

Robust Transmit Designs for Secrecy Rate Constrained MISO NOMA System

Binbin Su
Lancaster University
Email: b.su@lancaster.ac.uk

Qiang Ni
Lancaster University
Email: q.ni@lancaster.ac.uk

Bingtao He
Xidian University
Email: hebingsu@stu.xidian.edu.cn

Abstract—This paper studies the secure transmission for downlink multiple-input single-output (MISO) non-orthogonal multiple access (NOMA) system in which imperfect channel state information (CSI) of the eavesdropper links is considered. We propose the novel robust beamforming strategies for the direct transmission NOMA (DT NOMA) and cooperative jamming NOMA (CJ NOMA) with a helper. We formulate our problem as the worst-case sum power minimization subject to secrecy rate constraint. The semidefinite relaxation (SDR) method is firstly applied to relax the quadratic terms and rank-one optimality is proved. Then an iterative algorithm based on successive convex approximation (SCA) is proposed to transform the nonconvex problem into convex approximations. Simulation results show that both the proposed NOMA schemes outperform the orthogonal multiple scheme, and CJ NOMA scheme can achieve much better system performance gain than DT NOMA scheme.

Index Terms—Non-orthogonal multiple access, worst-case based optimization, physical layer security

I. INTRODUCTION

Non-orthogonal multiple access (NOMA) is regarded as a promising candidate for 5G wireless communication systems due to its potential to significantly improve spectral efficiency [1]. Different from previous multiple access schemes, NOMA can simultaneously serve multiple users via power domain and thus significantly improves system performance. The performance of downlink NOMA with randomly deployed users was investigated in [2]. The sum rate maximization problem in the downlink single-input single-output (SISO) NOMA system has been analyzed in [3].

Due to the broadcast nature of wireless medium, wireless networks confronts severe security problems [4]. Physical layer security (PLS) has been recognized as an efficient method to meet the requirement of secure data transmission for the 5G wireless communication networks. Recently, PLS has drawn great interests for the secure transmission in NOMA networks. For example, in [5], Y. Zhang et al. investigated the secrecy sum rate optimization problem of the NOMA system. The problem of minimizing the transmit power subject to the secrecy outage constraints was studied in [6]. All the above researches are based on the assumption that

perfect channel state information (CSI) of both main channel and wiretap channel is known at the BS. However, in most wireless applications, it is difficult to get perfect CSI from the eavesdropper. Motivated by this, it is meaningful to design secure transmission schemes for MISO NOMA system, considering imperfect CSI of eavesdropper.

From the perspective of both secure transmission and energy efficient design, in this paper, we study the power minimization problem of a downlink MISO NOMA system with and without a helper, where each user has a target secrecy rate requirement. It is assumed that perfect CSI of each legitimate user is available at the base station (BS) and helper, while only imperfect CSI of the eavesdropper links is known. 1) We investigate the robust beamforming design to minimize the required power for direct transmission NOMA (DT NOMA) and cooperative jamming NOMA (CJ NOMA). 2) For both cases, the first step is to apply the semidefinite relaxation (SDR) technique to transform the original problem into a more manageable form. The rank-one optimality is proved to demonstrate the SDR tightness. 3) Then we solve the inner maximization problem over the bounded set with the S -procedure [7], and an iterative algorithm based on successive convex approximation (SCA) is applied to approximate the constraints by convex ones.

II. SYSTEM MODEL

We consider a downlink MISO transmission scenario where the BS wants to send confidential message to two users in the presence of an eavesdropper with and without a helper. The BS and the helper are both equipped with N_t antennas while the two users and the eavesdropper each have a single antenna. The channel coefficients from the BS to the i -th user, $i \in \{1, 2\}$, and Eve are denoted as \mathbf{h}_i and \mathbf{h}_e respectively. We assume that the BS has perfect CSI of two users, while only imperfect CSI of Eve is available. NOMA is adopted for information transmission, according to the principle of NOMA, the signals for two users are superpositioned at the BS, i.e., $\mathbf{x} = \mathbf{w}_1 x_1 + \mathbf{w}_2 x_2$, where x_1 and x_2 are the messages for user 1 and user 2, \mathbf{w}_1 and \mathbf{w}_2 are the corresponding precoding vectors. The power of the transmitted symbol is normalized, i.e.,

$\mathbb{E}\|x_1\|^2 = \mathbb{E}\|x_2\|^2 = 1$, The detailed process of two transmission models are described as follows.

A. Direct Transmission

For the case that there is no available helper, the received signals at two users and Eve can be modeled as

$$y_i = \mathbf{h}_i^H \mathbf{x} + n_i, \quad i = 1, 2, \quad (1a)$$

$$y_e = \mathbf{h}_e^H \mathbf{x} + n_e, \quad (1b)$$

where n_i and n_e are the noise at users and Eve, and it is assumed that n_i and n_e are zero-mean circular complex Gaussian with the same variance, i.e. $\sigma_i^2 = \sigma_e^2 = 1$.

Without loss of generality, we assume that user 1 is a strong user with better channel conditions and user 2 is a weak user. Successive interference cancellation (SIC) will be applied at user 1 to cancel the co-channel interference of user 2 and then detect the signal of user 1. With respect to user 2, the message of user 1 will be treated as noise. Therefore, the achievable codeword data rate of each user can be written as

$$R_b^1 = \log_2(1 + |\mathbf{h}_1 \mathbf{w}_1|^2), \quad (2a)$$

$$R_b^2 = \log_2\left(1 + \frac{|\mathbf{h}_2 \mathbf{w}_2|^2}{|\mathbf{h}_2 \mathbf{w}_1|^2 + 1}\right). \quad (2b)$$

Then the achievable data rate of Eve to detect each user can be given as

$$R_e^1 = \log_2(1 + |\mathbf{h}_e \mathbf{w}_1|^2), \quad (3a)$$

$$R_e^2 = \log_2\left(1 + \frac{|\mathbf{h}_e \mathbf{w}_2|^2}{|\mathbf{h}_e \mathbf{w}_1|^2 + 1}\right). \quad (3b)$$

B. Secure Transmission with Helper

When there exists a helper, in addition to the transmitted signal, the helper will generate the cooperative jamming signal to degrade the signal received by Eve. Then the two users and Eve can receive

$$y_i = \mathbf{h}_i^H \mathbf{x} + \mathbf{g}_i^H \mathbf{z} + n_i, \quad i = 1, 2, \quad (4a)$$

$$y_e = \mathbf{h}_e^H \mathbf{x} + \mathbf{g}_e^H \mathbf{z} + n_e, \quad (4b)$$

where \mathbf{g}_i and \mathbf{g}_e denotes the channel coefficients from the helper to the i -th user and Eve respectively. In this case, the corresponding data rate of users and Eve can be expressed as

$$R_{b_h}^1 = \log_2\left(1 + \frac{|\mathbf{h}_1 \mathbf{w}_1|^2}{|\mathbf{g}_1 \mathbf{z}|^2 + 1}\right), \quad (5a)$$

$$R_{b_h}^2 = \log_2\left(1 + \frac{|\mathbf{h}_2 \mathbf{w}_2|^2}{|\mathbf{h}_2 \mathbf{w}_1|^2 + |\mathbf{g}_2 \mathbf{z}|^2 + 1}\right), \quad (5b)$$

$$R_{e_h}^1 = \log_2\left(1 + \frac{|\mathbf{h}_e \mathbf{w}_1|^2}{|\mathbf{g}_e \mathbf{z}|^2 + 1}\right), \quad (5c)$$

$$R_{e_h}^2 = \log_2\left(1 + \frac{|\mathbf{h}_e \mathbf{w}_2|^2}{|\mathbf{h}_e \mathbf{w}_1|^2 + |\mathbf{g}_e \mathbf{z}|^2 + 1}\right). \quad (5d)$$

C. Channel Mismatch

For the eavesdropper links to both the BS \mathbf{h}_e , and that to the helper \mathbf{g}_e , only the estimates $\tilde{\mathbf{h}}_e$ and $\tilde{\mathbf{g}}_e$ are available at the BS. Therefore, the channels can be characterized as follows respectively:

$$\mathbf{h}_e = \tilde{\mathbf{h}}_e + \tilde{\mathbf{e}}_{h_e}, \quad (6a)$$

$$\mathbf{g}_e = \tilde{\mathbf{g}}_e + \tilde{\mathbf{e}}_{g_e}. \quad (6b)$$

The channel mismatches are assumed to lie in the bounded sets as $\varepsilon_{h_e} = \{\tilde{\mathbf{e}}_{h_e} : \|\tilde{\mathbf{e}}_{h_e}\|^2 \leq \epsilon_{h_e}^2\}$ and $\varepsilon_{g_e} = \{\tilde{\mathbf{e}}_{g_e} : \|\tilde{\mathbf{e}}_{g_e}\|^2 \leq \epsilon_{g_e}^2\}$, where $\epsilon_{h_e}^2$ and $\epsilon_{g_e}^2$ are known constants.

III. ROBUST DIRECTION TRANSMISSION

In this section, we will examine the system performance where there is no jamming support from the helper. The secrecy rate of two users is given as [8]

$$R_s^1 = R_b^1 - R_e^1, \quad (7a)$$

$$R_s^2 = R_b^2 - R_e^2. \quad (7b)$$

We consider the case where perfect CSI of users is available while only imperfect CSI of eavesdropper link is known at the BS. The goal is to minimize the transmission power while satisfying secrecy rate requirement for the worst-case based channel mismatch $\tilde{\mathbf{e}}_h$ in the bounded set ϵ_h , which leads to the following optimization problem

$$\text{P1: } \min_{\mathbf{w}_1, \mathbf{w}_2} \max_{\tilde{\mathbf{e}}_{h_e} \in \epsilon_{h_e}} \|\mathbf{w}_1\|_2^2 + \|\mathbf{w}_2\|_2^2 \quad (8a)$$

$$\text{s.t. } R_b^1 - R_e^1 \geq \gamma_1, \quad (8b)$$

$$R_b^2 - R_e^2 \geq \gamma_2, \quad (8c)$$

where γ_1 and γ_2 are target secrecy data rate of two users.

By introducing two auxiliary variables $\beta_1 \geq 0$, $\beta_2 \geq 0$, and equation (2) and (3), P1 is equivalent to

$$\text{P2: } \min_{\beta_1, \beta_2, \mathbf{w}_1, \mathbf{w}_2} \max_{\tilde{\mathbf{e}}_{h_e} \in \epsilon_{h_e}} \|\mathbf{w}_1\|_2^2 + \|\mathbf{w}_2\|_2^2 \quad (9a)$$

$$\text{s.t. } \log_2(1 + |\mathbf{h}_e \mathbf{w}_1|^2) \leq \beta_1, \quad (9b)$$

$$\beta_1 \leq \log_2(1 + |\mathbf{h}_1 \mathbf{w}_1|^2) + \gamma_1, \quad (9c)$$

$$\log_2\left(1 + \frac{|\mathbf{h}_e \mathbf{w}_2|^2}{|\mathbf{h}_e \mathbf{w}_1|^2 + 1}\right) \leq \beta_2, \quad (9d)$$

$$\beta_2 \leq \log_2\left(1 + \frac{|\mathbf{h}_2 \mathbf{w}_2|^2}{|\mathbf{h}_2 \mathbf{w}_1|^2 + 1}\right) + \gamma_2. \quad (9e)$$

It can be easily verified that problem P2 is non-convex. This is not only due to the logarithm terms of the constraints, but also for the inner minimization over $\tilde{\mathbf{e}}_{h_e}$. To solve it, we will firstly relax the original problem by SDR approach. To illustrate the SDR approach, we replace the beamforming vector \mathbf{w}_i by semidefinite positive matrices \mathbf{W}_i , i.e.,

$$\mathbf{W}_i = \mathbf{w}_i \mathbf{w}_i^H \succeq 0, \quad i = 1, 2. \quad (10)$$

By adopting the SDR technique and leading several slack variables, problem P2 can be further reformulated as

$$P3 : \min_{\beta_1, \beta_2, \mathbf{w}_1, \mathbf{w}_2} \max_{\tilde{\mathbf{e}}_{h_e} \in \epsilon_{h_e}} \text{Tr}(\mathbf{W}_1) + \text{Tr}(\mathbf{W}_2) \quad (11a)$$

$$s.t. \quad \text{Tr}(\mathbf{H}_e \mathbf{W}_1) \leq t_1, \quad (11b)$$

$$t_1 \leq 2^{\beta_1} - 1, \quad (11c)$$

$$\text{Tr}(\mathbf{H}_e \mathbf{W}_2) \leq t_2, \quad (11d)$$

$$t_2 \leq (2^{\beta_2} - 1)(\text{Tr}(\mathbf{H}_e \mathbf{W}_1) + 1), \quad (11e)$$

$$2^{\beta_1 + \gamma_1} - 1 \leq \text{Tr}(\mathbf{H}_1 \mathbf{W}_1), \quad (11f)$$

$$2^{\beta_2 + \gamma_2} - 1 \leq \frac{\text{Tr}(\mathbf{H}_2 \mathbf{W}_2)}{\text{Tr}(\mathbf{H}_2 \mathbf{W}_1) + 1}. \quad (11g)$$

Proposition 1: P3 always has an optimal solution $(\mathbf{W}_1^*, \mathbf{W}_2^*)$ with $\text{rank}(\mathbf{W}_i) = 1$, $i=1,2$, whenever it is feasible.

Proof: The proof is provided in Appendix A.

To investigate the maximization over $\tilde{\mathbf{e}}_{h_e}$, constraint (11b) can also be expressed as

$$(\tilde{\mathbf{h}}_e + \tilde{\mathbf{e}}_{h_e})^H \mathbf{W}_1 (\tilde{\mathbf{h}}_e + \tilde{\mathbf{e}}_{h_e}) \leq 0, \quad (12a)$$

$$\tilde{\mathbf{e}}_{h_e}^H \tilde{\mathbf{e}}_{h_e} \leq \epsilon_{h_1}^2, \quad (12b)$$

which is equivalent to

$$-\tilde{\mathbf{e}}_h^H \mathbf{W}_1 \tilde{\mathbf{e}}_h + 2\text{Re} \left(\tilde{\mathbf{h}}_e^H \mathbf{W}_1 \tilde{\mathbf{h}}_e \right) - \tilde{\mathbf{h}}_e^H \mathbf{W}_1 \tilde{\mathbf{h}}_e + t_1 \geq 0, \quad (13a)$$

$$-\tilde{\mathbf{e}}_{h_1}^H \tilde{\mathbf{e}}_{h_1} + \epsilon_{h_1}^2 \geq 0, \quad (13b)$$

By using the S -procedure [7], we know that both (13a) and (13b) can be satisfied with a proper $\tilde{\mathbf{e}}_{h_e}$ if and only if there exists a $\nu_1 \geq 0$ such that

$$\begin{bmatrix} \nu_1 \mathbf{I}_{N_t} - \mathbf{W}_1 & -\mathbf{W}_1 \tilde{\mathbf{h}}_e \\ -\tilde{\mathbf{h}}_e^H \mathbf{W}_1 & -\tilde{\mathbf{h}}_e^H \mathbf{W}_1 \tilde{\mathbf{h}}_e - \nu_1 \epsilon_{h_e}^2 + t_1 \end{bmatrix} \succeq 0, \quad (14)$$

With the same method, denote that $t = 1 - t_3$, constraint (11d) and (11e) can be reformulated as

$$\begin{bmatrix} \nu_2 \mathbf{I}_{N_t} - \mathbf{W}_2 & -\mathbf{W}_2 \tilde{\mathbf{h}}_e \\ -\tilde{\mathbf{h}}_e^H \mathbf{W}_2 & -\tilde{\mathbf{h}}_e^H \mathbf{W}_2 \tilde{\mathbf{h}}_e - \nu_2 \epsilon_{h_e}^2 + t_2 \end{bmatrix} \succeq 0, \quad (15a)$$

$$\begin{bmatrix} \nu_3 \mathbf{I}_{N_t} - \mathbf{W}_1 & -\mathbf{W}_1 \tilde{\mathbf{h}}_e \\ -\tilde{\mathbf{h}}_e^H \mathbf{W}_1 & -\tilde{\mathbf{h}}_e^H \mathbf{W}_1 \tilde{\mathbf{h}}_e - \nu_3 \epsilon_{h_e}^2 + t \end{bmatrix} \succeq 0, \quad (15b)$$

$$\frac{t_2}{t_4} \leq t_3, \quad (15c)$$

$$t_4 \leq 2^{\beta_2 - 1}. \quad (15d)$$

Besides, (11c) and (15d) can be approximated by first-order Taylor approximation as follows

$$\ln(t_1^{(n)} + 1) + \frac{1}{t_1^{(n)} + 1} (t_1 - t_1^{(n)} + 1) \leq \beta_1 \ln 2, \quad (16a)$$

$$\ln(t_4^{(n)} + 1) + \frac{1}{t_4^{(n)} + 1} (t_4 - t_4^{(n)} + 1) \leq \beta_2 \ln 2, \quad (16b)$$

where $t_1^{(n)}$ and $t_4^{(n)}$ represent the value of t_1 and t_4 at the n -th iteration respectively.

As to (15c), by epigraph reformulation it can be equivalently written as

$$\mu^2 \geq t_2, \quad (17a)$$

$$\begin{bmatrix} t_3 & \mu \\ \mu & t_4 \end{bmatrix} \succeq 0, \quad (17b)$$

which consists of a nonconvex quadratic inequality constraint (17a) and a convex linear matrix inequality (LMI) (17b).

Performing the first-order Taylor approximation, a convex lower bound of (17a) can be obtained as

$$2\mu^{(n)}\mu - (\mu^{(n)})^2 \geq t_2, \quad (18)$$

where $\mu^{(n)}$ denote the value of μ at the n -th iteration.

The only remaining nonconvex constraint is (11g). As perfect CSI of users is available, denote that $\alpha = 2^{\beta_2 + \gamma_2} - 1$, we can use arithmetic-geometric mean (AGM) inequality-based method to get a convex approximation

$$(\kappa^{(n)}\alpha)^2 + (\text{Tr}(\mathbf{H}_2 \mathbf{W}_1)/\kappa^{(n)})^2 \leq 2\text{Tr}(\mathbf{H}_2 \mathbf{W}_2) - 2\alpha, \quad (19)$$

where $\kappa^{(n)}$ represents the value of κ at the n -th iteration and can be updated as

$$\kappa^{(n)} = \sqrt{\text{Tr}(\mathbf{H}_2 \mathbf{W}_1)^{(n-1)}/\alpha}. \quad (20)$$

Therefore, the problem has been transformed into convex formulation and during the n -th iteration, we need to solve the following problem:

$$P4 : \min_{\alpha, \kappa, \mathbf{w}_1, \mathbf{w}_2} \text{Tr}(\mathbf{W}_1) + \text{Tr}(\mathbf{W}_2) \quad (21a)$$

$$s.t. \quad (\kappa^{(n)}\alpha)^2 + (\text{Tr}(\mathbf{H}_2 \mathbf{W}_1)/\kappa^{(n)})^2 \leq 2\text{Tr}(\mathbf{H}_2 \mathbf{W}_2) - 2\alpha, \quad (21b)$$

$$(11f), (14), (15a), (15b), (16a), (16b), (17b), (18), \quad (21c)$$

which is a convex problem that can be efficiently solved with existing solvers.

Accordingly, the SCA-based iterative algorithm is outlined as Algorithm 1.

Algorithm 1 SCA-based method to solve P4

- 1: Initialization: given randomly feasible solution $\Lambda^{(0)}$.
 - 2: $n=0$;
 - 3: Repeat
 - 4: Solve problem P4;
 - 5: Set $n = n + 1$;
 - 6: Update $\mu^{(n)}, \kappa^{(n)}$;
 - 7: Until Convergence or required number of iterations.
-

The convergence of the SCA method has been verified by [9] which means that the proposed Algorithm 1 converges to a KKT point of problem P1.

IV. ROBUST COOPERATIVE JAMMING

In this section, the helper provides cooperative jamming to increase the secrecy rate and we want to solve the following optimization problem

$$\text{P5: } \min_{\mathbf{w}_1, \mathbf{w}_2, \mathbf{z}} \max_{\tilde{\mathbf{e}}_h \in \epsilon_h} \|\mathbf{w}_1\|_2^2 + \|\mathbf{w}_2\|_2^2 + \|\mathbf{z}\|_2^2 \quad (22a)$$

$$s.t. \quad R_{e_h}^1 \leq \beta_1 \leq R_{b_h}^1 + \gamma_1, \quad (22b)$$

$$R_{e_h}^2 \leq \beta_2 \leq R_{b_h}^2 + \gamma_2, \quad (22c)$$

By substituting (5a)-(5d) and after some mathematical reformulation, problem P5 can be described as

$$\text{P6: } \min_{\mathbf{w}_1, \mathbf{w}_2, \mathbf{z}} \max_{\tilde{\mathbf{e}}_h \in \epsilon_h} \|\mathbf{w}_1\|_2^2 + \|\mathbf{w}_2\|_2^2 + \|\mathbf{z}\|_2^2 \quad (23a)$$

$$s.t. \quad |\mathbf{h}_e \mathbf{w}_1|^2 \leq t_1, \quad (23b)$$

$$t_1 \leq (2^{\beta_1} - 1)(|\mathbf{g}_e \mathbf{z}|^2 + 1), \quad (23c)$$

$$|\mathbf{h}_e \mathbf{w}_2|^2 \leq t_2, \quad (23d)$$

$$t_2 \leq (2^{\beta_2} - 1)(|\mathbf{h}_e \mathbf{w}_1|^2 + |\mathbf{g}_e \mathbf{z}|^2 + 1), \quad (23e)$$

$$2^{\beta_1 + \gamma_1} - 1 \leq \frac{|\mathbf{h}_1 \mathbf{w}_1|^2}{|\mathbf{g}_1 \mathbf{z}|^2 + 1}, \quad (23f)$$

$$2^{\beta_2 + \gamma_2} - 1 \leq \frac{|\mathbf{h}_2 \mathbf{w}_2|^2}{|\mathbf{h}_2 \mathbf{w}_1|^2 + |\mathbf{g}_2 \mathbf{z}|^2 + 1}. \quad (23g)$$

The first step is also to apply the SDR technique. One can note that the jamming signal is noise and we do not need to decode it, therefore, the covariance of the jamming signal is not required to be rank-one. As to \mathbf{W}_1 and \mathbf{W}_2 , the proof is similar to proposition 1.

We can see that constraint (23b) and (23d) have already been solved in the last section. Constraint (23c) can be reformulated as below by the S -procedure

$$\begin{bmatrix} \nu_3 \mathbf{I}_{N_t} + \mathbf{Z} & \mathbf{Z} \tilde{\mathbf{g}}_e \\ \tilde{\mathbf{g}}_e^H \mathbf{Z} & \tilde{\mathbf{g}}_e^H \mathbf{Z} \tilde{\mathbf{g}}_e - \nu_3 \epsilon_{g_e}^2 + 1 - t_3 \end{bmatrix} \succeq 0, \quad (24a)$$

$$\begin{bmatrix} t_3 & \mu \\ \mu & t_4 \end{bmatrix} \succeq 0, \quad (24b)$$

$$2\mu_1^{(n)} \mu_1 - (\mu_1^{(n)})^2 \geq t_1, \quad (24c)$$

$$\ln(t_4^{(n)} + 1) + \frac{1}{t_4^{(n)} + 1} (t_4 - t_4^{(n)} + 1) \leq \beta_1 \ln 2. \quad (24d)$$

(23e) can be reformulated as

$$\begin{bmatrix} \nu_4 \mathbf{I}_{N_t} + \mathbf{W}_1 & \mathbf{W}_1 \tilde{\mathbf{h}}_e \\ \tilde{\mathbf{h}}_e^H \mathbf{W}_1 & \tilde{\mathbf{h}}_e^H \mathbf{W}_1 \tilde{\mathbf{h}}_e + t_5 - \nu_4 \epsilon_{h_e}^2 - t_6 \end{bmatrix} \succeq 0, \quad (25a)$$

$$\begin{bmatrix} \nu_5 \mathbf{I}_{N_t} + \mathbf{Z} & \mathbf{Z} \tilde{\mathbf{g}}_e \\ \tilde{\mathbf{g}}_e^H \mathbf{Z} & \tilde{\mathbf{g}}_e^H \mathbf{Z} \tilde{\mathbf{g}}_e - \nu_5 \epsilon_{g_e}^2 - t_5 \end{bmatrix} \succeq 0, \quad (25b)$$

$$\begin{bmatrix} t_6 & \mu_2 \\ \mu_2 & t_7 \end{bmatrix} \succeq 0, \quad (25c)$$

$$2\mu_2^{(n)} \mu_2 - (\mu_2^{(n)})^2 \geq t_2, \quad (25d)$$

$$\ln(t_7^{(n)} + 1) + \frac{1}{t_7^{(n)} + 1} (t_7 - t_7^{(n)} + 1) \leq \beta_2 \ln 2. \quad (25e)$$

For constraint (23f) and (23g), denote $\alpha_1 = 2^{\beta_1 + \gamma_1} - 1$, $\alpha_2 = 2^{\beta_2 + \gamma_2} - 1$ and $\phi = \text{Tr}(\mathbf{H}_2 \mathbf{W}_1) + \text{Tr}(\mathbf{G}_1 \mathbf{Z})$, AGM inequality can be used to get convex approximation as below

$$(\kappa_1^{(n)} \alpha_1)^2 + (\text{Tr}(\mathbf{G}_1 \mathbf{Z}) / \kappa_1^{(n)})^2 \leq 2\text{Tr}(\mathbf{H}_1 \mathbf{W}_1) - 2\alpha_1, \quad (26a)$$

$$(\kappa_2^{(n)} \alpha_2)^2 + (\phi / \kappa_2^{(n)})^2 \leq 2\text{Tr}(\mathbf{H}_2 \mathbf{W}_2) - 2\alpha_2, \quad (26b)$$

where $\kappa_1^{(n)}$ and $\kappa_2^{(n)}$ can be updated as

$$\kappa_1^{(n)} = \sqrt{(\text{Tr}(\mathbf{G}_1 \mathbf{Z})^{(n-1)} / \alpha_1^{(n-1)})}, \quad (27a)$$

$$\kappa_2^{(n)} = \sqrt{\phi^{(n-1)} / \alpha_2^{(n-1)}}. \quad (27b)$$

As a result, the original problem has been approximated as a convex program. We can solve the following convex optimization problem at the n -th iteration

$$\text{P7: } \min_{\beta, \mathbf{w}_1, \mathbf{w}_2} \text{Tr}(\mathbf{W}_1) + \text{Tr}(\mathbf{W}_2) + \text{Tr}(\mathbf{Z}) \quad (28a)$$

$$s.t. \quad (14), (15a), (24a), (24b), (25a), \quad (28b)$$

$$(25b), (25c), (25d), (25e), (26a) \text{ and } (26b). \quad (28c)$$

The algorithm to solve P7 is similar to Algorithm 1 and omitted here due to space limitation.

V. NUMERICAL RESULTS

In this section, we present numerical results to examine the performance of the proposed robust transmission schemes through Monte Carlo simulations for Rayleigh fading channel. In the following simulations, it is assumed that the BS is located at the origin, user 1 is randomly deployed within a disc of 3 meters, while the distance from user 2 and Eve to the BS is between 3 meters and 6 meters. We assume that the BS and the Helper both have six antennas, i.e., $N_t=6$. All the background noise power is assumed to be 1, and the transmit power is defined in dB relative to the noise power. All results are calculated by solving the robust optimization problem for 2,000 times. We will evaluate the performance of direct transmission NOMA (DT NOMA) and cooperative jamming NOMA (CJ NOMA) schemes. Also, cooperative jamming TDMA (CJ TDMA) is introduced to act as a comparable scheme.

Fig. 1 shows the impact of desired secrecy rate for DT NOMA, CJ NOMA and traditional CJ TDMA schemes, assuming the channel mismatch bounds $\tilde{\mathbf{e}}_{h_e} = \tilde{\mathbf{e}}_{g_e} = 0.01$ and two users have the same target rate $\gamma_1 = \gamma_2$. It can be seen from the figure that the robust design for DT NOMA and CJ NOMA yields better performance than the traditional TDMA scheme. For example, when the desired secrecy rate is 1.5 bit/s/Hz, the required transmit power for DT NOMA and CJ NOMA are 1.5 dB and 1.59 dB respectively, while for CJ TDMA scheme, it needs 1.9 dB. Besides, when the desired secrecy rate increases, the gap between NOMA and TDMA becomes

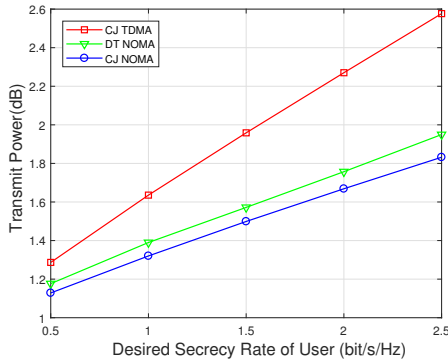


Fig. 1. Worst-case measured transmit power vs. desired secrecy rate of user.

larger, implying that NOMA scheme works significantly better with a higher secrecy rate.

In Fig. 2, the target secrecy rate is given as $\gamma_1=\gamma_2=1$ bit/s/Hz and we investigate the impact of increasing the value of the channel mismatch on the required transmit power. We observe that although the transmit power increases for all of the schemes as the error variance becomes bigger, the benefit of NOMA over TDMA is obvious since DT NOMA and CJ NOMA requires much less power to satisfy certain error variance. Results also suggest that, the error variance has little influence on the scheme of CJ NOMA compared with DT NOMA, which proves that cooperative jamming with a helper can provide better system performance than direct transmission in NOMA design.

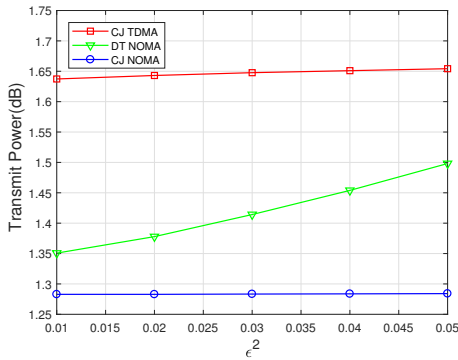


Fig. 2. Worst-case measured transmit power vs. channel mismatch.

VI. CONCLUSION

In this paper, we have investigated the robust beamforming designs of MISO NOMA wiretap channels to minimize the transmit power for both direct transmission and cooperative jamming scenario with a helper based on worst-case optimization, under the assumption that the CSI for the eavesdropper is imperfect. We have equivalently transformed the formulated nonconvex optimization problem with SDR method by proving the rank-one optimality. Then the reformulated problem

can be readily transformed into convex approximations with an iterative SCA-based method. The main results show that NOMA can decrease transmit power for both direct transmission and cooperative jamming by careful beamforming design compared with OMA which demonstrates the superiority of NOMA.

APPENDIX A PROOF OF PROPOSITION 1

P3 is equivalent to the following problem:

$$P8: \min_{\beta_1, \beta_2, \mathbf{w}_1, \mathbf{w}_2} \max_{\tilde{\mathbf{e}}_{h_e} \in \epsilon_{h_e}} \text{Tr}(\mathbf{W}_1) + \text{Tr}(\mathbf{W}_2) \quad (29a)$$

$$s.t. \quad \text{Tr}(\mathbf{H}_e \mathbf{W}_1) \leq 2^{\beta_1} - 1, \quad (29b)$$

$$\text{Tr}(\mathbf{H}_e \mathbf{W}_2) \leq (2^{\beta_2} - 1)(\text{Tr}(\mathbf{H}_e \mathbf{W}_1) + 1), \quad (29c)$$

$$2^{\beta_1 + \gamma_1} - 1 \leq \text{Tr}(\mathbf{H}_1 \mathbf{W}_1), \quad (29d)$$

$$(2^{\beta_2 + \gamma_2} - 1)(\text{Tr}(\mathbf{H}_2 \mathbf{W}_1) + 1) \leq \text{Tr}(\mathbf{H}_2 \mathbf{W}_2). \quad (29e)$$

Assume that P8 is feasible and it is also dual feasible. As can be seen from problem P8, there are four linear constraints related to the optimal solution $(\mathbf{W}_1^*, \mathbf{W}_2^*)$ and according to [10, Theorem 3.2], we have that:

$$\text{rank}^2(\mathbf{W}_1^*) + \text{rank}^2(\mathbf{W}_2^*) \leq 4. \quad (30)$$

If P8 is feasible, from (29b), we can find that $\mathbf{W}_1^* \succeq \mathbf{0}$ and $\mathbf{W}_1^* \neq \mathbf{0}$; for (29c), we have that $\mathbf{W}_2^* \succeq \mathbf{0}$ and $\mathbf{W}_2^* \neq \mathbf{0}$. Furthermore, considering the constraint (30), we can conclude that only when $\text{rank}(\mathbf{W}_i) = 1$, $i=1,2$, the inequality can be satisfied. If $\text{rank}(\mathbf{W}_1^*) = \text{rank}(\mathbf{W}_2^*) = 1$, then the optimal beamforming vector \mathbf{w}_1^* and \mathbf{w}_2^* can be obtained from \mathbf{W}_1^* and \mathbf{W}_2^* by eigen-decomposition respectively.

REFERENCES

- [1] Y. Saito, Y. Kishiyama, A. Benjebbour, T. Nakamura, A. Li, and K. Higuchi, "Non-orthogonal multiple access (NOMA) for cellular future radio access," in *VTC Spring*, 2013, pp. 1–5.
- [2] Z. Ding, Z. Yang, P. Fan, and H. V. Poor, "On the performance of non-orthogonal multiple access in 5G systems with randomly deployed users," *IEEE Signal. Proc. Lett.*, vol. 21, no. 12, pp. 1501–1505, 2014.
- [3] Z. Yang, W. Xu, C. Pan, Y. Pan, and M. Chen, "On the optimality of power allocation for noma downlinks with individual QoS constraints," *IEEE Commun. Lett.*, 2017.
- [4] A. D. Wyner, "The wire-tap channel," *Bell Labs Tech. J.*, vol. 54, no. 8, pp. 1355–1387, 1975.
- [5] Y. Zhang, H.-M. Wang, Q. Yang, and Z. Ding, "Secrecy sum rate maximization in non-orthogonal multiple access," *IEEE Commun. Lett.*, vol. 20, no. 5, pp. 930–933, 2016.
- [6] B. He, A. Liu, N. Yang, and V. K. Lau, "On the design of secure non-orthogonal multiple access systems," *IEEE J. Sel. Areas Commun.*, vol. 35, no. 10, pp. 2196–2206, 2017.
- [7] S. Boyd and L. Vandenberghe, *Convex optimization*. Cambridge university press, 2004.
- [8] 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, 2012.
- [9] B. R. Marks and G. P. Wright, "A general inner approximation algorithm for nonconvex mathematical programs," *Oper. Res.*, vol. 26, no. 4, pp. 681–683, 1978.
- [10] Y. Huang and D. P. Palomar, "Rank-constrained separable semidefinite programming with applications to optimal beamforming," *IEEE Trans. Signal Process.*, vol. 58, no. 2, pp. 664–678, 2010.