

Robust Secure Transmit Design with Artificial Noise in the Presence of Multiple Eavesdroppers

Xiaochen Liu¹, Yuanyuan Gao^{1*}, Nan Sha¹, Guozhen Zang¹, and Shijie. Wang¹

¹ Collage of Communications Engineering, University of Army Engineering University of PLA
Nanjing, 210007 - China

[e-mail: liuxiaochenyt@163.com, njyygao@sina.com, njshanan@163.com, zgz78@sina.com,
world900214@gmail.com]

*Corresponding author: Yuanyuan Gao

*Received May 4, 2018; revised October 6, 2019; accepted March 16, 2021;
published June 30, 2021*

Abstract

This paper studies secure wireless transmission from a multi-antenna transmitter to a single-antenna intended receiver overheard by multiple eavesdroppers with considering the imperfect channel state information (CSI) of wiretap channel. To enhance security of communication link, the artificial noise (AN) is generated at transmitter. We first design the robust joint optimal beamforming of secret signal and AN to minimize transmit power with constraints of security quality of service (QoS), i.e., minimum allowable signal-to-interference-and-noise ratio (SINR) at receiver and maximum tolerable SINR at eavesdroppers. The formulated design problem is shown to be nonconvex and we transfer it into linear matrix inequalities (LMIs). The semidefinite relaxation (SDR) technique is used and the approximated method is proved to solve the original problem exactly. To verify the robustness and tightness of proposed beamforming, we also provide a method to calculate the worst-case SINR at eavesdroppers for a designed transmit scheme using semidefinite programming (SDP). Additionally, the secrecy rate maximization is explored for fixed total transmit power. To tackle the nonconvexity of original formulation, we develop an iterative approach employing sequential parametric convex approximation (SPCA). The simulation results illustrate that the proposed robust transmit schemes can effectively improve the transmit performance.

Keywords: Physical-layer security, artificial noise, imperfect CSI, transmit power minimization, secrecy rate maximization

1. Introduction

Because of the broadcast characteristics of wireless communication, its security problem has attracted great attention. Traditional key-based cryptography assumes that the eavesdropper has limited computing resources, but it is not always reliable due to the great improvement of computing power. Besides, due to the large amount of computation, this strategy may not be suitable for high-speed transmission of future communication. Therefore, the concept of physical layer security has been paid increasing attention.

The notion of security based on information theory was first introduced in [1]. [2] studied the wiretap channel and secrecy capacity considering the imperfections introduced by the channel. [3] studied a more general vision of wiretap channel and considered transmission of secret messages over broadcast channels. Meanwhile, multi-antenna transmission is considered to be an effective and practical method to improve the capacity and reliability of wireless communication [4-6]. For multiple-input single-output (MISO) case, [7] studied the beamforming schemes and got the optimal scheme using generalized eigenvalues. [8] proposed the AN-aided transmission, in case the main channel is worse than the wiretap channel. For the cases where multiple eavesdroppers exist, [9] proposed the joint optimization of transmit weights and AN. [10] considered the problem of secure communication in fading channels and obtained a closed-form expression of achievable secrecy rate. [11, 12] researched the AN-aided secure schemes in cognitive radio. When multiple help jammers are available, [13] proposed the optimal power allocation scheme to maximize the secrecy rate. For multiple-input multiple-output (MIMO) case, [14] computed the perfect secrecy capacity of the multiple antenna MIMO broadcast channel. [15] tried to obtain the optimal beamforming schemes for MIMO transmission with the tool of generalized singular value decomposition (GSVD). When the squared M-square quadrature amplitude modulated (M-QAM) modulation scheme is adopted, [16] found that the AN in the form of QAM or rotated QAM phase selection performs better than the Gaussian AN in improving the symbol error rate (SER) performance. Meanwhile, the secure transmission in massive MIMO system is attracting increasing attention [17-19].

In practice, the channel state information (CSI) is usually estimated with errors. Generally, there are mainly two ways describing the CSI estimation error: the stochastic and the deterministic models. For the former, the CSI errors are considered as complex random variables. Based on this assumption, [20, 21] considered robust transmit strategies against the imperfectness of CSI in MISO and MIMO channel, respectively. The later model assumes that the CSI errors lie in a known set of possible values. Based on deterministic model, [22, 23] studied the secure transmission in MISO channel. [24, 25] considered secure transmit schemes for MISO wiretap channels with cooperative jamming from helper. Recently, [26] proposes a Lagrangian dual based method by using the statistical characteristics of the CSI errors for full-duplex secure communication. In [27], considering the proximity of the legitimate receiver and eavesdropper, the impact of the shadowing correlation and composite fading parameters on secrecy performance is studied. In addition, with the fast fading channel, [28] analyzed the impact of outdated CSI on secrecy performance.

In this paper, we take the deterministic model to describe the CSI errors, and study the robust transmit schemes. It is assumed that the receiver and the eavesdroppers are located far enough, and the antenna distance is long enough. The correlation among the eavesdroppers and intended receiver channel, and the correlation among different antennas can be ignored.

The slow fading channel is studied, and the outdated CSI is not considered here. It is also assumed that the transmitter generates Gaussian information signal and no help jammer is available. The main contributions of this paper are as following.

- We design the robust joint optimal beamforming for minimizing transmit power with considering the CSI errors of wiretap channel based on deterministic model. Assuming the passive method of eavesdroppers, it is difficult to obtain accurate CSI of wiretap channel, which greatly degrades the performance of transmit schemes based on accurate instantaneous CSI. Although the robust transmit schemes were proposed in [22, 29], these papers did not consider the improvement for the application of AN. The work in [9] did not consider influence of CSI errors.
- We manage to show the tightness and robustness of the proposed power optimization design by calculating the worst signal-to-interference-and-noise ratio (SINR) at eavesdroppers. [24] proposed a way to calculate the worst-case SINR at intended receiver in the case of single-antenna eavesdroppers by dual theory. However, the problem is more difficult for the scenario of multi-antenna eavesdroppers interfered by AN. In this paper, we derive a method to calculate the worst-case SINR using semidefinite programming (SDP), which is flexible for this more delicate case.
- With given total transmit power, the secrecy rate maximization is studied for the case of single-antenna eavesdroppers. The original problem is fractional and non-convex, hence we propose an iterative method by relaxing it into tractable formulation with recently presented sequential parametric convex approximation (SPCA) method. The sub-optimal solution can be obtained using the proposed method. Our proposed transmit scheme shows obvious performance gains compared with the existing schemes.

The paper is organized as following. Section 2 introduces transmit model and problem formulations. In section 3, we design the transmit power optimization with imperfect CSI. The work to derive the worst-case SINR at eavesdroppers is also included. Section 4 describes the robust secrecy rate optimization. The simulation results are shown in section 5 and conclusion is drawn in section 6.

The notation of this paper is as follows. Boldface lowercase and uppercase letters are used to denote vectors and matrices, respectively. \mathbf{I}_n denotes the n -by- n identity matrix, $\mathbf{0}$ is a zero matrix. By $\mathbf{X} \succeq \mathbf{0}$, we mean that \mathbf{X} is a Hermitian positive semidefinite matrix. The operators $(\cdot)^T$, $(\cdot)^H$, $\text{vec}(\cdot)$, $\text{Tr}(\cdot)$, ∇ and $|\cdot|$ represent the transpose, Hermitian, trace, vectorization, gradient and determinant operations, respectively. $\mathcal{R}^{m \times n}$ and $\mathcal{C}^{m \times n}$ stand for the set of matrices with real- and complex-valued entries. The symbol $\mathbb{E}\{\cdot\}$ represents the statistical expectation of the argument. The Frobenius norm is denoted by $\|\cdot\|_F$. \otimes denotes the Kronecker product and $\text{Re}\{\cdot\}$ represents the real part of a complex value.

2. Transmit Model and Problem Formulation

2.1 System Model

The communication system contains a transmitter, an intended receiver and K illegal eavesdroppers. The transmitter and eavesdropper k ($1 \leq k \leq K$) are equipped with N_t and N_{e_k} antennas, respectively. The eavesdroppers try to tap confidential messages from the transmitter passively without collusion. The scenario is described in Fig. 1.

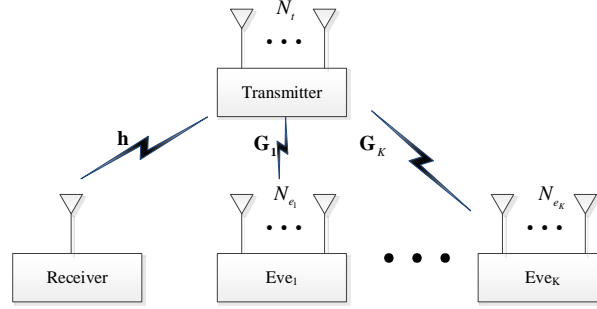


Fig. 1. System Model

The transmit signal vector is denoted as $\mathbf{x}(t) \in \mathbb{C}^{N_t}$, the received signals at the receiver and eavesdropper k are

$$\begin{aligned} y_r(t) &= \mathbf{h}^H \mathbf{x}(t) + n_r \\ \mathbf{y}_{e_k}(t) &= \mathbf{G}_k \mathbf{x}(t) + \mathbf{n}_{e_k} \quad k = 1, 2, \dots, K \end{aligned} \quad (1)$$

Here, $\mathbf{h} \in \mathbb{C}^{N_t}$ denotes the channel from the transmitter to receiver, $\mathbf{G}_k \in \mathbb{C}^{N_{e_k} \times N_t}$ denotes the channel from transmitter to eavesdropper k . $y_r(t) \in \mathbb{C}$ and $\mathbf{y}_{e_k}(t) \in \mathbb{C}^{N_{e_k}}$ are the signal obtained by receiver and eavesdropper, respectively. $n_r \in \mathbb{C}$ and $\mathbf{n}_{e_k} \in \mathbb{C}^{N_{e_k}}$ denote independent and identical distributed (i.i.d.) complex white Gaussian noises with variances σ_r^2 and $\sigma_{e_k}^2 \mathbf{I}_{N_{e_k}}$.

This paper studies the AN-aided transmit schemes [8]. Considering this way, the transmit signal vector can be denoted as

$$\mathbf{x}(t) = \mathbf{w}s(t) + \mathbf{Z}\mathbf{v} \quad (2)$$

where $s(t) \in \mathbb{C}$ is confidential information for the receiver, $\mathbf{v} \in \mathbb{C}^{N_t \times 1}$ denotes the AN vector following an zero-mean i.i.d. complex Gaussian distribution generated by transmitter. $\mathbf{w} \in \mathbb{C}^{N_t \times 1}$ and $\mathbf{Z} \in \mathbb{C}^{N_t \times N_t}$ denote the signal beamforming vector and AN beamforming matrix, respectively. It is set $\mathbb{E}\{|s(t)|^2\} = 1$ and $\mathbb{E}\{\mathbf{v}\mathbf{v}^H\} = \mathbf{I}_{N_t}$ without loss of generality.

In reality, the transmitter usually captures imperfect CSI of the wiretap channel. A Time Division Duplex (TDD) system is considered in this paper. In this case, the main channel \mathbf{h} can be reliably estimated throughout the transmission period, while the wiretap channel \mathbf{G}_k is inaccurate [30]. To depict this scenario, we introduce the deterministic model [31]. The CSI errors are defined as

$$\mathbf{\Delta}_k = \mathbf{G}_k - \hat{\mathbf{G}}_k \quad (3)$$

where $\hat{\mathbf{G}}_k$ is the estimated wiretap channel. $\mathbf{\Delta}_k$ represents the CSI corresponding estimation error. We have $\mathbf{\Delta}_k \in \{\mathbf{\Delta} : \|\mathbf{\Delta}\|_F \leq \varepsilon_k\}$ with ε_k denoting the uncertainty.

2.2 Problem Formulations

According to the transmit model above, the SINR at receiver is

$$\text{SINR}_r(\mathbf{w}, \mathbf{Q}_z) = \frac{\text{Tr}(\mathbf{h}^H \mathbf{w} \mathbf{w}^H \mathbf{h})}{\text{Tr}(\mathbf{h}^H \mathbf{Q}_z \mathbf{h}) + \sigma_r^2} \quad (4)$$

where $\mathbf{Q}_z = \mathbf{Z}\mathbf{Z}^H$. With CSI errors, the SINR at eavesdropper k can be expressed as

$$SINR_{e_k}(\mathbf{w}, \mathbf{Q}_z) = \frac{Tr((\hat{\mathbf{G}}_k + \Delta_k)\mathbf{w}\mathbf{w}^H(\hat{\mathbf{G}}_k + \Delta_k)^H)}{Tr((\hat{\mathbf{G}}_k + \Delta_k)\mathbf{Q}_z(\hat{\mathbf{G}}_k + \Delta_k)^H) + N_{e_k}\sigma_{e_k}^2} \quad (5)$$

Assuming that the minimum SINR required at receiver is Γ_r and maximum tolerable SINR at eavesdropper k is Γ_{e_k} , the robust transmit power minimization is described as

$$\begin{aligned} \min_{\mathbf{w}, \mathbf{Q}_z} \quad & |\mathbf{w}|^2 + Tr(\mathbf{Q}_z) \\ \text{s.t.} \quad & SINR_r(\mathbf{w}, \mathbf{Q}_z) \geq \Gamma_r \\ & SINR_{e_k}(\mathbf{w}, \mathbf{Q}_z) \leq \Gamma_{e_k}, \quad k = 1, \dots, K \\ & \|\Delta_k\|_F \leq \varepsilon_k, \quad k = 1, \dots, K \\ & \mathbf{Q}_z \succeq \mathbf{0} \end{aligned} \quad (6)$$

It is set that Γ_r is much larger than Γ_{e_k} for available secrecy rate. It should be noted that the formula may not be feasible, but if the constraint is not too tight, the problem is not serious. In most cases, the formulation above is feasible. The following lemma shows this problem in detail.

Lemma 1: Defining $\mathbf{Q}_h = \mathbf{h}\mathbf{h}^H$ and $\tilde{\mathbf{G}}_k = (\hat{\mathbf{G}}_k + \Delta_k)^H(\hat{\mathbf{G}}_k + \Delta_k)$, if $\mathbf{Q}_h \neq \rho\tilde{\mathbf{G}}_k$ for any $k = 1, 2, \dots, K$, where ρ is a constant, the problem (6) is feasible.

The proof of Lemma 1 is in Appendix A.

With CSI errors of wiretap channel, the secrecy rate is given as [32]

$$R_s = \log_2 \left(1 + \frac{\mathbf{h}^H \mathbf{w}\mathbf{w}^H \mathbf{h}}{\mathbf{h}^H \mathbf{Z}\mathbf{Z}^H \mathbf{h} + \sigma_r^2} \right) - \max_{1 \leq k \leq K} \log_2 \left| \mathbf{I} + \frac{(\hat{\mathbf{G}}_k + \Delta_k)\mathbf{w}\mathbf{w}^H(\hat{\mathbf{G}}_k + \Delta_k)^H}{(\hat{\mathbf{G}}_k + \Delta_k)\mathbf{Z}\mathbf{Z}^H(\hat{\mathbf{G}}_k + \Delta_k)^H + \sigma_{e_k}^2 \mathbf{I}} \right| \quad (7)$$

The robust secrecy rate maximization is defined as

$$\begin{aligned} \max_{\mathbf{w}, \mathbf{Q}_z} \min_{\Delta_k} \quad & R_s \\ \text{s.t.} \quad & |\mathbf{w}|^2 + Tr(\mathbf{Q}_z) \leq P_{\max} \\ & \|\Delta_k\|_F \leq \varepsilon_k, \quad k = 1, \dots, K \\ & \mathbf{Q}_z = \mathbf{Z}\mathbf{Z}^H, \mathbf{Q}_z \succeq \mathbf{0} \end{aligned} \quad (8)$$

P_{\max} denotes the maximum total power at transmitter. In this design, we aim to maximize the worst case secrecy rate with considering the CSI errors.

3. Robust Transmit Power Minimization

This section is motivated by power saving for secure transmission. Excessive energy consumption brings a heavy burden to the communication systems as well as raises serious environment concerns. So, green communication attracts increasing attention. We consider minimizing the transmit power with the SINR constraints at the receiver and eavesdroppers, i.e. guaranteeing the SINR at receiver higher than requirement and keeping the maximum

SINR at eavesdroppers lower than the threshold. In this way, the communication with reliable secure rate is available. In this section, it is assumed that all the eavesdroppers are multiple-antenna. The estimation of main channel is accurate, while the estimation of wiretap channel is not. For the CSI errors of wiretap channel, it is set the Frobenius norm $F = 2$.

3.1 Beamforming Design

Letting $\mathbf{W} = \mathbf{w}\mathbf{w}^H$, $\mathbf{Q}_h = \mathbf{h}\mathbf{h}^H$, $\mathbf{Q}_{G_k} = \mathbf{G}_k \mathbf{G}_k^H$ and $\mathbf{Q}_z = \mathbf{Z}\mathbf{Z}^H$, problem (6) can be rewritten as

$$\min_{\mathbf{W}, \mathbf{Q}_z} \text{Tr}(\mathbf{W}) + \text{Tr}(\mathbf{Q}_z) \quad (9a)$$

$$\text{s.t.} \quad \frac{1}{\Gamma_r} \text{Tr}(\mathbf{W}\mathbf{Q}_h) - \text{Tr}(\mathbf{Q}_z\mathbf{Q}_h) \geq \sigma_r^2 \quad (9b)$$

$$\frac{1}{\Gamma_{e_k}} \text{Tr}((\hat{\mathbf{G}}_k + \Delta_k)\mathbf{W}(\hat{\mathbf{G}}_k + \Delta_k)^H) - \text{Tr}((\hat{\mathbf{G}}_k + \Delta_k)\mathbf{Q}_z(\hat{\mathbf{G}}_k + \Delta_k)^H) \leq N_{e_k} \sigma_{e_k}^2, \quad k = 1, \dots, K \quad (9c)$$

$$\|\Delta_k\|_2 \leq \varepsilon_k, \quad k = 1, \dots, K \quad (9d)$$

$$\mathbf{Q}_z \succeq \mathbf{0}, \mathbf{W} \succeq \mathbf{0}, \text{rank}(\mathbf{W}) = 1 \quad (9e)$$

The problem (9) is solved to get the optimal transmit scheme with CSI errors in the wiretap channel.

Theorem 1: Given the main channel \mathbf{h} , inaccurate estimation wiretap channel \mathbf{G}_k with $\hat{\mathbf{g}}_k = \text{vec}(\hat{\mathbf{G}}_k)$, required SINR at the receiver Γ_r and threshold SINR at the eavesdroppers Γ_{e_k} , the optimal transmit power can be calculated as

$$\min_{\mathbf{W}, \mathbf{Q}_z} \text{Tr}(\mathbf{W}) + \text{Tr}(\mathbf{Q}_z) \quad (10a)$$

$$\text{s.t.} \quad \frac{1}{\Gamma_r} \text{Tr}(\mathbf{W}\mathbf{Q}_h) - \text{Tr}(\mathbf{Q}_z\mathbf{Q}_h) \geq \sigma_r^2 \quad (10b)$$

$$\begin{bmatrix} (\mathbf{Q}_{e_k}^T - \mu_k \mathbf{I}_{N_e}) \otimes \mathbf{I}_{N_e} & (\mathbf{Q}_{e_k}^T \otimes \mathbf{I}_{N_{e_k}}) \hat{\mathbf{g}}_k \\ \hat{\mathbf{g}}_k^H (\mathbf{Q}_{e_k}^T \otimes \mathbf{I}_{N_{e_k}})^H & \hat{\mathbf{g}}_k^H (\mathbf{Q}_{e_k}^T \otimes \mathbf{I}_{N_{e_k}}) \hat{\mathbf{g}}_k - N_{e_k} \sigma_{e_k}^2 + \mu_k \varepsilon_k^2 \end{bmatrix} \succeq \mathbf{0}, \quad k = 1, \dots, K \quad (10c)$$

$$\mathbf{Q}_{e_k} = \frac{1}{\Gamma_{e_k}} \mathbf{W} - \mathbf{Q}_z, \mu_k \geq 0, \quad k = 1, \dots, K \quad (10d)$$

$$\mathbf{Q}_z \succeq \mathbf{0}, \mathbf{W} \succeq \mathbf{0} \quad (10e)$$

Proof : To get the result, we transform constraints in (9c) into linear matrix inequalities (LMIs) based on S -Procedure [33].

Lemma 2 (S -Procedure): Let $f_k(\mathbf{x}), k = 1, 2$, be defined as

$$f_k(\mathbf{x}) = \mathbf{x}^H \mathbf{A}_k \mathbf{x} + 2 \text{Re}\{\mathbf{b}_k^H \mathbf{x}\} + c_k$$

Where $\mathbf{A}_k = \mathbf{A}_k^H \in \mathbb{C}^{n \times n}$, $\mathbf{b}_k \in \mathbb{C}^n$ and $c_k \in \mathbb{R}$. Then, the implication $f_1(\mathbf{x}) \leq 0 \Rightarrow f_2(\mathbf{x}) \leq 0$ hold if and only if there exist $\mu \geq 0$ such that

$$\mu \begin{pmatrix} \mathbf{A}_1 & \mathbf{b}_1 \\ \mathbf{b}_1^H & c_1 \end{pmatrix} - \begin{pmatrix} \mathbf{A}_2 & \mathbf{b}_2 \\ \mathbf{b}_2^H & c_2 \end{pmatrix} \succeq \mathbf{0},$$

Provided there exists a point $\hat{\mathbf{x}}$ with $f_k(\hat{\mathbf{x}}) > 0$.

We can transfer (10c) as

$$\text{Tr} \left[(\hat{\mathbf{G}}_k + \Delta_k) \left(\frac{1}{\Gamma_{e_k}} \mathbf{W} - \mathbf{Q}_z \right) (\hat{\mathbf{G}}_k + \Delta_k)^H \right] \leq N_{e_k} \sigma_{e_k}^2 \quad (11)$$

Defining $\hat{\mathbf{g}}_k = \text{vec}(\hat{\mathbf{G}}_k)$, $\delta_k = \text{vec}(\Delta_k)$, $\mathbf{Q}_{e_k} = \frac{1}{\Gamma_{e_k}} \mathbf{W} - \mathbf{Q}_z$, (11) can be rewritten as

$$\delta_k^H (\mathbf{Q}_{e_k}^T \otimes \mathbf{I}_{N_{e_k}}) \delta_k + 2 \text{Re} \{ \hat{\mathbf{g}}_k^H (\mathbf{Q}_{e_k}^T \otimes \mathbf{I}_{N_{e_k}}) \delta_k \} + \hat{\mathbf{g}}_k^H (\mathbf{Q}_{e_k}^T \otimes \mathbf{I}_{N_{e_k}}) \hat{\mathbf{g}}_k \leq N_{e_k} \sigma_{e_k}^2 \quad (12)$$

According to (9d), we can get

$$\|\Delta_k\|_2 \leq \varepsilon_k \Rightarrow \text{Tr}(\Delta_k \Delta_k^H) = \text{Tr}(\delta_k \delta_k^H) \leq \varepsilon_k^2 \quad (13)$$

Combining (12) and (13), based on Lemma 2, we can get that there exists $\mu_k \geq 0$ such that

$$- \begin{bmatrix} (\mathbf{Q}_{e_k}^T - \mu_k \mathbf{I}_{N_{e_k}}) \otimes \mathbf{I}_{N_{e_k}} & (\mathbf{Q}_{e_k}^T \otimes \mathbf{I}_{N_{e_k}}) \hat{\mathbf{g}}_k \\ \hat{\mathbf{g}}_k^H (\mathbf{Q}_{e_k}^T \otimes \mathbf{I}_{N_{e_k}})^H & \hat{\mathbf{g}}_k^H (\mathbf{Q}_{e_k}^T \otimes \mathbf{I}_{N_{e_k}}) \hat{\mathbf{g}}_k - N_{e_k} \sigma_{e_k}^2 + \mu_k \varepsilon_k^2 \end{bmatrix} \succeq \mathbf{0} \quad (14)$$

Neglecting the constraint $\text{rank}(\mathbf{W}) = 1$, the Theorem 1 is proved. (10) is a SDP which can be solved efficiently (e.g. with CVX software [34]). And we introduce the following proposition to yield a rank-one solution of optimal \mathbf{W}^* .

Proposition 1: Given the SDR problem (10) is feasible, we can always get the optimal solution \mathbf{W}^* which satisfies $\text{rank}(\mathbf{W}^*) = 1$.

The proof is in Appendix B.

3.2 Worst-case SINR with Imperfect CSI

Through Theorem 1, we have designed robust transmit scheme which guarantees the SINR at eavesdroppers lower than the threshold considering CSI errors. Actually, the *S*-Procedure based method introduces safe approximation of (9), which may waste extra power if the estimation is excessively conservative. Hence, a method is needed to evaluate the tightness of the proposed scheme. Besides, we want to measure the robustness of existing designs based on the accurate instantaneous CSI, i.e. the worst-case SINR [24] at eavesdroppers with the designed signal beamforming vector \mathbf{w}^* and AN beamforming matrix \mathbf{Z}^* . As this calculation is challenging for the analytical methods, in this part we will present the derivation of worst-case SINR with SDP based on deterministic model.

For the eavesdropper k , the maximum SINR at eavesdropper k can be expressed as

$$\begin{aligned} \max_{\Delta_k} & \frac{\text{Tr} \left[(\hat{\mathbf{G}}_k + \Delta_k) \mathbf{W}^* (\hat{\mathbf{G}}_k + \Delta_k)^H \right]}{\text{Tr} \left[(\hat{\mathbf{G}}_k + \Delta_k) \mathbf{Q}_z^* (\hat{\mathbf{G}}_k + \Delta_k)^H \right] + N_{e_k} \sigma_{e_k}^2} \\ \text{s.t.} & \quad \|\Delta_k\|_F \leq \varepsilon_k \end{aligned} \quad (15)$$

where $\mathbf{W}^* = \mathbf{w}^* \mathbf{w}^{*H}$ and $\mathbf{Q}_z^* = \mathbf{Z}^* \mathbf{Z}^{*H}$. Letting $\hat{\mathbf{g}}_k = \text{vec}(\hat{\mathbf{G}}_k)$, $\delta_k = \text{vec}(\Delta_k)$, (15) can be rewritten as

$$\max_{\hat{\mathbf{g}}_k} \frac{\text{Tr}\left[(\hat{\mathbf{g}}_k + \hat{\boldsymbol{\delta}}_k)(\mathbf{W}^* \otimes \mathbf{I}_{N_{e_k}})(\hat{\mathbf{g}}_k + \hat{\boldsymbol{\delta}}_k)^H\right]}{\text{Tr}\left[(\hat{\mathbf{g}}_k + \hat{\boldsymbol{\delta}}_k)(\mathbf{Q}_z^* \otimes \mathbf{I}_{N_{e_k}})(\hat{\mathbf{g}}_k + \hat{\boldsymbol{\delta}}_k)^H\right] + N_{e_k} \sigma_{e_k}^2} \quad (16a)$$

$$s.t. \quad \text{Tr}(\hat{\boldsymbol{\delta}}_k \hat{\boldsymbol{\delta}}_k^H) \leq \varepsilon_k^2 \quad (16b)$$

To employ SDR programming, we introduce auxiliary variable t and make $t^2 = 1$. Defining $\tilde{\boldsymbol{\delta}}_k = (\hat{\boldsymbol{\delta}}_k^T, t)^T$, according to (16a) it can be obtained that

$$\frac{\text{Tr}\left[(\hat{\mathbf{g}}_k + \hat{\boldsymbol{\delta}}_k)(\mathbf{W}^* \otimes \mathbf{I}_{N_{e_k}})(\hat{\mathbf{g}}_k + \hat{\boldsymbol{\delta}}_k)^H\right]}{\text{Tr}\left[(\hat{\mathbf{g}}_k + \hat{\boldsymbol{\delta}}_k)(\mathbf{Q}_z^* \otimes \mathbf{I}_{N_{e_k}})(\hat{\mathbf{g}}_k + \hat{\boldsymbol{\delta}}_k)^H\right] + N_{e_k} \sigma_{e_k}^2} = \frac{\text{Tr}(\tilde{\boldsymbol{\delta}}_k \mathbf{\Pi}_W \tilde{\boldsymbol{\delta}}_k^H)}{\text{Tr}(\tilde{\boldsymbol{\delta}}_k \mathbf{\Pi}_Q \tilde{\boldsymbol{\delta}}_k^H) + N_{e_k} \sigma_{e_k}^2} \quad (17)$$

where we define

$$\mathbf{\Pi}_W = \begin{pmatrix} \mathbf{W}^* \otimes \mathbf{I}_{N_{e_k}} & (\mathbf{W}^* \otimes \mathbf{I}_{N_{e_k}}) \hat{\mathbf{g}}_k \\ \hat{\mathbf{g}}_k^H (\mathbf{W}^* \otimes \mathbf{I}_{N_{e_k}}) & \hat{\mathbf{g}}_k^H (\mathbf{W}^* \otimes \mathbf{I}_{N_{e_k}}) \hat{\mathbf{g}}_k \end{pmatrix}, \quad \mathbf{\Pi}_Q = \begin{pmatrix} \mathbf{Q}_z^* \otimes \mathbf{I}_{N_{e_k}} & (\mathbf{Q}_z^* \otimes \mathbf{I}_{N_{e_k}}) \hat{\mathbf{g}}_k \\ \hat{\mathbf{g}}_k^H (\mathbf{Q}_z^* \otimes \mathbf{I}_{N_{e_k}}) & \hat{\mathbf{g}}_k^H (\mathbf{Q}_z^* \otimes \mathbf{I}_{N_{e_k}}) \hat{\mathbf{g}}_k \end{pmatrix}$$

Based on (17), problem (16) can be relaxed as

$$\max_{\mathbf{Q}_{\tilde{\boldsymbol{\delta}}_k}} \frac{\text{Tr}(\mathbf{Q}_{\tilde{\boldsymbol{\delta}}_k} \mathbf{\Pi}_W)}{\text{Tr}(\mathbf{Q}_{\tilde{\boldsymbol{\delta}}_k} \mathbf{\Pi}_Q) + N_{e_k} \sigma_{e_k}^2} \quad (18a)$$

$$s.t. \quad \text{Tr}(\mathbf{Q}_{\tilde{\boldsymbol{\delta}}_k} \tilde{\mathbf{I}}_{N_i \times N_e}) \leq \varepsilon_k^2, \quad k = 1, 2, \dots, K \quad (18b)$$

$$\text{Tr}(\mathbf{Q}_{\tilde{\boldsymbol{\delta}}_k} \mathbf{\Xi}) = 1 \quad (18c)$$

$$\mathbf{Q}_{\tilde{\boldsymbol{\delta}}_k} \succeq \mathbf{0} \quad (18d)$$

Where $\mathbf{Q}_{\tilde{\boldsymbol{\delta}}_k} = \tilde{\boldsymbol{\delta}}_k \tilde{\boldsymbol{\delta}}_k^H$, $\tilde{\mathbf{I}}_{N_i \times N_e} = \begin{pmatrix} \mathbf{I}_{N_i \times N_e} & 0 \\ 0 & 0 \end{pmatrix}$, $\mathbf{\Xi} = \begin{pmatrix} \mathbf{0}_{N_i \times N_e} & 0 \\ 0 & 1 \end{pmatrix}$. (18c) is used to guarantee the

constraint $t^2 = 1$. (18) is a quasi-convex problem, we can solve it through the Charnes-Cooper transformation [35]. Letting $\boldsymbol{\Theta}_{\tilde{\boldsymbol{\delta}}_k} = \lambda \mathbf{Q}_{\tilde{\boldsymbol{\delta}}_k}$ where $\lambda \geq 0$ is a slack variable, (18) is transferred as

$$\begin{aligned} & \max_{\boldsymbol{\Theta}_{\tilde{\boldsymbol{\delta}}_k}, \lambda} l_k \\ & s.t. \quad \text{Tr}(\boldsymbol{\Theta}_{\tilde{\boldsymbol{\delta}}_k} \mathbf{\Pi}_W) \geq l_k \\ & \quad \lambda N_{e_k} \sigma_{e_k}^2 + \text{Tr}(\boldsymbol{\Theta}_{\tilde{\boldsymbol{\delta}}_k} \mathbf{\Pi}_Q) = 1 \\ & \quad \text{Tr}(\boldsymbol{\Theta}_{\tilde{\boldsymbol{\delta}}_k} \tilde{\mathbf{I}}_{N_i \times N_e}) \leq \lambda \varepsilon_k^2, \text{Tr}(\boldsymbol{\Theta}_{\tilde{\boldsymbol{\delta}}_k} \mathbf{\Xi}) = \lambda \\ & \quad \boldsymbol{\Theta}_{\tilde{\boldsymbol{\delta}}_k} \succeq \mathbf{0}, \lambda \geq 0 \end{aligned} \quad (19)$$

l_k is a slack variable and the maximum value denotes the maximum SINR at the eavesdropper k . (19) is a SDP problem and can be solved effectively. It is easy to obtain that the optimal solution satisfy that $\text{rank}(\boldsymbol{\Theta}_{\tilde{\boldsymbol{\delta}}_k}^*) = 1$, the proof is identical to that of Proposition 1 and thus is omitted. Based on the derivation above, we can get Theorem 2.

Theorem 2: Given the signal beamforming vector \mathbf{w}^* and AN beamforming matrix \mathbf{Z}^* , the maximum SINR at eavesdroppers who do not collude is $\max\{t_1, t_2, \dots, t_K\}$, where t_k is defined in (19).

The proof of Theorem 2 is obvious. It should be noticed that Theorem 2 is available not only for the optimal beamforming proposed in Theorem 1 but also for all possible beamforming schemes.

4. Robust Secrecy Rate Maximization

In this section, we will get approach to the secrecy rate maximization with given total transmit power. Suppose that all the eavesdroppers are single-antenna. The estimation of main channel is accurate, while the estimation of wiretap channel is noisy with Frobenius norm $F = 2$. The maximum total power at transmitter is P_{\max} . By introducing a slack variable τ , the problem (8) can be expressed as

$$\max_{\mathbf{W}, \mathbf{Q}_z} \min_{\hat{\mathbf{g}}_k} \log_2 \left(1 + \frac{\mathbf{h}^H \mathbf{W} \mathbf{h}}{\mathbf{h}^H \mathbf{Q}_z \mathbf{h} + \sigma_r^2} \right) - \tau \quad (20a)$$

$$s.t. \quad \log_2 \left(1 + \frac{(\hat{\mathbf{g}}_k + \delta_k)^H \mathbf{W} (\hat{\mathbf{g}}_k + \delta_k)}{(\hat{\mathbf{g}}_k + \delta_k)^H \mathbf{Q}_z (\hat{\mathbf{g}}_k + \delta_k) + \sigma_{e_k}^2} \right) \leq \tau, \quad k = 1, \dots, K \quad (20b)$$

$$\|\delta_k\|_2 \leq \varepsilon_k, \quad k = 1, \dots, K \quad (20c)$$

$$Tr(\mathbf{W}) + Tr(\mathbf{Q}_z) \leq P_{\max} \quad (20d)$$

$$\mathbf{Q}_z \succeq \mathbf{0}, \mathbf{W} \succeq \mathbf{0}, \text{rank}(\mathbf{W}) = 1 \quad (20e)$$

with $\mathbf{W} = \mathbf{w}\mathbf{w}^H$ and $\mathbf{Q}_z = \mathbf{Z}\mathbf{Z}^H$. $\hat{\mathbf{g}}_k$ and δ_k represent wiretap channel and the corresponding CSI errors for the case of single-antenna eavesdroppers. Then, the rate maximization can be divided into two sub-problems. The outer one is an one-variable optimization problem with respect to (w.r.t.) τ

$$R_s^* = \max_{0 \leq \tau \leq \tau_{\max}} R(\tau) = \max_{0 \leq \tau \leq \tau_{\max}} \max_{\mathbf{W}, \mathbf{Q}_z} \log_2 \left(1 + \frac{\mathbf{h}^H \mathbf{W} \mathbf{h}}{\mathbf{h}^H \mathbf{Q}_z \mathbf{h} + \sigma_r^2} \right) - \tau \quad (21)$$

The upper bound τ_{\max} is calculated as the achievable rate of main channel neglecting eavesdroppers

$$\tau_{\max} = \log_2 \left(1 + \frac{P_{\max} \mathbf{h}^H \mathbf{h}}{\sigma_r^2} \right) \quad (22)$$

The inner problem of (20) is getting the maximum secrecy rate with fixed τ (calculating $R(\tau)$), which is equivalent to

$$\max_{\mathbf{W}, \mathbf{Q}_z} \min_{\hat{\mathbf{g}}_k} F(\mathbf{W}, \mathbf{Q}_z) = \log(\mathbf{h}^H \mathbf{W} \mathbf{h}) - \log(\mathbf{h}^H \mathbf{Q}_z \mathbf{h} + \sigma_r^2) \quad (23a)$$

$$s.t. \quad (\hat{\mathbf{g}}_k + \delta_k)^H \left(\mathbf{Q}_z - \frac{\mathbf{W}}{2^\tau} \right) (\hat{\mathbf{g}}_k + \delta_k) \geq 0, \quad k = 1, \dots, K \quad (23b)$$

$$\delta_k^H \delta_k \leq \varepsilon_k^2, \quad k = 1, \dots, K \quad (23c)$$

$$Tr(\mathbf{W}) + Tr(\mathbf{Q}_z) \leq P_{\max} \quad (23d)$$

$$\mathbf{Q}_z \succeq \mathbf{0}, \mathbf{W} \succeq \mathbf{0}, \text{rank}(\mathbf{W}) = 1 \quad (23e)$$

Notice that in (23a), $F(\mathbf{W}, \mathbf{Q}_z)$ is concave w.r.t. \mathbf{W} and convex w.r.t. \mathbf{Q}_z . To deal with this obstacle, the SPCA method [36] is introduced. Suppose a nonconcave term $f(\mathbf{X})$ and a concave function $g(\mathbf{X}, \mathbf{X}_0)$ in \mathbf{X} , with $f(\mathbf{X}) \geq g(\mathbf{X}, \mathbf{X}_0)$ for given \mathbf{X}_0 . The SPCA is an iterative scheme, for the n iteration, which satisfies that

$$\begin{aligned} f(\mathbf{X}) &= g(\mathbf{X}, \mathbf{X}_{0,n}) \\ \nabla f(\mathbf{X}) &= \nabla g(\mathbf{X}, \mathbf{X}_{0,n}) \end{aligned}$$

where $\mathbf{X}_{0,n}$ denotes the optimal solution \mathbf{X}^* of the last iteration. In this paper, we derive the low bound of $F(\mathbf{W}, \mathbf{Q}_z)$ by its first order Taylor series approximation, i.e.

$$G(\mathbf{W}, \mathbf{Q}_z, \mathbf{Q}_{z0,n}) \triangleq \log(\mathbf{h}^H \mathbf{W} \mathbf{h}) - \log(\mathbf{h}^H \mathbf{Q}_{z0,n} \mathbf{h} + \sigma_r^2) - Tr \left(\frac{\mathbf{h} \mathbf{h}^H}{\mathbf{h}^H \mathbf{Q}_{z0,n} \mathbf{h} + \sigma_r^2} (\mathbf{Q}_z - \mathbf{Q}_{z0,n}) \right) \quad (24)$$

where $\mathbf{Q}_{z0,n}$ is a preset matrix. $G(\mathbf{W}, \mathbf{Q}_z, \mathbf{Q}_{z0,n})$ is concave in both \mathbf{W} and \mathbf{Q}_z . Hence, the tractable formulation of problem (23) in n iteration is expressed as

$$\max_{\mathbf{W}_n, \mathbf{Q}_{z,n}} G(\mathbf{W}_n, \mathbf{Q}_{z,n}, \mathbf{Q}_{z0,n}) \quad (25a)$$

$$s.t. \quad \begin{bmatrix} \mathbf{Q}_{z,n} - \frac{\mathbf{W}_n}{2^\tau} + u_k \mathbf{I} & (\mathbf{Q}_{z,n} - \frac{\mathbf{W}_n}{2^\tau}) \hat{\mathbf{g}} \\ \hat{\mathbf{g}}^H (\mathbf{Q}_{z,n} - \frac{\mathbf{W}_n}{2^\tau}) & \hat{\mathbf{g}}^H (\mathbf{Q}_{z,n} - \frac{\mathbf{W}_n}{2^\tau}) \hat{\mathbf{g}} - u_k \varepsilon_k^2 + \sigma_k^2 \end{bmatrix} \succeq \mathbf{0}, \quad k=1, \dots, K \quad (25b)$$

$$Tr(\mathbf{W}_n) + Tr(\mathbf{Q}_{z,n}) \leq P_{\max} \quad (25c)$$

$$\mathbf{Q}_{z,n} \succeq \mathbf{0}, \mathbf{W}_n \succeq \mathbf{0}, u_k \geq 0, \quad k=1, \dots, K \quad (25d)$$

where (25b) is obtained using Lemma 2 and we set $\mathbf{Q}_{z0,n} = \mathbf{Q}_{z,n-1}^*$ with $\mathbf{Q}_{z,n-1}^*$ denoting the optimal solution of $n-1$ iteration. We introduce SDR by relaxing the rank constraint in (25) and get the accurate optimal solution according to the following proposition.

Proposition 2: Given the SDR problem (25), we can always get the optimal solution \mathbf{W}_n^* which satisfies $rank(\mathbf{W}_n^*) = 1$.

The proof is shown in Appendix C.

Let $G_n(\tau)$ be the output of (25a) for n iteration, the derivation of inner problem (23) using SPCA method is summarized in Algorithm 1.

Algorithm 1: SPCA procedure for solving (23)

Initialization:

P_{\max} , the tolerable error η

$\mathbf{Q}_{z0,1}$, $G_1(\tau) - G_0(\tau) \geq \eta$, $n=1$

While $|G_n(\tau) - G_{n-1}(\tau)| \geq \eta$ **do**

 Update $n = n + 1$

 Set $\mathbf{Q}_{z0,n} = \mathbf{Q}_{z,n-1}^*$

 Solve problem (25) with $\mathbf{Q}_{z0,n}$ and get the optimal solution $\mathbf{W}_n^*, \mathbf{Q}_{z,n}^*, G_n(\tau)$

End while

Get the optimal solution $\mathbf{W}_n^*, \mathbf{Q}_{z,n}^*$ and corresponding $G_n(\tau)$.

Proposition 3: Setting $\{G_n(\tau)\}$ be the sequence of output in (25a) obtained by Algorithm 1, then $\{G_n(\tau)\}$ converges.

Proof: Suppose that in $n-1$ iteration, we get the optimal solution $\mathbf{W}_{n-1}^*, \mathbf{Q}_{z,n-1}^*$ and the corresponding $G_{n-1}(\tau)$. Apply $\mathbf{Q}_{z0,n} = \mathbf{Q}_{z,n-1}^*$ in (25a) and solve problem (25) for n iteration, we can get the updated optimal solution $\mathbf{W}_n^*, \mathbf{Q}_{z,n}^*, G_n(\tau)$. It is obvious that $G(\mathbf{W}_n^*, \mathbf{Q}_{z,n}^*, \mathbf{Q}_{z,n-1}^*) \geq G(\mathbf{W}_{n-1}^*, \mathbf{Q}_{z,n-1}^*, \mathbf{Q}_{z0,n-1})$, hence $G_n(\tau) \geq G_{n-1}(\tau)$. In addition it satisfies that $G(\mathbf{W}, \mathbf{Q}_z, \mathbf{Q}_{z0,n}) \leq F(\mathbf{W}, \mathbf{Q}_z)$, hence we can conclude that $\{G_n(\tau)\}$ converges.

Having solved the inner problem (23), we can perform a one-dimension search over τ (e.g. golden section search [37]) for the outer problem. Then the robust secrecy rate maximization problem (8) is solved.

5. Simulation Results

In this section, the simulation results are provided to show the performance of the transmit schemes proposed in this paper. The isotropic AN scheme [8] referred as iso-AN scheme and optimal transmit design without AN [22] referred as no-AN scheme are introduced for comparison. For the former, the signal beamforming vector and AN beamforming matrix are designed as

$$\mathbf{w} = \sqrt{\alpha} \frac{\mathbf{h}}{\|\mathbf{h}\|}, \quad \mathbf{Z} = \sqrt{\beta} \mathbf{P}_{\mathbf{h}}^{\perp} \quad (26)$$

where $\mathbf{P}_{\mathbf{h}}^{\perp}$ denotes the orthogonal complement projector of main channel \mathbf{h} . The channel realizations $\mathbf{h}, \mathbf{G}_1, \dots, \mathbf{G}_K$ are i.i.d. complex Gaussian distributed with zero mean and unite variance. The noise power at receiver is $\sigma_r^2 = 0dB$ and all eavesdroppers have the same noise power $\sigma_e^2 \stackrel{\Delta}{=} \sigma_{e_1}^2 = \sigma_{e_2}^2 \dots = \sigma_{e_K}^2 = 0dB$, unless specified. The CSI errors in (3) is limited as

$\mathbf{\Lambda}_k \in \{\mathbf{\Lambda} : \|\mathbf{\Lambda}\|_F \leq \varepsilon_k\}$. Defining $\varepsilon_k^2 = u \|\hat{\mathbf{G}}_k\|_F^2$, in which the parameter u represents uncertainty of channel estimation. All simulation results were based on 1000 Monte-Carlo trials.

We first verify Theorem 1 in Fig. 2 and our proposed robust joint optimal beamforming is referred as RJOBF. In this simulation, the required SINR at receiver is $\Gamma_r = 10dB$ while the threshold SINR at eavesdroppers is $\Gamma_e \stackrel{\Delta}{=} \Gamma_{e_1} = \Gamma_{e_2} = \dots = \Gamma_{e_K} = 0dB$. It is assumed that the number of eavesdroppers $K = 3$ equipped with the same number of antennas. The noise power at receiver is $\sigma_r^2 = 0dB$ and uncertainty $u = 0.1$. Fig. 2 shows minimum transmit power satisfying the security QoS requirement as a function of noise power at eavesdroppers with perfect CSI. We introduce the robust iso-AN and robust no-AN scheme for comparison which also can satisfy security QoS requirement considering imperfect CSI [13]. The proposed RJOBF scheme outperforms the other schemes in saving transmit power under the same QoS requirement. In Fig. 2(a), when $1/\sigma_e^2 = 15dB$ our proposed RJOBF scheme can save around 7dB power compared with robust iso-AN scheme while robust no-AN scheme becomes completely invalid.

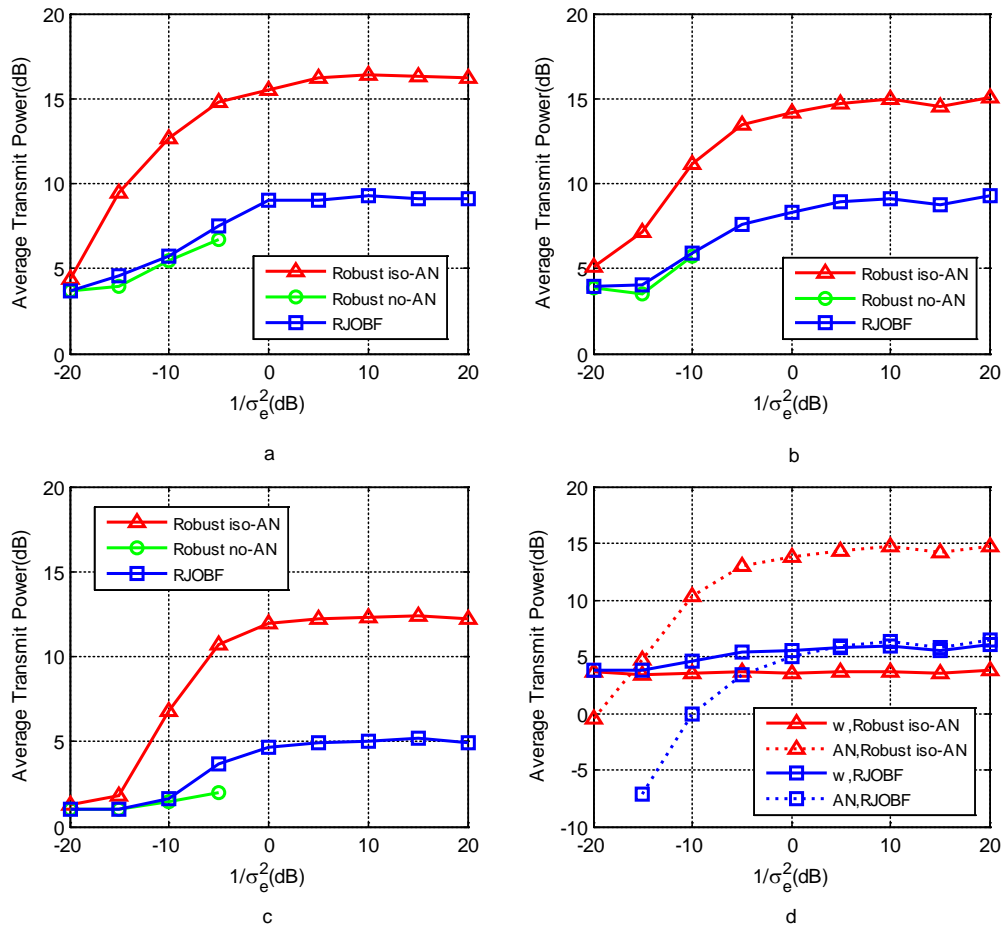


Fig. 2. Comparison of different transmit schemes with imperfect CSI for $u = 0.1$; (a) transmit power versus eavesdroppers' noise for $N_t = 8, N_e = 2$; (b) transmit power versus eavesdroppers' noise for $N_t = 8, N_e = 4$; (c) transmit power versus eavesdroppers' noise for $N_t = 10, N_e = 4$; (d) power allocations of isotropic AN scheme and proposed robust AN scheme for $N_t = 8, N_e = 4$.

Comparing **Fig. 2(b)** and **Fig. 2(a)**, it can be found that with increasing number of antennas at eavesdroppers, no more transmit power is needed to guarantee the required security performance for RJOBF scheme and robust iso-AN scheme. This is because the eavesdroppers receive more AN than signal power in these cases, consequently offset the increase in the number of antennas. However for the robust no-AN design which can only works well in high noise cases, when wiretap channel gets better this scheme couldn't handle the enhanced eavesdropping ability. From **Fig. 2(c)**, we can find that all the three schemes require less transmit power equipped with more transmit antennas which provides more freedom degree for transmit design. The power allocated to the signal is represented by solid line and dotted line in **Fig. 2(d)**, respectively., respectively. For power allocated to AN, the difference between RJOBF scheme and robust iso-AN scheme is about 10dB. Therefore, the main advantage of the scheme is better utilization of AN power. This result is consistent with the conclusion of [9].

Next, we study the performance of Theorem 2. For Monte-Carlo simulation, we first establish estimated wiretap channel and then produce 10,000 estimation error realizations to obtain the maximum SINR at eavesdroppers. We introduce the non-robust iso-AN, non-robust no-AN and the joint optimal beamforming with accurate CSI (JOBF) scheme [9] as comparison. The results are shown using different kind of points in Fig. 3. The worst-case SINR calculated by Theorem 2 is depicted by dashed line for different transmit schemes. We can find that the theoretical calculation and measured value through Monte-Carlo method are well matched especially when the wiretap channel uncertainty is no larger than 25%, which shows the validity of Theorem 2.

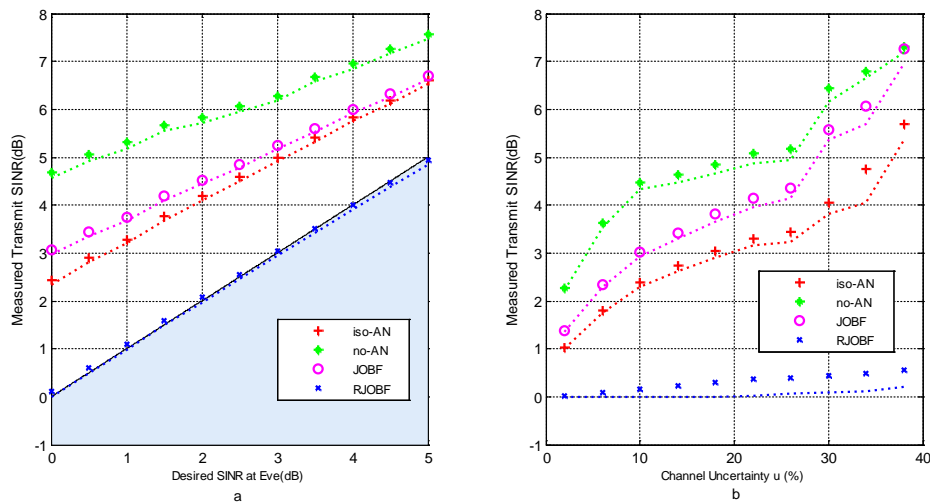


Fig. 3. Robustness of different transmit schemes with imperfect CSI; (a) Worst-case SINR at eavesdroppers versus desired SINR threshold for $\mu=0.1$; (b) Worst-case SINR at eavesdroppers versus wiretap channel uncertainty for $N_t=8, N_e=4, K=3$.

Fig. 3(a) shows the maximum measured SINR with an increasing SINR threshold at eavesdroppers. The points located in shadow area can satisfy the secure transmit constraints. Obviously, only the RJOBF design lies in the shadow. Besides, we can find that the safe approximation in RJOBF scheme is tight enough. The no-AN scheme and the JOBF scheme depend more on the wiretap channel estimation, so the two schemes behave worse than iso-AN scheme without considering the CSI errors. In Fig. 3(b), the SINR threshold at eavesdroppers is set to 0 dB. The results show that with the increasing of channel uncertainty, the proposed RJOBF scheme is less sensitive to wiretap channel uncertainty.

In Fig. 4, we show minimum transmit power versus the uncertainty of wiretap channel. As seen that the transmit power monotonically increases as channel uncertainty gets larger, meanwhile the gap between RJOBF scheme and robust iso-AN scheme is around 6 dB. From Fig. 4(b), we can find that the power allocated to signal almost keep constant as channel uncertainty gets large for the both two schemes. This is because we assume the estimation of main channel is accurate and the wiretap channel uncertainty mainly affects the power for AN.

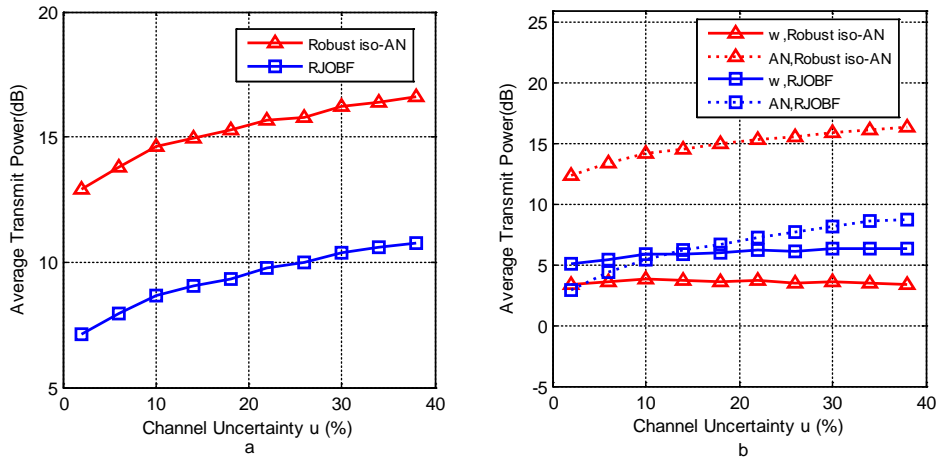


Fig. 4. Transmit power versus channel uncertainty for $N_t = 8, N_e = 4, K = 3$; (a) transmit power versus wiretap channel uncertainty; (b) power allocations of robust iso-AN and RJOBF.

Fig. 5 depicts transmit power versus the number of eavesdroppers. As shown, both the transmit schemes acquire more power to deal with more eavesdroppers. **Fig. 5(b)** shows that the power allocated to signal of RJOBF scheme is about 2dB more than robust iso-AN scheme. This indicates for resisting more eavesdroppers with enhanced eavesdropping ability, the RJOBF scheme introduces AN in main channel. To maintain SINR requirement at receiver, this scheme has to increase transmit power for signal and this design is proved superior to isotropic AN transmitted only in the null space of main channel.

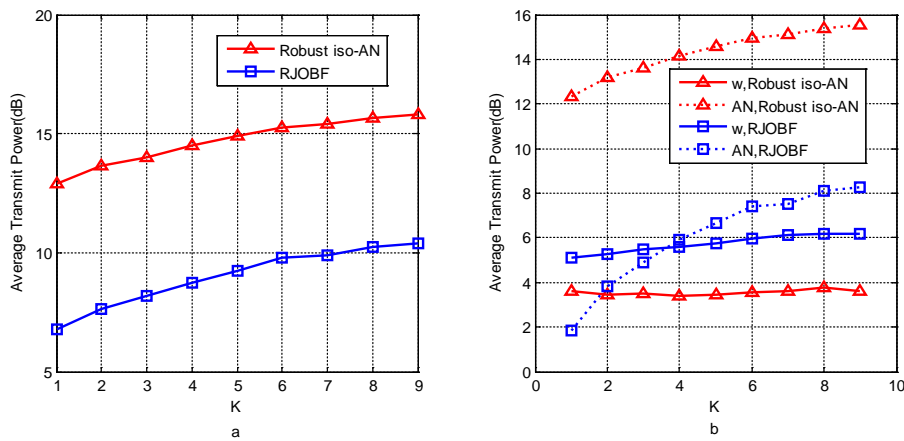


Fig. 5. Transmit power versus the number of eavesdroppers for $N_t = 8, N_e = 4, \mu = 0.1$; (a) transmit power versus eavesdroppers number; (b) power allocations of robust iso-AN and RJOBF.

Fig. 6 shows the performance of Algorithm 1 with transmit power upper limit $P_{\max} = 10dB$ and $\tau = 1$. We generate three different channel realizations. It can be noticed that the value of objective function in (25) i.e. the output of $R(1)$, converges quickly which verifies the conclusion of Proposition 3. For the same channel realization, we take different Q_{z_0} for

initialization and the proposed beamforming schemes achieve the same value. It shows that Algorithm 1 converges independent of initial set.

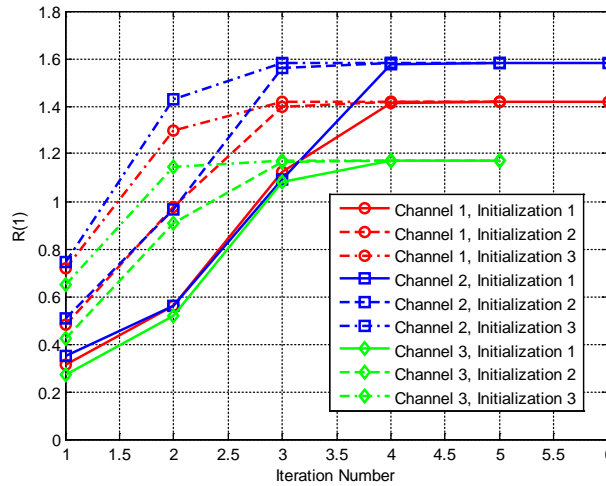


Fig. 6. Convergence of of Algorithm 1 for $N_t = 8, K = 3, \mu = 0.1$.

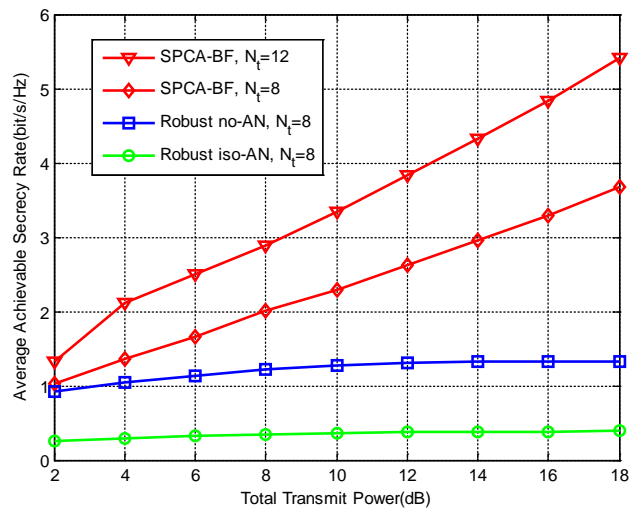


Fig. 7. Average achievable secrecy rate versus total transmit power for different transmit schemes with $K = 3, \mu = 0.1$.

In Fig. 7, we investigate the maximum secrecy rate versus total transmit power for different transmit schemes. We can conclude that under same condition, our proposed SPCA based transmit beamforming design (SPCA-BF) outperform the suboptimal schemes. Compared with robust no-AN, the SPCA-BF shows high performance especially under large transmit power condition. Meanwhile the gap between robust iso-AN and SPCA-BF is at least . In addition, it reveals that increasing number of antennas at transmitter will improve the transmit performance of SPCA-BF. The simulation shows the superiority of optimal designed AN-aided beamforming.

6. Conclusion

In this paper, we have designed the AN-aided secrecy transmit schemes in the presence of multiple eavesdroppers with imperfect CSI. We first derive the robust transmit power minimization, which is shown nonconvex. Considering CSI errors, the original problem is transferred into LMIs and solved using the well studied SDR technique. The rank-one property of the optimal solution is provided. To investigate the tightness and robustness of the proposed scheme, we also have proposed a SDP based method to calculate the worst-case SINR at eavesdroppers for the given transmit schemes. Then, the robust secrecy rate maximization has been studied. Due to the nonconvex and fractional formulation of original problem, we propose the iterative SPCA based method along with SDR. Besides, we also prove the rank-one property of each iteration optimal solution as well as the convergence of proposed approximate algorithm. The simulation results demonstrate validity of our proposed transmit schemes.

Appendix A

Proof of Lemma 1.

To prove problem (6) is feasible, we try to demonstrate that the robust iso-AN scheme provides a feasible solution for the formulation with the constraint in Lemma 1.

As (26), the signal beamforming vector and AN beamforming matrix are:

$$\mathbf{w} = \sqrt{\alpha} \frac{\mathbf{h}}{\|\mathbf{h}\|}, \quad \mathbf{Z} = \sqrt{\beta} \mathbf{P}_{\mathbf{h}}^{\perp}$$

where $\mathbf{P}_{\mathbf{h}}^{\perp}$ denotes the null space of main channel \mathbf{h} . Then, (6) is transferred as

$$\min_{\alpha, \beta} \quad \alpha + \beta(N_t - 1) \quad (27a)$$

$$s.t. \quad \alpha \geq \frac{\Gamma_r \sigma_r^2}{Tr(\mathbf{Q}_h)} \quad (27b)$$

$$\beta \geq \frac{\alpha Tr(\mathbf{P}_{\mathbf{h}}^{\perp} \mathbf{W}) - N_{e_k} \sigma_{e_k}^2 \Gamma_{e_k}}{Tr(\mathbf{P}_{\mathbf{h}}^{\perp} \tilde{\mathbf{G}}_k)}, \quad k = 1, \dots, K \quad (27c)$$

$$\|\Delta_k\|_F \leq \varepsilon_k, \quad k = 1, \dots, K \quad (27d)$$

Notice that $\mathbf{Q}_h \neq \rho \tilde{\mathbf{G}}_k$, so the denominator of left-hand side (LHS) in (27c) $Tr(\mathbf{P}_{\mathbf{h}}^{\perp} \tilde{\mathbf{G}}_k) \neq 0$. To deal with β , we can convert (27c) and (27d) into solving the problem

$$\max_{\Delta_k} \quad \frac{\alpha Tr(\mathbf{P}_{\mathbf{h}}^{\perp} \mathbf{W}) - N_{e_k} \sigma_{e_k}^2 \Gamma_{e_k}}{Tr(\mathbf{P}_{\mathbf{h}}^{\perp} \tilde{\mathbf{G}}_k)} \quad (28)$$

$$s.t. \quad \|\Delta_k\|_F \leq \varepsilon_k$$

For $k = 1, \dots, K$. Given the signal power α , the problem is quasi-convex and can be solved, hence we can assume the optimal solution of problem (28) is p_k . So, problem (11) can be solved as

$$\alpha = \frac{\Gamma_r \sigma_r^2}{Tr(\mathbf{Q}_h)} \quad (29)$$

$$\beta = \max\{0, p_1, p_2, \dots, p_K\}$$

As the robust isotropic AN scheme can always provide a feasible solution, problem (6) is proved to be feasible.

Appendix B

Proof of Proposition 1

In this part, we show that the problem (10) has a rank-one solution \mathbf{W}^* . We first transfer (10c) as

$$\begin{aligned} \mathbf{A}_k &= \begin{bmatrix} (\mathbf{Q}_{e_k}^T - \mu_k \mathbf{I}_{N_t}) \otimes \mathbf{I}_{N_{e_k}} & (\mathbf{Q}_{e_k}^T \otimes \mathbf{I}_{N_{e_k}}) \hat{\mathbf{g}}_k \\ \hat{\mathbf{g}}_k^H (\mathbf{Q}_{e_k}^T \otimes \mathbf{I}_{N_{e_k}})^H & \hat{\mathbf{g}}_k^H (\mathbf{Q}_{e_k}^T \otimes \mathbf{I}_{N_{e_k}}) \hat{\mathbf{g}}_k - N_{e_k} \sigma_{e_k}^2 + \mu_k \varepsilon_k^2 \end{bmatrix} \\ &= \begin{pmatrix} 1 & \hat{\mathbf{g}}_k \end{pmatrix}^H \begin{pmatrix} 1 \\ \Gamma_{e_k} \end{pmatrix} \begin{pmatrix} \mathbf{W} \otimes \mathbf{I}_{N_{e_k}} \\ \mathbf{I}_{N_{e_k}} \end{pmatrix} \begin{pmatrix} 1 & \hat{\mathbf{g}}_k \end{pmatrix} - \begin{bmatrix} \mathbf{Q}_z^T \otimes \mathbf{I}_{N_{e_k}} + \mu_k \mathbf{I}_{N_t} \otimes \mathbf{I}_{N_{e_k}} & (\mathbf{Q}_z^T \otimes \mathbf{I}_{N_{e_k}}) \hat{\mathbf{g}}_k \\ \hat{\mathbf{g}}_k^H (\mathbf{Q}_z^T \otimes \mathbf{I}_{N_{e_k}})^H & \hat{\mathbf{g}}_k^H (\mathbf{Q}_z^T \otimes \mathbf{I}_{N_{e_k}}) \hat{\mathbf{g}}_k + N_{e_k} \sigma_{e_k}^2 - \mu_k \varepsilon_k^2 \end{bmatrix} \end{aligned} \quad (30)$$

The Lagrangian function of (10) is as following

$$l(\mathbf{W}, \mathbf{Q}_z, \varphi, \mathbf{C}_k, \mathbf{Z}) = \text{Tr}(\mathbf{W}) + \text{Tr}(\mathbf{Q}_z) - \frac{\varphi}{\Gamma_r} \text{Tr}(\mathbf{W} \mathbf{Q}_h) + \varphi \text{Tr}(\mathbf{Q}_z \mathbf{Q}_h) + \varphi \sigma_r^2 + \sum_{k=1}^K \text{Tr}(\mathbf{C}_k \mathbf{A}_k) - \text{Tr}(\mathbf{Z} \mathbf{W}) \quad (31)$$

where $\varphi \geq 0, \mathbf{C}_k \succeq \mathbf{0}, \mathbf{Z} \succeq \mathbf{0}$ are dual variables for (10b), (10c), (10d), respectively. In addition,

$$\frac{\partial l}{\partial \mathbf{W}} = \mathbf{I} - \varphi \mathbf{Q}_h - \mathbf{Z} + \sum_{k=1}^K \sum_{n=1}^{N_{e_k}} T_{e_k}(n, n) \quad (32)$$

where Hermitian positive definite matrix $T_{e_k}(n, n) \in \mathbb{C}^{N_t \times N_t}$ is block submatrices of $\begin{pmatrix} 1 & \hat{\mathbf{g}}_k \end{pmatrix} \mathbf{C}_k \begin{pmatrix} 1 & \hat{\mathbf{g}}_k \end{pmatrix}^H$, which can be expressed as

$$\begin{pmatrix} 1 & \hat{\mathbf{g}}_k \end{pmatrix} \mathbf{C}_k \begin{pmatrix} 1 & \hat{\mathbf{g}}_k \end{pmatrix}^H = \begin{bmatrix} T_{e_k}(1, 1) & \cdots & T_{e_k}(1, n_{e_k}) \\ \vdots & \ddots & \vdots \\ T_{e_k}(n_{e_k}, n) & \cdots & T_{e_k}(n_{e_k}, n_{e_k}) \end{bmatrix}$$

According Karush-Kuhn-Tucker (K.K.T.) conditions, we have

$$\frac{\partial l}{\partial \mathbf{W}} = \mathbf{0} \quad (33a)$$

$$\mathbf{Z} \mathbf{W}^* = \mathbf{0} \quad (33b)$$

From (34a), it can be obtained

$$\begin{aligned} \mathbf{Z} &= \mathbf{I} - \varphi \mathbf{Q}_h + \sum_{k=1}^K \sum_{n=1}^{N_{e_k}} T_{e_k}(n, n) \\ &= \mathbf{I} - \varphi \mathbf{h} \mathbf{h}^H + \sum_{k=1}^K \sum_{n=1}^{N_{e_k}} T_{e_k}(n, n) \end{aligned} \quad (34)$$

According to (34), we can get $\text{rank}(\mathbf{Z}) \geq N_t - 1$. From (33b), \mathbf{W}^* lies in the nullspace of \mathbf{Z} , so it can be got that $\text{rank}(\mathbf{W}^*) = N_t - \text{rank}(\mathbf{Z})$. Since $\mathbf{W} = \mathbf{0}$ is not a feasible solution to problem (10), we can conclude $\text{rank}(\mathbf{W}^*) = 1$. The proof is completed.

Appendix C

Proof of Proposition 2

Let $\mathbf{D}_k \succeq \mathbf{0}$, $\lambda \geq 0$ be the Lagrangian dual variables for the constraints (25b) and (25c), respectively. $\mathbf{Y} \succeq \mathbf{0}$, $\mathbf{X} \succeq \mathbf{0}$ and $v_k \geq 0$, $k = 1, 2, \dots, K$ are the dual variables for the semidefinite constraint $\mathbf{W} \succeq \mathbf{0}$, $\mathbf{Q}_z \succeq \mathbf{0}$ and $u_k \geq 0$.

The Lagrangian function of (25) can be expressed as

$$\begin{aligned}
 l(\mathbf{D}_k, \lambda, \mathbf{Y}, \mathbf{X}, v_k) &= \log(\mathbf{h}^H \mathbf{W} \mathbf{h}) - \log(\mathbf{h}^H \mathbf{Q}_{z0,n} \mathbf{h} + \sigma_r^2) - Tr \left(\frac{\mathbf{h} \mathbf{h}^H}{\mathbf{h}^H \mathbf{Q}_{z0,n} \mathbf{h} + \sigma_r^2} (\mathbf{Q}_z - \mathbf{Q}_{z0,n}) \right) \\
 &- \sum_{k=1}^K \left(Tr \left(\mathbf{D}_k \frac{\mathbf{W}}{2^\tau} (\mathbf{1} \hat{\mathbf{g}}_k)(\mathbf{1} \hat{\mathbf{g}}_k)^H \right) \right) + \sum_{k=1}^K Tr \left(\mathbf{D}_k \begin{bmatrix} \mathbf{Q}_{z,n} + u_k \mathbf{I} & \mathbf{Q}_{z,n} \hat{\mathbf{g}} \\ \hat{\mathbf{g}}^H \mathbf{Q}_{z,n} & \hat{\mathbf{g}}^H \mathbf{Q}_{z,n} \hat{\mathbf{g}} - u_k \varepsilon_k^2 + \sigma_k^2 \end{bmatrix} \right) \\
 &+ \lambda (P_{\max} - Tr(\mathbf{W}_n) + Tr(\mathbf{Q}_{z,n})) + Tr(\mathbf{Y} \mathbf{W}) + Tr(\mathbf{X} \mathbf{Q}_z) + \sum_{k=1}^K v_k u_k
 \end{aligned} \quad (35)$$

The derivative w. r. t. \mathbf{W} is shown as

$$\frac{\partial l}{\partial \mathbf{W}} = \frac{\mathbf{h} \mathbf{h}^H}{\mathbf{h}^H \mathbf{W} \mathbf{h}} - \sum_{k=1}^K \left(\mathbf{D}_k (\mathbf{1} \hat{\mathbf{g}}_k)(\mathbf{1} \hat{\mathbf{g}}_k)^H \right) - \lambda \mathbf{I} + \mathbf{Y} \quad (36)$$

The corresponding K.K.T. conditions are

$$\mathbf{Y} = \lambda \mathbf{I} - \frac{\mathbf{h} \mathbf{h}^H}{\mathbf{h}^H \mathbf{W} \mathbf{h}} + \sum_{k=1}^K \left(\mathbf{D}_k (\mathbf{1} \hat{\mathbf{g}}_k)(\mathbf{1} \hat{\mathbf{g}}_k)^H \right) \quad (37a)$$

$$\mathbf{Y} \mathbf{W}^* = \mathbf{0} \quad (37b)$$

Similar to Appendix B, we can get $rank(\mathbf{W}^*) = N_t - rank(\mathbf{Y})$, which is satisfied that $rank(\mathbf{Y}) \geq N_t - 1$. Since $\mathbf{W}^* = \mathbf{0}$ is not a feasible solution to problem (15), we can get $rank(\mathbf{W}^*) = 1$. The proof is completed.

References

- [1] C. E. Shannon, "Communication theory of secrecy systems," *Bell Labs Tech.*, vol. 28, no. 4, pp. 656–715, Oct. 1949. [Article \(CrossRef Link\)](#)
- [2] Wyner, and D. A., "The wire-tap channel," *Bell Labs Tech.*, vol. 54, no. 8, pp. 1355-1387, Oct. 1975. [Article \(CrossRef Link\)](#)
- [3] I. Csiszar, and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, May 1978. [Article \(CrossRef Link\)](#)
- [4] E. Telatar, "Capacity of Multi - antenna Gaussian Channels," *Eur. Trans. Telecommun.*, vol. 10, no. 6, pp. 585-595, 1999. [Article \(CrossRef Link\)](#)
- [5] G. J. Foschini, and M. J. Gans, "On Limits of Wireless Communications in a Fading Environment when Using Multiple Antennas," *Wirel. Pers. Commun.*, vol. 6, no. 3, pp. 311-335, Mar. 1998.
- [6] G. G. Raleigh, and J. M. Cioffi, "Spatio-temporal coding for wireless communications," *IEEE Trans. Commun.*, vol. 46, no. 3, pp. 357-366, Mar. 1998. [Article \(CrossRef Link\)](#)
- [7] Khisti, Wornell, and W. G., "Secure Transmission With Multiple Antennas I: The MISOME Wiretap Channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 7, pp. 3088-3104, Jul. 2010. [Article \(CrossRef Link\)](#)
- [8] S. Goel, and R. Negi, "Guaranteeing Secrecy using Artificial Noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180-2189, Jun. 2008. [Article \(CrossRef Link\)](#)

- [9] 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. [Article \(CrossRef Link\)](#)
- [10] X. Zhou, and M. R. McKay, "Secure Transmission With Artificial Noise Over Fading Channels: Achievable Rate and Optimal Power Allocation," *IEEE Trans. Veh. Technol.*, vol. 59, no. 8, pp. 3831-3842, Oct. 2010. [Article \(CrossRef Link\)](#)
- [11] F. Zhou, Z. Li, J. Cheng, Q. Li, and J. Si, "Robust AN-Aided Beamforming and Power Splitting Design for Secure MISO Cognitive Radio With SWIPT," *IEEE Trans. Wireless Commun.*, vol. 16, no. 4, pp. 2450-2464, Apr. 2017. [Article \(CrossRef Link\)](#)
- [12] Y. Huang, Z. Li, F. Zhou, and R. Zhu, "Robust AN-Aided Beamforming Design for Secure MISO Cognitive Radio Based on a Practical Nonlinear EH Model," *IEEE Access*, vol. 5, pp. 14011-14019, 2017. [Article \(CrossRef Link\)](#)
- [13] K. Cumanan, G. C. Alexandropoulos, Z. Ding, and G. K. Karagiannidis, "Secure communications with cooperative jamming: Optimal power allocation and secrecy outage analysis," *IEEE Trans. Veh. Technol.*, vol. 66, no. 8, pp. 7495-7505, Aug. 2017. [Article \(CrossRef Link\)](#)
- [14] F. Oggier, and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," in *Proc. of 2008 IEEE International Symposium on Information Theory*, pp. 524-528, 2008. [Article \(CrossRef Link\)](#)
- [15] A. Khisti, and G. W. Wornell, "Secure Transmission With Multiple Antennas—Part II: The MIMOME Wiretap Channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 11, pp. 5515–5532, Nov. 2010. [Article \(CrossRef Link\)](#)
- [16] Y. Liu, L. Li, G. Alexandropoulos, and M. Pesavento, "Securing relay networks with artificial noise: An error performance-based approach," *Entropy*, vol. 19, no. 8, pp. 384, Jul. 2017. [Article \(CrossRef Link\)](#)
- [17] T. R. Dean, and A. J. Goldsmith, "Physical-Layer Cryptography Through Massive MIMO," in *Proc. of 2013 IEEE Information Theory Workshop (ITW)*, pp. 1-5, 2013. [Article \(CrossRef Link\)](#)
- [18] J. Zhu, Y. Li, N. Wang, and W. Xu, "Wireless Information and Power Transfer in Secure Massive MIMO Downlink With Phase Noise," *IEEE Wireless Commun. Lett.*, vol. 6, no. 3, pp. 298-301, Jun. 2017. [Article \(CrossRef Link\)](#)
- [19] J. Zhu, W. Xu, and N. Wang, "Secure Massive MIMO Systems With Limited RF Chains," *IEEE Trans. Veh. Technol.*, vol. 66, no. 6, pp. 5455-5460, Jun. 2017. [Article \(CrossRef Link\)](#)
- [20] J. Wang, and D. P. Palomar, "Worst-Case Robust MIMO Transmission With Imperfect Channel Knowledge," *IEEE Trans. Signal Process.*, vol. 57, no. 8, pp. 3086-3100, Aug. 2009. [Article \(CrossRef Link\)](#)
- [21] S. Ma, M. Hong, E. Song, X. Wang, and D. Sun, "Outage Constrained Robust Secure Transmission for MISO Wiretap Channels," *IEEE Trans. Wireless Commun.*, vol. 13, no. 10, pp. 5558-5570, Oct. 2014. [Article \(CrossRef Link\)](#)
- [22] 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. [Article \(CrossRef Link\)](#)
- [23] L. Li, Z. Chen, and J. Fang, "Robust transmit design for secure AF relay networks based on worst-case optimization," in *Proc. of 2014 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, Florence, Italy, pp. 2719-2723, 2014. [Article \(CrossRef Link\)](#)
- [24] 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. [Article \(CrossRef Link\)](#)
- [25] X. Zhou, Z. Rezk, B. Alomair, and M. S. Alouini, "Achievable Rates of Secure Transmission in Gaussian MISO Channel with Imperfect Main Channel Estimation," *IEEE Trans. Wireless Commun.*, vol. 15, no. 6, pp. 4470-4485, Jun. 2016. [Article \(CrossRef Link\)](#)
- [26] Q. Li, Y. Zhang, J. Lin, and S. X. Wu, "Full-Duplex Bidirectional Secure Communications Under Perfect and Distributionally Ambiguous Eavesdropper's CSI," *IEEE Trans. Signal Process.*, vol. 65, no. 17, pp. 4684–4697, Sep. 2017. [Article \(CrossRef Link\)](#)

- [27] G. C. Alexandropoulos, and K. P. Peppas, "Secrecy outage analysis over correlated composite Nakagami-m Gamma fading channels," *IEEE Commun. Lett.*, vol. 22, no. 1, pp. 77-80, Jan. 2017. [Article \(CrossRef Link\)](#)
- [28] Y. Huang, P. Zhang, Q. Wu, and J. Wang, "Secrecy performance of wireless powered communication networks with multiple eavesdroppers and outdated CSI," *IEEE Access*, vol. 6, pp. 33774-33788, 2018. [Article \(CrossRef Link\)](#)
- [29] Z. Chu, H. Xing, M. Johnston, and S. L. Goff, "Secrecy Rate Optimizations for a MISO Secrecy Channel with Multiple Multiantenna Eavesdroppers," *IEEE Trans. Wireless Commun.*, vol. 15, no. 1, pp. 283-297, Jan. 2016. [Article \(CrossRef Link\)](#)
- [30] D. W. K. Ng, E. S. Lo, and R. Schober, "Robust Beamforming for Secure Communication in Systems With Wireless Information and Power Transfer," *IEEE Trans. Wireless Commun.*, vol. 13, no. 8, pp. 4599-4615, Aug. 2014. [Article \(CrossRef Link\)](#)
- [31] C. Shen, T. H. Chang, K. Y. Wang, Z. Qiu, and C. Y. Chi, "Distributed Robust Multicell Coordinated Beamforming With Imperfect CSI: An ADMM Approach," *IEEE Trans. Signal Process.*, vol. 60, no. 6, pp. 2988-3003, Jun. 2012. [Article \(CrossRef Link\)](#)
- [32] S. Shafiee, and S. Ulukus, "Achievable Rates in Gaussian MISO Channels with Secrecy Constraints," in *Proc. of 2007 IEEE International Symposium on Information Theory*, Nice, France, pp. 2466-2470, 2007. [Article \(CrossRef Link\)](#)
- [33] L. El Ghaoui, and S. L. Niculescu, "Advances in linear matrix inequality methods in control: advances in design and control," *Society for Industrial & Applied Mathematics Philadelphia Pa*, 1999.
- [34] M. Grant and S. Boyd. (Mar. 2014). CVX: MATLAB Software for Disciplined Convex Programming, Version 2.1. [Online]. Available: <http://cvxr.com/cvx>
- [35] 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. [Article \(CrossRef Link\)](#)
- [36] A. Beck, A. Ben-Tal, and L. Tetrushvili, "A sequential parametric convex approximation method with applications to nonconvex truss topology design problems," *J. Global Optim.*, vol. 47, no. 1, pp. 29-51, May 2010. [Article \(CrossRef Link\)](#)
- [37] S. G. Nash, "Linear and Nonlinear Programming," *International Encyclopedia of the Social & Behavioral Sciences*, vol. 67, no. 2, pp. 8868-8874, 2001.



Xiaochen Liu received the B.S. and M.S. degrees in Communications Engineering from College of Communications Engineering (CCE), PLA University of Science and Technology (PLAUST), Nanjing, China, in 2013 and 2016, respectively. He received the Ph.D. degree in communications engineering from the Army Engineering University of PLA, Nanjing, China, in 2019. His research topics include wireless communication, physical layer security, signal processing and convex optimization.



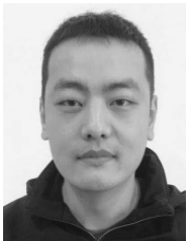
Yuan Yuan Gao received the B.S., M.S. and Ph.D. degrees in Communications Engineering from College of Communications Engineering (CCE), PLA University of Science and Technology (PLAUST), Nanjing, China, in 1990, 1994 and 2005, respectively. She is now a Full Professor with the College of Communication Engineering, Army Engineering University of PLA, Nanjing, China. Her research topics span a large spectrum including space-time coding, MIMO, cooperative communications and physical layer security.



Nan Sha received the B.S., M.S. and Ph.D. degrees in Communications Engineering from College of Communications Engineering (CCE), PLA University of Science and Technology (PLAUST), Nanjing, China, in 2003, 2006 and 2014, respectively. His research interests include physical-layer network coding and cooperative communications.



Guozhen Zang received the B.S., M.S. and Ph.D degrees in Communications Engineering from College of Communications Engineering (CCE), PLA University of Science and Technology (PLAUST), Nanjing, China, in 1999, 2002 and 2006, respectively. Her current research interests include cooperative communication, spread spectrum communications and satellite communications.



Shijie Wang received the B.S. and M.S. degrees in communications engineering from the College of Communications Engineering, PLA University of Science and Technology, Nanjing, China, in 2012 and 2015, respectively. He received the Ph.D. degree in communications engineering from the Army Engineering University of PLA, Nanjing, China, in 2019. His research topics include wireless communication, physical layer security, and stochastic geometry.