\cdot)$ denotes the inverse cumulative distribution function of a Chi-square random variable with $2N_tN_{e,k}$ degrees of freedom. Then, problem (18) *is a safe approximation to the OCR-SRM problem* (29)*, in the sense that every feasible point of problem* (18) *is also feasible to problem* (29)*, and thus satisfies the secrecy rate satisfaction probability constraint* (29b)*.*

The insight behind Proposition 3 is that the robust nature of WCR-SRM should lead to certain secrecy rate satisfaction probability values; especially, the larger ε_k are, the more conservative the design would be and the higher the secrecy rate satisfaction probability should be. Eq. (30) is essentially a sufficient condition under which any feasible point of the WCR-SRM problem satisfies the OCR-SRM probability constraint in (29b).

Proof of Proposition 3: By noting the independence between $\mathbf{G}_k$ and $\mathbf{G}_l,\ \forall k\neq l$, we have

$$\text{(29b)}\Longleftrightarrow\prod_{k=1}^{K}\text{Pr}_{\Delta\mathbf{G}_k}\left\{C_b(\mathbf{W},\mathbf{\Sigma})-C_{e,k}(\mathbf{W},\mathbf{\Sigma})\geq R_s\right\}\geq 1-\delta, \tag{31a}$$

$$\Longleftarrow\text{Pr}_{\Delta\mathbf{G}_k}\left\{C_b(\mathbf{W},\mathbf{\Sigma})-C_{e,k}(\mathbf{W},\mathbf{\Sigma})\geq R_s\right\}\geq 1-\bar{\delta},\ \forall k \tag{31b}$$

where $\bar{\delta}=1-(1-\delta)^{1/K}$. Our next step is to derive a safe approximation to (31b). This is done by exploiting the following implication:

$$\begin{aligned}&C_b(\mathbf{W},\mathbf{\Sigma})-C_{e,k}(\mathbf{W},\mathbf{\Sigma})\geq R_s,\ \forall\ \|\Delta\mathbf{G}_k\|_F^2\leq\varepsilon_k^2\\ \Longrightarrow&\text{Pr}_{\Delta\mathbf{G}_k}\left\{C_b(\mathbf{W},\mathbf{\Sigma})-C_{e,k}(\mathbf{W},\mathbf{\Sigma})\geq R_s\right\}\geq 1-\bar{\delta},\end{aligned} \tag{32}$$

where the uncertainty radius ε_k is chosen to satisfy $\text{Pr}_{\Delta\mathbf{G}_k}\{\|\Delta\mathbf{G}_k\|_F^2\leq\varepsilon_k^2\}=1-\bar{\delta}$. The above implication can be deduced using an intuitive argument called sphere bounding. Specifically, in the left-hand side of (32), we set a spherical boundary ε_k to the unbounded random error $\Delta\mathbf{G}_k$, such that $1-\bar{\delta}$ portion of $\Delta\mathbf{G}_k$'s realizations lies in the sphere, and meanwhile, for all of these $\Delta\mathbf{G}_k$ in the sphere, the worst secrecy rate is ensured no less than R_s. For such a choice of ε_k, the right-hand side of (32) apparently holds. In addition, it follows from (28) that ε_k can be explicitly calculated by (30). Readers are referred to the literature, such as [36], for more complete descriptions of the sphere bounding method. Now, by applying the implications (31) and (32) to the probabilistic constraint (29b), we obtain a restriction of, or safe approximation to, the OCR-SRM problem (29):

$$\max_{\mathbf{W},\boldsymbol{\Sigma},R_s} \; R_s \tag{33a}$$

$$\text{s.t. } C_b(\mathbf{W},\boldsymbol{\Sigma}) - C_{e,k}(\mathbf{W},\boldsymbol{\Sigma}) \geq R_s, \forall\; \|\Delta\mathbf{G}_k\|_F^2 \leq \varepsilon_k^2,\; k=1,\ldots,K, \tag{33b}$$

$$\mathrm{Tr}\left(\boldsymbol{\Phi}_l(\mathbf{W}+\boldsymbol{\Sigma})\right) \leq \rho_l,\; \forall l \in \mathcal{L}, \tag{33c}$$

$$\mathrm{Tr}(\mathbf{W}+\boldsymbol{\Sigma}) \leq P,\; \mathbf{W} \succeq \mathbf{0},\; \boldsymbol{\Sigma} \succeq \mathbf{0}. \tag{33d}$$

Note that any feasible point of (33) is also feasible to the OCR-SRM problem (29), by (31) and (32). It can be easily seen that problem (33) is equivalent to the WCR-SRM problem (18). ■

V. Simulation Results

In this section, we use Monte Carlo simulations to demonstrate the performance of the AN-aided SRM design obtained by the proposed SDP-based optimization technique.

A. Example 1: Secrecy Rate Performance under the Sum Power Constraint

In this example, our goal is to illustrate the secrecy rate performance of the standard AN-aided SRM design; i.e., problem (4) with the sum power constraint (4b) only. We compare the performance of the proposed AN-aided SRM design (Section III) with that of two existing designs, namely, the isotropic AN design [7] and the optimal no-AN SRM design [15]. In the isotropic AN design, the transmit and AN covariances are given by [7]

$$\mathbf{W}_{\text{iso}-\text{AN}} = \frac{P}{2\|\mathbf{h}\|^2}\mathbf{h}\mathbf{h}^H, \qquad \boldsymbol{\Sigma}_{\text{iso}-\text{AN}} = \frac{P}{2}\frac{\boldsymbol{\Pi}_{\mathbf{h}}^{\perp}}{\|\boldsymbol{\Pi}_{\mathbf{h}}^{\perp}\|_F^2}, \tag{34}$$

where $\boldsymbol{\Pi}_{\mathbf{h}}^{\perp} = \mathbf{I} - \mathbf{h}\mathbf{h}^H/\|\mathbf{h}\|^2$ denotes the orthogonal complement projector of $\mathbf{h}$. In words, the isotropic AN design uses half of the transmit power to transmit the confidential information via straight beamforming, and uses the other half to transmit AN on the nullspace of $\mathbf{h}$ isotropically. The no-AN SRM design is the solution of problem (4), but with $\boldsymbol{\Sigma}$ prefixing as $\mathbf{0}$. The no-AN SRM design can be obtained by solving one SDP, as shown in our previous work [15] (also [37]).

The simulation settings are as follows. The number of transmit antennas at Alice is $N_t = 5$. The number of receive antennas at Eves is $N_{e,k} = 3$ for all k. In each simulation trial, Bob and Eves' channels are randomly generated following an i.i.d. complex Gaussian distribution with zero mean and unit variance.

Fig. 2 plots the secrecy rates of the various designs w.r.t. the sum power P. We examine two cases, namely, one Eve ($K = 1$) and three Eves ($K = 3$), respectively. The more interesting case is the three Eves case, while the one Eve case aims to serve as a reference. We will elaborate on this soon. For the two cases, it can be seen that the proposed AN-aided SRM design achieves a secrecy rate performance at least no worse than the other two designs. In fact, the performance gain of the AN-aided SRM design can be quite significant. For example, for the case of $K = 3$, the secrecy rate gap between the AN-aided SRM design and the isotropic AN design can be close to 2 bits per channel use when P is large. Moreover, the gap between AN-aided and no-AN SRM designs (for $K = 3$) is even more dramatic.

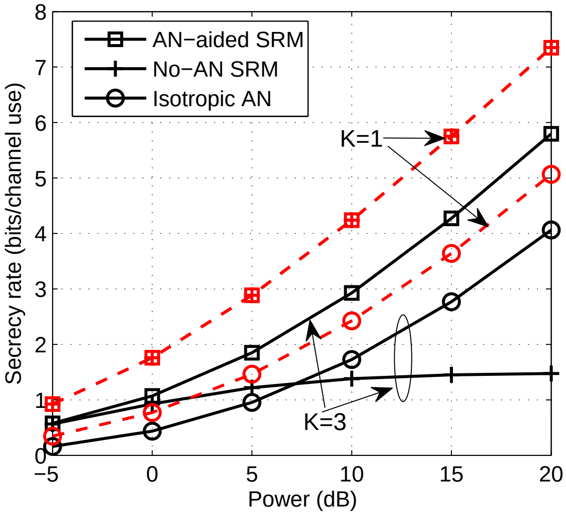
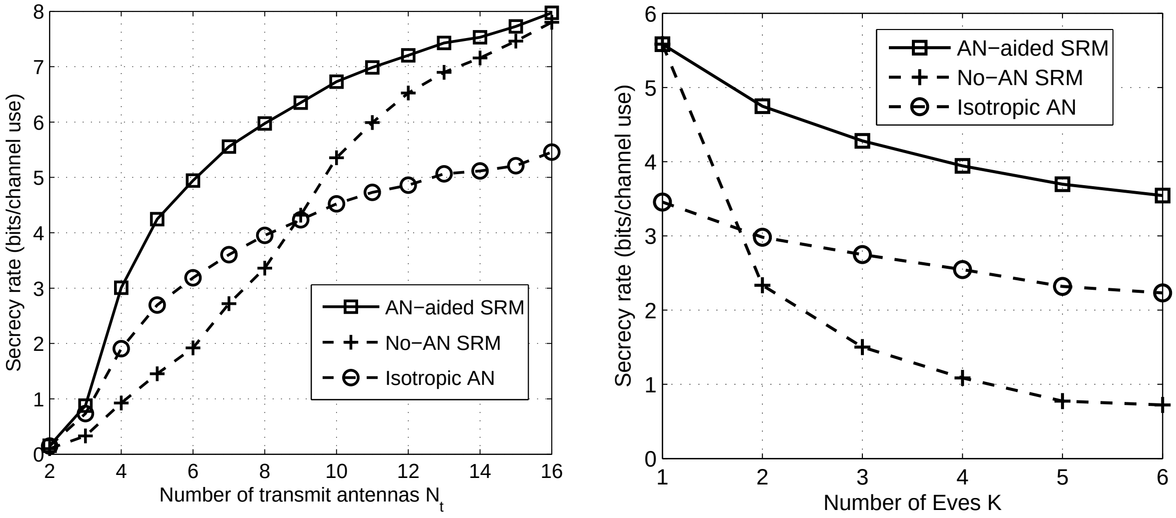


Fig. 2. Secrecy rates versus the sum power.

Fig. 2 reveals an interesting phenomenon. We see that for $K = 1$, the secrecy rates of the AN-aided and no-AN SRM designs are exactly the same. This means that AN may be not necessary for the one Eve case. In fact, it is known that the no-AN SRM design achieves the secrecy capacity for the one Eve case [4], and the simulation result here has further confirmed that. However, the picture becomes drastically different when there are more than one Eves. For $K = 3$, we can clearly observe from Fig. 2 that the secrecy rate gap between the no-AN and AN-aided SRM designs are widening quite substantially with P. In fact, the secrecy rate of the no-AN SRM design almost stays unaltered for $P \geq 10$dB, that even the isotropic AN design can provide better secrecy rate performance. At this point, we should mention that the combined d.o.f. of Eves is $\sum_{k=1}^{K} N_{e,k} = 9$, which is higher than the transmit d.o.f. $N_t = 5$. The



(a)

(b)

Fig. 3. Secrecy rates versus (a) the number of transmit antennas with $(N_{e,k}, K) = (3, 3)$, and (b) the number of Eves with $(N_t, N_{e,k}) = (5, 3)$.

insufficient transmit d.o.f. to deal with Eves is the reason for the unsatisfactory performance of the no-AN SRM design. To verify this, we plot the secrecy rate versus the number of transmit antennas N_t and the number of Eves K in Fig. 3(a) and (b), respectively. The sum power is fixed at $P = 15$dB. From Fig. 3(a) we can see that the secrecy rate of the no-AN SRM design increases with N_t and approaches that of AN-aided SRM design for large N_t; this implies that if the transmitter has sufficiently large d.o.f., we need little or no AN. On the other hand, from Fig. 3(b) we can see that the secrecy rate of the no-AN SRM design drops rapidly with K. In comparison, the AN-aided SRM design yields superior performance, even for the case of $K = 6$ (which corresponds to an Eves' combined d.o.f. of $\sum_{k=1}^{K} N_{e,k} = 18$). Hence, the simulation results in Fig. 3(a) and (b) further confirm that incorporating AN in the transmit design is a powerful means to combat the d.o.f. bottleneck.

B. Example 2: Secrecy Rate Performance with Additional Interference Temperature Constraints

This example considers SRM design with additional interference temperature constraints (ITCs). The simulation settings are the same as the previous, namely, $N_t = 5$, $N_{e,k} = 3$ for all k, $K = 3$, and there is one primary user with two receive antennas, i.e., $L = 1$, $N_{p,1} = 2$. The primary user's channel $\mathbf{R}$ is generated from a standard complex Gaussian distribution. The ITC level is set to $\rho = 5$dB; cf. Eq. (6). The proposed AN-aided SRM design is benchmarked against the no-AN SRM design; see [37]. The isotropic AN design is not applicable here since it was not designed under ITC constraints. Fig. 4 shows the simulation results. We can see that the proposed AN-aided SRM design offers better secrecy rate performance, especially when P is large.

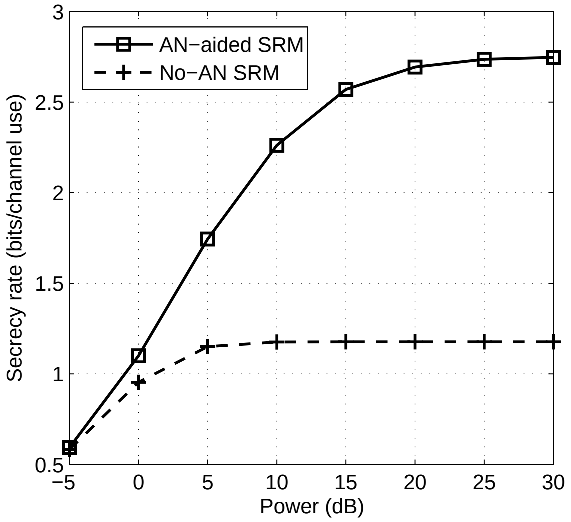


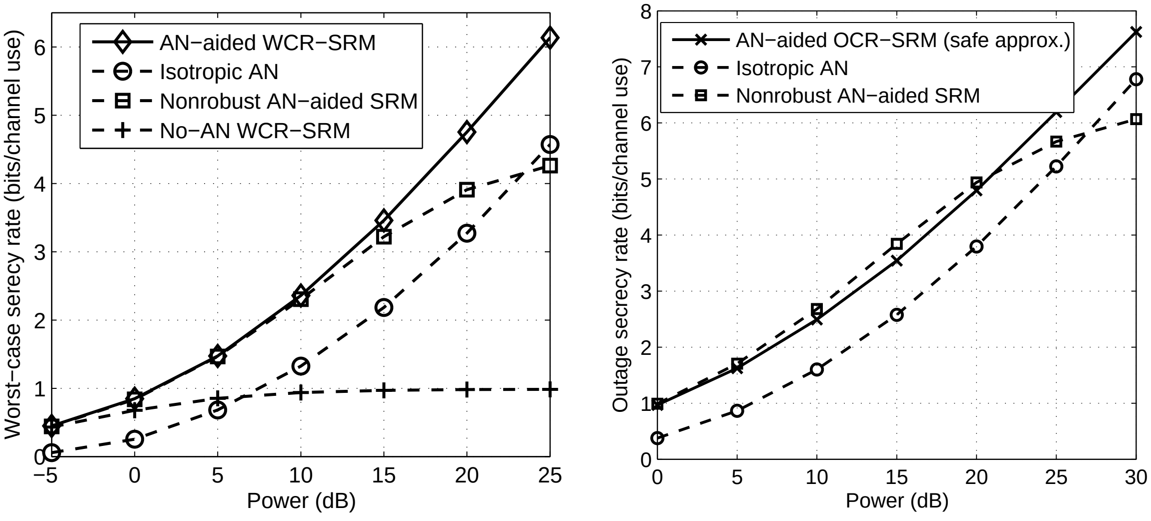
Fig. 4. Secrecy rates versus the sum power with the interference temperature constraint $\rho = 5\,\mathrm{dB}$.

C. Example 3: Secrecy Rate Performance under Imperfect CSI

In this last example, our aim is to illustrate the robustness of the WCR-SRM and OCR-SRM designs (Section IV) when there are uncertainties with Eves' CSI. The simulation settings are as follows: $N_t = 5$, $K = 3$, $N_{e,k} = 3$, sum power constraint only, i.i.d. complex Gaussian generated $\mathbf{h}$ and $\bar{\mathbf{G}}_k$.

Fig. 5(a) shows the performance of the various designs under the worst-case robust scenario. We set $\varepsilon_k = 0.2$ for all k. The performance measure used is the worst-case secrecy rate, which is the objective function of the WCR-SRM problem in (18). Notice that for a given design $(\mathbf{W}, \mathbf{\Sigma})$, the worst-case secrecy rate does not have a closed form. In the simulation, we computed the worst-case secrecy rates of the various designs by using the WCR-SRM optimization method derived in Section IV-A (specifically, solving (24) with $(\mathbf{W}, \mathbf{\Sigma})$ fixing to be a given design); hence the development there serves a dual purpose of enabling worst-case secrecy rate computations. In the legend of Fig. 5(a), “no-AN WCR-SRM” is the no-AN worst-case robust SRM design in [15], and “nonrobust AN-aided SRM” refers to the AN-aided SRM design in Section III, where we apply the presumed CSIs $\mathbf{h}, \bar{\mathbf{G}}_1, \ldots, \bar{\mathbf{G}}_K$ (rather than the true ones) to perform the transmit design in the simulations and then evaluate the resultant worst-case secrecy rate. From Fig. 5(a), we can see that nonrobust AN-aided SRM is sensitive to CSI uncertainties. Specifically, for $P \geq 15$dB, nonrobust AN-aided SRM exhibits performance degradation that tends to worsen as P increases. Moreover, the proposed AN-aided WCR-SRM design achieves the best worst-case secrecy rate performance compared to the other designs.

We turn our attention to the outage-constrained robust scenario. We set $\delta = 1\%$ and $\sigma_k = 0.05$ for all k. The performance measure used this time is the outage-constrained secrecy rate; Monte Carlo-based evaluation was used to compute the outage-constrained secrecy rates of the considered designs. Fig. 5(b) shows the outage-constrained secrecy rates of the various designs. The results are generally consistent with their worst-case robust counterparts in Fig. 5(a), with one difference. Specifically, nonrobust AN-aided SRM is seen to yield slightly better outage-constrained secrecy rate performance than AN-aided OCR-SRM for $P \leq 20$dB. The reason is that the method for AN-aided OCR-SRM (see Section IV-B) is a safe approximation. Nevertheless, nonrobust AN-aided SRM possesses the same performance degradation behavior as in the worst-case scenario, and AN-aided OCR-SRM (by safe approximation) generally yields the best outage-constrained secrecy rate performance.



(a) (b)

Fig. 5. (a) Worst-case secrecy rates versus the sum power P; (b) outage secrecy rates versus the sum power P.

VI. Conclusion and Discussion

This paper has considered the AN-aided secrecy rate maximization problem for an MISO channel overheard by multiple multi-antenna Eves and under both perfect and imperfect CSI. The SRM problem is challenging to solve due to its intrinsically complex problem structures. By resorting to an SDP-based optimization approach, we show that the SRM problem and its worst-case robust generalization can be efficiently handled by solving a sequence of SDPs. Moreover, the development itself indicates that transmit beamforming is generally an optimal strategy for the confidential information transmission. In addition, we also propose a safe approximation to an outage-constrained robust SRM problem by using worst-case robust SRM. Simulation results demonstrate that the proposed designs can achieve better performance than the optimal SRM design without AN and the design with isotropic AN, especially when the number of Eves is large. These observations confirm the efficacy of AN in enhancing transmission security, as well as the necessity of optimizing AN in order to effectively interfere Eves.

As briefly mentioned in introduction, several existing AN-aided physical-layer secrecy approaches [3]–[8], [13], [16], [17] employ a design constraint that AN lies in the nullspace of the legitimate user's channel; i.e., $\mathbf{h}^H\boldsymbol{\Sigma}\mathbf{h} = 0$. This nullspace AN constraint is reasonable, since the use of AN is intended to interfere the eavesdroppers, but not the legitimate user. Also, using the nullspace AN constraint may help simplify design and analysis. The AN-aided SRM problem considered here does not incorporate the nullspace AN constraint, although it is possible to do so—we can add the nullspace AN constraint to the AN-aided SRM problem (more precisely, problem (4) with an extra constraint $\mathbf{h}^H\boldsymbol{\Sigma}\mathbf{h} = 0$), and the resulting problem can be handled by essentially the same SDP-based optimization approach described in this paper, with some minor modification. We found that the nullspace AN constraint does not help simplify the optimization of the SRM problem. However, we examined by simulations that the SRM problem with the nullspace AN constraint can achieve secrecy rate performance quite close to that without the nullspace AN constraint; the simulation results are not shown here due to the page limit. This observation suggests that it is sound to consider the nullspace AN constraint. As a future work, it would be interesting to analyze the SRM-optimal AN solution, studying how close it approaches the nullspace AN condition.

VII. Acknowledgment

The authors would like to sincerely thank the anonymous reviewers for their helpful and insightful comments.

Appendix

A. Proof of Proposition 1

The idea of the proof is to establish some lower bounds on the left-hand side (LHS) of (9a). First, note the following equivalence

$$\log\det\left(\mathbf{I} + \left(\mathbf{I} + \mathbf{G}^H\boldsymbol{\Sigma}\mathbf{G}\right)^{-1}\mathbf{G}^H\mathbf{W}\mathbf{G}\right) \leq \log\beta \tag{35a}$$

$$\Longleftrightarrow \det\left(\mathbf{I} + \mathbf{U}^{-\frac{1}{2}}\mathbf{G}^H\mathbf{W}\mathbf{G}\mathbf{U}^{-\frac{1}{2}}\right) \leq \beta, \tag{35b}$$

where $\mathbf{U} = \mathbf{I} + \mathbf{G}^H \boldsymbol{\Sigma} \mathbf{G}$. Eq. (35b) is obtained by applying the basic matrix result $\det(\mathbf{I} + \mathbf{AB}) = \det(\mathbf{I} + \mathbf{BA})$ to (35a). Moreover, (35b) implies that $\beta \geq 1$. To proceed further, we need the following lemma, which provides a lower bound on the LHS of (35b).

Lemma 2 ([15])**.** *Let $\mathbf{A} \succeq \mathbf{0}$. It holds true that*

$$\det(\mathbf{I} + \mathbf{A}) \geq 1 + \mathrm{Tr}(\mathbf{A}), \tag{36}$$

and that the equality in (36) *holds if and only if* $\mathrm{rank}(\mathbf{A}) \leq 1$.

Applying Lemma 2 to the LHS of (35b) yields

$$\det\left(\mathbf{I} + \mathbf{U}^{-\frac{1}{2}} \mathbf{G}^H \mathbf{W} \mathbf{G} \mathbf{U}^{-\frac{1}{2}}\right) \geq 1 + \mathrm{Tr}\left(\mathbf{U}^{-\frac{1}{2}} \mathbf{G}^H \mathbf{W} \mathbf{G} \mathbf{U}^{-\frac{1}{2}}\right). \tag{37}$$

Combining (35) and (37), we get

$$\text{(35a)} \Longrightarrow \mathrm{Tr}\left(\mathbf{U}^{-\frac{1}{2}} \mathbf{G}^H \mathbf{W} \mathbf{G} \mathbf{U}^{-\frac{1}{2}}\right) \leq \beta - 1. \tag{38}$$

In light of $\mathbf{U}^{-\frac{1}{2}} \mathbf{G}^H \mathbf{W} \mathbf{G} \mathbf{U}^{-\frac{1}{2}} \succeq \mathbf{0}$, and the fact that $\mathrm{Tr}(\mathbf{A}) \geq \lambda_{\max}(\mathbf{A})$ holds for any $\mathbf{A} \succeq \mathbf{0}$, we have

$$\begin{aligned} \text{(35a)} \;\; &\Longrightarrow \lambda_{\max}\left(\mathbf{U}^{-\frac{1}{2}} \mathbf{G}^H \mathbf{W} \mathbf{G} \mathbf{U}^{-\frac{1}{2}}\right) \leq \beta - 1, && \text{(39a)} \\ &\Longleftrightarrow \mathbf{U}^{-\frac{1}{2}} \mathbf{G}^H \mathbf{W} \mathbf{G} \mathbf{U}^{-\frac{1}{2}} \preceq (\beta - 1)\mathbf{I}, && \text{(39b)} \\ &\Longleftrightarrow (\beta - 1)\mathbf{U} \succeq \mathbf{G}^H \mathbf{W} \mathbf{G}, && \text{(39c)} \end{aligned}$$

as desired. As for the equivalence part of Proposition 1, we verify it as follows. By Lemma 2, the equality in (37) holds if $\mathrm{rank}(\mathbf{W}) \leq 1$. This is because $\mathrm{rank}(\mathbf{W}) \leq 1$ implies $\mathrm{rank}\left(\mathbf{U}^{-\frac{1}{2}} \mathbf{G}^H \mathbf{W} \mathbf{G} \mathbf{U}^{-\frac{1}{2}}\right) \leq 1$ and thus the equality condition in Lemma 2 holds. Next we show that (39a) also implies the right-hand side of (38) when $\mathrm{rank}(\mathbf{W}) \leq 1$. By the following fact

$$\mathbf{A} \succeq \mathbf{0}, \;\; \mathrm{rank}(\mathbf{A}) \leq 1 \Longleftrightarrow \mathbf{A} = \boldsymbol{a}\boldsymbol{a}^H \text{ for some vector } \boldsymbol{a},$$

we have $\mathbf{U}^{-\frac{1}{2}} \mathbf{G}^H \mathbf{W} \mathbf{G} \mathbf{U}^{-\frac{1}{2}} = \boldsymbol{w}\boldsymbol{w}^H$ for some vector $\boldsymbol{w} \in \mathbb{C}^{N_t}$. Therefore, (39a) can be re-expressed as $\lambda_{\max}(\boldsymbol{w}\boldsymbol{w}^H) \leq (\beta - 1)$, which is equivalent to the right-hand side of (38) by noting that $\lambda_{\max}(\boldsymbol{w}\boldsymbol{w}^H) = \mathrm{Tr}(\boldsymbol{w}\boldsymbol{w}^H)$.

B. *Proof of Theorem 1*

For ease of exposition, we recall the SRM problem (8) and its relaxed problem (10), which are respectively given by

$$R^{\star} = \max_{\beta \geq 1} \left\{ \begin{array}{rl} \displaystyle\max_{\mathbf{W} \succeq \mathbf{0}, \mathbf{\Sigma} \succeq \mathbf{0}} & \log\left(\frac{1+\mathbf{h}^H(\mathbf{W}+\mathbf{\Sigma})\mathbf{h}}{\beta(1+\mathbf{h}^H\mathbf{\Sigma}\mathbf{h})}\right) \\ \text{s.t.} & \log\det\Big(\mathbf{I} + \left(\mathbf{I} + \mathbf{G}_k^H\mathbf{\Sigma}\mathbf{G}_k\right)^{-1}\mathbf{G}_k^H\mathbf{W}\mathbf{G}_k\Big) \leq \log\beta,\ \forall k \in \mathcal{K} \\ & \mathrm{Tr}(\mathbf{W}+\mathbf{\Sigma}) \leq P, \quad \mathrm{Tr}(\mathbf{\Phi}_l\left(\mathbf{W}+\mathbf{\Sigma}\right)) \leq \rho_l,\ \forall l \in \mathcal{L}, \end{array} \right\} \tag{40}$$

and

$$\bar{R}^{\star} = \max_{\beta \geq 1} \left\{ \begin{array}{rl} \displaystyle\max_{\mathbf{W} \succeq \mathbf{0}, \mathbf{\Sigma} \succeq \mathbf{0}} & \log\left(\frac{1+\mathbf{h}^H(\mathbf{W}+\mathbf{\Sigma})\mathbf{h}}{\beta(1+\mathbf{h}^H\mathbf{\Sigma}\mathbf{h})}\right) \\ \text{s.t.} & (\beta-1)(\mathbf{I}+\mathbf{G}_k^H\mathbf{\Sigma}\mathbf{G}_k) - \mathbf{G}_k^H\mathbf{W}\mathbf{G}_k \succeq \mathbf{0},\ \forall k \in \mathcal{K} \\ & \mathrm{Tr}(\mathbf{W}+\mathbf{\Sigma}) \leq P, \quad \mathrm{Tr}(\mathbf{\Phi}_l\left(\mathbf{W}+\mathbf{\Sigma}\right)) \leq \rho_l,\ \forall l \in \mathcal{L} \end{array} \right\}. \tag{41}$$

The proof consists of two steps: First, we show that for any given feasible β, there exists an optimal $\mathbf{W}$ for the inner maximization problem of (41) such that $\mathrm{rank}(\mathbf{W}) \leq 1$; second, we show that such a $\mathbf{W}$ is also optimal for the inner maximization problem of (40), and hence a solution correspondence is established between Problems (40) and (41).

Step 1: Given a feasible β of (41), let $\bar{R}_\beta$ denote the optimal value of the inner maximization problem of (41). Consider the following power minimization problem:

$$\min_{\mathbf{W} \succeq \mathbf{0}, \mathbf{\Sigma} \succeq \mathbf{0}} \ \mathrm{Tr}(\mathbf{W}+\mathbf{\Sigma}) \tag{42a}$$

$$\text{s.t.}\ \log\big(\frac{1+\mathbf{h}^H(\mathbf{W}+\mathbf{\Sigma})\mathbf{h}}{\beta(1+\mathbf{h}^H\mathbf{\Sigma}\mathbf{h})}\big) \geq \bar{R}_\beta, \tag{42b}$$

$$(\beta-1)(\mathbf{I}+\mathbf{G}_k^H\mathbf{\Sigma}\mathbf{G}_k) \succeq \mathbf{G}_k^H\mathbf{W}\mathbf{G}_k,\ \forall k \in \mathcal{K}, \tag{42c}$$

$$\mathrm{Tr}\left(\mathbf{\Phi}_l(\mathbf{W}+\mathbf{\Sigma})\right) \leq \rho_l,\ \forall l \in \mathcal{L}. \tag{42d}$$

Here, problem (42) aims to minimize the total transmit power subject to a minimum requirement of the secrecy rate $\bar{R}_\beta$. The reason why we consider problem (42) is as follows (we will prove them later): First, the optimal solution of (42) is also optimal for the inner maximization problem of (41); second, the optimal solution $\mathbf{W}$ of (42) must satisfy $\mathrm{rank}(\mathbf{W}) \leq 1$. Combining the above two claims, the existence of an optimal $\mathbf{W}$ with $\mathrm{rank}(\mathbf{W}) \leq \mathbf{1}$ is readily established for the inner maximization problem of (41).

Let $(\bar{\mathbf{W}}, \bar{\mathbf{\Sigma}})$ and $(\hat{\mathbf{W}}, \hat{\mathbf{\Sigma}})$ denote the optimal solutions of the inner maximization problems of (41) and (42), respectively. One can easily verify that $(\bar{\mathbf{W}}, \bar{\mathbf{\Sigma}})$ is a feasible solution of (42). It follows that

$$\mathrm{Tr}(\hat{\mathbf{W}}+\hat{\mathbf{\Sigma}}) \leq \mathrm{Tr}(\bar{\mathbf{W}}+\bar{\mathbf{\Sigma}}) \leq P, \tag{43}$$

where the first inequality is due to the fact that $(\hat{\mathbf{W}}, \hat{\boldsymbol{\Sigma}})$ minimizes $\mathrm{Tr}(\hat{\mathbf{W}} + \hat{\boldsymbol{\Sigma}})$ (cf. Problem (42a)); the second inequality follows from the feasibility of $(\bar{\mathbf{W}}, \bar{\boldsymbol{\Sigma}})$ w.r.t. (41). The inequality (43), together with (42d), imply that $(\hat{\mathbf{W}}, \hat{\boldsymbol{\Sigma}})$ is a feasible solution of (41), i.e.,

$$\log\left(\frac{1 + \mathbf{h}^H(\hat{\mathbf{W}} + \hat{\boldsymbol{\Sigma}})\mathbf{h}}{\beta(1 + \mathbf{h}^H\hat{\boldsymbol{\Sigma}}\mathbf{h})}\right) \leq \bar{R}_\beta. \tag{44}$$

Combining (44) with (42b) yields

$$\log\left(\frac{1 + \mathbf{h}^H(\hat{\mathbf{W}} + \hat{\boldsymbol{\Sigma}})\mathbf{h}}{\beta(1 + \mathbf{h}^H\hat{\boldsymbol{\Sigma}}\mathbf{h})}\right) = \bar{R}_\beta.$$

Therefore, $(\hat{\mathbf{W}}, \hat{\boldsymbol{\Sigma}})$ is an optimal solution of the inner maximization problem of (41).

To show $\mathrm{rank}(\hat{\mathbf{W}}) \leq 1$, we check the Karush-Kuhn-Tucker (KKT) optimality conditions of problem (42). Let us rewrite (42) as

$$\min_{\mathbf{W}\succeq\mathbf{0}, \boldsymbol{\Sigma}\succeq\mathbf{0}} \ \mathrm{Tr}(\mathbf{W} + \boldsymbol{\Sigma}) \tag{45a}$$

$$\mathrm{s.t.}\ \mathbf{h}^H\left(\mathbf{W} + \mu\boldsymbol{\Sigma}\right)\mathbf{h} + \mu \geq 0, \tag{45b}$$

$$\mathbf{T}_k(\mathbf{W}, \boldsymbol{\Sigma}) \succeq \mathbf{0},\ \mathrm{Tr}\left(\boldsymbol{\Phi}_l(\mathbf{W} + \boldsymbol{\Sigma})\right) \leq \rho_l,\ \forall k, l, \tag{45c}$$

where $\mu = 1 - \beta 2^{\bar{R}_\beta}$, and $\mathbf{T}_k(\mathbf{W}, \boldsymbol{\Sigma}) \triangleq (\beta - 1)(\mathbf{I} + \mathbf{G}_k^H\boldsymbol{\Sigma}\mathbf{G}_k) - \mathbf{G}_k^H\mathbf{W}\mathbf{G}_k,\ \forall k$. The Lagrangian of problem (45) is given by

$$\begin{aligned}\mathcal{L}(\mathcal{X}) =& \mathrm{Tr}(\mathbf{W} + \boldsymbol{\Sigma}) + \textstyle\sum_{l=1}^{L} \eta_l \big(\mathrm{Tr}\left(\boldsymbol{\Phi}_l(\mathbf{W} + \boldsymbol{\Sigma})\right) - \rho_l\big) \\ & - \lambda\big(\mathbf{h}^H(\mathbf{W} + \mu\boldsymbol{\Sigma})\mathbf{h} + \mu\big) - \textstyle\sum_{k=1}^{K} \mathrm{Tr}\big(\mathbf{A}_k\mathbf{T}_k(\mathbf{W}, \boldsymbol{\Sigma})\big) - \mathrm{Tr}(\mathbf{Q}\mathbf{W}) - \mathrm{Tr}(\mathbf{M}\boldsymbol{\Sigma}),\end{aligned}$$

where $\mathcal{X}$ denotes a collection of all the primal and dual variables of problem (45); $\mathbf{Q} \in \mathbb{H}_+^{N_t}$, $\mathbf{M} \in \mathbb{H}_+^{N_t}$, $\lambda \in \mathbb{R}_+$, $\mathbf{A}_k \in \mathbb{H}_+^{N_{e,k}}$ and $\eta_l \in \mathbb{R}_+$ are dual variables associated with $\mathbf{W} \succeq \mathbf{0}$, $\boldsymbol{\Sigma} \succeq \mathbf{0}$, (45b), and (45c), respectively. Assuming that problem (45) satisfies some constraint qualifications [33], the KKT conditions that are relevant to the proof are given by

$$\mathbf{I} - \lambda\mathbf{h}\mathbf{h}^H + \textstyle\sum_{k=1}^{K} \mathbf{G}_k\mathbf{A}_k\mathbf{G}_k^H + \sum_{l=1}^{L} \eta_l\boldsymbol{\Phi}_l - \mathbf{Q} = \mathbf{0}, \tag{46a}$$

$$\mathbf{Q}\mathbf{W} = \mathbf{0}, \tag{46b}$$

$$\mathbf{W} \succeq \mathbf{0}, \quad \mathbf{A}_k \succeq \mathbf{0},\ \forall k, \quad \eta_l \geq 0, \forall l, \tag{46c}$$

Postmultiplying (46a) by $\mathbf{W}$ and making use of (46b) yield

$$\big(\mathbf{I} + \textstyle\sum_{k=1}^{K} \mathbf{G}_k\mathbf{A}_k\mathbf{G}_k^H + \sum_{l=1}^{L} \eta_l\boldsymbol{\Phi}_l\big)\mathbf{W} = \lambda\mathbf{h}\mathbf{h}^H\mathbf{W}, \tag{47}$$

which implies that

$$\operatorname{rank}\big((\mathbf{I}+\textstyle\sum_{k=1}^{K}\mathbf{G}_k\mathbf{A}_k\mathbf{G}_k^H+\sum_{l=1}^{L}\eta_l\mathbf{\Phi}_l)\mathbf{W}\big)=\operatorname{rank}(\lambda\mathbf{h}\mathbf{h}^H\mathbf{W})\leq 1. \tag{48}$$

Since $\mathbf{I}+\sum_{k=1}^{K}\mathbf{G}_k\mathbf{A}_k\mathbf{G}_k^H+\sum_{l=1}^{L}\eta_l\mathbf{\Phi}_l\succ\mathbf{0}$, the following relation holds

$$\operatorname{rank}(\mathbf{W})=\operatorname{rank}\big((\mathbf{I}+\textstyle\sum_{k=1}^{K}\mathbf{G}_k\mathbf{A}_k\mathbf{G}_k^H+\sum_{l=1}^{L}\eta_l\mathbf{\Phi}_l)\mathbf{W}\big). \tag{49}$$

Finally, using (48) and (49) produces the desired result $\operatorname{rank}(\mathbf{W})\leq 1$.

Step 2: Let $\phi_\beta(\mathbf{W},\mathbf{\Sigma})$ be the objective function of the inner maximization problem of (40) (or problem (41)) for a particular β, and $(\breve{\mathbf{W}},\breve{\mathbf{\Sigma}})$ and $(\bar{\mathbf{W}},\bar{\mathbf{\Sigma}})$ be the corresponding optimal solutions of the inner maximization problem of (40) and (41), respectively. Without loss of generality, we assume $\operatorname{rank}(\bar{\mathbf{W}})\leq 1$. Since the inner maximization problem of (41) is a relaxation of that of (40) (cf. Proposition 1), we have

$$\phi_\beta(\bar{\mathbf{W}},\bar{\mathbf{\Sigma}})\geq\phi_\beta(\breve{\mathbf{W}},\breve{\mathbf{\Sigma}}).$$

On the other hand, the condition $\operatorname{rank}(\bar{\mathbf{W}})\leq 1$ implies that $(\bar{\mathbf{W}},\bar{\mathbf{\Sigma}})$ is also a feasible solution of the inner maximization problem of (40), owing to the equivalence condition in Proposition 1. As a result, we have

$$\phi_\beta(\bar{\mathbf{W}},\bar{\mathbf{\Sigma}})\leq\phi_\beta(\breve{\mathbf{W}},\breve{\mathbf{\Sigma}}).$$

Combining the above two inequalities, we conclude that $\phi_\beta(\bar{\mathbf{W}},\bar{\mathbf{\Sigma}})=\phi_\beta(\breve{\mathbf{W}},\breve{\mathbf{\Sigma}})$, i.e., $(\bar{\mathbf{W}},\bar{\mathbf{\Sigma}})$ is also optimal for the inner maximization problem of (40).

We have established a solution correspondence between (40) and (41) for any given feasible β, which includes the optimal $\beta^\star$. Subsequently, the results in Theorem 1 are obtained.

C. Proof of Theorem 2

The proof is reminiscent of Theorem 1. Re-express (24) as

$$\bar{R}^\star=\max_{\beta\geq 1}\left\{\begin{array}{c}\displaystyle\max_{\mathbf{W},\mathbf{\Sigma},\{t_k\}}\quad\log\left(\frac{1+\mathbf{h}^H(\mathbf{W}+\mathbf{\Sigma})\mathbf{h}}{\beta(1+\mathbf{h}^H\mathbf{\Sigma}\mathbf{h})}\right)\\ \text{s.t. }\ \mathbf{T}_k(\beta,\mathbf{W},\mathbf{\Sigma},t_k)\succeq\mathbf{0},\ t_k\geq 0,\ \forall k\in\mathcal{K},\\ \operatorname{Tr}\left(\mathbf{\Phi}_l(\mathbf{W}+\mathbf{\Sigma})\right)\leq\rho_l,\ \ \forall l\in\mathcal{L},\\ \operatorname{Tr}(\mathbf{W}+\mathbf{\Sigma})\leq P,\ \ \mathbf{W}\succeq\mathbf{0},\ \ \mathbf{\Sigma}\succeq\mathbf{0}\end{array}\right\} \tag{50}$$

Given a feasible β of (50), let $\bar{R}_\beta$ denote the optimal value of the inner maximization problem of (50). Consider the following secrecy-rate constrained power minimization problem

$$\begin{aligned} \min_{\mathbf{W}\succeq\mathbf{0},\boldsymbol{\Sigma}\succeq\mathbf{0},t_1,\ldots,t_K} \;& \mathrm{Tr}(\mathbf{W}+\boldsymbol{\Sigma}) \\ \text{s.t. } & \log\Big(\frac{1+\mathbf{h}^H(\mathbf{W}+\boldsymbol{\Sigma})\mathbf{h}}{\beta(1+\mathbf{h}^H\boldsymbol{\Sigma}\mathbf{h})}\Big) \geq \bar{R}_\beta, \\ & \mathbf{T}_k(\beta,\mathbf{W},\boldsymbol{\Sigma},t_k)\succeq\mathbf{0}, \quad t_k\geq 0,\ \forall k\in\mathcal{K}, \\ & \mathrm{Tr}\left(\boldsymbol{\Phi}_l(\mathbf{W}+\boldsymbol{\Sigma})\right)\leq\rho_l,\ \forall l\in\mathcal{L}. \end{aligned} \tag{51}$$

Following the same argument in the proof of Theorem 1, one can easily verify that the optimal solution of (51) must be optimal for the inner maximization problem of (50). Next, we show that the optimal solution of (51) has a rank no greater than one by checking its KKT conditions. Rewrite (51) as

$$\min_{\mathbf{W},\boldsymbol{\Sigma},\{t_k\}_{k\in\mathcal{K}}} \; \mathrm{Tr}(\mathbf{W}+\boldsymbol{\Sigma}) \tag{52a}$$

$$\text{s.t. } \mathbf{h}^H(\mathbf{W}+\mu\boldsymbol{\Sigma})\mathbf{h}+\mu\geq 0, \tag{52b}$$

$$\tilde{\mathbf{G}}_k^H\left((\beta-1)\boldsymbol{\Sigma}-\mathbf{W}\right)\tilde{\mathbf{G}}_k+\begin{bmatrix}(\beta-1-t_k)\mathbf{I} & \mathbf{0}\\ \mathbf{0} & \frac{t_k}{\epsilon_k^2}\mathbf{I}\end{bmatrix}\succeq\mathbf{0},\ t_k\geq 0,\ \forall k\in\mathcal{K} \tag{52c}$$

$$\mathrm{Tr}\left(\boldsymbol{\Phi}_l(\mathbf{W}+\boldsymbol{\Sigma})\right)\leq\rho_l,\ \forall l\in\mathcal{L}, \tag{52d}$$

$$\mathbf{W}\succeq\mathbf{0},\quad \boldsymbol{\Sigma}\succeq\mathbf{0}, \tag{52e}$$

where $\mu=1-2^{\bar{R}_\beta}\beta$ and $\tilde{\mathbf{G}}_k=[\ \bar{\mathbf{G}}_k,\ \mathbf{I}\ ]$. The Lagrangian of problem (52) is given by

$$\begin{aligned} \mathcal{L}(\mathcal{X}) = & \ \mathrm{Tr}(\mathbf{W}+\boldsymbol{\Sigma})-\textstyle\sum_{k=1}^K\mathrm{Tr}(\mathbf{A}_k\mathbf{T}_k(\beta,\mathbf{W},\boldsymbol{\Sigma},t_k)) \\ & +\textstyle\sum_{l=1}^L\eta_l\left(\mathrm{Tr}\left(\boldsymbol{\Phi}_l(\mathbf{W}+\boldsymbol{\Sigma})\right)-\rho_l\right)-\mathrm{Tr}(\boldsymbol{\Sigma}\mathbf{M}) \\ & -\mathrm{Tr}(\mathbf{W}\mathbf{Q})-\nu\left(\mathbf{h}^H(\mathbf{W}+\mu\boldsymbol{\Sigma})\mathbf{h}+\mu\right)-\textstyle\sum_{k=1}^K\lambda_k t_k, \end{aligned}$$

where $\mathcal{X}$ denotes a collection of all primal and dual variables; $\mathbf{Q}\in\mathbb{H}_+^{N_t}$, $\mathbf{M}\in\mathbb{H}_+^{N_t}$, $\nu\in\mathbb{R}_+$, $\mathbf{A}_k\in\mathbb{H}_+^{N_{e,k}+N_t}$, $\lambda_k\in\mathbb{R}_+,\forall k$ and $\eta_l\in\mathbb{R}_+,\forall l$ are dual variables associated with $\mathbf{W}$, $\boldsymbol{\Sigma}$, (52b), (52c) and (52d), respectively. Parts of the KKT conditions of problem (52) are listed below:

$$\mathbf{I}+\sum_{k=1}^K\tilde{\mathbf{G}}_k\mathbf{A}_k\tilde{\mathbf{G}}_k^H+\sum_{l=1}^L\eta_l\boldsymbol{\Phi}_l-\nu\mathbf{h}\mathbf{h}^H-\mathbf{Q}=\mathbf{0}, \tag{53a}$$

$$\mathbf{Q}\mathbf{W}=\mathbf{0}, \tag{53b}$$

$$\mathbf{W}\succeq\mathbf{0},\quad \mathbf{Q}\succeq\mathbf{0},\quad \mathbf{A}_k\succeq\mathbf{0},\forall k\in\mathcal{K},\quad \eta_l\geq 0,\forall l\in\mathcal{L}, \tag{53c}$$

Postmultiplying (53a) by $\mathbf{W}$ and making use of (53b), we obtain

$$(\mathbf{I}+\textstyle\sum_{k=1}^K\tilde{\mathbf{G}}_k\mathbf{A}_k\tilde{\mathbf{G}}_k^H+\sum_{l=1}^L\eta_l\boldsymbol{\Phi}_l)\mathbf{W}=\nu\mathbf{h}\mathbf{h}^H\mathbf{W},$$

which implies that

$$\mathrm{rank}\big((\mathbf{I}+\textstyle\sum_{k=1}^{K}\tilde{\mathbf{G}}_k\mathbf{A}_k\tilde{\mathbf{G}}_k^H+\sum_{l=1}^{L}\eta_l\mathbf{\Phi}_l)\mathbf{W}\big)=\mathrm{rank}(\nu\mathbf{h}\mathbf{h}^H\mathbf{W})\leq 1. \tag{54}$$

Since $\mathbf{I}+\sum_{k=1}^{K}\tilde{\mathbf{G}}_k\mathbf{A}_k\tilde{\mathbf{G}}_k^H+\sum_{l=1}^{L}\eta_l\mathbf{\Phi}_l\succ\mathbf{0}$, it holds that

$$\mathrm{rank}(\mathbf{W})=\mathrm{rank}\big((\mathbf{I}+\textstyle\sum_{k=1}^{K}\tilde{\mathbf{G}}_k\mathbf{A}_k\tilde{\mathbf{G}}_k^H+\sum_{l=1}^{L}\eta_l\mathbf{\Phi}_l)\mathbf{W}\big). \tag{55}$$

Combining (55) and (54) yields $\mathrm{rank}(\mathbf{W})\leq 1$.

To complete the proof, we still need to argue that such an optimal $\mathbf{W}$ is also optimal for (19) for the same β. The proof is essentially identical to that of Theorem 1, and thus is omitted for brevity.

References

[1] A. D. Wyner, “The wiretap channel,” in *The Bell System Technical Journal*, vol. 54, October 1975, pp. 1355–1387.

[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] R. Negi and S. Goel, “Secret communication using artificial noise,” in *IEEE Vehicular Technology Conference (VTC)*, Sept. 2005, pp. 1906–1910.

[4] 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.

[5] A. L. Swindlehurst, “Fixed SINR solution for the MIMO wiretap channel,” in *Proc. IEEE Int. Conf. Acoustics, Speech, and Signal Processing (ICASSP) 2009*, April 2009, pp. 2437–2440.

[6] A. Mukherjee and A. L. Swindlehurst, “Fixed-rate power allocation strategies for enhanced secrecy in MIMO wiretap channels,” in *Proc. IEEE Signal Process. Advances in Wireless Commun. (SPAWC) 2009*, June 2009, pp. 344–348.

[7] 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.

[8] 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.

[9] E. A. Jorswieck, “Secrecy capacity of single- and multi-antenna channels with simple helpers,” in *Proc. of International ITG Conference on Source and Channel Coding (SCC)*, Jan. 2010.

[10] A. Mukherjee and A. L. Swindlehurst, “Detecting passive eavesdroppers in the MIMO wiretap channel,” in *Proc. IEEE Int. Conf. Acoustics, Speech, and Signal Processing (ICASSP) 2012, Kyoto, Japan*, Mar. 2012.

[11] S. Fakoorian and A. L. Swindlehurst, “Solution for the MIMO Gaussian wiretap channel with a cooperative jammer,” *IEEE Trans. Signal Process.*, vol. 59, no. 10, pp. 5013–5022, Oct. 2011.

[12] 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.

[13] 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.

[14] A. Wolf and E. A. Jorswieck, “Maximization of worst-case secrecy rates in MIMO wiretap channels,” in *Proc. of the Asilomar Conference on Signals, Systems, and Computers, Pacific Grove, USA*, Nov. 2010.

[15] 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.

[16] 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.

[17] S. Luo, J. Li, and A. P. Petropulu, "Outage constrained secrecy rate maximization using cooperative jamming," in *IEEE Statistical Signal Processing Workshop (SSP)*, Aug. 2012.

[18] J. Li, A. P. Petropulu, and S. Weber, "On cooperative relaying schemes for wireless physical layer security," *IEEE Trans. Signal Process.*, vol. 59, no. 10, pp. 4985–4997, Oct. 2011.

[19] G. Zheng, L.-C. Choo, and K.-K. Wong, "Optimal cooperative jamming to enhance physical layer security using relays," *IEEE Trans. Signal Process.*, vol. 59, no. 3, pp. 1317–1322, Mar. 2011.

[20] Y. Pei, Y.-C. Liang, L. Zhang, K. Teh, and K. H. Li, "Secure communication over MISO cognitive radio channels," *IEEE Trans. Wireless Commun.*, vol. 9, no. 4, pp. 1494–1502, Apr. 2010.

[21] Y. Pei, Y.-C. Liang, K. Teh, and K. H. Li, "Secure communication in multiantenna cognitive radio networks with imperfect channel state information," *IEEE Trans. Signal Process.*, vol. 59, no. 4, pp. 1683–1693, Apr. 2011.

[22] J. Zhang and M. C. Gursoy, "Collaborative relay beamforming for secrecy," in *Proc. IEEE Int. Conf. Communications (ICC)*, 2010.

[23] M. Pei, J. Wei, K.-K. Wong, and X. Wang, "Masked beamforming for multiuser MIMO wiretap channels with imperfect CSI," *IEEE Trans. Wireless Commun.*, vol. 11, no. 2, pp. 544–549, Feb. 2012.

[24] 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/.

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

[26] S. Shafiee and S. Ulukus, "Achievable rates in Gaussian MISO channels with secrecy constraints," in *IEEE Int'l Symp. on Inform. Theory*, June 2007, pp. 2466–2470.

[27] 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.

[28] W. Yu and T. Lan, "Transmitter optimization for the multi-antenna downlink with per-antenna power constraints," *IEEE Trans. Signal Process.*, vol. 55, no. 6, pp. 2646–2660, June 2007.

[29] H. Huh, H. C. Papadopoulos, and G. Caire, "Multiuser MISO transmitter optimization for intercell interference mitigation," *IEEE Trans. Signal Process.*, vol. 58, no. 8, pp. 4272–4285, Aug. 2010.

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

[31] T. Kolda, R. Lewis, and V. Torczon, "Optimization by direct search: new perspectives on some classical and modern methods," *SIAM Review*, vol. 45, no. 3, pp. 385–482, 2003.

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

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

[34] Z.-Q. Luo, J. F. Sturm, and S. Zhang, "Multivariate nonnegative quadratic mappings," *SIAM J. Optim.*, vol. 14, no. 4, pp. 1140–1162, 2004.

[35] 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.

[36] 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`.

[37] Q. Li and W.-K. Ma, “Optimal transmit design for MISO secrecy-rate maximization with general covariance constraints,” in *Intl. Symp. Intelligent Signal Process. and Commun. Syst.*, Dec. 2010.