QoS-Based Transmit Beamforming in the Presence of Eavesdroppers: An Optimized Artificial-Noise-Aided Approach

Wei-Cheng Liao, Tsung-Hui Chang, *Member, IEEE*, Wing-Kin Ma, *Member, IEEE*, and Chong-Yung Chi, *Senior Member, IEEE*

***Abstract*—Secure transmission techniques have been receiving growing attention in recent years, as a viable, powerful alternative to blocking eavesdropping attempts in an open wireless medium. This paper proposes a secret transmit beamforming approach using a quality-of-service (QoS)-based perspective. Specifically, we establish design formulations that: i) constrain the maximum allowable signal-to-interference-and-noise ratios (SINRs) of the eavesdroppers, and that ii) provide the intended receiver with a satisfactory SINR through either a guaranteed SINR constraint or SINR maximization. The proposed designs incorporate a relatively new idea called artificial noise (AN), where a suitable amount of AN is added in the transmitted signal to confuse the eavesdroppers. Our designs advocate joint optimization of the transmit weights and AN spatial distribution in accordance with the channel state information (CSI) of the intended receiver and eavesdroppers. Our formulated design problems are shown to be NP-hard in general. We deal with this difficulty by using semidefinite relaxation (SDR), an approximation technique based on convex optimization. Interestingly, we prove that SDR can exactly solve the design problems for a practically representative class of problem instances; e.g., when the intended receiver's instantaneous CSI is known. Extensions to the colluding-eavesdropper scenario and the multi-intended-receiver scenario are also examined. Extensive simulation results illustrate that the proposed AN-aided designs can yield significant power savings or SINR enhancement compared to some other methods.**

***Index Terms*—Artificial noise, physical-layer secure communications, semidefinite relaxation, transmit beamforming.**

I. Introduction

TRANSMIT beamforming designs through quality-of-service (QoS) optimizations have recently flourished as an important class of multi-antenna transmission techniques. QoS-based transmit beamforming has proven to be a viable, versatile approach to a variety of communication scenarios, such as downlink unicast [2]–[5], downlink multicast [6], and multi-group multicast (a combination of unicast and multicast) [7]. In this topic, the challenges usually lie in the optimization of a desired, possibly nonconvex, design formulation; and convex optimization has been playing a significant role in this aspect, providing tractable solutions that can either exactly solve or well approximate the considered design formulation. For a general coverage of convex optimization for transmit beamforming, readers are referred to the magazine article [8] and the book chapter [9]; see also [10]–[13] for some further studies on the capability of convex optimization, and [14], [15] for some emerging applications.

This paper explores a relatively new problem in QoS-based transmit beamforming—secure transmission in the presence of eavesdroppers. To illustrate the problem, consider a commercial wireless downlink scenario, where some participating users of the system attempt to access service requiring additional charges (e.g., high-definition video) by overhearing. While overhearing cannot be stopped in an open wireless medium, a base station equipped with multiple transmit antennas may perform a countermeasure by transmit beamforming. The premise of this is that the base station has eavesdroppers' channel state information (CSI), which would be true for active eavesdroppers or participating system users. With transmit beamforming, one can utilize the spatial degree of freedom (DoF) to cripple eavesdroppers' interceptions.

In fact, we should point out that information secrecy using physical-layer transmit designs, commonly known as *physical-layer secrecy* in the present literature, has caught growing attention recently. The motivation behind is that under open wireless media, information security using crytographic encryption (in the network layer) may be subject to vulnerabilities, such as problems with secret key distribution and management. Physical-layer secrecy may serve as an alternative to, or a complement to, crytographic encryption. In a classical physical-layer secrecy setting where there is one legitimate receiver single-input-single-output (SISO) channel and one eavesdropper SISO channel (i.e., the so-called Gaussian wiretap channel), it was already shown back in the 1970s [16], [17] that the transmitter can send a message reliably to the legitimate receiver, at a positive rate and with the eavesdropper being unable to extract almost any information, if the eavesdropper's channel is a degraded version of the legitimate receiver's. The recent interest in physical-layer secrecy may be seen as a renewed one, but it is also a timely one: with multi-input-multi-output (MIMO)

Manuscript received January 26, 2010; revised July 20, 2010, November 03, 2010; accepted November 07, 2010. Date of publication November 22, 2010; date of current version February 09, 2011. The associate editor coordinating the review of this manuscript and approving it for publication was Dr. Martin Schubert. This work was supported by the National Science Council, R.O.C., by Grants NSC 99-2221-E007-052-MY3, NSC-98-2219-E007-003, and NSC-98-2219-E007-005; and by a General Research Fund awarded by Research Grant Council, Hong Kong (Project No. CUHK 415908). The material in this paper was presented at the IEEE ICASSP 2010, Dallas, TX, March 14–19, 2010.

W.-C. Liao, T.-H. Chang, and C.-Y. Chi are with the Institute of Communications Engineering and Department of Electrical Engineering, National Tsing Hua University, Hsinchu, Taiwan 30013, R.O.C. (e-mail: weicliao@gmail.com; tsunghui.chang@gmail.com; changth@mx.nthu.edu.tw; cychi@ee.nthu.edu.tw).

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

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TSP.2010.2094610

systems, one may exploit the available spatial DoF to degrade eavesdroppers' effective channels substantially. The MIMO secrecy capacity problems are considered in [18]–[21]; see also [22] for fast fading channels. Many present works, such as the aforementioned, focus on information theoretic aspects. Nevertheless, very recently there has been growing interest from the signal processing side in the designs and optimization of secret transmit schemes; see, e.g., [23]–[27].

In addition to using the transmit DoF to weaken eavesdroppers' receptions, another meaningful idea in physical-layer secrecy is that of artificial noise (AN) [24], [25], [28]. In AN-aided methods, a fraction of the transmit power is allocated to send artificially generated noise signals, usually in form of an almost[1] isotropically distributed spatial noise process, to interfere the eavesdroppers. Presently, the AN-aided methods are considered mostly for the case of passive eavesdroppers where no eavesdroppers' CSI is known to the transmitter, which is important especially to military applications. In principle, one may also consider utilizing the eavesdroppers' CSI (assuming active eavesdroppers) to steer the AN towards eavesdropper's directions for more effective blocking, rather than keeping the AN isotropic. The idea of making AN spatially focused is very recently considered in some concurrent studies; e.g., interference alignment in [25], and cooperative jamming in [23].

In this paper, we establish secret transmit beamforming designs using a QoS-based perspective. Specifically, the QoS refers to the signal-to-interference-and-noise ratio (SINR). The proposed designs assume CSI on the legitimate receiver and eavesdroppers, either in form of the instantaneous channel realization or the channel correlation matrix. Moreover, spatially focused AN is employed. In the proposed designs we degrade eavesdroppers' interceptions by constraining their maximum allowable SINRs, while, at the same time, we enhance the legitimate receiver's SINR either by constraining its minimum SINR requirement or by maximizing its SINR. It is interesting to point out that without AN, the design formulations described above are very similar to those for the cognitive radio (CR) application [15], [26], [29], [30]. Essentially, avoiding eavesdroppers from overhearing in physical-layer secrecy is reminiscent of protecting primary users from being interfered in CRs. However, this relationship does not hold when the former employs AN, which is the case in this work (primary users in CR may not be interfered, unlike eavesdroppers).

The proposed secret transmit designs advocate joint optimization of the transmit weights and AN spatial distribution. However, the resultant designs are difficult problems in a worst-case sense. We show that the proposed design problems are NP-hard in general. While this is the case, we also show that our design problems can be exactly solved for a class of practically representative problem instances. We consider semidefinite relaxation (SDR), a convex-optimization-based approximation technique that has been proven to be a powerful tool for handling a wide variety of signal processing problems [8], [31], [32]. Our analysis reveals that SDR can lead to exact (or globally optimal) solutions to the proposed design problems for some instances; e.g., when the legitimate receiver's CSI is known, or when the spatial covariances of the legitimate receiver's and eavesdroppers' CSIs are white. Moreover, two extensions, namely, those for colluding eavesdroppers and multiple legitimate receivers, are examined.

This paper is organized as follows. Section II provides the problem formulation. The optimization aspects of the formulated designs are addressed in Sections III and IV, respectively. Section V describes extensions of the present work to more complex scenarios. Simulation results and conclusions are given in Sections VI and VII, respectively.

The notation of this paper is as follows. Boldface lowercase and uppercase letters, such as $\boldsymbol{a}$ and $\boldsymbol{A}$, are used to represent vectors and matrices, respectively. The symbol $\mathbf{I}_n$ denotes the n-by-n identity matrix, $\mathbf{0}$ a zero vector or matrix, and $\mathbf{e}_i$ a unit vector where the ith entry is one and the other entries zero. The superscripts 'T' and 'H' stand for the transpose and conjugate transpose, respectively. The set of all n-dimensional complex vectors is denoted by $\mathbb{C}^n$. The set of all complex Hermitian n-by-n matrices is denoted by $\mathbb{H}^n$. $\mathrm{Range}\{\cdot\}$ denotes the range space of the argument. The Euclidean norm is denoted by $\|\cdot\|$. The trace operator is denoted by $\mathrm{Tr}(\cdot)$. When we write $\boldsymbol{A} \succeq \boldsymbol{B}$, it means that $\boldsymbol{A}-\boldsymbol{B}$ is positive semidefinite (PSD). Similarly, $\boldsymbol{A} \succ \boldsymbol{B}$ means that $\boldsymbol{A}-\boldsymbol{B}$ is positive definite. The PSD square root factor of a Hermitian PSD matrix $\boldsymbol{A}$ is denoted by $\boldsymbol{A}^{1/2}$. The symbol $\mathrm{E}\{\cdot\}$ represents the statistical expectation of the argument. The notation $\boldsymbol{x} \sim \mathcal{CN}(\boldsymbol{\mu}, \boldsymbol{\Sigma})$ means that $\boldsymbol{x}$ is a random vector following a complex circular Gaussian distribution with mean $\boldsymbol{\mu}$ and covariance $\boldsymbol{\Sigma}$.

II. Problem Formulation

In this section, we describe the system model and formulate the proposed secret transmit beamforming designs.

A. Signal Model

Our scenario of interest is that of one single-antenna legitimate receiver overheard by multiple single-antenna eavesdroppers. A simple diagram is depicted in Fig. 1 to illustrate the scenario. For convenience, we will refer to the transmitter, the legitimate receiver, and the eavesdroppers as Alice, Bob, and Eves, respectively. Alice is equipped with N_t transmit antennas, using transmit beamforming to send information to a single-antenna Bob; the transmission is overheard by M single-antenna Eves. At this moment we assume that Eves do not collude. By letting $\boldsymbol{x}(t) \in \mathbb{C}^{N_t}$ be the transmit signal vector of Alice, the received signals at Bob and Eves are, respectively, modeled as

$$y_b(t) = \mathbf{h}^H \boldsymbol{x}(t) + n(t) \quad (1)$$

$$y_{e,m}(t) = \boldsymbol{g}_m^H \boldsymbol{x}(t) + v_m(t), \quad m = 1, \ldots, M \quad (2)$$

where $\mathbf{h} \in \mathbb{C}^{N_t}$ is the channel from Alice to Bob, $\boldsymbol{g}_m \in \mathbb{C}^{N_t}$ is the channel from Alice to the mth Eve, and $n(t)$ and $v_m(t)$ are independent and identically distributed (i.i.d.) complex circular Gaussian noises with variances $\sigma_n^2 > 0$ and $\sigma_{v,m}^2 > 0$, respectively.

This paper considers AN-aided transmit beamforming. In such a scheme, the transmit vector $\boldsymbol{x}(t)$ takes the structure

$$\boldsymbol{x}(t) = \boldsymbol{w} s(t) + \mathbf{z}(t) \in \mathbb{C}^{N_t}. \quad (3)$$

Here, $s(t) \in \mathbb{C}$ is the data stream intended for Bob only, where we assume $\mathrm{E}\{|s(t)|^2\} = 1$ without loss of generality; $\boldsymbol{w} \in \mathbb{C}^{N_t}$

[1]By "almost," we mean that the AN is isotropically distributed on the orthogonal complement subspace of the legitimate receiver's channel. Physically it means that the AN does not interfere the legitimate receiver.

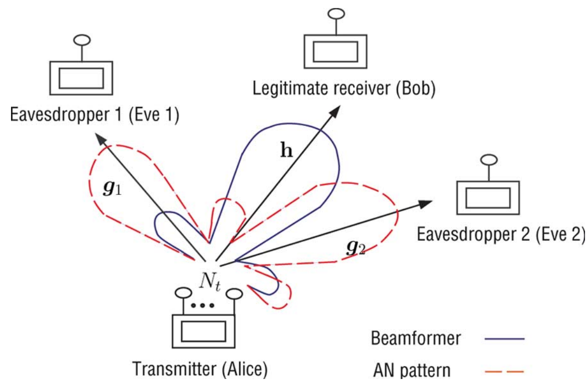


Fig. 1. The idea of AN-aided transmit beamforming.

is the transmit weight vector corresponding to $s(t)$; $\mathbf{z}(t) \in \mathbb{C}^{N_t}$ is a noise vector artificially generated by Alice to interfere Eves; i.e., the so-called AN. We assume that

$$\mathbf{z}(t) \sim \mathcal{CN}(\mathbf{0}, \mathbf{\Sigma}) \quad (4)$$

where $\mathbf{\Sigma} \succeq \mathbf{0}$ denotes the AN spatial covariance. It is worthwhile to point out that most existing endeavors assume isotropic AN; i.e., the AN covariance is chosen as $\mathbf{\Sigma} = \beta \mathbf{P}_{\mathbf{h}}^{\perp}$, where $\mathbf{P}_{\mathbf{h}}^{\perp} = \mathbf{I}_{N_t} - \mathbf{h}\mathbf{h}^H/||\mathbf{h}||^2$ is the orthogonal complement projector of $\mathbf{h}$, and $\beta \geq 0$ is a scale factor determining the power invested on AN [24], [25], [28]. The isotropic AN is often used when Eves' CSI is unknown, and it is found to be effective for such passive Eves cases. The interest here is in active Eves cases, where Alice has knowledge of Eves' CSI to a certain extent and $\mathbf{\Sigma}$ can be spatially non-isotropic to interfere Eves selectively.

B. The QoS Measure

The proposed QoS-based secret transmit beamforming designs, to be presented in the next subsection, is based on the SINR measure. Suppose that the Alice-to-Bob channel $\mathbf{h}$ is random with mean $\bar{\mathbf{h}}$ and covariance $\mathbf{C}_h$. From Bob's model (1) and the AN-aided transmit structure (3), the SINR of Bob with respect to $(\boldsymbol{w}, \mathbf{\Sigma})$ can be defined as (see, e.g., [3])

$$\mathsf{SINR}_b(\boldsymbol{w}, \mathbf{\Sigma}) = \frac{\mathrm{E}\left\{|\mathbf{h}^H \boldsymbol{w} s(t)|^2\right\}}{\mathrm{E}\left\{|\mathbf{h}^H \mathbf{z}(t)|^2\right\} + \sigma_n^2} = \frac{\boldsymbol{w}^H \mathbf{R}_h \boldsymbol{w}}{\mathrm{Tr}(\mathbf{\Sigma}\mathbf{R}_h) + \sigma_n^2} \quad (5)$$

where

$$\mathbf{R}_h = \mathrm{E}\{\mathbf{h}\mathbf{h}^H\} = \bar{\mathbf{h}}\bar{\mathbf{h}}^H + \mathbf{C}_h \quad (6)$$

is the correlation matrix of $\mathbf{h}$. It will be assumed in the sequel that $\mathbf{R}_h$ is known to Alice. Moreover, for the case where the instantaneous channel realization of Bob is known to Alice, we should redefine $\mathbf{R}_h$ as $\mathbf{R}_h = \mathbf{h}\mathbf{h}^H$.

Likewise, the SINRs of Eves under the model (2) are

$$\begin{aligned}\mathsf{SINR}_{e,m}(\boldsymbol{w}, \mathbf{\Sigma}) &= \frac{\mathrm{E}\{|\boldsymbol{g}_m^H \boldsymbol{w} s(t)|^2\}}{\mathrm{E}\{|\boldsymbol{g}_m^H \mathbf{z}(t)|^2\} + \sigma_{v,m}^2} \\ &= \frac{\boldsymbol{w}^H \mathbf{R}_{g,m} \boldsymbol{w}}{\mathrm{Tr}(\mathbf{\Sigma}\mathbf{R}_{g,m}) + \sigma_{v,m}^2} \end{aligned} \quad (7)$$

where, for the case where the instantaneous channel realizations of Eves are known to Alice, we define $\mathbf{R}_{g,m} = \boldsymbol{g}_m \boldsymbol{g}_m^H$; and, for the case where only Eves' channel correlation matrices are available to Alice, we define $\mathbf{R}_{g,m} = \mathrm{E}\{\boldsymbol{g}_m \boldsymbol{g}_m^H\} = \bar{\boldsymbol{g}}_m \bar{\boldsymbol{g}}_m^H + \mathbf{C}_{g,m}$ with $\bar{\boldsymbol{g}}_m$ and $\mathbf{C}_{g,m}$ being the mean and covariance of $\boldsymbol{g}_m$, respectively. Again, $\mathbf{R}_{g,1}, \ldots, \mathbf{R}_{g,M}$ are assumed to be available to Alice. We should note that for the correlation-based CSI case, the channel covariances $\mathbf{C}_{g,m}$ characterize the uncertainty to Eves' channels $\boldsymbol{g}_m$ in a second-order statistics sense. In particular, in an extreme setting of $\mathbf{R}_{g,m} = \sigma_{g,m}^2 \mathbf{I}_{N_t}$ for some $\sigma_{g,m}^2 > 0$, the physical meaning is that we have no information about the channel direction of that Eve.

C. The Proposed Design Formulations

With the SINRs defined in the last subsection, we can now describe the proposed secret transmit beamforming design formulations. As previously mentioned, our general goal is to jointly optimize the transmit weight vector $\boldsymbol{w}$ and AN spatial covariance $\mathbf{\Sigma}$ such that Bob's and Eves' SINRs are enhanced and degraded, respectively. To this end, we propose two design formulations. The first formulation is a power minimization formulation, described as follows:

Formulation 1 (minimizing the total power subject to SINR constraints on Bob and Eves): *Given a minimum SINR requirement on Bob* $\gamma_b > 0$ *and a maximum allowable SINR threshold on Eves* $\gamma_e > 0$, *design* $(\boldsymbol{w}, \mathbf{\Sigma})$ *by solving*

$$\begin{aligned} \min_{\boldsymbol{w} \in \mathbb{C}^{N_t}, \mathbf{\Sigma} \in \mathbb{H}^{N_t}} \quad & ||\boldsymbol{w}||^2 + \mathrm{Tr}(\mathbf{\Sigma}) \\ \text{s.t.} \quad & \mathsf{SINR}_b(\boldsymbol{w}, \mathbf{\Sigma}) \geq \gamma_b \\ & \mathsf{SINR}_{e,m}(\boldsymbol{w}, \mathbf{\Sigma}) \leq \gamma_e, \quad m = 1, \ldots, M \\ & \mathbf{\Sigma} \succeq \mathbf{0}. \end{aligned} \quad (8)$$

It should be noticed that the specification (γ_b, γ_e), which is chosen by the system operator, is meaningful only when γ_b is much greater than γ_e; say, e.g., $\gamma_b = 10$ dB, $\gamma_e = 0$ dB. Moreover, in principle, there may exist circumstances where there is no feasible solution $(\boldsymbol{w}, \mathbf{\Sigma})$ for Formulation 1; e.g., when the specification (γ_b, γ_e) is set too demanding. Fortunately, it can be shown that feasibility is not a serious issue for the case where Bob's instantaneous CSI is available.

Lemma 1: *Suppose that* $\mathbf{R}_h = \mathbf{h}\mathbf{h}^H$, *and* $\mathbf{R}_{g,m} \neq \alpha \mathbf{R}_h$ *for any* α *and for* $m = 1, \ldots, M$. *Then, (8) in Formulation 1 is feasible.*

Proof: The proof is to exploit the fact that an isotropic AN solution is a feasible point of (8). Suppose that we fix the structure of $(\boldsymbol{w}, \mathbf{\Sigma})$ as

$$\boldsymbol{w} = \sqrt{\rho}\mathbf{h}, \quad \mathbf{\Sigma} = \beta \mathbf{P}_{\mathbf{h}}^{\perp} \quad (9)$$

for some ρ, $\beta > 0$. It can be verified that $(\boldsymbol{w}, \mathbf{\Sigma})$ satisfies all the SINR constraints in (8) if ρ, β are chosen as

$$\rho = \frac{\sigma_n^2 \gamma_b}{||\mathbf{h}||^4} \quad (10a)$$

$$\beta = \max\left\{0, \max_{m=1,\ldots,M} \frac{\frac{\rho}{\gamma_e}\mathbf{h}^H \mathbf{R}_{g,m}\mathbf{h} - \sigma_{v,m}^2}{\mathrm{Tr}(\mathbf{P}_{\mathbf{h}}^{\perp}\mathbf{R}_{g,m})}\right\}. \quad (10b)$$

Note that $\mathrm{Tr}(\mathbf{P}_{\mathbf{h}}^{\perp}\mathbf{R}_{g,m}) > 0$ under the premise of $\mathbf{R}_{g,m} \neq \alpha \mathbf{R}_h$ for any α. As an aside, the power allocation in (10) can be shown to yield the smallest total power under the isotropic AN structure

(9). We therefore have shown that (8) is always feasible under the assumption in Lemma 1. ∎

The second design formulation is as follows.

Formulation 2 (maximizing Bob's SINR subject to constraints on power and Eves' SINRs): *Given a maximum allowable SINR threshold on Eves* $\gamma_e > 0$ *and a transmit power limit* $P_{\max} > 0$, *design* $(\boldsymbol{w}, \boldsymbol{\Sigma})$ *by solving*

$$\begin{aligned} \max_{\boldsymbol{w}\in\mathbb{C}^{N_t},\boldsymbol{\Sigma}\in\mathbb{H}^{N_t}} \quad & \mathsf{SINR}_b(\boldsymbol{w},\boldsymbol{\Sigma}) \\ \text{s.t.} \quad & \|\boldsymbol{w}\|^2 + \mathrm{Tr}(\boldsymbol{\Sigma}) \le P_{\max} \\ & \mathsf{SINR}_{e,m}(\boldsymbol{w},\boldsymbol{\Sigma}) \le \gamma_e, \quad m = 1,\ldots,M \\ & \boldsymbol{\Sigma} \succeq \mathbf{0}. \end{aligned} \tag{11}$$

The design criterion of Formulation 2 is to offer the best possible SINR on Bob, given a power specification $P_{\max}$ and an SINR limit on Eves γ_e. Problem (11) always has a feasible solution. However, in some instances; e.g., demanding specifications and/or having many Eves, it is possible that the best SINR on Bob found by (11) be lower than γ_e. Under such circumstances, the system operator should consider relaxing the power specification $P_{\max}$ such that a reasonable SINR on Bob is attained.

The goal of this paper lies in finding the optimal transmit design solutions of the above two design formulations. This will be addressed in the following two sections.

III. Optimization in the Power Minimization Design

This section considers the optimization aspects of the power minimization design for AN-aided transmit beamforming. The first subsection studies the nature and challenge of the problem, while the second subsection describes the proposed approach to handling the problem.

A. The Problem Nature

Let us explicitly express the power minimization design (8) as

$$\min_{\boldsymbol{w},\boldsymbol{\Sigma}} \quad \|\boldsymbol{w}\|^2 + \mathrm{Tr}(\boldsymbol{\Sigma}) \tag{12a}$$

$$\text{s.t.} \quad \frac{1}{\gamma_b}\boldsymbol{w}^H\mathbf{R}_h\boldsymbol{w} \ge \mathrm{Tr}(\boldsymbol{\Sigma}\mathbf{R}_h) + \sigma_n^2, \tag{12b}$$

$$\frac{1}{\gamma_e}\boldsymbol{w}^H\mathbf{R}_{g,m}\boldsymbol{w} \le \mathrm{Tr}(\boldsymbol{\Sigma}\mathbf{R}_{g,m}) + \sigma_{v,m}^2, \quad m = 1,\ldots,M \tag{12c}$$

$$\boldsymbol{\Sigma} \succeq \mathbf{0}. \tag{12d}$$

It is interesting to note that (12) is related to a CR transmit design problem [15], [30], when we remove all the AN terms in (12) to form the following no-AN design:

$$\min_{\boldsymbol{w}} \quad \|\boldsymbol{w}\|^2 \tag{13a}$$

$$\text{s.t.} \quad \frac{1}{\sigma_n^2}\boldsymbol{w}^H\mathbf{R}_h\boldsymbol{w} \ge \gamma_b \tag{13b}$$

$$\frac{1}{\sigma_{v,m}^2}\boldsymbol{w}^H\mathbf{R}_{g,m}\boldsymbol{w} \le \gamma_e, \quad m = 1,\ldots,M. \tag{13c}$$

In particular, from a CR perspective, (13c) represents interference temperature constraints for keeping interference to the primary users below a tolerable level. The no-AN design (13) is generally nonconvex, but can be turned to a convex problem for the case of $\mathbf{R}_h = \mathbf{h}\mathbf{h}^H$ (i.e., instantaneous CSI on Bob). In that case, (13) can be reformulated as a second order cone program [1], [3], [5]. However, one may verify that the same convex reformulation trick does not work for the AN-aided design (12).

The AN-aided design (12) is a nonconvex quadratic optimization problem, only because of Bob's nonconvex SINR constraint in (12b). Unfortunately, the fact that only one constraint in (12) is nonconvex leads to the claim that (12) is a very difficult problem in general.

Lemma 2: *Both (12) and (13) are NP-hard in general.*

The proof of Lemma 2 is shown in Appendix A. We should mention that the NP-hardness claim in Lemma 2 is based on the argument that for a general class of problem instances $\gamma_b,\ \gamma_e > 0$, $\mathbf{R}_h, \mathbf{R}_{g,1}, \ldots, \mathbf{R}_{g,M} \succeq \mathbf{0}$, there exist problem instances where (12) can become very hard to solve. While this means that we may not be able to find an optimization algorithm that can solve (12) efficiently for all problem instances, it might be possible that (12) can be handled quite well for most of the problem instances that are of practical interest. This motivates our endeavor to use SDR to handle (12), the development of which is presented in the next subsection.

B. Semidefinite Relaxation, and Its Optimality Conditions

To describe the application of SDR to the AN-aided design (12), let us define $\mathbf{W} = \boldsymbol{w}\boldsymbol{w}^H$ and rewrite (12) as

$$\min_{\mathbf{W},\boldsymbol{\Sigma}\in\mathbb{H}^{N_t}} \quad \mathrm{Tr}(\mathbf{W}) + \mathrm{Tr}(\boldsymbol{\Sigma}) \tag{14a}$$

$$\text{s.t.} \quad \frac{1}{\gamma_b}\mathrm{Tr}(\mathbf{W}\mathbf{R}_h) - \mathrm{Tr}(\mathbf{R}_h\boldsymbol{\Sigma}) \ge \sigma_n^2 \tag{14b}$$

$$\frac{1}{\gamma_e}\mathrm{Tr}(\mathbf{W}\mathbf{R}_{g,m}) - \mathrm{Tr}(\mathbf{R}_{g,m}\boldsymbol{\Sigma}) \le \sigma_{v,m}^2, \quad m = 1,\ldots,M \tag{14c}$$

$$\boldsymbol{\Sigma} \succeq \mathbf{0},\ \mathbf{W} \succeq \mathbf{0},\ \mathrm{rank}(\mathbf{W}) = 1 \tag{14d}$$

where the constraints $\mathbf{W} \succeq 0$, $\mathrm{rank}(\mathbf{W}) = 1$ in (14d) are equivalent to constraining $\mathbf{W} = \boldsymbol{w}\boldsymbol{w}^H$. In the SDR approach, we relax (14) by neglecting the constraint $\mathrm{rank}(\mathbf{W}) = 1$ in (14d)

$$\min_{\mathbf{W},\boldsymbol{\Sigma}} \quad \mathrm{Tr}(\mathbf{W}) + \mathrm{Tr}(\boldsymbol{\Sigma}) \tag{15a}$$

$$\text{s.t.} \quad \frac{1}{\gamma_b}\mathrm{Tr}(\mathbf{W}\mathbf{R}_h) - \mathrm{Tr}(\mathbf{R}_h\boldsymbol{\Sigma}) \ge \sigma_n^2 \tag{15b}$$

$$\frac{1}{\gamma_e}\mathrm{Tr}(\mathbf{W}\mathbf{R}_{g,m}) - \mathrm{Tr}(\mathbf{R}_{g,m}\boldsymbol{\Sigma}) \le \sigma_{v,m}^2, \quad m = 1,\ldots,M \tag{15c}$$

$$\boldsymbol{\Sigma} \succeq \mathbf{0},\ \mathbf{W} \succeq \mathbf{0}. \tag{15d}$$

The relaxed problem above, which we will call the SDR problem of the original design problem (12), is convex—it is a semidefinite program whose optimal solution can be efficiently obtained by available interior-point algorithms; e.g., the off-the-shelf solvers SeDuMi [33] and CVX [34].

The SDR (15) is generally an approximation to the AN-aided design (12), because the former does not guarantee a rank-one optimal $\mathbf{W}$ given an arbitrary problem instance $\mathbf{R}_h, \mathbf{R}_{g,1}, \ldots, \mathbf{R}_{g,M} \succeq \mathbf{0}$, γ_b, $\gamma_e > 0$. There are standard methods for generating a suboptimal transmit weight $\boldsymbol{w}$ from SDR; see [9], [32], and the references therein. But, for instances where an SDR optimal $\mathbf{W}$ happens to be of rank one, we can simply extract the rank-one decomposition of that SDR optimal $\mathbf{W}$ (essentially, the principal eigenvector of $\mathbf{W}$) and the SDR for those instances is optimal to the original AN-aided design (12).

Interestingly, we are able to show that for a practically representative class of problem instances, SDR always yields a rank-one transmit beamforming solution [or SDR is an exact solver of the AN-aided design (12)]. This is described in the following proposition.

Proposition 1: *Consider the AN-aided power minimization design (12), and its SDR problem (15). Suppose that* $\mathbf{R}_h, \mathbf{R}_{g,1}, \ldots, \mathbf{R}_{g,M} \succeq \mathbf{0}$ *satisfy either one of the following conditions:*

C1) *(Instantaneous CSI on Bob)* $\mathbf{R}_h = \mathbf{h}\mathbf{h}^H$, *while* $\mathbf{R}_{g,1}, \ldots, \mathbf{R}_{g,M} \succeq \mathbf{0}$ *are arbitrary PSD matrices.*

C2) *(Correlation-based CSI on Bob and Eves, with white channel covariance)* $N_t > M$, *and the channel correlation matrices take the form*

$$\mathbf{R}_h = \bar{\mathbf{h}}\bar{\mathbf{h}}^H + \sigma_h^2 \mathbf{I}_{N_t}$$
$$\mathbf{R}_{g,m} = \bar{\boldsymbol{g}}_m \bar{\boldsymbol{g}}_m^H + \sigma_{g,m}^2 \mathbf{I}_{N_t}, \quad m = 1, \ldots, M$$

where $\sigma_h^2, \sigma_{g,1}^2, \ldots, \sigma_{g,M}^2 \geq 0$, *and* $\bar{\mathbf{h}}, \bar{\boldsymbol{g}}_1, \ldots, \bar{\boldsymbol{g}}_M \in \mathbb{C}^{N_t}$ *are such that* $\bar{\mathbf{h}} \notin \mathrm{Range}\{\bar{\boldsymbol{g}}_1, \ldots, \bar{\boldsymbol{g}}_M\}$.

C3) *(The number of Eves is no greater than two)* $M \leq 2$, *and* $\mathbf{R}_h, \mathbf{R}_{g,1}, \ldots, \mathbf{R}_{g,M}$ *are arbitrary.*

Also, suppose that the SDR problem (15) is feasible. Then, there exists an optimal SDR solution, denoted by $(\mathbf{W}^\star, \mathbf{\Sigma}^\star)$, *for which* $\mathbf{W}^\star$ *is of rank one; viz.*

$$\mathbf{W}^\star = \boldsymbol{w}^\star (\boldsymbol{w}^\star)^H.$$

Moreover, for Cases C1) and C2), any optimal SDR solution $(\mathbf{W}^\star, \mathbf{\Sigma}^\star)$ *must have rank-one* $\mathbf{W}^\star$.

The rank-one optimality of SDR for Cases C1) and C2) was obtained by examining the Karush-Kuhn-Tucker (KKT) conditions of the SDR problem (15), where we found that any SDR optimal solution has to have rank-one $\mathbf{W}^\star$. As for Case C3), it is a direct consequence of the SDP rank reduction result [13], [35], which identifies existence of a rank-one SDR solution; readers are referred to [13] for further details, such as the generation of a rank-one SDR solution. The proof of Proposition 1 is given in Appendix B.

IV. Optimization in the SINR Maximization Design

We now turn our attention to Formulation 2, the SINR maximization design alternative. The design problem, according to (11), can be expressed as

$$\max_{\boldsymbol{w}, \mathbf{\Sigma}} \quad \frac{\boldsymbol{w}^H \mathbf{R}_h \boldsymbol{w}}{\mathrm{Tr}(\mathbf{\Sigma}\mathbf{R}_h) + \sigma_n^2} \tag{16a}$$

$$\text{s.t.} \quad \frac{1}{\gamma_e} \boldsymbol{w}^H \mathbf{R}_{g,m} \boldsymbol{w} \leq \mathrm{Tr}(\mathbf{\Sigma}\mathbf{R}_{g,m}) + \sigma_{v,m}^2, \; m = 1, \ldots, M \tag{16b}$$

$$\|\boldsymbol{w}\|^2 + \mathrm{Tr}(\mathbf{\Sigma}) \leq P_{\max}, \tag{16c}$$

$$\mathbf{\Sigma} \succeq \mathbf{0}. \tag{16d}$$

In the same spirit as treating the power minimization design in the last section, we will handle (16) using the SDR approach.

The SINR maximization design (16) is also a very difficult problem. We show in Appendix C that

Lemma 3: *Problem (16) is NP-hard in general.*

Let us consider applying SDR to (16). Using the same idea as described in Section III-B, the SDR problem for (16) is shown to be

$$\max_{\mathbf{W}, \mathbf{\Sigma}} \quad \frac{\mathrm{Tr}(\mathbf{W}\mathbf{R}_h)}{\mathrm{Tr}(\mathbf{\Sigma}\mathbf{R}_h) + \sigma_n^2} \tag{17a}$$

$$\text{s.t.} \quad \frac{1}{\gamma_e} \mathrm{Tr}(\mathbf{W}\mathbf{R}_{g,m}) \leq \mathrm{Tr}(\mathbf{\Sigma}\mathbf{R}_{g,m}) + \sigma_{v,m}^2, \quad m = 1, \ldots, M \tag{17b}$$

$$\mathrm{Tr}(\mathbf{W}) + \mathrm{Tr}(\mathbf{\Sigma}) \leq P_{\max} \tag{17c}$$

$$\mathbf{\Sigma} \succeq \mathbf{0}, \; \mathbf{W} \succeq \mathbf{0}. \tag{17d}$$

Unlike the SDR of the power minimization design, the SDR problem (17) does not immediately lead to an SDP. The SDR problem (17) is a quasi-convex problem, due to the linear fractional structure of its objective (17a). A standard approach to solving this kind of quasi-convex problems is to employ a bisection methodology [5], [36], where the globally optimal solution is sequentially searched by solving a sequence (often many) of SDPs.

Here we develop a simpler alternative to solving (17). The idea is to reformulate the quasi-convex problem (17) to a convex SDP through the Charnes-Cooper transformation [37]. Let

$$\eta = \frac{1}{\mathrm{Tr}(\mathbf{\Sigma}\mathbf{R}_h) + \sigma_n^2}. \tag{18}$$

By using the following transformation of variables

$$\bar{\mathbf{W}} = \eta \mathbf{W}, \quad \bar{\mathbf{\Sigma}} = \eta \mathbf{\Sigma} \tag{19}$$

we may rewrite (17) as an SDP

$$\max_{\bar{\mathbf{W}}, \bar{\mathbf{\Sigma}}, \eta} \quad \mathrm{Tr}(\bar{\mathbf{W}}\mathbf{R}_h) \tag{20a}$$

$$\text{s.t.} \quad \mathrm{Tr}(\bar{\mathbf{\Sigma}}\mathbf{R}_h) + \eta\sigma_n^2 = 1 \tag{20b}$$

$$\frac{1}{\gamma_e} \mathrm{Tr}(\bar{\mathbf{W}}\mathbf{R}_{g,m}) \leq \mathrm{Tr}(\bar{\mathbf{\Sigma}}\mathbf{R}_{g,m}) + \eta\sigma_{v,m}^2, \quad m = 1, \ldots, M \tag{20c}$$

$$\mathrm{Tr}(\bar{\mathbf{W}}) + \mathrm{Tr}(\bar{\mathbf{\Sigma}}) \leq \eta P_{\max} \tag{20d}$$

$$\bar{\mathbf{W}} \succeq \mathbf{0}, \; \bar{\mathbf{\Sigma}} \succeq \mathbf{0}, \; \eta \geq 0 \tag{20e}$$

under the assumption that an optimal solution of (20), denoted by $(\bar{\mathbf{W}}^\star, \bar{\mathbf{\Sigma}}^\star, \eta^\star)$, has $\eta^\star > 0$. In general, it is true that $\eta^\star > 0$: If $\eta^\star = 0$, then, according to (20d), we have $\bar{\mathbf{W}}^\star = \bar{\mathbf{\Sigma}}^\star = \mathbf{0}$. However, that $(\bar{\mathbf{W}}^\star, \bar{\mathbf{\Sigma}}^\star, \eta^\star)$ violates (20b). Hence, we arrive at the following conclusion.

Proposition 2: *The quasi-convex SDR problem in (17) is equivalent to the SDP in (20). The equivalence lies in that if* $(\bar{\mathbf{W}}^\star, \bar{\boldsymbol{\Sigma}}^\star, \eta^\star)$ *is optimal to (20), then* $(\bar{\mathbf{W}}^\star/\eta^\star, \bar{\boldsymbol{\Sigma}}^\star/\eta^\star)$ *is optimal to (17).*

The above described equivalent SDP reformulation of the SDR problem not only provides a computationally more efficient way of solving SDR (compared to the bisection search), it also sheds light into conditions under which SDR exactly solves the SINR maximization design. By examining the equivalent SDR problem (20), we show in Appendix D that

Proposition 3: *Consider the AN-aided SINR maximization design (16), and its SDR problem (17). Suppose that* $\mathbf{R}_h, \mathbf{R}_{g,1}, \ldots, \mathbf{R}_{g,M} \succeq \mathbf{0}$ *satisfy either one of the following conditions:*

C1) *(Instantaneous CSI on Bob)* $\mathbf{R}_h = \mathbf{h}\mathbf{h}^H$, *while* $\mathbf{R}_{g,m} \neq \alpha\mathbf{R}_h$ *for any scaling* α, *for all* $m = 1, \ldots, M$.

C2) *(Correlation-based CSI on Bob and Eves, with white channel covariance)* $N_t > M$, *and the channel correlation matrices take the form*

$$\mathbf{R}_h = \bar{\mathbf{h}}\bar{\mathbf{h}}^H + \sigma_h^2 \mathbf{I}_{N_t}$$
$$\mathbf{R}_{g,m} = \bar{\boldsymbol{g}}_m \bar{\boldsymbol{g}}_m^H + \sigma_{g,m}^2 \mathbf{I}_{N_t}, \quad m = 1, \ldots, M$$

where $\sigma_h^2, \sigma_{g,1}^2, \ldots, \sigma_{g,M}^2 \geq 0$, *and* $\bar{\mathbf{h}}, \bar{\boldsymbol{g}}_1, \ldots, \bar{\boldsymbol{g}}_M \in \mathbb{C}^{N_t}$ *are such that* $\bar{\mathbf{h}} \notin \mathrm{Range}\{\bar{\boldsymbol{g}}_1, \ldots, \bar{\boldsymbol{g}}_M\}$.

C3) *(The number of Eves is no greater than two)* $M \leq 2$, *and* $\mathbf{R}_h, \mathbf{R}_{g,1}, \ldots, \mathbf{R}_{g,M}$ *are arbitrary.*

There exists an optimal SDR solution, denoted by $(\mathbf{W}^\star, \boldsymbol{\Sigma}^\star)$, *for which* $\mathbf{W}^\star$ *is of rank one. Moreover, for Cases C1) and C2), any optimal SDR solution* $(\mathbf{W}^\star, \boldsymbol{\Sigma}^\star)$ *must have rank-one* $\mathbf{W}^\star$.

Interestingly, the cases for which SDR is identified to give exactly optimal solutions to the SINR maximization design, as shown above, are almost the same as those for the power minimization design (see Proposition 1).

V. EXTENSIONS

We herein describe two possible extensions of the above described AN-aided secret transmit beamforming designs, namely, to the colluding-Eve scenario and the multigroup multicast scenario. They are, respectively, considered in the following two subsections.

A. Colluding Eves

We consider a scenario where some Eves cooperate to form joint receive beamforming, in an attempt to improve their interception. For ease of exposition of the ideas, we assume that all Eves are colluding. Moreover, Eves are assumed to perform joint maximum SINR receive beamforming. Following the model in (1) and (2), the maximum receive SINR achieved by colluding Eves is defined to be

$$\mathsf{SINR}_{ce}(\boldsymbol{w}, \boldsymbol{\Sigma}) = \max_{\mathbf{r} \neq \mathbf{0}} \frac{\mathrm{E}\left\{\left|\mathbf{r}^H \mathbf{G}^H \boldsymbol{w} s(t)\right|^2\right\}}{\mathrm{E}\left\{\left|\mathbf{r}^H (\mathbf{G}^H \mathbf{z}(t) + \mathbf{v}(t))\right|^2\right\}} \quad (21)$$

where $\mathbf{r} \in \mathbb{C}^M$ denotes the receive beamformer weight of Eves, $\mathbf{G} = [\boldsymbol{g}_1, \ldots, \boldsymbol{g}_M]$, and $\mathbf{v}(t) = [\; v_1(t), \ldots, v_M(t) \;]^T$. It is shown that the SINR in (21) can be reduced to

$$\mathsf{SINR}_{ce}(\boldsymbol{w}, \boldsymbol{\Sigma}) = \max_{\mathbf{r} \neq \mathbf{0}} \frac{\mathbf{r}^H \boldsymbol{\mathcal{A}}(\boldsymbol{w}\boldsymbol{w}^H)\mathbf{r}}{\mathbf{r}^H (\boldsymbol{\mathcal{A}}(\boldsymbol{\Sigma}) + \mathbf{D}^2)\mathbf{r}} \quad (22)$$

where $\mathbf{D} = \mathrm{Diag}(\sigma_{v,1}, \ldots, \sigma_{v,M})$, and $\boldsymbol{\mathcal{A}}(\cdot) : \mathbb{H}^{N_t} \longrightarrow \mathbb{H}^M$ is a linear matrix function whose $(k,\ell)\mathrm{th}$ entry is

$$[\boldsymbol{\mathcal{A}}(\mathbf{W})]_{(k,\ell)} = \mathrm{Tr}\left(\mathbf{W}\mathbf{R}_{g,(\ell,k)}\right) \quad (23)$$

with $\mathbf{R}_{g,(\ell,k)} = \mathrm{E}\{\boldsymbol{g}_\ell \boldsymbol{g}_k^H\}$ for the correlation-based CSI case; and $\mathbf{R}_{g,(\ell,k)} = \boldsymbol{g}_\ell \boldsymbol{g}_k^H$ for the instantaneous CSI case.

Our idea is to bound $\mathsf{SINR}_{ce}(\boldsymbol{w}, \boldsymbol{\Sigma})$ below a known threshold by bounding the per-Eve SINRs $\mathsf{SINR}_{e,m}(\boldsymbol{w}, \boldsymbol{\Sigma})$. We found by analysis that bounding the per-Eve SINRs may not be enough to bound the colluding-Eve SINR, but there is a simple remedy as described in the following proposition.

Proposition 4: *Consider a variation of Formulations 1 and 2, where we add the following convex constraint on their respective design problems in (8) and (11):*

$$\mathbf{D}^{-1}\boldsymbol{\mathcal{A}}(\boldsymbol{\Sigma})\mathbf{D}^{-1} \succeq \frac{1}{M}\mathrm{Tr}\left(\mathbf{D}^{-1}\boldsymbol{\mathcal{A}}(\boldsymbol{\Sigma})\mathbf{D}^{-1}\right)\mathbf{I}_M. \quad (24)$$

For such modified design problems, it holds true that any feasible $(\boldsymbol{w}, \boldsymbol{\Sigma})$ *satisfies*

$$\mathsf{SINR}_{ce}(\boldsymbol{w}, \boldsymbol{\Sigma}) \leq M\gamma_e. \quad (25)$$

The proof of Proposition 4 is described in Appendix E. Proposition 4 indicates that by adding the constraint (24) in the designs, the maximum allowable colluding-Eve SINR is constrained below $M\gamma_e$ indirectly. We should emphasize that the SDRs of the resultant modified designs are simply those of the original [(15) and (20)] with the addition of the constraint (24). Those modified SDRs are again convex SDPs, and it can be verified that the SDR rank-one optimality for Cases C1) and C2) in Propositions 1 and 3 still holds for the modified SDRs.

B. Multigroup Multicast

In multigroup multicast, we consider a general multi-Bob setting described as follows. Alice is intended to transmit multiple data streams to multiple groups of Bobs. The transmit signal vector at Alice becomes

$$\boldsymbol{x}(t) = \sum_{q=1}^{Q} \boldsymbol{w}_q s_q(t) + \mathbf{z}(t) \quad (26)$$

where Q is the number of data streams, $s_q(t)$ is the $q\mathrm{th}$ data stream which is assumed to be independent of one another, $\boldsymbol{w}_q \in \mathbb{C}^{N_t}$ is the transmit weight vector corresponding to $s_q(t)$, and $\mathbf{z}(t)$ is again the AN. There are K Bobs to be served, and the received signal of each Bob is modeled as

$$y_{b,k}(t) = \mathbf{h}_k^H \boldsymbol{x}(t) + n_k(t), \quad k = 1, \ldots, K \quad (27)$$

where $\mathbf{h}_k$ is the channel vector from Alice to the kth Bob, and $n_k(t)$ is a complex circular Gaussian noise with zero mean and variance $\sigma_{n,k}^2 > 0$. Again, there are M Eves eavesdropping, and that their received signal model is the same as in (2). Each Bob is assigned to receive only one data stream. We denote $\mathcal{G}_q \subseteq \{1, 2, \ldots, K\}$ to be the set of Bobs assigned to the qth data stream; i.e., if $k \in \mathcal{G}_q$ then it means that the kth Bob is intended to receive $s_q(t)$ only. These grouping sets $\mathcal{G}_q$ are disjoint and $\sum_{q=1}^{Q} |\mathcal{G}_q| = K$.

Following the signal model in (26) and (27), the SINR of the kth Bob is formulated as

$$\mathsf{SINR}_{b,k}(\boldsymbol{w}_1, \ldots, \boldsymbol{w}_Q, \boldsymbol{\Sigma}) = \frac{\boldsymbol{w}_q^H \mathbf{R}_{h,k} \boldsymbol{w}_q}{\sum_{p \neq q} \boldsymbol{w}_p^H \mathbf{R}_{h,k} \boldsymbol{w}_p + \mathrm{Tr}(\boldsymbol{\Sigma} \mathbf{R}_{h,k}) + \sigma_{n,k}^2}, \quad k \in \mathcal{G}_q \tag{28}$$

where $\mathbf{R}_{h,k} = \mathrm{E}\{\mathbf{h}_k \mathbf{h}_k^H\} = \bar{\mathbf{h}}_k \bar{\mathbf{h}}_k^H + \mathbf{C}_{h,k}$ if we assume that $\mathbf{h}_k$ is random with known mean $\bar{\mathbf{h}}_k$ and covariance $\mathbf{C}_{h,k}$, and $\mathbf{R}_{h,k} = \mathbf{h}_k \mathbf{h}_k^H$ if we assume perfect knowledge of the instantaneous CSI of the kth Bob. The SINR for the mth Eve to eavesdrop the qth data stream is

$$\mathsf{SINR}_{e,m}^{(q)}(\boldsymbol{w}_1, \ldots, \boldsymbol{w}_Q, \boldsymbol{\Sigma}) = \frac{\boldsymbol{w}_q^H \mathbf{R}_{g,m} \boldsymbol{w}_q}{\sum_{p \neq q} \boldsymbol{w}_p^H \mathbf{R}_{g,m} \boldsymbol{w}_p + \mathrm{Tr}(\boldsymbol{\Sigma} \mathbf{R}_{g,m}) + \sigma_{v,m}^2} \tag{29}$$

where $q \in \{1, \ldots, Q\}$ and $m \in \{1, \ldots, M\}$.

We consider a transmit design formulation that follows the max-min-fair criterion for standard multigroup multicast [7], and that is an extension of the SINR maximization design in the previous section (the power minimization formulation may also be employed; we skip this alternative due to limit of space). The design problem is formulated as follows:

$$\max_{\substack{\boldsymbol{w}_1, \ldots, \boldsymbol{w}_Q \in \mathbb{H}^{N_t}, \\ \boldsymbol{\Sigma} \in \mathbb{H}^{N_t}}} \left\{ \min_{\substack{k \in \mathcal{G}_q \\ q = 1, \ldots, Q}} \mathsf{SINR}_{b,k}(\boldsymbol{w}_1, \ldots, \boldsymbol{w}_Q, \boldsymbol{\Sigma}) \right\} \tag{30a}$$

$$\text{s.t.} \quad \mathsf{SINR}_{e,m}^{(q)}(\boldsymbol{w}_1, \ldots, \boldsymbol{w}_Q, \boldsymbol{\Sigma}) \leq \gamma_e^{(q)}, \quad m = 1, \ldots, M, \; q = 1, \ldots, Q \tag{30b}$$

$$\sum_{q=1}^{Q} \|\boldsymbol{w}_q\|^2 + \mathrm{Tr}(\boldsymbol{\Sigma}) \leq P_{\max} \tag{30c}$$

$$\boldsymbol{\Sigma} \succeq 0, \tag{30d}$$

where $\gamma_e^{(q)} > 0$ specifies the maximum allowable SINR threshold for Eves to eavesdrop the qth data stream, and $P_{\max}$ is a given transmit power limit. As seen in (30), the design goal is to maximize the weakest SINR among all Bobs, under SINR constraints on Eves and a total transmit power constraint.

Problem (30) is more complicated than the one-Bob SINR maximization formulation in the previous section. However, SDR remains applicable. The SDR of (30) can be shown in (31), at the bottom of the page. The resultant SDR problem, shown above, is a quasi-convex problem. Its optimal solution can be obtained by applying a bisection search in which a sequence of SDPs is solved; see [36] for the details.

In the study of standard multigroup multicast, it has been known that SDR may not yield rank-one solution [7]. Hence, for the secret multigroup multicast design (30), we need a procedure that turns the SDR solution in (31) to an approximate solution to (30). In Table I, we provide such an approximate solution generation procedure custom-designed for (30). See (32a)–(32c) at the bottom of the next page. The principle is based on that of Gaussian randomization; see [32] for a general review of the notion of randomization, and [7] for specific details on randomization for standard multigroup multicast.

VI. Simulation Results

We now demonstrate the performance of the proposed AN-aided secret transmit beamforming designs by simulations. In the simulation examples to be shown soon, we will adopt either one of the following two CSI settings:

i) *Instantaneous CSI Case*: Both the CSIs of Bob and Eves are instantaneous; i.e., $\mathbf{R}_h = \mathbf{h}\mathbf{h}^H$ (or $\mathbf{R}_{h,k} = \mathbf{h}_k \mathbf{h}_k^H$ for all k for the multigroup multicast extension), and $\mathbf{R}_{g,m} = \boldsymbol{g}_m \boldsymbol{g}_m^H$ for all m. The channel realizations $\mathbf{h}, \boldsymbol{g}_1, \ldots, \boldsymbol{g}_M$ are i.i.d. Gaussian distributed. Specifically, in the simulations, the channels were randomly generated by $\mathbf{h}$, $\boldsymbol{g}_m \sim \mathcal{CN}(\mathbf{0}, \mathbf{I}_{N_t}/N_t)$ on a per-trial basis.

$$\max_{\substack{\mathbf{W}_1, \ldots, \mathbf{W}_Q \in \mathbb{H}^{N_t}, \\ \boldsymbol{\Sigma} \in \mathbb{H}^{N_t}}} \left\{ \min_{\substack{k \in \mathcal{G}_q \\ q = 1, \ldots, Q}} \frac{\mathrm{Tr}(\mathbf{W}_q \mathbf{R}_{h,k})}{\sum_{p \neq q} \mathrm{Tr}(\mathbf{W}_p \mathbf{R}_{h,k}) + \mathrm{Tr}(\boldsymbol{\Sigma} \mathbf{R}_{h,k}) + \sigma_{n,k}^2} \right\} \tag{31a}$$

$$\text{s.t.} \quad \frac{1}{\gamma_e^{(q)}} \mathrm{Tr}(\mathbf{W}_q \mathbf{R}_{g,m}) \leq \sum_{p \neq q} \mathrm{Tr}(\mathbf{W}_p \mathbf{R}_{g,m}) + \mathrm{Tr}(\boldsymbol{\Sigma} \mathbf{R}_{g,m}) + \sigma_{v,m}^2, \; \forall (m, q) \tag{31b}$$

$$\sum_{q=1}^{Q} \mathrm{Tr}(\mathbf{W}_q) + \mathrm{Tr}(\boldsymbol{\Sigma}) \leq P_{\max} \tag{31c}$$

$$\boldsymbol{\Sigma} \succeq \mathbf{0}, \; \mathbf{W}_1 \succeq \mathbf{0}, \ldots, \mathbf{W}_Q \succeq \mathbf{0}. \tag{31d}$$

ii) *Correlation-based CSI Case*: In this case, the channels of Bob and Eves are assumed to be random with correlation matrices given, respectively, by

$$\mathbf{R}_h = \alpha\bar{\mathbf{h}}\bar{\mathbf{h}}^H + (1-\alpha)\frac{\mathbf{I}_{N_t}}{N_t}, \quad (33)$$

$$\mathbf{R}_{g,m} = \alpha\bar{\boldsymbol{g}}_m\bar{\boldsymbol{g}}_m^H + (1-\alpha)\frac{\mathbf{I}_{N_t}}{N_t}, \quad m=1,\ldots,M \quad (34)$$

where $\alpha \in [0,1]$ describes the level of channel uncertainty ($\alpha = 1$ means instantaneous CSI, $\alpha = 0$ means no knowledge of the channel directions at all). The channel means $\bar{\mathbf{h}}, \bar{\boldsymbol{g}}_1, \ldots, \bar{\boldsymbol{g}}_M$ are isotropically distributed on a unit sphere. Specifically, for $\bar{\mathbf{h}}$, we generate in each simulation trial a random vector $\tilde{\mathbf{h}} \sim \mathcal{CN}(\mathbf{0}, \mathbf{I}_{N_t})$, and then set $\bar{\mathbf{h}} = \tilde{\mathbf{h}}/||\tilde{\mathbf{h}}||$. The same generation procedure applies to each $\bar{\boldsymbol{g}}_m$.

The following settings are assumed for all the following simulation examples, unless specified: Bob's noise power is $\sigma_n^2 =$ 0 dB. All Eves have identical noise powers, and we denote $\sigma_v^2 \triangleq \sigma_{v,1}^2 = \cdots = \sigma_{v,M}^2$. The number of trials for Monte Carlo simulations is 1000. All the optimization problems involved in the proposed designs were solved by SeDuMi [33].

A. Example 1: Power Minimization Design, Instantaneous CSI Case

This example demonstrates the performance of the proposed AN-aided design under the power minimization formulation in Formulation 1. The instantaneous CSI case is assumed. The chosen design is solved by SDR; cf., Proposition 1, Case C1). We also consider two other designs in our simulations, namely, the no-AN design in (13), and the isotropic AN design in (9) and (10). These two designs are based on the power minimization formulation, with some restrictions on the transmit structures. The other simulation settings are $N_t = 4$, $M = 3$, $\gamma_e = 0$ dB, $\gamma_b = 10$ dB.

The simulation results are shown in Fig. 2. In Fig. 2(a), the average transmit powers of the various designs are plotted over a wide range of values of $1/\sigma_v^2$. Note that large $1/\sigma_v^2$ physically means strong (clean) overhearing ability for Eves, while small $1/\sigma_v^2$ means weak (noisy) overhearing ability. We observe that for $1/\sigma_v^2 < -10$ dB, the powers used in all the designs are quite similar. This is because the designs do not need to spend much resource to deal with weak Eves. However, for $1/\sigma_v^2 > 0$ dB, there are significant performance differences. The proposed AN-aided design generally yields the smallest powers among the three designs, and its performance gaps relative to the other two designs are wider as $1/\sigma_v^2$ increases. For example, at $1/\sigma_v^2 = 20$ dB, the performance gap between the proposed and no-AN designs is 12 dB in power, while that between the proposed and isotropic AN designs is 4 dB. Fig. 2(a) also reveals that for the strong Eves regime (say, $1/\sigma_v^2 > 0$ dB), using AN, even in an isotropic manner, would give better performance than not using AN.

To get more insights, in Fig. 2(b) we separately plot the transmit powers of the transmit weight vector and AN. It can be seen that the power allocated to AN increases with $1/\sigma_v^2$. This further confirms that using AN is the reason behind the good power saving performance of the proposed AN design. The figure also shows that the power allocated to AN in the proposed design is less than that in the isotropic AN design.

We are also interested in seeing how the transmit powers of the various designs change with the number of Eves. The simulation settings are the same as the previous, except that we modify $N_t = 20$ and we fix $1/\sigma_v^2 = 15$ dB. The results are

TABLE I
GAUSSIAN RANDOMIZATION PROCEDURE FOR THE MAX-MIN-FAIR PROBLEM (30)

Given a number of randomizations L, and an optimal solution $(\mathbf{W}_1^\star, \ldots, \mathbf{W}_Q^\star, \mathbf{\Sigma}^\star)$ of the SDR problem (31).

Step 1. For each $q = 1, \ldots, Q$, generate a set of L random vectors $\boldsymbol{w}_q^{(\ell)}$, $\ell = 1, \ldots, L$, from the complex Gaussian distribution $\mathcal{CN}(\mathbf{0}, \mathbf{W}_q^\star)$.

Step 2. For $\ell = 1, \ldots, L$, let $\bar{\boldsymbol{w}}_q^{(\ell)} = \boldsymbol{w}_q^{(\ell)}/\|\boldsymbol{w}_q^{(\ell)}\|$ for all $q = 1, \ldots, Q$, $\bar{\mathbf{\Sigma}} = \mathbf{\Sigma}/\mathrm{Tr}(\mathbf{\Sigma})$, and solve the power control problem (32) using an available generalized linear -fractional programming method (e.g., by bisection search). For each ℓ, let $\gamma_b^{(\ell)}$ be the associated optimal objective value.

Step 3. Let

$$\ell^\star = \arg \max_{\ell=1,\ldots,L} \gamma_b^{(\ell)},$$

and output $\hat{\boldsymbol{w}}_q^\star = \sqrt{\alpha_q^{\ell^\star}}\bar{\boldsymbol{w}}_q^{(\ell^\star)}$, $q = 1, \ldots, Q$, $\hat{\mathbf{\Sigma}}^\star = \beta^{(\ell^\star)}\bar{\mathbf{\Sigma}}$, as an approximate solution to problem (30).

$$\left\{\alpha_1^{(\ell)}, \ldots, \alpha_Q^{(\ell)}, \beta^{(\ell)}\right\} = \arg \max_{\substack{\alpha_q \geq 0,\, q=1,\ldots,Q,\\ \beta\geq 0}} \left\{ \min_{\substack{k\in\mathcal{G}_q\\ q=1,\ldots,Q}} \frac{\alpha_q \left(\bar{\boldsymbol{w}}_q^{(\ell)}\right)^H \mathbf{R}_{h,k}\bar{\boldsymbol{w}}_q^{(\ell)}}{\sum_{p\neq q} \alpha_p \left(\bar{\boldsymbol{w}}_p^{(\ell)}\right)^H \mathbf{R}_{h,k}\bar{\boldsymbol{w}}_p^{(\ell)} + \beta \mathrm{Tr}\left(\bar{\mathbf{\Sigma}}\mathbf{R}_{h,k}\right) + \sigma_{n,k}^2} \right\} \quad (32a)$$

$$\text{s.t.} \quad \frac{1}{\gamma_e^{(q)}}\alpha_q \left(\bar{\boldsymbol{w}}_q^{(\ell)}\right)^H \mathbf{R}_{g,m}\bar{\boldsymbol{w}}_q^{(\ell)} \leq \sum_{p\neq q} \alpha_p \left(\bar{\boldsymbol{w}}_p^{(\ell)}\right)^H \mathbf{R}_{g,m}\bar{\boldsymbol{w}}_p^{(\ell)} + \beta\mathrm{Tr}(\bar{\mathbf{\Sigma}}\mathbf{R}_{g,m}) + \sigma_{v,m}^2, \ \forall(m,q) \quad (32b)$$

$$\sum_{q=1}^{Q} \alpha_q + \beta \leq P_{\max} \quad (32c)$$

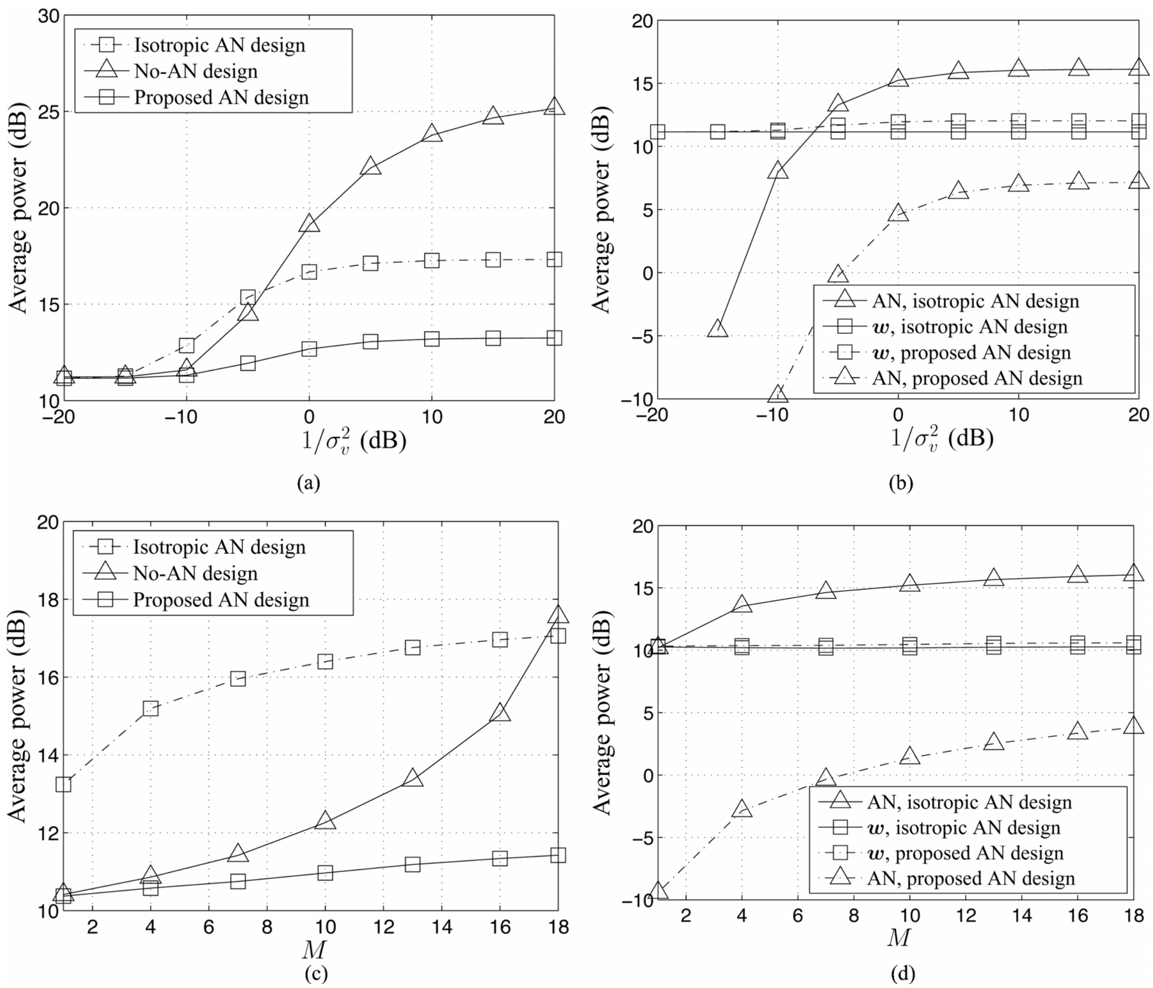


Fig. 2. Performance of the various secret transmit designs under the power minimization formulation; (a) transmit powers versus the reciprocals of Eves' noise powers, $N_t = 4, M = 3$; (b) power allocations of the isotropic and proposed AN designs, corresponding to the result in (a); (c) transmit powers versus the number of Eves, $N_t = 20, 1/\sigma_v^2 = 15$ dB; (d) power allocations of the isotropic and proposed AN designs, corresponding to the result in (c).

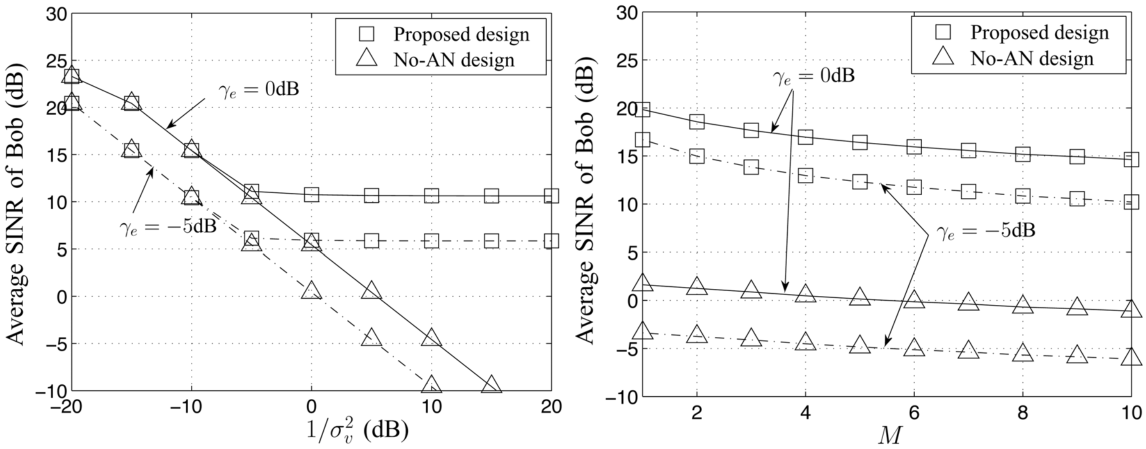
shown in Fig. 2(c). Again, the proposed design is seen to exhibit the best performance. Moreover, the no-AN design provides better performance than the isotropic AN design, except at $M = 18$. We should recall that the no-AN design focuses on manipulating the transmit DoF to deal with Eves, while the isotropic AN design does not. In Fig. 2(d) where the transmit weight and AN power allocations corresponding to Fig. 2(c) are shown, we see that the proposed design tends to use less AN for small M. Hence, our interpretation with the results is that for small numbers of Eves, using transmit DoF to degrade Eves would be more effective than using AN.

B. Example 2: SINR Maximization Design, Correlation-Based CSI Case

We consider the SINR maximization formulation, operating under the correlation-based CSI case. The simulation results, together with the simulation settings, are given in Fig. 3. The figures only show the performance of the proposed AN-aided design and the no-AN design, since the isotropic AN design is not applicable when Bob's CSI is correlation-based. Once again, we see that the proposed design can yield SINR performance significantly better than that of the no-AN design.

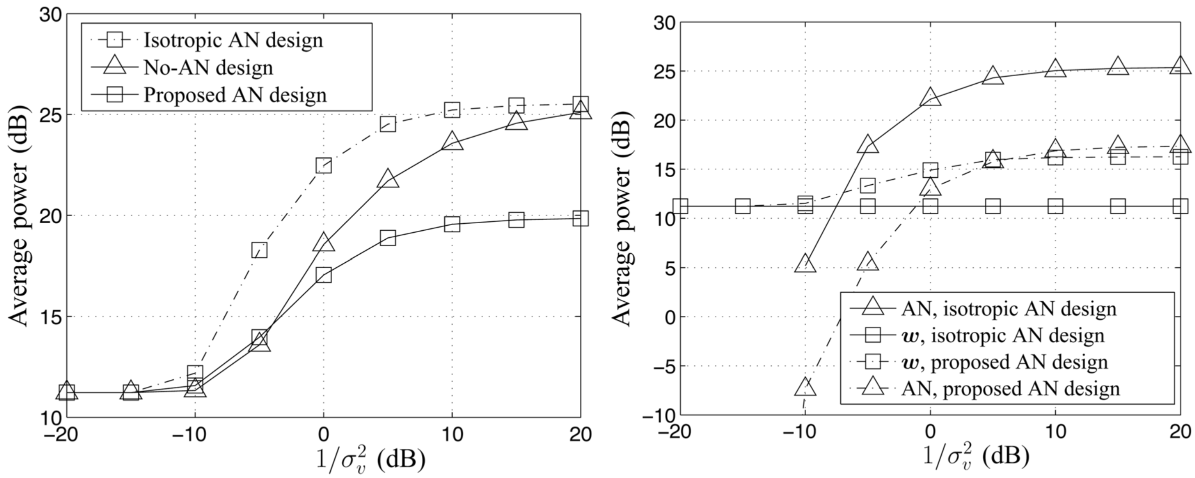
From Fig. 3(a) we notice the following phenomenon: When $1/\sigma_v^2 > 5$ dB, Bob's SINR achieved by the no-AN design is even lower than the Eves' maximum SINRs specification γ_e, which is not reasonable from a system design viewpoint. In fact, from an information theoretic perspective, this means that the no-AN design may fail to provide information secrecy for such operating conditions [25]. We also see from Fig. 3(a) that the proposed AN-aided design does not have such an issue.

We should point out that as our numerical experience with this simulation example, SDR was always found to yield a rank-one solution; i.e., an exactly optimal solution to the SINR maximization design formulation. For the result in Fig. 3(b) with $M < 10$, this is somewhat expected since those settings fit into the SDR rank-one optimality result in Proposition 3, specifically, Case 2). However, the result in Fig. 3(a) does not fall into that case, where we have $N_t = M$ [instead of $N_t > M$ required in Case 2) of Proposition 3]. In fact, Proposition 3 shows only sufficient conditions for which SDR is provably optimal to the SINR maximization design, and they are not the necessary conditions. This



(a) (b)

Fig. 3. Performance of the various secret transmit designs under the SINR maximization formulation with $P_{\max} = 25$ dB (a) Correlation-based CSI with $\alpha = 0.6$, $N_t = 4$, $M = 4$; (b) correlation-based CSI with $\alpha = 0.6$, $N_t = 10$, $1/\sigma_v^2 = 10$ dB.



(a) (b)

Fig. 4. Performance of the various designs in the colluding Eves scenario under the power minimization formulation, $N_t = 4$, $M = 3$, $\gamma_b = 10$ dB, and $M\gamma_e = 5$ dB, and $1/\sigma_n^2 = 0$ dB.

empirical observation suggests that SDR may be more powerful in practice than what the presently available analysis outlines.

C. Example 3: Colluding Eves, Power Minimization Design, Instantaneous CSI Case

This example considers the colluding-Eve scenario. The simulation settings are the same as those in Example 1. We should reiterate that the proposed design incorporates the indirect method in Proposition 4 for bounding the colluding-Eve SINR. As for the no-AN and isotropic AN designs, their simple transmit structures enable them to deal with the colluding-Eve SINR [cf., (22)] directly. In the simulation, the maximum allowable colluding-Eve SINR threshold is set to $M\gamma_e = 5$ dB. The simulation results are shown in Fig. 4. We see that the proposed design exhibits marginal performance loss compared to the no-AN design for -10 dB $< 1/\sigma_v^2 < -5$ dB, but the proposed design outperform the other two designs for $1/\sigma_v^2 > 0$ dB.

D. Example 4: Multigroup Multicast, Max-Min-Fair Design, Instantaneous CSI Case

This last example demonstrates the viability of the proposed design in the multigroup multicast scenario. We consider a two-group multicast transmission, where there are four Bobs and two Bobs form one group (thereby $K = 4$, $Q = 2$, $\mathcal{G}_1 = \{1,2\}$, $\mathcal{G}_2 = \{3,4\}$). There are four Eves ($M = 4$). The number of transmit antennas at Alice is $N_t = 6$. The instantaneous CSI case is assumed. The max-min-fair design formulation and the subsequent SDR approximation described in Section V-B is used to provide the AN-aided and no-AN designs. The transmit power limit is $P_{\max} = 25$ dB. The number of randomizations in the SDR approximation is $L = 30$. The respective simulation results are shown in Fig. 5(a), where we plot the worst-Bob SINR with respect to $1/\sigma_v^2$. It is observed that for the specification $\gamma_e = 0$ dB, the SINR gaps between the no-AN and AN-aided designs are small and do not exceed 1.1 dB. Our speculation for such a marginal performance difference is that the no-AN design can wisely exploit interferences between transmit beams

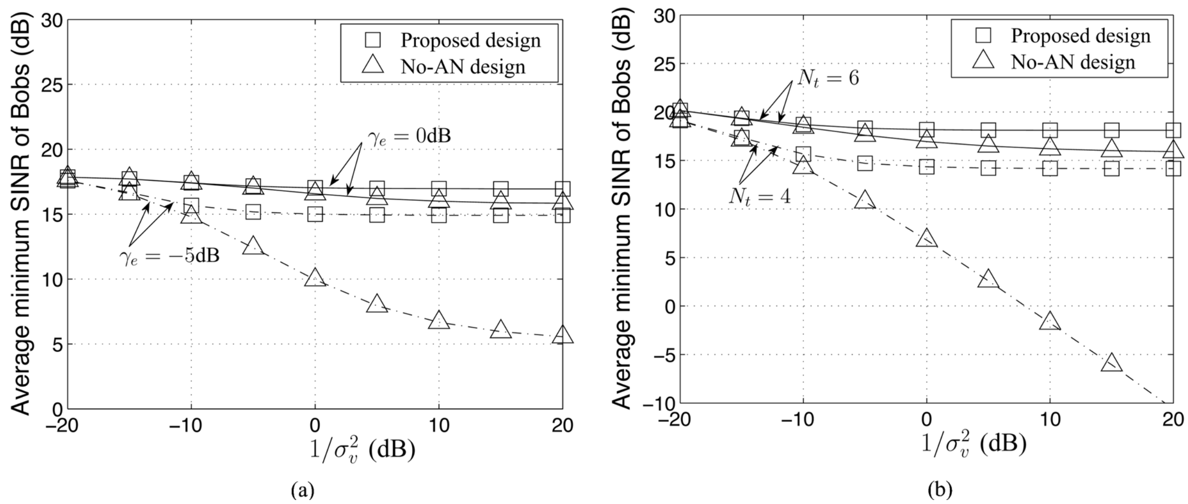


Fig. 5. Performance in the multigroup multicast scenario with instantaneous CSI, $K = 4$, $M = 4$, $P_{\max} = 25$ dB: (a) 2-group multicast ($Q = 2$, $|\mathcal{G}_q| = K/Q = 2$), $N_t = 6$ (b) 1-group multicast ($Q = 1$), $\gamma_e = -5$ dB.

to block Eves' interceptions, making the need of AN not as significant as in the previous examples. But, when we apply a more stringent specification on Eves by setting $\gamma_e = -5$ dB, we can see in Fig. 5(a) that the AN-aided design significantly outperforms the no-AN design for large $1/\sigma_v^2$.

We also consider a one-group multicast transmission with four Bobs (i.e., $K = 4$, $Q = 1$, $\mathcal{G}_1 = \{1,2,3,4\}$). We fix $\gamma_e = -5$ dB and the other simulation settings are the same as above. The results are shown in Fig. 5(b). We notice that for $N_t = 6$, the SINR gaps of the two designs are no greater than 2.2 dB. We believe that $N_t = 6$ may have provided sufficient spatial DoF for the no-AN design to suppress Eves' interceptions effectively. However, when we reduce the number of transmit antennas to $N_t = 4$, we see from Fig. 5(b) that, for large $1/\sigma_v^2$, the SINR performance of the no-AN design is much deteriorated; for example, for $1/\sigma_v^2 \geq 15$ dB, Bob's SINR achieved by the no-AN design is even lower than the Eves' maximum SINRs specification γ_e. In comparison, the AN-aided design provides promising SINR performance even for large $1/\sigma_v^2$.

VII. Conclusion

In this paper, we have established a secret transmit beamforming approach using a QoS-oriented perspective. A particularly meaningful part of this work is judicious utilization of artificial noise, via joint optimization of its spatial distribution and the transmit weights. This has enabled us to cripple eavesdroppers' interceptions significantly, as compared to a no-AN approach or an isotropic AN approach. The formulated designs turn out to be difficult optimization problems, and we employ the SDR technique to approximate the designs. Interestingly, we show that SDR is actually an exact solver of the formulated designs for a practically representative class of problem instances. The extensions to the multigroup multicast scenario and the colluding-Eve scenario are also considered. Simulation results show that the proposed AN-aided transmit beamforming designs are highly effective in blocking eavesdroppers' interceptions, especially when there are many eavesdroppers and/or when the eavesdroppers' channels have good overhearing ability.

Appendix

A. Proof of Lemma 2

The NP-hardness of (12) is claimed by showing that (12) includes the following complex quadratic program as a special case:

$$\begin{aligned} \min_{\boldsymbol{z}\in\mathbb{C}^{N_t}} \quad & \boldsymbol{z}^H \mathbf{A} \boldsymbol{z} \\ \text{s.t.} \quad & |z_i|^2 = 1, \quad i = 1,\ldots,N_t \end{aligned} \tag{A1}$$

where $\mathbf{A} \succeq \mathbf{0}$. Problem (A1) has been shown to be NP-hard [38]. Let us consider a transformation of variables

$$\boldsymbol{z} = \mathbf{R}_h^{1/2}\boldsymbol{w}, \quad \boldsymbol{\Phi} = \mathbf{R}_h^{1/2}\boldsymbol{\Sigma}\mathbf{R}_h^{1/2}.$$

By letting $\mathbf{A} = \mathbf{R}_h^{-1}$, and $\mathbf{B}_m = \mathbf{R}_h^{-1/2}\mathbf{R}_{g,m}\mathbf{R}_h^{-1/2}$ for all m (which we have assumed that $\mathbf{R}_h$ is invertible), we can rewrite (12) as

$$\begin{aligned} \min_{\boldsymbol{z}\in\mathbb{C}^{N_t},\boldsymbol{\Phi}\succeq\mathbf{0}} \quad & \boldsymbol{z}^H\mathbf{A}\boldsymbol{z} + \mathrm{Tr}(\mathbf{A}\boldsymbol{\Phi}) \\ \text{s.t.} \quad & \|\boldsymbol{z}\|^2 \geq \gamma_b(\mathrm{Tr}(\boldsymbol{\Phi}) + \sigma_n^2) \\ & \boldsymbol{z}^H\mathbf{B}_m\boldsymbol{z} \leq \gamma_e(\mathrm{Tr}(\boldsymbol{\Phi}\mathbf{B}_m) + \sigma_{v,m}^2) \\ & m = 1,\ldots,M. \end{aligned} \tag{A2}$$

Suppose that we have $\sigma_n^2 = \sigma_{v,1}^2 = \cdots = \sigma_{v,M}^2 = 1$, $\gamma_b = N_t$, $M = N_t$, $\gamma_e = 1$, and $\mathbf{B}_m = \mathbf{e}_m\mathbf{e}_m^T$ for $m = 1,\ldots,M$. The resultant problem in (A2) is

$$\min_{\boldsymbol{z},\boldsymbol{\Phi}\succeq\mathbf{0}} \quad \boldsymbol{z}^H\mathbf{A}\boldsymbol{z} + \mathrm{Tr}(\mathbf{A}\boldsymbol{\Phi}) \tag{A3a}$$

$$\text{s.t.} \quad \|\boldsymbol{z}\|^2 \geq N_t\mathrm{Tr}(\boldsymbol{\Phi}) + N_t \tag{A3b}$$

$$|z_i|^2 \leq \Phi_{ii} + 1, \quad i = 1,\ldots,N_t. \tag{A3c}$$

We see that for $N_t \geq 2$, (A3b) and (A3c) are satisfied simultaneously only when $\mathbf{\Phi} = \mathbf{0}$. With $\mathbf{\Phi} = \mathbf{0}$, the constraints in (A3b) and (A3c) are the same as $|z_i|^2 = 1 \; \forall i$. Hence, (A3) is equivalent to the NP-hard problem in (A1). This completes the proof of the NP-hardness of (12).

Moreover, (13) can be shown to be NP-hard by following the same proof as above. ■

B. *Proof of Proposition 1*

The proof of Proposition 1 for the three cases is as follows.

Case C1: The idea of the proof is that the KKT conditions of the SDR problem (15) automatically restrict its optimal solution $(\mathbf{W}^\star, \mathbf{\Sigma}^\star)$ to have rank-one $\mathbf{W}^\star$. Let $\lambda^\star \geq 0$ be an optimal dual variable for the constraint (15b), $\mu_m^\star \geq 0$, $m = 1, \ldots, M$, be those for the constraints (15c), and $\mathbf{Y}^\star \succeq \mathbf{0}$ be that for the constraint $\mathbf{W} \succeq \mathbf{0}$. We consider only the KKT equations relevant to $\mathbf{W}^\star$, given as follows:

$$\mathbf{Y}^\star = \mathbf{I}_{N_t} + \sum_{m=1}^{M} \mu_m^\star \mathbf{R}_{g,m} - \lambda^\star \mathbf{R}_h \succeq \mathbf{0} \quad \text{(A4a)}$$

$$\mathbf{Y}^\star \mathbf{W}^\star = \mathbf{0} \quad \text{(A4b)}$$

$$\lambda^\star \geq 0, \; \mu_m^\star \geq 0, \quad m = 1, \ldots, M. \quad \text{(A4c)}$$

Equation (A4b) implies that the columns of $\mathbf{W}^\star$ must lie in the nullspace of $\mathbf{Y}^\star$. Therefore, we get

$$\text{rank}(\mathbf{W}^\star) \leq \text{Nullity}(\mathbf{Y}^\star) = N_t - \text{rank}(\mathbf{Y}^\star). \quad \text{(A5)}$$

We will show that the occurrence of C1) implies that $\text{rank}(\mathbf{Y}^\star) \geq N_t - 1$, and, subsequently, $\text{rank}(\mathbf{W}^\star) \leq 1$. Since $\mathbf{W}^\star = \mathbf{0}$ is not a feasible point due to (15b), the remaining possibility is that $\text{rank}(\mathbf{W}^\star) = 1$.

Under Case C1), the KKT equation (A4a) can be expressed as

$$\mathbf{Y}^\star = \mathbf{B} - \lambda^\star \mathbf{h}\mathbf{h}^H \quad \text{(A6)}$$

$$\mathbf{B} = \mathbf{I}_{N_t} + \sum_{m=1}^{M} \mu_m^\star \mathbf{R}_{g,m}. \quad \text{(A7)}$$

Since $\mathbf{R}_{g,m} \succeq \mathbf{0}$ and $\mu_m^\star \geq 0$ for all $m = 1, \ldots, M$, the matrix $\mathbf{B}$ in (A7) is positive definite. Thus, its square root factor $\mathbf{B}^{1/2}$ is invertible. Using this result, we can rewrite (A6) as

$$\mathbf{Y}^\star = \mathbf{B}^{1/2}(\mathbf{I}_{N_t} - \lambda^\star (\mathbf{B}^{-1/2}\mathbf{h})(\mathbf{B}^{-1/2}\mathbf{h})^H)\mathbf{B}^{1/2}. \quad \text{(A8)}$$

From (A8) and by basic matrix analysis concepts, one can show that

$$\text{rank}(\mathbf{Y}^\star) = \text{rank}(\mathbf{I}_{N_t} - \lambda^\star (\mathbf{B}^{-1/2}\mathbf{h})(\mathbf{B}^{-1/2}\mathbf{h})^H) \quad \text{(A9)}$$

and that $\text{rank}(\mathbf{I}_{N_t} - \lambda^\star (\mathbf{B}^{-1/2}\mathbf{h})(\mathbf{B}^{-1/2}\mathbf{h})^H) \geq N_t - 1$ due to the underlying matrix structure. As a result, we have $\text{rank}(\mathbf{Y}^\star) \geq N_t - 1$ under Case C1).

Case C2: The proof is similar to that of Case C1), where the key is to prove that $\text{rank}(\mathbf{Y}^\star) \geq N_t - 1$. Under Case C2), the dual variable $\mathbf{Y}^\star$ in (A4a) is expressed as

$$\mathbf{Y}^\star = \mathbf{B} - \lambda^\star \bar{\mathbf{h}}\bar{\mathbf{h}}^H \succeq \mathbf{0} \quad \text{(A10)}$$

$$\mathbf{B} = \tau \mathbf{I}_{N_t} + \sum_{m=1}^{M} \mu_m^\star \bar{\boldsymbol{g}}_m \bar{\boldsymbol{g}}_m^H \quad \text{(A11)}$$

$$\tau = 1 + \sum_{m=1}^{M} \mu_m^\star \sigma_{g,m}^2 - \lambda^\star \sigma_h^2. \quad \text{(A12)}$$

Let us assume $\tau > 0$, in which case $\mathbf{B}$ in (A11) is positive definite. Following the same derivations as in C1), one can show that $\text{rank}(\mathbf{Y}^\star) \geq N_t - 1$. On the other hand, assume that $\tau \leq 0$. Let us construct a vector

$$\boldsymbol{x} = \mathbf{P}_{\bar{\boldsymbol{G}}}^{\perp} \bar{\mathbf{h}}$$

where $\mathbf{P}_{\bar{\boldsymbol{G}}}^{\perp} = \mathbf{I}_{N_t} - \bar{\boldsymbol{G}}(\bar{\boldsymbol{G}}^H \bar{\boldsymbol{G}})^\dagger \bar{\boldsymbol{G}}^H$, $\bar{\boldsymbol{G}} = [\bar{\boldsymbol{g}}_1, \ldots, \bar{\boldsymbol{g}}_M]$, is the orthogonal complement projector of $\{\bar{\boldsymbol{g}}_1, \ldots, \bar{\boldsymbol{g}}_M\}$ (here the superscript † denotes the pseudo inverse). Since $\bar{\mathbf{h}} \notin \text{Range}\{\bar{\boldsymbol{g}}_1, \ldots, \bar{\boldsymbol{g}}_M\}$, we have $\boldsymbol{x} \neq \mathbf{0}$. Moreover, $\boldsymbol{x}$ satisfies $\boldsymbol{x}^H \bar{\boldsymbol{g}}_m = 0$ for all m, and $\boldsymbol{x}^H \bar{\mathbf{h}} = \bar{\mathbf{h}}^H \mathbf{P}_{\bar{\boldsymbol{G}}}^{\perp} \bar{\mathbf{h}} > 0$. Now, let us inspect the quadratic form

$$\boldsymbol{x}^H \mathbf{Y}^\star \boldsymbol{x} = \tau \|\boldsymbol{x}\|^2 - \lambda^\star |\boldsymbol{x}^H \bar{\mathbf{h}}|^2. \quad \text{(A13)}$$

Since $\tau \leq 0$ implies $\lambda^\star > 0$ by (A12), we have $\boldsymbol{x}^H \mathbf{Y}^\star \boldsymbol{x} < 0$. This further implies that $\mathbf{Y}^\star$ is not PSD, which in turn violates the KKT condition in (A4a). Hence, we conclude that $\tau > 0$ must hold. Subsequently we have $\text{rank}(\mathbf{Y}^\star) \geq N_t - 1$ under Case C2).

Case C3: The proof is based on a rank reduction result for general SDPs, namely, Lemma 3.1 in [13]. By that lemma, there exists an optimal solution $(\mathbf{W}^\star, \mathbf{\Sigma}^\star)$ to the SDR problem (15) that satisfies

$$\text{rank}^2(\mathbf{W}^\star) + \text{rank}^2(\mathbf{\Sigma}^\star) \leq 1 + M. \quad \text{(A14)}$$

The SDR problem may have $\mathbf{\Sigma}^\star = \mathbf{0}$ and hence we generally get $\text{rank}(\mathbf{\Sigma}^\star) \geq 0$. Moreover, we have $\text{rank}(\mathbf{W}^\star) \geq 1$, since $\mathbf{W}^\star = \mathbf{0}$ is not feasible. Putting these results together, we conclude that $\text{rank}(\mathbf{W}^\star) = 1$ for $M \leq 2$. ■

C. *Proof of Lemma 3*

We show that the SINR maximization design in (16) includes the following complex quadratic program as a special case:

$$\begin{aligned} \max_{\boldsymbol{w} \in \mathbb{C}^{N_t}} \quad & \boldsymbol{w}^H \mathbf{A} \boldsymbol{w} \\ \text{s.t.} \quad & |w_i|^2 \leq 1, \quad i = 1, \ldots, N_t \end{aligned} \quad \text{(A15)}$$

where $\mathbf{A} \succeq \mathbf{0}$. Problem (A15) is known to be NP-hard [38]. Suppose that $\sigma_n^2 = 1$, $M = N_t$, $P_{\max} = N_t$, $\sigma_{v,m}^2 = 1/\gamma_e$, and $\mathbf{R}_{g,m} = \mathbf{e}_m \mathbf{e}_m^T$, for $m = 1, \ldots, M$. Problem (16) becomes

$$\begin{aligned} \max_{\boldsymbol{w} \in \mathbb{C}^{N_t}, \mathbf{\Sigma} \succeq \mathbf{0}} \quad & \frac{\boldsymbol{w}^H \mathbf{R}_h \boldsymbol{w}}{\text{Tr}(\mathbf{\Sigma}\mathbf{R}_h) + 1} \\ \text{s.t.} \quad & |w_i|^2 \leq \gamma_e \Sigma_{ii} + 1, \quad i = 1, \ldots, N_t \\ & \|\boldsymbol{w}\|^2 + \text{Tr}(\mathbf{\Sigma}) \leq N_t. \end{aligned} \quad \text{(A16)}$$

Let us take $\gamma_e \longrightarrow 0$ for all i, in which case (A16) is reduced to

$$\begin{aligned} \max_{\boldsymbol{w} \in \mathbb{C}^{N_t}, \mathbf{\Sigma} \succeq \mathbf{0}} \quad & \frac{\boldsymbol{w}^H \mathbf{R}_h \boldsymbol{w}}{\text{Tr}(\mathbf{\Sigma}\mathbf{R}_h) + 1} \\ \text{s.t.} \quad & |w_i|^2 \leq 1, \quad i = 1, \ldots, N_t \\ & \|\boldsymbol{w}\|^2 + \text{Tr}(\mathbf{\Sigma}) \leq N_t. \end{aligned} \quad \text{(A17)}$$

Furthermore, consider that $\mathbf{R}_h \succ \mathbf{0}$. Then, an optimal solution to (A17), denoted by $(\boldsymbol{w}^\star, \boldsymbol{\Sigma}^\star)$, must have $\boldsymbol{\Sigma}^\star = \mathbf{0}$. This can be shown by contradiction: Suppose that $\boldsymbol{\Sigma}^\star \neq \mathbf{0}$. Then we have

$$\frac{(\boldsymbol{w}^\star)^H \mathbf{R}_h \boldsymbol{w}^\star}{\mathrm{Tr}(\boldsymbol{\Sigma}^\star \mathbf{R}_h) + 1} < (\boldsymbol{w}^\star)^H \mathbf{R}_h \boldsymbol{w}^\star. \tag{A18}$$

Equation (A18) suggests that $(\boldsymbol{w}^\star, \mathbf{0})$ yields an objective value greater than $(\boldsymbol{w}^\star, \boldsymbol{\Sigma}^\star)$. Since $(\boldsymbol{w}^\star, \mathbf{0})$ is also feasible to (A16), it is a contradiction that $(\boldsymbol{w}^\star, \boldsymbol{\Sigma}^\star)$, $\boldsymbol{\Sigma}^\star \neq \mathbf{0}$, is optimal. Hence, (A17) is equivalent to

$$\begin{aligned} \max_{\boldsymbol{w} \in \mathbb{C}^{N_t}} \quad & \boldsymbol{w}^H \mathbf{R}_h \boldsymbol{w} \\ \text{s.t.} \quad & |w_i|^2 \leq 1, \quad i = 1, \ldots, N_t \end{aligned} \tag{A19}$$

where we fix $\boldsymbol{\Sigma} = \mathbf{0}$. Problem (A19) is identical to the NP-hard problem in (A15). ■

D. Proof of Proposition 3

The proof is similar to that of Proposition 1 in Appendix B.

Case C1: Let $\nu^\star$, $\mu_m^\star \geq 0$, $m = 1, \ldots, M$, and $\zeta^\star \geq 0$ be the optimum dual variables associated with the constraints in (20b)–(20d), respectively. Moreover, let $\mathbf{Y}^\star \succeq \mathbf{0}$ and $\mathbf{Z}^\star \succeq \mathbf{0}$ be the optimum dual variables associated with the PSD constraints $\bar{\mathbf{W}}^\star$ and $\bar{\boldsymbol{\Sigma}}^\star$, respectively. The KKT equations relevant to the proof are as follows:

$$\mathbf{Y}^\star = \zeta^\star \mathbf{I}_{N_t} + \sum_{m=1}^{M} \mu_m^\star \mathbf{R}_{g,m} - \mathbf{R}_h \succeq \mathbf{0} \tag{A20}$$

$$\mathbf{Z}^\star = \nu^\star \mathbf{R}_h - \sum_{m=1}^{M} \mu_m^\star \gamma_e \mathbf{R}_{g,m} + \zeta^\star \mathbf{I}_{N_t} \succeq \mathbf{0} \tag{A21}$$

$$\mathbf{Y}^\star \bar{\mathbf{W}}^\star = \mathbf{0}. \tag{A22}$$

$$\zeta^\star \geq 0, \; \mu_m^\star \geq 0, \quad m = 1, \ldots, M. \tag{A23}$$

Suppose that Case C1) holds. We consider two cases, namely $\zeta^\star > 0$ and $\zeta^\star = 0$. For $\zeta^\star > 0$, we can use the same proof as in Appendix B to show that $\mathbf{W}^\star$ must be of rank one under the KKT conditions (A20) and (A22). For $\zeta^\star = 0$, we show that the KKT condition (A21) can never be satisfied. Under C1) and $\zeta^\star = 0$, (A21) is expressed as

$$\mathbf{Z}^\star = \nu^\star \mathbf{h}\mathbf{h}^H - \bar{\mathbf{R}} \succeq \mathbf{0} \tag{A24}$$

where $\bar{\mathbf{R}} = \sum_{m=1}^{M} \mu_m^\star \gamma_e \mathbf{R}_{g,m} \succeq \mathbf{0}$. Note that $\bar{\mathbf{R}} \neq \mathbf{0}$: Having $\bar{\mathbf{R}} = \mathbf{0}$ is equivalent to $\mu_1^\star = \cdots = \mu_M^\star = 0$, but the latter violates (A20) under the assumption $\zeta^\star = 0$. Let $\mathcal{R}_\perp(\mathbf{h})$ define the orthogonal complement subspace of $\mathbf{h}$. Since $\mathbf{Z}^\star$ is PSD, we have, for any $\boldsymbol{q} \in \mathcal{R}_\perp(\mathbf{h})$

$$\boldsymbol{q}^H \mathbf{Z}^\star \boldsymbol{q} = -\boldsymbol{q}^H \bar{\mathbf{R}} \boldsymbol{q} \geq 0. \tag{A25}$$

On the other hand, the positive semidefiniteness of $\bar{\mathbf{R}}$ implies $\boldsymbol{q}^H \bar{\mathbf{R}} \boldsymbol{q} \geq 0$ for all $\boldsymbol{q} \in \mathcal{R}_\perp(\mathbf{h})$. It follows that $\boldsymbol{q}^H \bar{\mathbf{R}} \boldsymbol{q} = 0$ for any $\boldsymbol{q} \in \mathcal{R}_\perp(\mathbf{h})$, or equivalently, $\bar{\mathbf{R}} = \alpha \mathbf{h}\mathbf{h}^H$ for some α. Such a condition can never be achieved under C1).

Case C2: The proof for Case C2) is essentially the same as that of Proposition 1 in Appendix B, and hence is omitted for brevity.

Case C3: By the SDP rank reduction result in Lemma 3.1 in [13], the equivalent SDR problem (20) has a solution $(\mathbf{W}^\star, \boldsymbol{\Sigma}^\star, \eta^\star)$ whose rank profile satisfies

$$\mathrm{rank}^2(\mathbf{W}^\star) + \mathrm{rank}^2(\boldsymbol{\Sigma}^\star) + \mathrm{rank}^2(\eta^\star) \leq 2 + M \tag{A26}$$

We have shown in Section IV that $\eta^\star > 0$. This means $\mathrm{rank}(\eta^\star) = 1$. Substituting this result into (A26) yields $\mathrm{rank}^2(\mathbf{W}^\star) + \mathrm{rank}^2(\boldsymbol{\Sigma}^\star) \leq 1 + M$. The remaining proof is identical to that in Appendix B. ■

E. Proof of Proposition 4

Any feasible point $(\boldsymbol{w}, \boldsymbol{\Sigma})$ of the design (12) or (16) satisfies $\mathsf{SINR}_{e,m}(\boldsymbol{w}, \boldsymbol{\Sigma}) \leq \gamma_e$ for all m. Those constraints can be expressed as

$$\begin{aligned} \mathrm{Tr}\left((\boldsymbol{w}\boldsymbol{w}^H) \left(\frac{1}{\sigma_{v,m}^2} \mathbf{R}_{g,m} \right) \right) \\ \leq \gamma_e \left(\mathrm{Tr}\left(\boldsymbol{\Sigma} \left(\frac{1}{\sigma_{v,m}^2} \mathbf{R}_{g,m} \right) \right) + 1 \right) \end{aligned} \tag{A27}$$

where $m = 1, \ldots, M$. By considering the sum of (A27) over all m and by using the notation in (23), we obtain

$$\mathrm{Tr}\left(\mathbf{D}^{-1} \boldsymbol{\mathcal{A}}(\boldsymbol{w}\boldsymbol{w}^H) \mathbf{D}^{-1} \right) \leq \gamma_e \left(\mathrm{Tr}\left(\mathbf{D}^{-1} \boldsymbol{\mathcal{A}}(\boldsymbol{\Sigma}) \mathbf{D}^{-1} \right) + M \right). \tag{A28}$$

On the other hand, we consider deriving a bound on the colluding-Eve SINR in (21). Let $\hat{\mathbf{r}}$ be an optimal receive beamformer weight of (21). Then, we have

$$\begin{aligned} &\mathsf{SINR}_{ce}(\boldsymbol{w}, \boldsymbol{\Sigma}) \\ &\quad = \frac{\hat{\mathbf{r}}^H \boldsymbol{\mathcal{A}}(\boldsymbol{w}\boldsymbol{w}^H) \hat{\mathbf{r}}}{\hat{\mathbf{r}}^H (\boldsymbol{\mathcal{A}}(\boldsymbol{\Sigma}) + \mathbf{D}^2) \hat{\mathbf{r}}} && \text{(A29a)} \\ &\quad = \frac{(\mathbf{D}\hat{\mathbf{r}})^H \left(\mathbf{D}^{-1} \boldsymbol{\mathcal{A}}(\boldsymbol{w}\boldsymbol{w}^H) \mathbf{D}^{-1} \right) (\mathbf{D}\hat{\mathbf{r}})}{(\mathbf{D}\hat{\mathbf{r}})^H \left(\mathbf{D}^{-1} \boldsymbol{\mathcal{A}}(\boldsymbol{\Sigma}) \mathbf{D}^{-1} + \mathbf{I}_M \right) (\mathbf{D}\hat{\mathbf{r}})} && \text{(A29b)} \\ &\quad \leq \frac{(\mathbf{D}\hat{\mathbf{r}})^H \left(\mathbf{D}^{-1} \boldsymbol{\mathcal{A}}(\boldsymbol{w}\boldsymbol{w}^H) \mathbf{D}^{-1} \right) (\mathbf{D}\hat{\mathbf{r}})}{(\lambda_{\min}(\mathbf{D}^{-1} \boldsymbol{\mathcal{A}}(\boldsymbol{\Sigma}) \mathbf{D}^{-1}) + 1) \|\mathbf{D}\hat{\mathbf{r}}\|^2} && \text{(A29c)} \\ &\quad \leq \frac{\mathrm{Tr}\left(\mathbf{D}^{-1} \boldsymbol{\mathcal{A}}(\boldsymbol{w}\boldsymbol{w}^H) \mathbf{D}^{-1} \right)}{\lambda_{\min}(\mathbf{D}^{-1} \boldsymbol{\mathcal{A}}(\boldsymbol{\Sigma}) \mathbf{D}^{-1}) + 1} && \text{(A29d)} \end{aligned}$$

where $\lambda_{\min}(\cdot)$ denotes the minimum eigenvalue of its argument. The inequalities in (A29c) and (A29d) are due to the basic matrix results $\boldsymbol{x}^H \boldsymbol{\mathcal{A}} \boldsymbol{x} \geq \lambda_{\min}(\boldsymbol{\mathcal{A}}) \|\boldsymbol{x}\|^2$, and $\boldsymbol{x}^H \boldsymbol{\mathcal{A}} \boldsymbol{x} \leq \mathrm{Tr}(\boldsymbol{\mathcal{A}}) \|\boldsymbol{x}\|^2$ for $\boldsymbol{\mathcal{A}} \succeq \mathbf{0}$, respectively. Moreover, the newly added constraint (24) is equivalent to (see, e.g., [36])

$$\lambda_{\min}(\mathbf{D}^{-1} \boldsymbol{\mathcal{A}}(\boldsymbol{\Sigma}) \mathbf{D}^{-1}) \geq \frac{1}{M} \mathrm{Tr}\left(\mathbf{D}^{-1} \boldsymbol{\mathcal{A}}(\boldsymbol{\Sigma}) \mathbf{D}^{-1} \right). \tag{A30}$$

By putting (A30) and then (A28) into (A29d), we obtain the end result $\mathsf{SINR}_{ce}(\boldsymbol{w}, \boldsymbol{\Sigma}) \leq M\gamma_e$. ■

ACKNOWLEDGMENT

The authors would like to sincerely thank Prof. S. Zhang of the Chinese University of Hong Kong, who gave us key advice regarding the NP-hardness of our considered problems. They would also like to thank the anonymous reviewers whose insightful comments have helped us improve the manuscript significantly.

REFERENCES

[1] W.-C. Liao, T.-H. Chang, W.-K. Ma, and C.-Y. Chi, "Joint transmit beamforming and artificial noise design for QoS discrimination in wireless downlink," in *Proc. IEEE ICASSP*, Dallas, TX, Mar. 14–19, 2010, pp. 2562–2565.

[2] F. Rashid-Farrokhi, K. J. R. Liu, and L. Tassiulas, "Transmit beamforming and power control for cellular wireless systems," *IEEE J. Sel. Areas Commun.*, vol. 16, no. 8, pp. 1437–1450, Oct. 1999.

[3] M. Bengtsson and B. Ottersten, "Optimal and suboptimal transmit beamforming," in *Handbook of Antennas in Wireless Communications*, L. C. Godara, Ed. Boca Raton, FL: CRC , 2001, ch. 18 .

[4] M. Schubert and H. Boche, "Solution of the multiuser downlink beamforming problem with individual SINR constraints," *IEEE Trans. Veh. Technol.*, vol. 53, no. 1, pp. 18–28, Jan. 2004.

[5] A. Wiesel, Y. C. Eldar, and S. Shamai, "Linear precoding via conic optimization for fixed MIMO receivers," *IEEE Trans. Signal Process.*, vol. 54, no. 1, pp. 161–176, Jan. 2006.

[6] N. D. Sidiropoulos, T. D. Davidson, and Z.-Q. Luo, "Transmit beamforming for physical-layer multicasting," *IEEE Trans. Signal Process.*, vol. 54, no. 6, pp. 2239–2251, Jun. 2006.

[7] E. Karipidis, N. D. Sidiropoulos, and Z.-Q. Luo, "Quality of service and max-min fair transmit beamforming to multiple cochannel multicast groups," *IEEE Trans. Signal Process.*, vol. 53, no. 3, pp. 1268–1279, Mar. 2008.

[8] A. B. Gershman, N. D. Sidiropoulos, S. Shahbazpanahi, M. Bengtsson, and B. Ottersten, "Convex optimization-based beamforming: From receive to transmit and network designs," *IEEE Signal Process. Mag.*, ser. Special Issue on Convex Optimiz. Signal Process., vol. 27, no. 3, pp. 62–75, May 2010.

[9] Z.-Q. Luo and T.-H. Chang, "SDP relaxation of homogeneous quadratic optimization: Approximation bounds and applications," in *Convex Optimization in Signal Processing and Communications*. Cambridge, U.K.: Cambridge Univ. Press, 2010, ch. 4.

[10] D. Hammarwall, M. Bengtsson, and B. Ottersten, "Downlink beamforming with indefinite shaping constraints," *IEEE Trans. Signal Process.*, vol. 54, no. 9, pp. 3566–3580, Sep. 2006.

[11] W. Yu and T. Lan, "Transmitter optimization for the multi-antenna downlink with per-antenna power constraints," *IEEE Trans. Signal Process.*, vol. 55, no. 1, pp. 2646–2660, Jun. 2007.

[12] E. Karipidis, N. D. Sidiropoulos, and Z.-Q. Luo, "Far-field multicast beamforming for uniform linear antenna arrays," *IEEE Trans. Signal Process.*, vol. 55, no. 10, pp. 4916–4927, Oct. 2007.

[13] Y. Huang and D. P. Palomar, "Rank-constrained separable semidefinite program with applications to optimal beamforming," *IEEE Trans. Signal Process.*, vol. 58, no. 2, pp. 664–678, Feb. 2010.

[14] V. Havary-Nassab, S. Shahbazpanahi, A. Grami, and Z.-Q. Luo, "Distributed beamforming for relay networks based on second-order statistics of the channel state information," *IEEE Trans. Signal Process.*, vol. 56, no. 9, pp. 4306–4316, Sep. 2008.

[15] K. T. Phan, S. A. Vorobyov, N. D. Sidiropoulos, and C. Tellambura, "Spectrum sharing in wireless networks via QoS-aware secondary multicast beamforming," *IEEE Trans. Signal Process.*, vol. 57, no. 6, pp. 2323–2335, Jun. 2009.

[16] A. D. Wyner, "The wiretap channel," *Bell Syst. Tech. J.*, vol. 54, pp. 1355–1387, 1975.

[17] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, pp. 339–348, May 1978.

[18] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," in *Proc. IEEE Int. Symp. Inf. Theory*, Jul. 6–11, 2008, pp. 524–528.

[19] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas: The MIMOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, pp. 5515–5532, Nov. 2010.

[20] T. Liu and S. Shamai (Shitz), "A note on the secrecy capacity of the multiple-antenna wiretap channel," *IEEE Trans. Inf. Theory*, vol. 55, pp. 2547–2553, Jun. 2009.

[21] R. Bustin, R. Liu, H. V. Poor, and S. Shamai (Shitz), "An MMSE approach to the secrecy capacity of the MIMO Gaussian wiretap channel," in *Proc. IEEE Int. Symp. Inf. Theory*, Seoul, Korea, Jun. 3, 2009, pp. 2602–2606.

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

[23] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperative relays," *IEEE Trans. Signal Process.*, vol. 58, no. 3, pp. 1875–1888, Mar. 2010.

[24] A. Mukherjee and A. L. Swindlehurst, "Fixed-rate power allocation strategies for enhanced secrecy in MIMO wiretap channels," in *Proc. IEEE SPAWC*, Perugia, Italy, Jun. 21–24, 2009, pp. 344–348.

[25] A. L. Swindlehurst, "Fixed SINR solutions for the MIMO wiretap channel," in *Proc. IEEE ICASSP*, Taipei, Taiwan, Apr. 19–24, 2009, pp. 2437–2440.

[26] L. Zhang, R. Zhang, Y.-C. Liang, Y. Xin, and S. Cui, "On the relationship between the multi-antenna secrecy communications and cognitive radio communications," *IEEE Trans. Commun.*, vol. 58, pp. 1877–1886, Jun. 2010.

[27] S. Gerbracht, A. Wolf, and E. A. Jorswieck, "Beamforming for fading wiretap channels with partial channel information," in *Proc. Int. ITG Workshop on Smart Antennas (WSA)*, Bremen, Germany, Feb. 2010 [Online]. Available: http://tnt.wcms-file2.tu-dresden.de/BibtexDbMng/upload/Gerbracht2010.pdf

[28] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE. Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, Jun. 2008.

[29] K. Cumanan, L. Musavian, S. Lambotharan, and A. B. Gershman, "SINR balancing technique for downlink beamforming in cognitive radio networks," *IEEE Signal Process. Lett.*, vol. 17, no. 2, pp. 133–136, Feb. 2010.

[30] R. Zhang, Y.-C. Liang, and S. Cui, "Dynamic resource allocation in cognitive radio networks: A convex optimization perspective," *IEEE Signal Process. Mag. (Special Issue on Convex Optimiz. Signal Process.)*, vol. 27, no. 3, pp. 102–114, May 2010.

[31] W.-K. Ma, T. N. Davidson, K. M. Wong, Z.-Q. Luo, and P.-C. Ching, "Quasi-maximum-likelihood multiuser detection using semidefinite relaxation with applications to synchronous CDMA," *IEEE Trans. Signal Process.*, vol. 50, no. 4, pp. 912–922, Apr. 2002.

[32] Z.-Q. Luo, W.-K. Ma, A. M.-C. So, Y. Ye, and S. Zhang, "Semidefinite relaxation of quadratic optimization problems: From its practical deployments and scope of applicability to key theoretical results," *IEEE Signal Process. Mag. (Special Issue on Convex Optimiz. Signal Process.)*, vol. 27, no. 3, pp. 20–34, May 2010.

[33] J. F. Sturm, "Using SeDuMi 1.02, a MATLAB toolbox for optimization over symmetric cones," *Optimiz. Methods and Software*, vol. 11–12, pp. 625–653, 1999.

[34] M. Grant and S. Boyd, CVX: MATLAB Software for Disciplined Convex Programming, Jun. 2009 [Online]. Available: http://stanford.edu/~boyd/cvx

[35] G. Pataki, "On the rank of extreme matrices in semidefinite programs and the multiplicity of optimal eigenvalues," *Math. Oper. Res.*, vol. 23, no. 2, pp. 339–358, 1998.

[36] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge, U.K.: Cambridge Univ. Press, 2004.

[37] A. Charnes and W. W. Cooper, "Programming with linear fractional functionals," *Naval Res. Logist. Quarter.*, vol. 9, pp. 181–186, Dec. 1962, doi: 10.1002/nav.3800090303.

[38] S. Zhang and Y. Huang, "Complex quadratic optimization and semidefinite programming," *SIAM J. Optimiz.*, vol. 3, pp. 871–890, 2006.

Wei-Cheng Liao received the B.S. degree in electrical engineering and the M.S. degree in communications engineering from the National Tsing Hua University, Hsinchu, Taiwan, in 2008 and 2010, respectively.

His research interests are in wireless communications and signal processing.

Tsung-Hui Chang (S'07–M'08) received the B.S. degree in electrical engineering and the Ph.D. degree in communications engineering from the National Tsing Hua University (NTHU), Hsinchu, Taiwan, in 2003 and 2008, respectively.

During September 2006 and February 2008, he was an exchange Ph.D. student of University of Minnesota, Minneapolis. Currently, he is a Postdoctoral Research Fellow with the Institute of Communications Engineering, NTHU. His research interests are widely in wireless communications, digital signal processing, and convex optimization and its applications.

Wing-Kin Ma (S'96–M'01) received the B.Eng. (first-class honors) degree in electrical and electronic engineering from the University of Portsmouth, Portsmouth, U.K., in 1995, and the M.Phil. and Ph.D. degrees, both in electronic engineering, from the Chinese University of Hong Kong (CUHK), Hong Kong, in 1997 and 2001, respectively. His Ph.D. dissertation was commended to be "of very high quality and well deserved honorary mentioning" by the Faculty of Engineering, CUHK, in 2001.

He is currently an Assistant Professor with the Department of Electronic Engineering, CUHK. From 2005 to 2007, he was also an Assistant Professor with the Institute of Communications Engineering, National Tsing Hua University, Taiwan, R.O.C., where he is still holding an adjunct position. Prior to becoming a faculty member, he held various research positions with McMaster University, Canada; CUHK; and the University of Melbourne, Australia. His research interests are in signal processing and communications, with a recent emphasis on MIMO techniques and convex optimization.

Dr. Ma currently serves as an Associate Editor of the IEEE TRANSACTIONS ON SIGNAL PROCESSING and the IEEE SIGNAL PROCESSING LETTERS. He has also served as a Guest Editor of the IEEE SIGNAL PROCESSING MAGAZINE on the Special Issue titled: Convex Optimization for Signal Processing in May 2010.

Chong-Yung Chi (S'83–M'83–SM'89) received the Ph.D. degree in electrical engineering from the University of Southern California, Los Angeles, in 1983.

From 1983 to 1988, he was with the Jet Propulsion Laboratory, Pasadena, CA. He has been a Professor with the Department of Electrical Engineering since 1989 and the Institute of Communications Engineering (ICE) since 1999 (also the Chairman of ICE during 2002–2005), National Tsing Hua University, Hsinchu, Taiwan. He has published more than 160 technical papers, including more than 50 journal papers (mostly in the IEEE TRANSACTIONS ON SIGNAL PROCESSING), two book chapters, and more than 100 peer-reviewed conference papers, as well as a graduate-level textbook *Blind Equalization and System Identification* (New York: Springer-Verlag, 2006). His current research interests include signal processing for wireless communications, convex analysis, and optimization for blind source separation, biomedical, and hyperspectral image analysis.

Dr. Chi has been a Technical Program Committee member for many IEEE sponsored and cosponsored workshops, symposiums, and conferences on signal processing and wireless communications, including Co-Organizer and General Co-Chairman of 2001 IEEE Workshop on Signal Processing Advances in Wireless Communications (SPAWC), and Co-Chair of Signal Processing for Communications (SPC) Symposium, ChinaCOM 2008 and Lead Co-Chair of SPC Symposium, ChinaCOM 2009. He is currently serving as Track Chair for MIMO, Signal Processing, and Smart in Antennas, 2011 IEEE Radio and Wireless Symposium in Radio and Wireless Week (RWW) 2011. He was an Associate Editor of the TRANSACTIONS ON SIGNAL PROCESSING (May 2001–April 2006), IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS II (January 2006–December 2007), IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS I (January 2008–December 2009), Associate Editor of the IEEE SIGNAL PROCESSING LETTERS (June 2006–May 2010), and a member of Editorial Board of EURASIP *Signal Processing Journal* (June 2005–May 2008), and an Editor (July 2003–December 2005) as well as a Guest Editor (2006) of EURASIP *Journal on Applied Signal Processing*. He was a member of the IEEE Signal Processing Committee on Signal Processing Theory and Methods (2005–2010). Currently, he is a member of the IEEE Signal Processing Committee on Signal Processing for Communications and Networking.