This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TWC.2020.3021725, IEEE Transactions on Wireless Communications

Robust Secure Beamforming Design for Two-user Downlink MISO Rate-Splitting Systems

Hao Fu, Suili Feng, *Member, IEEE,*, Weijun Tang, and Derrick Wing Kwan Ng, *Senior Member, IEEE*

***Abstract*—In this paper, we consider max-min fairness for a downlink two-user multi-input single-output (MISO) system with imperfect channel state information available at transmitter (CSIT) taking into account the total power constraint and the physical layer security. Considering the worst-case channel uncertainty for a potential eavesdropper (PE), we study the robust secure beamforming algorithm design which maximizes the minimum achieved worst-case secrecy rate among single-antenna legitimate users. In contrast to existing schemes adopted in the literatures, we propose a rather unorthodox rate splitting (RS) scheme which advocates the dual use of a common message serving both as a desired message and artificial noise (AN) for legitimate users and the PE, respectively. The algorithm design is formulated as a non-convex optimization problem which is generally intractable. As a compromise approach, we apply the successive convex approximation (SCA) method which facilitates the design of a low-complexity suboptimal iterative algorithm. In each iteration, a rank-constrained semi-definite program (SDP) is solved optimally by SDP relaxation (SDR). Simulation results demonstrate that our proposed robust secure beamforming scheme in the MISO-RS secure transmission system outperforms that of the non-robust counterpart. Moreover, our results also unveil that the proposed RS scheme can achieve a superior performance compared to the existing non-orthogonal multiple access (NOMA) schemes and the traditional scheme.**

***Index Terms*—Rate splitting, physical layer security, robust beamforming, max-min fairness, worst-case optimization.**

I. INTRODUCTION

UBIQUITOUS and high data-rate communications are the basic requirements for the next generation wireless communication systems. In practice, multi-antenna techniques have been extensively investigated from the perspective of providing ultra-high throughput, enhanced capacity, and reliable communication service for 5G and beyond 5G [1]-[3]. However, due to the broadcast nature of the wireless medium, security has become a crucial issue for wireless communication systems, which has received much attention in both academia and industry [4]-[25].

Traditionally, secure communication is achieved by applying cryptographic encryption methods which are based on the assumption of limited computational capabilities of potential eavesdroppers and the availability of perfect secure key management [4]. However, with the advanced development of new computing technologies (e.g. quantum computers), this assumption will no longer valid in future networks. Hence, a large amount of works have been devoted to information-theoretic physical (PHY) layer security, e.g. [4]-[25], as an alternative or complement to cryptographic encryption methods. The principle of PHY layer security is to exploit the physical characteristics of a wireless fading channel for providing perfect secrecy communication, which was firstly proposed by Wyner [6] focusing on a classical wire-tap channel. In particular, to guarantee the PHY layer security, the legitimate user is required to maintain a better channel condition than that of the eavesdroppers. However, this may not be always possible in practice. Inspired by this, to alleviate the dependence of secrecy performance on the channel condition, a promising approach is to exploit the beamforming technique in multi-antenna systems, which can focus the transmit power on the directions of legitimate users while reducing the potential of power leakage to eavesdroppers. For example, [7] and [8] studied the design of secure beamforming for cooperative cognitive radio networks. Also, the secure beamforming problem for simultaneous wireless information and power transfer (SWIPT) networks was investigated in [9], [10]. Besides, [11] pioneered the study of PHY layer security in heterogeneous networks. Furthermore, in [12], the authors studied secure wideband beamforming for two-way relaying systems recently. Also, the power-efficient secure beamforming algorithm designed for multiuser full-duplex wireless communication systems was investigated in [13]. In addition, there are growing research interests in secrecy communication over non-orthogonal multiple access (NOMA) transmission schemes and [14]-[17] investigated secure beamforming for NOMA systems under various system settings.

Among different multi-antenna techniques, artificial noise (AN) is one of the most effective means for guaranteeing secure communication. In particular, the designed AN can be deliberately injected into the wireless communication channels to impair the received signal quality at the eavesdroppers. In fact, the notion of adopting AN to enhance the PHY layer security was first introduced in [18] and has received much attention in recent studies, e.g. [17], [19]-[30]. In practice, the design of AN depends on the availability of the eavesdropper's channel state information at the transmitter (E-CSIT). For instance, if E-CSIT is not available, isotropic AN was proposed in [18]-[20], where AN is uniformly radiated over the null space of spatial channels spanned by legitimate users to avoid

This work is supported in part by the Guangdong Science and Technology Plan under Grant 2016A010101009, and in part by the Fundamental Research Funds for the Central Universities. D. W. K. Ng is supported by funding from the UNSW Digital Grid Futures Institute, UNSW, Sydney, under a cross-disciplinary fund scheme and by the Australian Research Council's Discovery Project (DP190101363).

Hao Fu, Suili Feng, and Weijun Tang are with the School of Electronic and Information Engineering, South China University of Technology, Guangzhou 510641, China (e-mail: eehaofu@mail.scut.edu.cn; fengsl@scut.edu.cn; tangwj@scut.edu.cn).

Derrick Wing Kwan Ng is with the School of Electrical Engineering and Telecommunications, University of New South Wales, Sydney, NSW 2052, Australia (e-mail: w.k.ng@unsw.edu.au).

undesired interference. In contrast, when perfect E-CSIT is available, the transmitter can effectively degrade the channel quality of the eavesdroppers by generating the optimized spatially selective AN, rather than isotropic AN [18]-[20]. However, perfect E-CSIT may not be always available at the transmitter in practice. As a result, the design of a robust secure transmit scheme with only the imperfect E-CSIT is an important issue, which is a more general and realistic problem. Thus, tackling imperfect E-CSIT in PHY layer security provisioning has become presently an emerging subject pursued via different approaches, e.g., the worst-case robust designs [25]-[28] and the outage-based robust designs [28]-[30]. To realize the improvement of the PHY layer secrecy sum-rate performance, one also needs to consider the transmission rate of legitimate users. As a result, multi-user (MU)-MISO downlink broadcasting has been considered to as a viable solution to improve secure data rate of the legitimate users. In fact, with perfect CSIT, traditional linear beamforming methods can be adopted to suppress inter-user interference efficiently. However, with the increasing development of the cellular Internet-of-Things (IoT), the future wireless networks are expected to support heterogeneous services over limited radio spectrum [11], [23]. On the other hand, the task for acquiring highly accurate and up-to-date CSIT becomes more challenging due to the mobility of users. Thus, it is expected that the existence of imperfect CSIT may magnify the impact of inter-user interference with the increasing transmit power, resulting in a system performance bottleneck of MU-MISO networks [1], [31].

For relieving the bottleneck created by inter-user interference, rate splitting multiple access (RSMA)-based transmission scheme, considered as a promising and powerful transmission technique, was firstly proposed in [32]. In fact, RSMA is a generalization framework which softly bridges NOMA and spatial division multiple access (SDMA). Thus, it has attracted attention widely [31], [33]-[43]. For example, the sum-rate performance of a system with limited channel feedback was analyzed in [33]. The sum rate performance of the RSMA scheme was maximized through several kinds of beamforming designs in [34]-[36]. Besides, the concept of RSMA was also extended to overloaded systems [37] and robust transmission systems with the consideration of imperfect CSIT [38]-[40], while the energy efficiency of RSMA was investigated in [41]. However, to the best of our knowledge, research on robust beamforming design for downlink RSMA secure transmission systems has not been reported, yet. Besides, as a special form of RSMA [42], although the secure transmission problem of NOMA systems has been widely investigated under various scenario settings in existing literature [14]-[17], [44], [45]. Yet, the non-orthogonal superimposed parts are treated as “waste” and assumed to be removed by SIC for both legitimate users and eavesdropper. Thus, the eavesdropper has a chance to decode some superimposed streams and eavesdrop the other streams with less interference, which would impair the security of the whole system.

In this paper, we propose the dual use of the common message for RSMA secure transmission systems, which is served as AN signal to confuse the potential eavesdropper (PE) and is adopted as a useful message to improve legitimate transmission sum-rate. Also, both robust transmission and max-min fairness are considered in the proposed scheme. Since the existing algorithms and solutions proposed by [14]-[17], [44], [45] are not applicable to the considered situation due to different natures of problems, it is desired to design advanced resource allocation strategy to optimize secure beamforming for secure communication provisioning. The main contributions of this paper are listed as below:

1) We pioneer the study of the application of RSMA framework in two-user MISO secure transmission systems with imperfect CSIT of the PE. Consider the possibility that the PE pretends to be a legitimate user to handle the common message as a legitimate user, we propose a novel secure transmission framework where the common message is adopted both as a useful message and AN signal for legitimate users and the PE, respectively. Furthermore, as NOMA transmission scheme is a subcase of RSMA scheme [42], we also apply our proposed secure transmission strategy to the NOMA scheme.

2) To simultaneously guarantee the fairness among users and the robustness during transmission, the considered robust secure beamforming design strategy is formulated as a non-convex problem which maximizes the minimum worst-case achievable secure user rate, while taking into account the impact of the imperfect CSIT of the PE (CSIT-PE). In order to solve the resulting intractable non-convex problem, we derive an equivalent reformulated problem of the original problem and propose a corresponding suboptimal iteration algorithm based on alternating optimization (AO) principle. In each iteration, an intermediate iteration problem is handled by employing several convex optimization methods, i.e., epigraph transformation, semi-definite relaxation (SDR), and successive convex approximation (SCA). Besides, the proposed optimization framework generally subsumes the case of the perfect CSIT-PE.

3) For the imperfect CSIT case of the PE under the worst-case channel uncertainty model, we derive the closed-form expressions of intermediate optimization variables by applying Cauchy-Schwartz inequality to ensure that the worst system performance is maximized in each iteration of the AO-based optimization algorithm. Moreover, the tightness of the SDR is verified and the convergence of the proposed algorithm to a Karush-Kuhn-Tucker (KKT) point is proved analytically.

4) Simulation results show that the proposed secure transmission schemes achieve a significantly higher system secure performance compared with several baseline schemes. Specifically, the proposed optimization framework is robust against the imperfect CSIT-PE in guaranteeing secure communication. Moreover, the proposed RSMA scheme always outperforms than that of the proposed NOMA scheme. Furthermore, the secrecy sum-rate performance obtained by DPC is also added as a benchmark for showing the quality of the KKT solution achieved by our proposed methodology. In addition, beam patterns are provided for the same scenario to unveil significant insights on the secure performance gains of MISO-RSMA scheme compared to other schemes. In particular, the proposed MISO-RSMA scheme can obtain extra protection from the dual use of the common message, which is not possible via

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TWC.2020.3021725, IEEE Transactions on Wireless Communications

traditional baseline schemes.

A. Notation

We adopt boldface capital and lower case letters to denote matrices and vectors, respectively. $\mathbf{A}^H$, $\mathrm{Tr}(\mathbf{A})$, and $\mathrm{Rank}(\mathbf{A})$ represent the Hermitian transpose, trace, and rank of matrix $\mathbf{A}$, respectively. $\mathbf{A} \succeq \mathbf{0}$ indicates that $\mathbf{A}$ is a positive semidefinite matrix. $\mathbb{H}^N$ represents the set of all N-by-N complex Hermitian matrices. $\mathbb{E}\{\cdot\}$ refers to the statistical expectation. $\mathbb{C}^{N\times N}$ denotes the $N\times N$ complex space. $\|\cdot\|$ is the Euclidean norm. $\mathbf{I}_N$ is the $N\times N$ identity matrix. $[a]^+$ stands for $\max\{a,0\}$. $\frac{\partial f(x)}{\partial x}$ represents the partial derivative of function $f(x)$ with respect to variable x. Furthermore, we use the big-O notation to describes the limiting behavior of a function, i.e., $f(x)=\mathcal{O}\left(g(x)\right)$, where $\limsup\limits_{x\to a}|\frac{f(x)}{g(x)}|<\infty$, and $g(x)$ is non-zero for values of x sufficiently close to a.

II. System Model

In this section, we define the channels, transmit signal, and channel state information (CSI) models of the considered two-user MISO-RSMA systems which are adopted for designing robust secure resource allocation algorithm.

A. Channel Model

In this paper, we consider a two-user downlink (DL) transmission system[1] which consists of a base station (BS), two legitimate DL users, and an idle user acting as a potential eavesdropper (PE). The BS is equipped with N_t antennas, while the two DL users and the PE[2] are single-antenna devices. We focus on a quasi-static fading environment and denote $\mathbf{h}_k, \forall k\in\mathcal{K}=\{1,2\}$, and $\mathbf{g}\in\mathbb{C}^{N_t\times 1}$ as the channel vectors from the BS to the k-th legitimate user and the PE, respectively. All the entries in the channel vectors $\{\mathbf{h}_k\}_{k\in\mathcal{K}}, \mathbf{g}$ are modeled by independent and identically distributed (i.i.d.) complex Gaussian random variables with zero-mean and unit variance, respectively. Moreover, for simplicity, we assume that all transceivers operate in the same time and frequency resource block.

B. Rate Splitting Signal Model

For the considered two-user RSMA system, there are two messages, W_1 and W_2, intended for user-1 and user-2, respectively. The message of each user is split into two parts, i.e., the common part $W_{\mathrm{c},1}$, the private part $W_{\mathrm{p},1}$ for user-1, and the common part $W_{\mathrm{c},2}$, the private part $W_{\mathrm{p},2}$ for user-2. The messages $W_{\mathrm{c},1}$ and $W_{\mathrm{c},2}$ are encoded together into a common stream s_{c} required to be decoded by both users. The messages $W_{\mathrm{p},1}$ and $W_{\mathrm{p},2}$ are encoded into the private stream s_1 for user-1 and s_2 for user-2, respectively. Then, the two private streams are mapped to the transmit antenna array in an unicast manner through some optimized multi-user (MU)-precoder, while the common stream is precoded in a multicast fashion such that it is delivered to all users, cf. Fig. 1. As a result, the three symbols of a given channel use are grouped in a vector $\mathbf{s}=[s_c,s_1,s_2]^T\in\mathbb{C}^{(K+1)\times 1}$, where $\mathbb{E}[\mathbf{s}\mathbf{s}^H]=\mathbf{I}_{K+1}$, [31], [42], [43]. Therefore, RS signal $\mathbf{x}\in\mathbb{C}^{N_t\times 1}$ of the considered two-user system transmitted from the BS is given by

$$\mathbf{x}=\mathbf{w}_c s_c+\mathbf{w}_1 s_1+\mathbf{w}_2 s_2, \tag{1}$$

where $\mathbf{w}_c\in\mathbb{C}^{N_t\times 1}$ and $\mathbf{w}_k\in\mathbb{C}^{N_t\times 1}, k\in\mathcal{K}$, denote the beamforming vectors for the common message and the private message intended for the k-th user, respectively. The received signals at the k-th legitimate user and the PE are given by

$$y_k=\mathbf{h}_k^H\mathbf{x}+n_k,\ \forall k\in\mathcal{K},\quad \text{and}\quad y_e=\mathbf{g}^H\mathbf{x}+n_e, \tag{2}$$

respectively, where $n_k\sim\mathcal{CN}(0,\sigma_k^2\mathbf{I}_{N_t})$ and $n_e\sim\mathcal{CN}(0,\sigma_e^2\mathbf{I}_{N_t})$ denote the additive Gaussian noise at the k-th legitimate user and the PE, respectively.

Remark 1: We note that the secrecy sum-rate performance of traditional SDMA and NOMA schemes would gradually saturate with the increasing transmit power, due to both the potential information leakage towards the PE and the inter-user interference [14]-[16]. Thus, to achieve a continuous growth of secrecy sum-rate, we propose a RSMA-based secure transmission strategy, dividing each message into two parts for creating extra degrees of freedom (DoF) [31], [37], [38]. In particular, we advocate the dual use of the common message in providing simultaneous secure and efficient data transmission.

C. Channel State Information

In this paper, we assume that some kind of CSI of all the wireless receivers is available at the BS for the design of resource allocation. Specifically, at the beginning of each

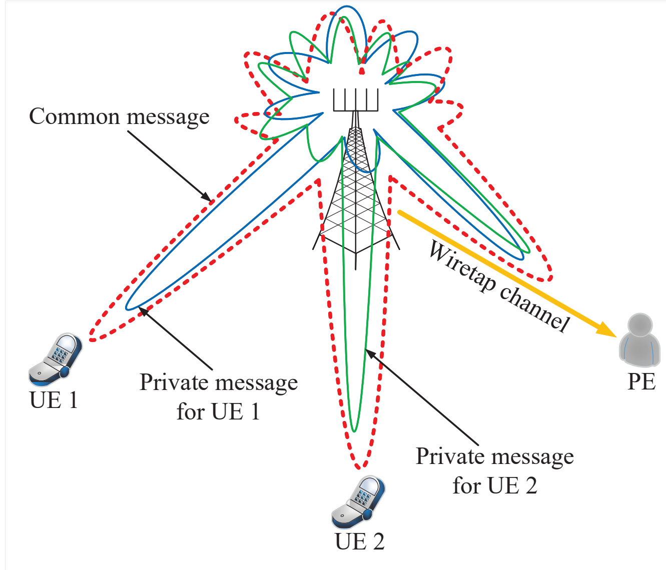


Fig. 1: A MISO-RSMA system model for $K=2$ legitimate users (UE) and a potential eavesdropper (PE).

[1]Note the sum-rate performance of RSMA would degrade to that of the traditional SDMA scheme eventually with the increasing number of users [34], [39]. Besides, the potential gain of RSMA can be sufficiently exploited by a two-user system with a low system complexity [42], [43]. As an initial attempt, adopting a two-user model is sufficient for us to show the advantages of our proposed secure transmission scheme.

[2]The considered single-antenna eavesdropper setup can be generalized to the case of a multi-antenna eavesdropper via a similar approach as in [17], [28], [49].

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TWC.2020.3021725, IEEE Transactions on Wireless Communications

scheduling slot, the legitimate users send handshaking signals to the BS to report their status and service requirements. Thus, the downlink CSI of the BS-to-legitimate user channels can be obtained accurately through measuring the uplink pilots in the handshaking signal by exploiting the channel reciprocity. Without loss of generality, we assume that the considered system adopts the time-division-duplex protocol in slow-time varying channels in each scheduling time slot. Therefore, the perfect CSI for the BS-to-desired k-th user link $\mathbf{h}_k, \forall k$, in each scheduling slot, is available for the BS during the whole transmission period. However, the CSI of the idle user, i.e., the PE, may be outdated during the transmission since there is no frequent and steady interaction between the transmitter and the idle user at the beginning of each scheduling slot. As a result, for the channel between the BS and the PE, only the estimated $\hat{\mathbf{g}}$ is available for the BS. To capture this effect, we define the channel uncertainty by the worst-case model [25]-[28]. The CSI of the link between the BS and the PE is given by

$$\mathbf{g} = \hat{\mathbf{g}} + \Delta\mathbf{g}, \text{ where } \Theta \triangleq \{\Delta\mathbf{g} \in \mathbb{C}^{N_t \times 1} : \Delta\mathbf{g}^H \Delta\mathbf{g} \le \varepsilon^2\}, \tag{3}$$

where $\hat{\mathbf{g}} \in \mathbb{C}^{N_t \times 1}$ is the channel estimate of the PE available for the BS, and $\Delta\mathbf{g}$ represents the unknown channel uncertainty of the PE. Specifically, $\varepsilon > 0$ denotes the size of the uncertainty region of the estimated CSI of the PE. In addition, the perfect CSI for the BS-to-PE link $\mathbf{g}$ is available when $\varepsilon = 0$, which is a subcase of the considered imperfect CSIT case.

III. Problem Formulation

In the following, we first discuss the performance metrics of the considered system. Then, the robust beamforming design is formulated as an optimization problem for maximizing the minimum individual secrecy rate among all legitimate users.

A. Performance Metrics and PHY Layer Security

In this section, we first define the adopted performance metrics. For the proposed RS-based secure transmission system, each legitimate user first decodes the common stream and extracts its own message from it by treating all private streams as noise, followed by decoding the private stream after removing the common stream via successive interference cancelation (SIC) [31], [38]. Hence, the corresponding output signal-to-interference-plus-noise ratio (SINR) of the common stream and the private stream at the k-th user can be written as

$$\gamma_{c,k} = \frac{|\mathbf{h}_k^H \mathbf{w}_c|^2}{|\mathbf{h}_k^H \mathbf{w}_1|^2 + |\mathbf{h}_k^H \mathbf{w}_2|^2 + \sigma_k^2}, \quad \forall k \in \mathcal{K}, \tag{4-1}$$

$$\gamma_k = \frac{|\mathbf{h}_k^H \mathbf{w}_k|^2}{|\mathbf{h}_k^H \mathbf{w}_i|^2 + \sigma_k^2}, \quad \forall i, k \in \mathcal{K}, i \ne k, \tag{4-2}$$

respectively. Under the Gaussian signaling, the achievable rate (bit/s/Hz) of the k-th legitimate user in decoding the common message and its desired private message are given by

$$R_{c,k} = \log_2(1 + \gamma_{c,k}) \quad \text{and} \quad R_k = \log_2(1 + \gamma_k), \ \forall k, \tag{5}$$

respectively. To ensure that the common message is decodable for each legitimate user, the actual transmission rate of the common message r_c from the BS should satisfy the condition: $r_c \le R_c$, where R_c is the achievable rate of the common message and is defined as $R_c \triangleq \min_k \{R_{c,k}\}, k \in \mathcal{K}$. For notational simplicity, the corresponding minimum SINR for supporting the actual transmission rate of the common message r_c can be written as $\gamma_c = 2^{r_c} - 1$.

In contrast, for the PE, it may try to decode and cancel the common message at the first stage so as to increase its chance in eavesdropping the desired private messages at the latter decoding stage. Hence, we aim to decrease the total eavesdropping capability of the PE. To this end, we design the beamformer of the common message, i.e., $\mathbf{w}_c$, such that it is not decodable at the PE. Then, the undecodable common messages at the PE would exist as a controllable interference which can efficiently protect the private messages. In order to achieve the goal, the condition, i.e., $C_{c,e} < r_c$, should be satisfied, where $C_{c,e}$ denotes the channel capacity between the BS and the PE for eavesdropping the common message. As a result, the corresponding SINR of the private message at the PE is degraded by the interference caused by the existing of the common message. Therefore, the achievable secrecy rate of the private message at its intended user, and the achievable secrecy sum-rate of the considered RSMA-based secure transmission scheme can be efficiently improved. To unlock the potential of the dual use of the common message, efficient resource allocation design is desired. Then, we define the corresponding received SINRs of the common data stream and the private data stream at the PE, which are given by

$$\gamma_{c,e} = \frac{|\mathbf{g}^H \mathbf{w}_c|^2}{|\mathbf{g}^H \mathbf{w}_1|^2 + |\mathbf{g}^H \mathbf{w}_2|^2 + \sigma_e^2}, \tag{6-1}$$

$$\gamma_{k,e} = \frac{|\mathbf{g}^H \mathbf{w}_k|^2}{|\mathbf{g}^H \mathbf{w}_c|^2 + |\mathbf{g}^H \mathbf{w}_i|^2 + \sigma_e^2}, \quad \forall i \in \mathcal{K}, i \ne k, \tag{6-2}$$

respectively. The corresponding achievable rate for the PE in attempting to decode the common message and the private message of the k-th user can be written as

$$C_{c,e} = \log_2(1 + \gamma_{c,e}) \quad \text{and} \quad C_{k,e} = \log_2(1 + \gamma_{k,e}), \ \forall k. \tag{7}$$

Thus, the achievable secrecy rate between the transmitter and the k-th user can be expressed as

$$R_{k,\mathrm{tot}}^{\mathrm{sec}} = R_{c,k}^{\mathrm{sec}} + R_k^{\mathrm{sec}}, \ \forall k \in \mathcal{K}, \tag{8}$$

where $R_{c,k}^{\mathrm{sec}} = \alpha_k [R_c - C_{c,e}]^+$ and $R_k^{\mathrm{sec}} = [R_k - C_{k,e}]^+$ denote the achievable secrecy rate of the common message and the private message intended to the k-th user, respectively. $0 \le \alpha_k \le 1$ corresponds the proportion[3] of the secrecy rate belonged to the k-th user, and satisfies $\sum_{k \in \mathcal{K}} \alpha_k = 1$.

B. The Max-Min Problem Formulation

Now, we focus on the robust secure beamforming design for the user secrecy rate maximization (SRM) problem in the considered MISO-RSMA system taking into account the

[3]Here, α_k is assumed to be a constant and the design of its optimal value for maximizing the system secrecy rate is left in future work.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TWC.2020.3021725, IEEE Transactions on Wireless Communications

$$
\begin{aligned}
R^{\rm sec}_{k,\rm tot} =& R^{\rm sec}_{c,k} + R^{\rm sec}_{k} = \alpha_k[R_c - C_{c,e}]^+ - [R_k - C_{k,e}]^+ \\
=& \underbrace{\alpha_k[r_c^{(n)} + \log_2(\mathbf{g}^H\mathbf{W}_1\mathbf{g} + \mathbf{g}^H\mathbf{W}_2\mathbf{g} + \sigma_e^2)] + \log_2(\mathbf{h}_k^H\mathbf{W}_1\mathbf{h}_k + \mathbf{h}_k^H\mathbf{W}_2\mathbf{h}_k + \sigma_k^2)}_{\Xi_{k,1}} \\
& + \underbrace{\log_2(\mathbf{g}^H\mathbf{W}_c\mathbf{g} + \mathbf{g}^H\mathbf{W}_i\mathbf{g} + \sigma_e^2)}_{\Xi_{k,2}} \underbrace{-\log_2(\mathbf{h}_k^H\mathbf{W}_i\mathbf{h}_k + \sigma_k^2)}_{\Psi_{k,1}} \\
& \underbrace{-\log_2(\mathbf{g}^H\mathbf{W}_c\mathbf{g} + \mathbf{g}^H\mathbf{W}_1\mathbf{g} + \mathbf{g}^H\mathbf{W}_2\mathbf{g} + \sigma_e^2)}_{\Psi_{k,2}}(\alpha_k + 1) \\
=& \Xi_k + \Psi_{k,1} + \Psi_{k,2}(\alpha_k + 1),\ (\Xi_k = \Xi_{k,1} + \Xi_{k,2},\ i,k \in \mathcal{K},\ i \neq k),
\end{aligned} \tag{11}
$$

impact of the imperfect CSIT of the PE. Therefore, the resource allocation design for the considered SRM problem of the RS system can be formulated as following optimization problem:

$$
\begin{aligned}
\underset{\mathbf{w}_c,\mathbf{w}_1,\mathbf{w}_2}{\text{maximize}} \ & \min_{k\in\mathcal{K},\Delta\mathbf{g}\in\Theta} \{R^{\rm sec}_{k,\rm tot}\} \\
\text{s.t.}\ \ & \text{C1: } R_{c,k} \geq r_c,\ \forall k \in \mathcal{K}, \\
& \text{C2: } \max_{\Delta\mathbf{g}\in\Theta} C_{c,e} \leq r_c, \\
& \text{C3: } \sum_{m\in\mathcal{M}} \|\mathbf{w}_m\|^2 \leq P_t,
\end{aligned} \tag{9}
$$

where r_c is the predefined target transmission rate of the common message. Besides, (9-C3) is the total transmission power constraint and $\mathcal{M}$ denotes a set, i.e., $\mathcal{M} = \{c, 1, 2\}$.

The SRM problem in (9) is a non-convex optimization problem which is challenging to solve. In general, there is no standard method for directly solving such non-convex optimization problems efficiently. To strike a balance between solution optimality and computational complexity, we aim to design an efficient suboptimal algorithm. To this end, we approximate the non-convex problem in (9) by a convex one, whose solution is a suboptimal solution of the original problem.

IV. Optimization Solution

The optimization problem in (9) is a neither convex nor concave optimization problem, which even involves infinitely many constraints. To obtain a tractable problem formulation and to solve the problem by using efficient convex optimization tools, we first introduce several transformations for problem (9) in the following.

A. Equivalent Reformulation of the Original Problem

It can be observed that the aim of problem (9) is to optimize the beamformers subject to a target transmission rate of the common message r_c. Constraints (C1) and (C2) are used to guarantee that the common message can be retrieved by the legitimate users with a given quality of service (QoS), while the PE only has limited reception performance. In other words, imposing these two constraints enables the dual use of the common message. To facilitate the design of an iterative suboptimal method based on successive convex approximation (SCA) algorithm, we first transform the problem into its epigraph form. By using the change of optimization variables, the problem of (9) can be equivalently rewritten as:

$$
\begin{aligned}
\underset{\mathbf{W}_c,\mathbf{W}_1,\mathbf{W}_2\in\mathbb{H}^{N_t},t}{\text{maximize}} \ & t \\
\text{s.t.}\ & \text{C1: } \min_{\Delta\mathbf{g}\in\Theta} R^{\rm sec}_{k,\rm tot} \geq t,\ \forall k \in \mathcal{K}, \\
& \text{C2: } \gamma_c \sum_{i\in\mathcal{K}} \mathrm{Tr}(\mathbf{R}_{\mathbf{h}_k}\mathbf{W}_i) + \gamma_c\sigma_k^2 - \mathrm{Tr}(\mathbf{R}_{\mathbf{h}_k}\mathbf{W}_c) \leq 0,\ \forall k, \\
& \text{C3: } \min_{\Delta\mathbf{g}\in\Theta} \mathrm{Tr}(\mathbf{R}_{\mathbf{g}}\mathbf{W}_c) - \gamma_c \sum_{i\in\mathcal{K}} \mathrm{Tr}(\mathbf{R}_{\mathbf{g}}\mathbf{W}_i) - \gamma_c\sigma_e^2 \leq 0, \\
& \text{C4: } \mathbf{W}_m \succeq \mathbf{0},\ \forall m \in \mathcal{M}, \\
& \text{C5: } \sum_{m\in\mathcal{M}} \mathrm{Tr}(\mathbf{W}_m) \leq P_t, \\
& \text{C6: } \mathrm{Rank}(\mathbf{W}_m) = 1,\ \forall m \in \mathcal{M},
\end{aligned} \tag{10}
$$

where $\mathbf{R}_{\mathbf{g}} = \mathbf{g}\mathbf{g}^H$, $\mathbf{R}_{\mathbf{h}_k} = \mathbf{h}_k\mathbf{h}_k^H$, t is an auxiliary optimization variable, and γ_c is the target SINR value for the two legitimate users to decode the common message, which is determined by r_c mentioned in problem (9). In addition, constraints (C4) and (C6) in (10) are imposed to guarantee that $\mathbf{W}_m = \mathbf{w}_m\mathbf{w}_m{}^H$ holds after optimization.

We note that the non-convexity of (10) arises from the reverse concave function in (C1), the semi-infinite constraints in (C1) and (C3), and the rank-one constraint in (C6). In fact, constraint (C6) can be easily handled by applying the SDR technique. Then, in the following, we focus on the methods for handling constraints (C1) and (C3).

B. SCA-based Reformulation of Constraint C1

For a given target transmit rate of the common message r_c, the left side of constraint (C1) can be represented as (11) shown at the top of this page. Since Ξ_k is a concave function and $\Psi_{k,1} + \Psi_{k,2}(\alpha_k + 1)$ is a convex function with respect to $\{\mathbf{W}_m\}_{m\in\mathcal{M}}$, the function described by (11) is neither convex nor concave. To facilitate the implementation of successive convex approximation (SCA) algorithm to obtain an efficient suboptimal solution, we replace the non-concave parts of (11) by their corresponding lower bound surrogate functions. In particular, in the n-th iteration, with given local points $\{\mathbf{W}_m^{(n-1)}\}_{m\in\mathcal{M}}$, we apply the following proposition to linearize the non-concave parts [46].

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TWC.2020.3021725, IEEE Transactions on Wireless Communications

Proposition 1 [46]: Let a be a positive scalar and $f(a) = -(ab/\ln 2) + \log_2 a + (1/\ln 2)$. We have

$$-\log_2 b = \max_{a>0} f(a), \tag{12}$$

and the optimal solution to the right-hand side of (12) is $a = 1/b$.

Proof: The proposition can be proved by setting $\frac{\partial f(a)}{\partial a} = 0$. ■

According to Proposition 1, in the n-th iteration, around the points $\{\mathbf{W}_m^{(n-1)}\}_{m\in\mathcal{M}}$ acquired in the $(n-1)$-th iteration, we approximate $\Psi_{k,1}$ and $\Psi_{k,2}$ as affine functions by using the corresponding surrogate lower bound functions given by

$$\begin{aligned}\Psi_{k,1}^{\mathrm{L}} = &\max_{a_{k,1}\in\mathbb{R}^{1\times1}} -\frac{a_{k,1}}{\ln 2}(\mathbf{h}_k^H\mathbf{W}_i\mathbf{h}_k + \sigma_k^2) \\ &+ \log_2 a_{k,1} + \frac{1}{\ln 2},\ \forall i \neq k, k \in \mathcal{K}, m \in \mathcal{M}, \end{aligned}\tag{13}$$

$$\begin{aligned}\Psi_{k,2}^{\mathrm{L}} = &\max_{a_{k,2}\in\mathbb{R}^{1\times1}} -\frac{a_{k,2}}{\ln 2}(\mathbf{g}^H\sum_{m\in\mathcal{M}}\mathbf{W}_m\mathbf{g} + \sigma_e^2) \\ &+ \log_2 a_{k,2} + \frac{1}{\ln 2},\ \forall m \in \mathcal{M}, \end{aligned}\tag{14}$$

respectively. In the n-th iteration, to guarantee a tight approximation, we update $a_{k,1}^{(n)}$ and $a_{k,2}^{(n)}$ which can be achieved as below:

$$\begin{aligned}a_{k,1}^{(n)} = &\arg\max_{a_{k,1}>0} -\frac{a_{k,1}}{\ln 2}(\mathbf{h}_k^H\mathbf{W}_i^{(n-1)}\mathbf{h}_k + \sigma_k^2) \\ &+ \log_2 a_{k,1} + \frac{1}{\ln 2},\ \forall i \neq k, \end{aligned}\tag{15}$$

$$\begin{aligned}a_{k,2}^{(n)} = &\arg\max_{a_{k,2}>0} -\frac{a_{k,2}}{\ln 2}\left(\mathbf{g}^H\sum_{m\in\mathcal{M}}\mathbf{W}_m^{(n-1)}\mathbf{g} + \sigma_k^2\right) \\ &+ \log_2 a_{k,2} + \frac{1}{\ln 2}. \end{aligned}\tag{16}$$

where $\mathbf{W}_m^{(n-1)}$ is the optimal $\{\mathbf{W}_m\}_{m\in\mathcal{M}}$ obtained in the $(n-1)$-th iteration. Since the perfect CSI of each legitimate user is available for the transmitter, we always have

$$a_{k,1}^{(n)} = (\mathbf{h}_k^H\mathbf{W}_i^{(n-1)}\mathbf{h}_k + \sigma_k^2)^{-1},\ \forall i \neq k,\ i,k \in \mathcal{K}, \tag{17}$$

according to Proposition 1. However, only the estimated imperfect CSI $\hat{\mathbf{g}}$ of the PE and the size of its uncertainty region are available at the transmitter. Thus, for the imperfect CSIT case of the PE, we consider the worst-case of the wiretap channel $\mathbf{g}$ to continue our investigation. It is due to the fact that the reformulated version of the objective function in problem (9), is concave with respect to $a_{k,2}$ and $\Delta\mathbf{g}$, respectively. Thus, for the imperfect CSIT case of the wiretap channel $\mathbf{g}$, we can rewrite the optimization problem (16) into (18) for $a_{k,2}^{(n)}$:

$$\begin{aligned}a_{k,2}^{(n)} = &\arg\max_{a_{k,2}>0} \log_2 a_{k,2} + \frac{1}{\ln 2} \\ &- \frac{a_{k,2}}{\ln 2}\left(\max_{\Delta\mathbf{g}}(\hat{\mathbf{g}}+\Delta\mathbf{g})^H\sum_{m\in\mathcal{M}}\mathbf{W}_m^{(n-1)}(\hat{\mathbf{g}}+\Delta\mathbf{g}) + \sigma_k^2\right). \end{aligned}\tag{18}$$

Before solving (18), we first handle the following maximization problem related to $\Delta\mathbf{g}$:

$$\begin{aligned}\mathbf{P}_{\mathrm{T}}: \mathrm{T} = &\underset{\Delta\mathbf{g}}{\text{maximize}}\ \mathrm{Tr}\left((\hat{\mathbf{g}}+\Delta\mathbf{g})(\hat{\mathbf{g}}+\Delta\mathbf{g})^H\sum_{m\in\mathcal{M}}\mathbf{W}_m^{(n-1)}\right) \\ &\text{s.t.}\quad \Delta\mathbf{g}^H\Delta\mathbf{g} \leq \varepsilon^2, \end{aligned}\tag{19}$$

where $\{\mathbf{W}_m^{(n-1)}\}_{m\in\mathcal{M}}$ is obtained in the $(n-1)$-th iteration. The Lagrange function of (19) is

$$\begin{aligned}\mathcal{L}_{\mathrm{T}} = &(\hat{\mathbf{g}}+\Delta\mathbf{g})^H\sum_{m\in\mathcal{M}}\mathbf{W}_m^{(n-1)}(\hat{\mathbf{g}}+\Delta\mathbf{g}) \\ &+ \lambda_{\mathrm{T}}(\Delta\mathbf{g}^H\Delta\mathbf{g} - \varepsilon^2), \end{aligned}\tag{20}$$

where λ_{T} denotes the Lagrange multiplier with respect to the constraint in (19). Since $\mathcal{L}_{\mathrm{T}}$ is convex in $\Delta\mathbf{g}$, the Karush-Kuhn-Tucker (KKT) conditions are necessary and sufficient for maximizing (19). Thus, we have

$$\begin{aligned}\mathrm{T}_{\max} = &\mathrm{Tr}\left(\sum_{m\in\mathcal{M}}\mathbf{W}_m^{(n-1)}(\hat{\mathbf{g}}\hat{\mathbf{g}}^H)\right) \\ &+ 2\varepsilon\sqrt{\mathrm{Tr}\left((\sum_{m\in\mathcal{M}}\mathbf{W}_m^{(n-1)}\hat{\mathbf{g}})(\hat{\mathbf{g}}^H\sum_{m\in\mathcal{M}}\mathbf{W}_m^{(n-1)^H})\right)} \\ &+ \varepsilon^2\sqrt{\sum_{m\in\mathcal{M}}\mathrm{Tr}\left(\mathbf{W}_m^{(n-1)}\mathbf{W}_m^{(n-1)^H}\right)}. \end{aligned}\tag{21}$$

Proof: See Appendix A. ■

Then, the closed-form solution[4] to problem (18) is

$$a_{k,2}^{(n)} = (\mathrm{T}_{\max} + \sigma_e^2)^{-1}. \tag{22}$$

For the special case, the perfect CSI of the PE is available for the transmitter, i.e., $\varepsilon = 0$. Same as (17), we can easily obtain the optimal $a_{k,2}^{(n)}$ by employing Proposition 1 directly, which is given by

$$a_{k,2}^{(n)} = \left(\mathbf{g}^H\sum_{m\in\mathcal{M}}\mathbf{W}_m^{(n-1)}\mathbf{g} + \sigma_e^2\right)^{-1}. \tag{23}$$

Similarly, $\Xi_k^{(n)}$ is used to denote the Ξ_k in the n-th iteration, which is given by (24) shown as below:

$$\begin{aligned}\Xi_k^{(n)} = &\alpha_k[r_c + \log_2(\mathbf{g}^H\mathbf{W}_1^{(n)}\mathbf{g} + \mathbf{g}^H\mathbf{W}_2^{(n)}\mathbf{g} + \sigma_e^2)] \\ &+ \log_2(\mathbf{h}_k^H\mathbf{W}_1^{(n)}\mathbf{h}_k + \mathbf{h}_k^H\mathbf{W}_2^{(n)}\mathbf{h}_k + \sigma_k^2) \\ &+ \log_2(\mathbf{g}^H\mathbf{W}_c^{(n)}\mathbf{g} + \mathbf{g}^H\mathbf{W}_i^{(n)}\mathbf{g} + \sigma_e^2),\ \forall i \neq k. \end{aligned}\tag{24}$$

According to the above derivations, problem (10) can be rewritten as (25) shown at the top of next page, where $\{\mathbf{W}_m^{(n)}\}_{m\in\mathcal{M}}$ are the optimization variables in the n-th iteration, and the corresponding rank-one constraints in (C6) have been relaxed by employing the SDR technique. $\Omega_k > 0, \forall k \in$

[4]For the implementation of SCA, Cauchy-Schwartz inequality is adopted to find the optimal values of intermediate optimization variables, i.e., $\{a_{k,2}^{(n)}\}_{k\in\mathcal{K}}$, to establish a surrogate function for the non-concave parts of the objective function.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TWC.2020.3021725, IEEE Transactions on Wireless Communications

$$\begin{aligned}
&\underset{\mathbf{W}_c^{(n)},\mathbf{W}_1^{(n)},\mathbf{W}_2^{(n)}\in\mathbb{H}^{N_t},t,\boldsymbol{\tau}}{\text{maximize}} \quad t \qquad (25)\\
\text{s.t.}\;\; &\text{C1: } \Omega_k\geq 0, k\in\mathcal{K}, \qquad \text{C2: } \gamma_c^{(n)}\sum_{i\in\mathcal{K}}\mathrm{Tr}(\mathbf{R}_{\mathbf{h}_k}\mathbf{W}_1^{(n)})+\gamma_c^{(n)}\sigma_k^2-\mathrm{Tr}(\mathbf{R}_{\mathbf{h}_k}\mathbf{W}_c^{(n)})\leq 0,\;\; k\in\mathcal{K},\\
&\text{C3: } \max_{\Delta\mathbf{g}\in\Theta}\;\mathrm{Tr}(\mathbf{R}_{\mathbf{g}}\mathbf{W}_c^{(n)})-\gamma_c^{(n)}\sum_{i\in\mathcal{K}}\mathrm{Tr}(\mathbf{R}_{\mathbf{g}}\mathbf{W}_i^{(n)})-\gamma_c^{(n)}\sigma_e^2\leq 0, \qquad \text{C4:}\mathbf{W}_m^{(n)}\succeq\mathbf{0},\,\forall m\in\mathcal{M},\\
&\text{C5: } \sum_{m\in\mathcal{M}}\mathrm{Tr}(\mathbf{W}_m^{(n)})\leq P_t, \qquad \text{C7: } \max_{\Delta\mathbf{g}\in\Theta}\;\mathbf{g}^H\mathbf{W}_m^{(n)}\mathbf{g}\leq\tau_m,\forall m\in\mathcal{M},\\
&\text{C8: } \mathbf{h}_1^H\mathbf{W}_2^{(n)}\mathbf{h}_1\leq\tau_4,\;\; \mathbf{h}_2^H\mathbf{W}_1^{(n)}\mathbf{h}_2\leq\tau_5, \quad \text{C9: } \mathbf{h}_1^H\mathbf{W}_1^{(n)}\mathbf{h}_1\geq\tau_3,\;\; \mathbf{h}_2^H\mathbf{W}_2^{(n)}\mathbf{h}_2\geq\tau_6.
\end{aligned}$$

$\mathcal{K}$, is the concave form of constraint (C1) shown by (26) as below[5]:

$$\begin{aligned}
\Omega_1=&\alpha_1[r_c+\log_2(\tau_1+\tau_2+\sigma_e^2)]+\log_2(\tau_3+\tau_4+\sigma_1^2)\\
&+\log_2(\tau_c+\tau_2+\sigma_e^2)-\frac{a_{1,1}^{(n)}}{\ln 2}(\tau_4+\sigma_1^2)+\log_2 a_{1,1}^{(n)}\\
&-\frac{a_{1,2}^{(n)}}{\ln 2}[\tau_c+\tau_1+\tau_2+\sigma_e^2]+\log_2 a_{1,2}^{(n)}+\frac{2}{\ln 2}-t,
\end{aligned} \tag{26-1}$$

$$\begin{aligned}
\Omega_2=&\alpha_2[r_c+\log_2(\tau_1+\tau_2+\sigma_e^2)]+\log_2(\tau_5+\tau_6+\sigma_2^2)\\
&+\log_2(\tau_c+\tau_1+\sigma_e^2)-\frac{a_{2,1}^{(n)}}{\ln 2}(\tau_5+\sigma_2^2)+\log_2 a_{2,1}^{(n)}\\
&-\frac{a_{2,2}^{(n)}}{\ln 2}[\tau_c+\tau_1+\tau_2+\sigma_e^2]+\log_2 a_{2,2}^{(n)}+\frac{2}{\ln 2}-t.
\end{aligned} \tag{26-2}$$

C. Transformation of the Semi-infinite Constraints

In addition, in problem (25), constraints (25-C3) and (25-C7) are convex with respect to the optimization variables. Yet, since only the imperfect CSI of the PE is available at the transmitter, constraints (25-C3) and (25-C7) involve infinitely many constraints which are generally intractable for beamforming design. To circumvent this difficulty, we first transform them into linear matrix inequalities (LMIs) by using the following lemma.

Lemma 1 (S-Procedure [47]): Let a function $f_m(\mathbf{x})$, $m\in\{1,2\}$, $\mathbf{x}\in\mathbb{C}^{N\times 1}$, be defined as

$$f_m(\mathbf{x})=\mathbf{x}^H\mathbf{A}_m\mathbf{x}+2\mathrm{Re}\{\mathbf{b}_m^H\mathbf{x}\}+c_m, \tag{27}$$

where $\mathbf{A}_m\in\mathbb{H}^N$, $b_m\in\mathbb{C}^{N\times 1}$, and $c_m\in\mathbb{R}^{1\times 1}$. Then, the implication $f_1(\mathbf{x})\leq 0\Rightarrow f_2(\mathbf{x})\leq 0$ holds if and only if there exists a $\delta\geq 0$ such that

$$\delta\begin{bmatrix}\mathbf{A}_1 & \mathbf{b}_1\\ \mathbf{b}_1^H & c_1\end{bmatrix}-\begin{bmatrix}\mathbf{A}_2 & \mathbf{b}_2\\ \mathbf{b}_2^H & c_2\end{bmatrix}\succeq\mathbf{0}, \tag{28}$$

provided that there exists a point $\hat{\mathbf{x}}$ such that $f_m(\hat{\mathbf{x}})\leq 0$. ■

By applying Lemma 1 to constraints (25-C3) and (25-C7) and introducing auxiliary slack variables $\delta_{\text{C3}}\geq 0$, $\delta_c\geq 0$, $\delta_1\geq 0$, and $\delta_2\geq 0$, we have

$$\begin{aligned}
\mathbf{S}_{\text{C3}}=&\begin{bmatrix}\delta_{\text{C3}}\mathbf{I}_{N_t} & \mathbf{0}\\ \mathbf{0} & -\delta_{\text{C3}}\varepsilon^2+\sigma_e^2\end{bmatrix}\\
&+\mathbf{U}_e^H\left(\mathbf{W}_1^{(n)}+\mathbf{W}_2^{(n)}-\frac{1}{\gamma_c^{(n)}}\mathbf{W}_c^{(n)}\right)\mathbf{U}_e\succeq\mathbf{0},
\end{aligned} \tag{29}$$

$$\mathbf{S}_{e_c}=\begin{bmatrix}\delta_c\mathbf{I}_{N_t} & \mathbf{0}\\ \mathbf{0} & -\delta_c\varepsilon^2+\tau_c\end{bmatrix}-\mathbf{U}_e^H\mathbf{W}_c^{(n)}\mathbf{U}_e\succeq\mathbf{0}, \tag{30}$$

$$\mathbf{S}_{e_1}=\begin{bmatrix}\delta_1\mathbf{I}_{N_t} & \mathbf{0}\\ \mathbf{0} & -\delta_1\varepsilon^2+\tau_1\end{bmatrix}-\mathbf{U}_e^H\mathbf{W}_1^{(n)}\mathbf{U}_e\succeq\mathbf{0}, \tag{31}$$

$$\mathbf{S}_{e_2}=\begin{bmatrix}\delta_2\mathbf{I}_{N_t} & \mathbf{0}\\ \mathbf{0} & -\delta_2\varepsilon^2+\tau_2\end{bmatrix}-\mathbf{U}_e^H\mathbf{W}_2^{(n)}\mathbf{U}_e\succeq\mathbf{0}, \tag{32}$$

where $\mathbf{U}_e=\begin{bmatrix}\mathbf{I}_{N_t} & \hat{\mathbf{g}}\end{bmatrix}$. Now, we note that constraints (29)-(32) involve only a finite number of constraints. Therefore, the robust secure beamforming problem, where only the imperfect CSI of the PE is known at the BS, can be given as

$$\begin{aligned}
&\underset{\mathbf{W}_c^{(n)},\mathbf{W}_1^{(n)},\mathbf{W}_2^{(n)}\in\mathbb{H}^{N_t},t,\boldsymbol{\tau},\boldsymbol{\delta}}{\text{maximize}} \quad t \qquad (33)\\
\text{s.t.}\;\; &\text{C1: } \Omega_k^{(n)}\leq 0,\;\; k\in\mathcal{K},\\
&\text{C2: } \gamma_c^{(n)}\sum_{i\in\mathcal{K}}\mathrm{Tr}(\mathbf{R}_{\mathbf{h}_k}\mathbf{W}_i^{(n)})+\gamma_c^{(n)}\sigma_k^2-\mathrm{Tr}(\mathbf{R}_{\mathbf{h}_k}\mathbf{W}_c^{(n)})\\
&\qquad\leq 0,\;\; k\in\mathcal{K},\\
&\text{C3: } \mathbf{S}_{\text{C3}}\succeq\mathbf{0}, \qquad \text{C4: } \mathbf{W}_m\succeq\mathbf{0},\;\forall m\in\mathcal{M},\\
&\text{C5: } \sum_{m\in\mathcal{M}}\mathrm{Tr}(\mathbf{W}_m^{(n)})\leq P_t,\\
&\text{C7: } \mathbf{S}_{e_c}\succeq\mathbf{0},\mathbf{S}_{e_1}\succeq\mathbf{0},\mathbf{S}_{e_2}\succeq\mathbf{0},\\
&\text{C8: } \mathbf{h}_1^H\mathbf{W}_2^{(n)}\mathbf{h}_1\leq\tau_4,\mathbf{h}_2^H\mathbf{W}_1^{(n)}\mathbf{h}_2\leq\tau_5,\\
&\text{C9: } \mathbf{h}_1^H\mathbf{W}_1^{(n)}\mathbf{h}_1\geq\tau_3,\mathbf{h}_2^H\mathbf{W}_2^{(n)}\mathbf{h}_2\geq\tau_6,
\end{aligned}$$

where t, $\boldsymbol{\tau}=\{\tau_c,\tau_1,\tau_2,\tau_3,\tau_4,\tau_5,\tau_6\}$, and $\boldsymbol{\delta}=\{\delta_{\text{C3}},\delta_c,\delta_1,\delta_2\}$ are auxiliary non-negative optimization variable vectors. Obviously, problem (33) is a typical SDP problem with a linear objective function and a number of LMI constraints. Thus, it can be solved by standard optimization tools such as CVX [48]. Furthermore, we can alternatively optimize $\{a_{k,1}^{(n)},a_{k,2}^{(n)}\}_{k\in\mathcal{K}}$ and $\{\mathbf{W}_m^{(n)}\}_{m\in\mathcal{M}}$ in each iteration until the problem converges to tighten the approximation, and the procedure is summarized in **Algorithm 1**.

Now, it is noted that the considered SDP problem (33) has relaxed the rank-one constraints. From the basic principles of

[5]To facilitate the application of the standard S-procedure to handle the infinitely many constraints in next subsection, we introduce auxiliary optimization variables $\{\tau_m\}_{m\in\mathcal{M}}$ to decouple the wire-tap channel vector in the objective function.

Algorithm 1 Optimization $\mathbf{W}_m, m \in \mathcal{M}$.

1. Set the convergence tolerance $\epsilon = 10^{-4}$, the iteration counter $n = 1$, and initialize $\mathbf{W}_m^{(0)}, m \in \mathcal{M}$ and r_c, i.e., γ_c, as an arbitrary positive semi-definite matrix and an arbitrary positive number, respectively;
2. **SCA Design:** In the n-th iteration, around the points $\mathbf{W}_m^{(n-1)}, \forall m$, acquired in the $(n-1)$-th iteration, $\Psi_{k,1}$ and $\Psi_{k,2}$ in (11) are transformed into affine functions by using the corresponding surrogate lower bound functions obtain by (13)-(16);
3. **AO Update:**
   (S1) Update $a_{k,1}^{(n)}$ and $a_{k,2}^{(n)}$ by (17) and (22);
   (S2) Solve problem (33) for given $a_{k,1}^{(n)}$, $a_{k,2}^{(n)}$, then, denote the optimal solution of the n-th iteration as $\mathbf{W}_m^{(n)},\ m \in \mathcal{M}$;
   (S3) $n = n + 1$;
4. **Convergence check:** If $|t^{(n)} - t^{(n-1)}| > \epsilon$, then go to Step 3. Otherwise, ϵ-convergence solution has been attained and output the solution.
5. $\mathbf{W}_m^* = P_m \mathbf{w}_m^* \mathbf{w}_m^{*H},\ \forall m \in \mathcal{M}$.

optimization theory, if the obtained solution $\{\mathbf{W}_m^*\}_{m\in\mathcal{M}}$ of the relaxed problem satisfies the rank-one condition, then it is the suboptimal solution of the original problem (9) with the imperfect CSIT of the PE. Then, the suboptimal $\{\mathbf{w}_m^*\}_{m\in\mathcal{M}}$ can be obtained by performing eigenvalue decomposition on $\{\mathbf{W}_m^*\}_{m\in\mathcal{M}}$. In the following theorem, we investigate the structure of the secure beamforming matrix.

Theorem 1: If problem (33) is feasible and $P_t > 0$, the rank of its optimal matrix $\mathbf{W}_m^*$, $m \in \mathcal{M}$, is $\mathrm{Rank}(\mathbf{W}_m^*) = 1$, $m \in \mathcal{M}$, which can be expressed as

$$\mathbf{W}_m^* = P_m \mathbf{w}_m^* \mathbf{w}_m^{*H},\ \forall m \in \mathcal{M}, \tag{34}$$

where $0 \le P_m \le P_t, m \in \mathcal{M}$, represents a constant, and $\mathbf{w}_m^*$, $m \in \mathcal{M}$ is the unit-norm eigenvector corresponding to the maximum eigenvalue of matrix $\mathbf{W}_m^*$, $m \in \mathcal{M}$.

Proof: Please refer to Appendix B. ■

Computational Complexity: For Algorithm 1, the computational complexity is mainly dominated by solving the SDP problems in (33). From [50], the computational complexity for solving a SDP problem is as follows:

$$\mathcal{O}\left(n_{\mathrm{sdp}}^{\frac{1}{2}}(m_{\mathrm{sdp}} n_{\mathrm{sdp}}^3 + m_{\mathrm{sdp}}^2 n_{\mathrm{sdp}}^2 + m_{\mathrm{sdp}}^3)\right)\log(\frac{1}{\epsilon}), \tag{35}$$

where m_{sdp} denotes the number of semi-definite cone constraints, n_{sdp} refers to the dimension of each semi-definite constraint, and $\epsilon > 0$ is the accuracy of solving the SDP. For problem (33), we have $m_{\mathrm{sdp}} = 13$ and $n_{\mathrm{sdp}} = N_t + 1$. Thus, the complexity of our proposed robust worst-case secure beamforming design algorithm for the considered MISO-RSMA secure transmission system in (33) is

$$\mathcal{O}\left((13(N_t+1)^{\frac{7}{2}} + 13^2(N_t+1)^{\frac{5}{2}} + 13^3(N_t+1)^{\frac{1}{2}})\right) L\log(\frac{1}{\epsilon}), \tag{36}$$

where L is the number of iterations of the alternating optimization and N_t is the number of transmit antennas equipped by the BS.

In the end, we provide the following proposition to show the convergence of Algorithm 1 theoretically.

Proposition 2: The sequence

$$\left\{\left(\mathbf{X}_m^{(n)}, a_{k,1}^{(n)}, a_{k,2}^{(n)}\right)\right\},\ k \in \mathcal{K}, m \in \mathcal{M},$$

generated by Algorithm 1, converges to a stationary point $\mathcal{P}^* = \left(\mathbf{X}_m^*, a_{k,1}^*, a_{k,2}^*\right)$, where $\{\mathbf{X}_m^*\}_{m\in\mathcal{M}}$ is a KKT point of the original problem (9) with the imperfect CSIT of the PE.

Proof: See Appendix C. ■

V. Simulation Results

In this section, we simulate the performance of the proposed scheme. We assume that all the entries in the channel vectors $\mathbf{h}_1$, $\mathbf{h}_2$, and $\mathbf{g}$ are i.i.d. complex Gaussian random variables with zero-mean and unit variance. To facilitate the presentation in the sequel, we define the normalized maximum channel estimation error of the potential eavesdropper (PE) as $\delta_e^2 = \varepsilon^2/(\|\hat{\mathbf{g}}\|^2 + \varepsilon^2)$. For brevity, $\alpha_k = 0.5, \forall k \in \mathcal{K}$, and the value of the predefined $r_c \in [0.5, 5.5]$ increases with transmit power. Besides, the traditional linear precoder, i.e., maximum ratio transmission (MRT) precoding, is adopted as the initial point of the beamformer of each private message, which is designed towards the direction of the desired legitimate user by applying the channel vector between the BS and the legitimate user. Moreover, the initial point of the common beamformer is generated randomly. For comparison, we also consider the performance of conventional NOMA frameworks. In particular, the NOMA scheme is a subcase of the proposed RSMA scheme, which can be easily obtained by allocating no power to the private message of UE 2 (i.e., the weak user), and merge the message of UE 2, i.e., s_2, into the common stream s_c. In other words, UE 2 works as a weak user, whose message is transmitted by the common stream, while UE 1 plays as the strong one. Thus, both UE 1 (i.e., the strong user) and UE 2 have to fully decode the common message which contains the message of UE 2.

A. Average Secrecy Sum Rate Versus Transmit SNR Under the Perfect CSIT

In Fig. 2, we depict the average secrecy sum rate (ASSR) performances of the proposed MISO-RSMA/NOMA secure transmission schemes versus the transmit SNR, where $N_t = 4$. For comparison, we provide the secure performance comparison of the proposed schemes with that of two existing baseline schemes, i.e., maximum ratio transmission (MRT) and the secure NOMA scheme proposed by [16]. In addition, to illustrate the quality of the obtained KKT solution, we show the secure performance of the secret DPC design [51]-[54] as a benchmark assuming the availability of perfect CSIT. The performance gap between the DPC scheme and the proposed scheme is shown in Fig. 2 and Fig. 3.

Obviously, the proposed schemes achieve a superior ASSR performance compared to the traditional baseline scheme, i.e., MRT scheme, which gradually saturates in the high SNR regimes. In fact, the considered system is more susceptible

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TWC.2020.3021725, IEEE Transactions on Wireless Communications

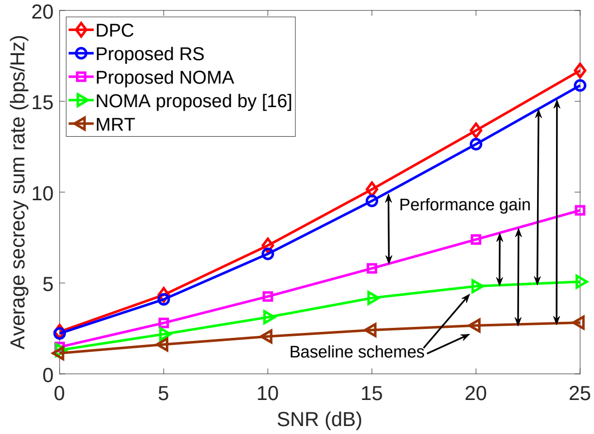
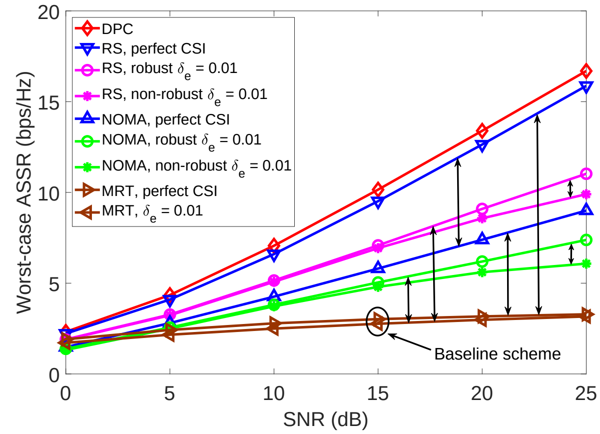
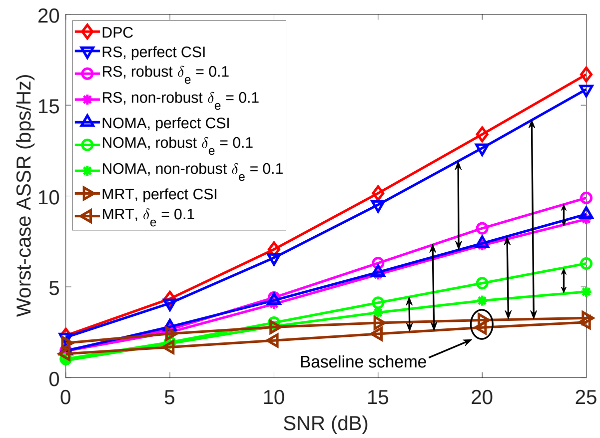


Fig. 2: Average secrecy sum rate versus transmit SNR for a comparison of our proposed MISO-RSMA/NOMA schemes and the two baseline schemes. Besides, the performance of the dirty paper coding (DPC) scheme is also shown as a benchmark, where the CSIT of the PE is perfect and $N_t = 4$. The double-sided arrows indicate the performance gain of security due to the proposed secure transmission schemes.



(a) $\delta_e^2 = 0.01$.



(b) $\delta_e^2 = 0.1$.

Fig. 3: Worst-case average secrecy sum rate versus transmit SNR. Performance comparison of our proposed MISO-RSMA/NOMA schemes and the baseline scheme is shown under the imperfect CSIT case of the PE with different variance of estimated channel errors, where $N_t = 4$. Besides, the performance of the DPC scheme is also shown as a benchmark. The double-sided arrows indicate the performance gain achieved by the proposed RSMA/NOMA scheme.

to eavesdropping in high SNR regimes as the eavesdropping capability of the PE improves with the received signal strength. Yet, the traditional baseline scheme is less capable of handling information leakage for guaranteeing communication security compared to the proposed schemes. Besides, the ASSR performance of the proposed MISO-NOMA scheme obviously outperforms the secure NOMA scheme proposed by [16]. This is because our proposed secure NOMA scheme exploits the dual-use of the non-orthogonal superposition signal as both desired signal and AN signal for legitimate users and the PE, respectively, to achieve efficient secure performance gain. Moreover, the proposed MISO-RSMA scheme outperforms the MISO-NOMA scheme prominently, as the RS transmission strategy offers a higher flexibility in resource allocation through the superimposed common message stream. In particular, the proposed optimization framework can strike an excellent balance between the power allocation in common and private message for improving the secure performance of the considered system. As a result, the ASSR performance of our proposed MISO-RSMA and MISO-NOMA scheme is able to scale with the increasing transmit power, shown as in Fig. 2. In addition, the secure performances of both the secret DPC scheme and the proposed RS scheme are almost identical in the low SNR regime, while the secure performance of DPC scheme slightly outperforms that of the RS scheme in the high SNR regime. This is because the BS adopting DPC scheme performs precoding for all legitimate users to mitigate inter-user interference while preventing the signal streams from leaking to the direction of PE. In contrast, for the RS secure transmission scheme, not only the private message of each legitimate user would interfere each other in the high SNR regime, but also the potential of private messages leakage to the PE still exist.

B. Worst-Case ASSR Performance Versus Transmit SNR and Number of Transmitting Antennas

In this section, we show the worst-case ASSR performance of the considered system under the imperfect CSIT case of the PE, with different resource allocation schemes. Fig. 3 depicts the worst-case ASSR performance versus the transmit SNR for the robust secure beamforming scheme (denoted as "robust" in the legend) and the non-robust secure beamforming scheme (denote as "non-robust") with different channel uncertainties of the PE, where the transmitter is equipped with $N_t = 4$ transmit antennas. It is expected that our proposed RS scheme always outperforms the optimized NOMA scheme, which is due to the fact that NOMA scheme sacrifices the spatial multiplexing gains for enabling each user to decode the non-orthogonal superposition message. As such, the degree of freedom (DoF) of the NOMA scheme is smaller than that of the DoF of the RS scheme for resource allocation [37]. Indeed, the advantages of the proposed RS secure transmission scheme rely on the simultaneous transmission of the common message and the private messages [31], [33], [37], and the

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TWC.2020.3021725, IEEE Transactions on Wireless Communications

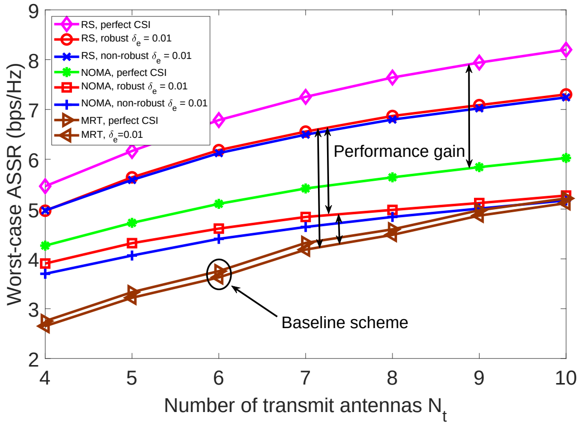


Fig. 4: Worst-case average secrecy sum rate versus the number of transmit antennas N_t. Performance comparison of the proposed RSMA/NOMA secure beamforming schemes and the baseline scheme based on the traditional MRT scheme, where SNR = 10 dB.

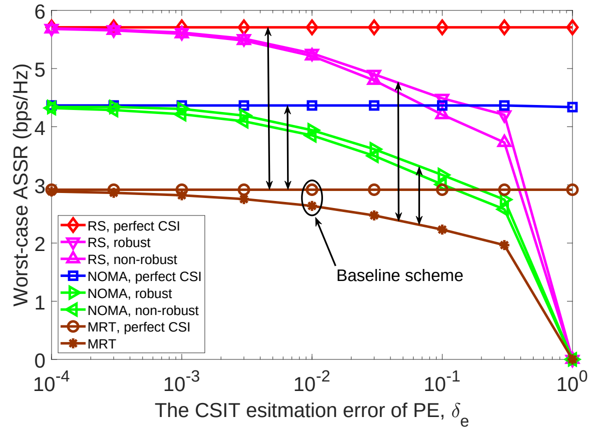


Fig. 5: Worst-case average secrecy sum rate versus the CSIT estimation error of PE, δ_e. Performance comparison of our proposed MISO-RSMA/NOMA schemes with the baseline scheme based on the traditional MRT scheme, where SNR $= 10$ dB and $N_t = 4$.

use of common messages as AN for the PE. Moreover, the proposed robust secure beamforming design algorithm for both the proposed RSMA and NOMA schemes outperform the non-robust ones under all the considered cases. It is due to the fact that the robust secure beamformers are designed with taking account into the imperfections of the CSIT estimation of the channel between the transmitter and the PE. In contrast, for the non-robust secure beamforming scheme, the estimated channel responses are treated as accurate channel responses without considering channel uncertainties to design the beamformers for secure communication. Thus, the system adopting non-robust strategy is unable to fully utilize the spatial resources for maximizing secure performance. In particular, the "non-robust" strategy fails to design accurate beamformers to focus the transmit power on the desired directions and increases the possibility of information leakage. As a result, the non-robust scheme achieves a worse secure performance compared to the robust beamforming design scheme, especially for the proposed MISO-NOMA schemes, since it sacrifices a part of spatial resource to realize the SIC of the non-orthogonal superimposition part.

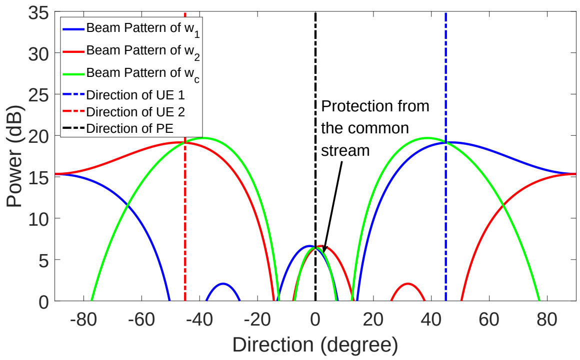
In addition, Fig. 4 depicts the worst-case ASSR performance versus the number of transmit antennas for the proposed RSMA and NOMA secure transmission schemes. Similarly, the worst-case ASSR performance of the robust secure beamforming scheme outperforms the non-robust one. In particular, with the increasing number of transmit antennas N_t, the worst-case ASSR performance of the considered system can be improved significantly, as there are more DoF introduced by the additional antennas. In other words, the transmitter is able to form sharp energy-focusing beams steered towards the desired users to improve transmit efficiency. Meanwhile, the pencil-like beams can reduce the potential information leakage to the PE. As a result, the secure performance of the considered system can be substantially improved, which is shown by Fig. 4. Furthermore, the secure performance of a baseline scheme (denoted as "MRT" in the legend) is also shown in Fig. 3 and Fig. 4 to reflect the performance gains obtained by our proposed schemes. It is noted that the ASSR performance of the baseline scheme will gradually saturate with the increasing transmit power. This is due to the fact that the inter-user interference creases a severe performance bottleneck in the high SNR regimes. On the other hand, the existence of the PE has not been considered in the baseline, which decreases its capability to guarantee communication security compared to the proposed schemes. Thus, the performance of the baseline scheme is always worse than the proposed schemes.

C. Worst-Case ASSR Performance Versus Channel Estimation Error δ_e

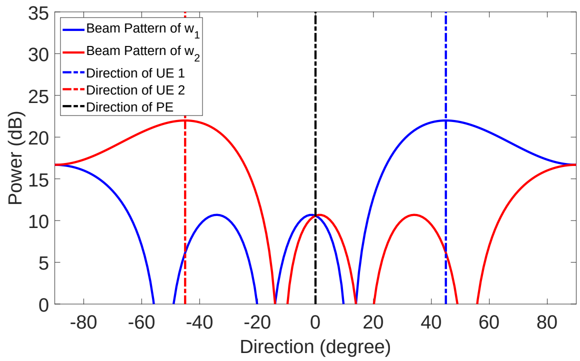
Fig. 5 shows the worst-case ASSR performance versus the channel estimation error of the PE, δ_e, for the proposed secure transmission schemes with robust and non-robust designed beamforming, where $N_t = 4$ and SNR $= 10$ dB. It can be observed that the average ASSR performance degrades for all the schemes when the quality of the CSIT decreases as inaccurate CSIT does not facilitate the formation of directional information carrying beams for secure communications. Moreover, thanks to the proposed optimization framework, the performance of the RS scheme still outperforms the NOMA scheme despite the existence of the imperfect CSIT.

In addition, Fig. 5 includes the performance of a benchmark scheme and a baseline scheme, based on the perfect CSIT case of the PE and the traditional MRT strategy, respectively. The benchmark scheme exploits the perfect CSIT of the PE which can fully exploit the spatial resources offered by the multiple-antenna system for secure beamforming design. Thus, its performance serves as a performance upper bound for the corresponding schemes that have only access to imperfect CSIT. In contrast, the performance of the traditional baseline scheme is worse than that of the proposed schemes. In particular, the baseline scheme is unable to fully exploit the spatial resources, since the beamformer designed by MRT strategy only focuses the power on the direction aimed to the desired user without considering the existing of the PE.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TWC.2020.3021725, IEEE Transactions on Wireless Communications

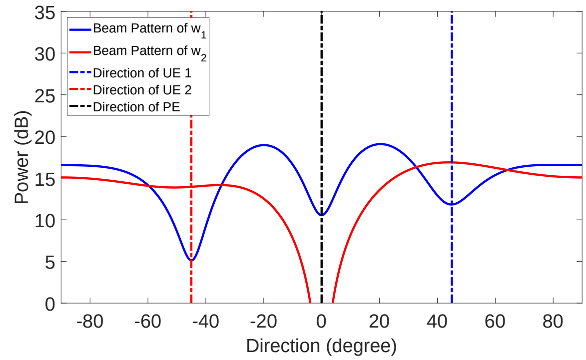


(a) The proposed RS secure beam patterns.

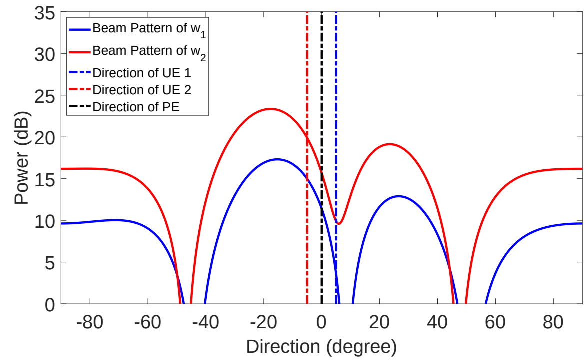


(b) Traditional MRT beam patterns.

Fig. 6: Comparison of our proposed RS and the traditional MRT secure beam patterns under the imperfect CSIT case, where δ_e = 0.01, SNR = 25 dB, and $\{\phi_1,\ \phi_2,\ \phi_e\}$=$\{45°, -45°, 0°\}$.



(a) With the orthogonal channel.



(b) With the degraded channel.

Fig. 7: Comparison of the orthogonal channel, i.e., $\{\phi_1,\phi_2,\phi_e\}$=$\{45°,-45°,0°\}$, and the degraded channel, i.e., $\{\phi_1,\phi_2,\phi_e\}$=$\{5°,-5°,0°\}$, for our proposed NOMA secure beam patterns under the imperfect CSIT case of the PE, where $\delta_e = 0.01$, SNR = 25 dB.

D. Beam Patterns of Each Beam Versus Beam Directions

To further analyze the efficacy of the proposed secure MISO-RSMA transmission scheme, we consider an illustrative example. In particular, the uniform linear array channel model for the space between successive array elements is half of the carrier wavelength where the channel vectors $\mathbf{h}_k, \forall k \in \mathcal{K}$ and $\mathbf{g}$ possess a Vandermonde structure [55], $\mathbf{v}(\phi) = \frac{1}{\sqrt{N_t}}[1,\ e^{j\theta},\ \ldots,\ e^{j(N_t-1)\theta}]^T$, where $j = \sqrt{-1}$, $\theta = -\pi\sin(\phi\pi/180)$, and $\phi \in [-90°, 90°)$. In Fig. 6, the beam patterns of the optimized beamforming vectors, achieved by solving problem (9) for the RS scheme with the imperfect CSIT of the PE, are shown, where SNR = 25 dB, $\{\phi_1,\ \phi_2,\ \phi_e\}$=$\{45°, -45°, 0°\}$, and $\mathbf{g} = \mathbf{v}(\phi_e), \mathbf{h}_k = \mathbf{v}(\phi_k), \forall k \in \mathcal{K}$. In addition, we study the beam patterns of the proposed NOMA scheme with both orthogonal and degraded channel conditions, i.e., $\{\phi_1,\ \phi_2,\ \phi_e\}$=$\{45°,\ -45°,\ 0°\}$, and $\{5°,\ -5°,\ 0°\}$, shown by Fig. 7(a) and Fig. 7(b) respectively. The orthogonal channel condition denotes that the channels of any two users are orthogonal to each other. The degraded channel condition denotes that the channel of UE 1 is aligned with that of UE 2. In this section, we introduce the definition in [42] that if the angle between any two channels is larger than $\frac{4\pi}{9}$ or less than $\frac{\pi}{9}$, then the channels of users are considered to be sufficiently orthogonal or aligned, respectively.

From Fig. 6, we can observe that the optimized private beamformer for a legitimate user in the RS scheme create some spatial null along the direction of the other one, which facilitates to decrease the inter-user interference. In contrast, the transmit powers of two private beamformers are steered towards the direction of the PE for effective mutual jamming. Moreover, the beam of the common message is also aimed to the direction of the PE. Yet, the optimized power carried by the common beam is not sufficient for enabling the common message to be decoded by the PE. As a result, the common message can be used as an AN signal for the PE to protect the private messages from eavesdropping. Thus, the optimized common beamformer was steered towards the direction of the PE with an appropriate optimized power, shown as the green line in Fig. 6(a). As a result, for the PE, the common message is used as AN to decrease the eavesdropping capacity of the private messages, which improves the security of the private messages. It reflects the ability of our proposed secure transmission scheme for guaranteeing the PHY layer security in downlink MISO systems.

In contrast, the signal beams in traditional MRT scheme, shown by Fig. 6(b), do not offer security protection as the common message does in the RSMA scheme. In addition, it is also noted that the beam intended to some legitimate user does not necessarily create a spatial null along the direction of the other one. Thus, with the increases of transmit SNR, the corresponding received SINR of each legitimate user

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TWC.2020.3021725, IEEE Transactions on Wireless Communications

$$\mathrm{Tr}(\sum_{m\in\mathcal{M}}\mathbf{W}_m^{(n-1)}(\hat{\mathbf{g}}\Delta\mathbf{g}^H)) = \Delta\mathbf{g}^H\left(\sum_{m\in\mathcal{M}}\mathbf{W}_m^{(n-1)}\right)\hat{\mathbf{g}} = \sqrt{\left(\Delta\mathbf{g}^H(\sum_{m\in\mathcal{M}}\mathbf{W}_m^{(n-1)})\hat{\mathbf{g}}\right)^2}$$
$$\leq \sqrt{\mathrm{Tr}(\Delta\mathbf{g}^H\Delta\mathbf{g})\mathrm{Tr}\left((\sum_{m\in\mathcal{M}}\mathbf{W}_m^{(n-1)})\hat{\mathbf{g}}\hat{\mathbf{g}}^H(\sum_{m\in\mathcal{M}}\mathbf{W}_m^{(n-1)^H})\right)} = \varepsilon\sqrt{\mathrm{Tr}\left((\sum_{m\in\mathcal{M}}\mathbf{W}_m^{(n-1)})\hat{\mathbf{g}}\hat{\mathbf{g}}^H(\sum_{m\in\mathcal{M}}\mathbf{W}_m^{(n-1)^H})\right)}. \quad (38)$$

$$\mathrm{Tr}(\sum_{m\in\mathcal{M}}\mathbf{W}_m^{(n-1)}(\Delta\mathbf{g}\Delta\mathbf{g}^H)) = \Delta\mathbf{g}^H\left(\sum_{m\in\mathcal{M}}\mathbf{W}_m^{(n-1)}\right)\Delta\mathbf{g} = \sqrt{\left(\Delta\mathbf{g}^H(\sum_{m\in\mathcal{M}}\mathbf{W}_m^{(n-1)})\Delta\mathbf{g}\right)^2}$$
$$\leq \sqrt{\mathrm{Tr}(\Delta\mathbf{g}^H\Delta\mathbf{g})\mathrm{Tr}\left((\sum_{m\in\mathcal{M}}\mathbf{W}_m^{(n-1)})\Delta\mathbf{g}\Delta\mathbf{g}^H(\sum_{m\in\mathcal{M}}\mathbf{W}_m^{(n-1)})^H\right)} = \varepsilon\sqrt{\mathrm{Tr}\left(\Delta\mathbf{g}^H(\sum_{m\in\mathcal{M}}\mathbf{W}_m^{(n-1)})^H(\sum_{m\in\mathcal{M}}\mathbf{W}_m^{(n-1)})\Delta\mathbf{g}\right)}$$
$$\leq \varepsilon^2\sqrt{\mathrm{Tr}\left((\sum_{m\in\mathcal{M}}\mathbf{W}_m^{(n-1)})^H(\sum_{m\in\mathcal{M}}\mathbf{W}_m^{(n-1)})\right)}. \quad (39)$$

will be degraded by each other's signal stream, i.e., inter-user interference. Similarly, the eavesdropping capability will eventually hit a ceiling due to the existence of strong inter-user interference in the high SNR regimes. As a result, the secrecy sum-rate performance of the conventional MRT scheme is driven to saturation in the high SNR regime, as confirmed in Fig. 2 and Fig. 3.

On the other hand, for the NOMA scheme based on the orthogonal channel condition shown as in Fig. 7(a), it can be noted that the beamformer for the weaker user, i.e., UE 2, also aims to UE 1, i.e., the strong user. Obviously, the power allocated to the beamformer of UE 2 is more powerful than that of UE 1, which facilitates the removal of the non-orthogonal superimposing message by applying the SIC technique. However, the beamformer of UE 2 creates some spatial null along the directions of the PE, which due to the fact that the NOMA scheme under the orthogonal channel condition cannot offer security protection for the message intended to UE 1. In contrast, for the degraded channel condition shown by Fig. 7(b), although some power of the beamforming aimed to UE 1 leaks to the direction of the PE, the more powerful signal intended to the weak user, i.e., UE 2, acts as AN offering security protection for the message intended to UE 1. Thus, NOMA scheme is more suitable for degraded channels.

VI. Conclusion

In this paper, we studied the robust resource allocation algorithm design for enabling secure MISO-RSMA wireless transmission system under the imperfect CSIT case of the PE, which was based on the worst-case uncertainties channel model. The algorithm design was formulated as a non-convex robust worst-case SRM problem via dually using the common message. The proposed problem aimed at simultaneously alleviating inter-user interference and maximizing the secrecy sum rate. We proposed an iterative algorithm based on SDP and SCA techniques which converge to a KKT point of the considered problem satisfying the rank-one constraint. Simulation results revealed the secure performance gains of the proposed transmission scheme in the high SNR regimes. Besides, the simulation results confirmed that the robustness of the proposed scheme outperforms the non-robust one which treats the estimated CSI as actual one for resource allocation. More importantly, our results revealed that the dual-used common message can guarantee the security of private messages in the proposed transmission scheme, which is not possible for the traditional scheme.

Appendix A
Proof of Equation (22)

According to (3) and problem (19), we can rewrite the objective function of (19) as:

$$\begin{aligned}\mathrm{T} =&\mathrm{Tr}\left(\sum_{m\in\mathcal{M}}\mathbf{W}_m^{(n-1)}(\hat{\mathbf{g}}\hat{\mathbf{g}}^H)\right)\\ &+2\mathrm{Re}\left\{\mathrm{Tr}\left(\sum_{m\in\mathcal{M}}\mathbf{W}_m^{(n-1)}(\hat{\mathbf{g}}\Delta\mathbf{g}^H)\right)\right\}\\ &+\mathrm{Tr}\left(\sum_{m\in\mathcal{M}}\mathbf{W}_m^{(n-1)}\Delta\mathbf{g}\Delta\mathbf{g}^H\right).\end{aligned} \quad (37)$$

Obviously, for given $\hat{\mathbf{g}}$ and $\mathbf{W}_m^{(n-1)}$ achieved by the $(n-1)$-th iteration, the first term of equality (37) is a constant. For the second term and the third term, we apply the Cauchy-Schwartz inequality, i.e., $\mathrm{Tr}[(\mathbf{A}^{\mathrm{T}}\mathbf{B})^2] \leq \mathrm{Tr}(\mathbf{A}^{\mathrm{T}}\mathbf{A})\mathrm{Tr}(\mathbf{B}^{\mathrm{T}}\mathbf{B})$, to find the maximal values. Besides, according to the optimization principle [47], when the optimal solution of problem (19) is achieved, the equality of the constraint in problem (19) must hold, i.e., $\Delta\mathbf{g}^H\Delta\mathbf{g} = \varepsilon^2$. Then, the processes are described by (38) and (39), shown at the top of this page. Here, the expression of (21) is proved.

Appendix B
Proof of Theorem 1

Here, we firstly investigate the rank condition of $\mathbf{W}_1^*$ by studying the KKT conditions of problem (33). By following a

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TWC.2020.3021725, IEEE Transactions on Wireless Communications

similar approach as in [46], [47], the Lagrangian function of problem (33) with respect to $\mathbf{W}_1^*$ can be expressed is given by (40) shown as below:

$$\begin{aligned}\mathcal{L}(\mathbf{W}_1^*) = &\sum_{k=1,2} \mu_k^*(\gamma_c \mathrm{Tr}(\mathbf{R}_{\mathbf{h}_k}\mathbf{W}_1^*)) - \mathrm{Tr}(\mathbf{M}_{\mathrm{C3}}^*\mathbf{S}_{\mathrm{C3}}) \\ &- \mathrm{Tr}(\mathbf{W}_1^*\mathbf{Y}_1^*) + \upsilon^*(\mathrm{Tr}(\mathbf{W}_1^*) - P_t) - \mathrm{Tr}(\mathbf{M}_{e_1}^*\mathbf{S}_{e_1}) \\ &+ \lambda_3^*(\tau_3 - \mathbf{h}_1^H\mathbf{W}_1^*\mathbf{h}_1) + \lambda_5^*(\mathbf{h}_2^H\mathbf{W}_1^*\mathbf{h}_2 - \tau_5), \quad (40)\end{aligned}$$

where $\mathbf{M}_{\mathrm{C3}}^*$, $\mathbf{Y}_1^*$, and $\mathbf{M}_{e_1}^* \succeq \mathbf{0}$ are the optimum dual variable matrices associated with constraints (33-C3), (33-C4), and $\mathbf{S}_{e_1} \succeq \mathbf{0}$ in (33-C7). Besides, $\mu_k^*, \forall k \in \mathcal{K}$, υ^*, λ_5^*, $\lambda_3^* \geq 0$ are the optimal dual variables associated with the constraints in (33-C2), (33-C5), and the constraints $\mathbf{h}_2^H\mathbf{W}_1^{(n)}\mathbf{h}_2 \leq \tau_5$, $\mathbf{h}_1^H\mathbf{W}_1^{(n)}\mathbf{h}_1 \geq \tau_3$ in (33-C8) and (33-C9), respectively. Then, the KKT conditions of (33) with respect to which are directly related to $\mathbf{W}_1^*$ are expressed as [47]:

$$\begin{aligned}&(41)\!: \mathbf{M}_{\mathrm{C3}}^*, \mathbf{Y}_1^*, \mathbf{M}_{e_1}^* \succeq \mathbf{0}, \qquad (42)\!: \mathbf{Y}_1^*\mathbf{W}_1^* = \mathbf{0}, \\ &(43)\!: \mathbf{W}_1^* \succeq \mathbf{0}, \qquad\qquad\quad (44)\!: \upsilon^*[\mathrm{Tr}(\mathbf{W}_1^*) - P_t] = 0.\end{aligned}$$

Next, we take partial derivative of $\mathcal{L}(\mathbf{W}_1^*)$ with respect to $\mathbf{W}_1^*$ and apply the KKT conditions, we have

$$\begin{aligned}\nabla_{\mathbf{W}_1^*}\mathcal{L}(\mathbf{W}_1^*) = &\sum_{k\in\mathcal{K}}(\mu_k^*\gamma_c\mathbf{h}_k\mathbf{h}_k^H) - \mathbf{Y}_1^* + \upsilon^*\mathbf{I}_{N_t} - \lambda_3^*\mathbf{h}_1\mathbf{h}_1^H \\ &+ \lambda_5^*\mathbf{h}_2\mathbf{h}_2^H + \mathbf{U}_e(\mathbf{M}_{e_1}^* - \mathbf{M}_{\mathrm{C3}}^*)\mathbf{U}_e^H. \quad (45)\end{aligned}$$

For $\nabla_{\mathbf{W}_1^*}\mathcal{L} = \mathbf{0}$, we have

$$\begin{aligned}\mathbf{Y}_1^* = &\upsilon^*\mathbf{I}_{N_t} - (\lambda_3^*\mathbf{h}_1\mathbf{h}_1^H + \mathbf{U}_e\mathbf{M}_{\mathrm{C3}}^*\mathbf{U}_e^H) \\ &+ \left(\sum_{k\in\mathcal{K}}\mu_k^*\gamma_c\mathbf{h}_k\mathbf{h}_k^H + \lambda_5^*\mathbf{h}_2\mathbf{h}_2^H + \mathbf{U}_e\mathbf{M}_{e_1}^*\mathbf{U}_e^H\right). \quad (46)\end{aligned}$$

For notational simplicity, we define

$$\begin{aligned}\mathbf{B}_1^* = &\lambda_3^*\mathbf{h}_1\mathbf{h}_1^H + \mathbf{U}_e\mathbf{M}_{\mathrm{C3}}^*\mathbf{U}_e^H \\ &- \left(\sum_{k\in\mathcal{K}}(\mu_k^*\gamma_c\mathbf{h}_k\mathbf{h}_k^H) + \lambda_5^*\mathbf{h}_2\mathbf{h}_2^H + \mathbf{U}_e\mathbf{M}_{e_1}^*\mathbf{U}_e^H\right), \quad (47)\end{aligned}$$

which is a Hermitian matrix. From (46), since matrix $\mathbf{Y}_1^* = \upsilon^*\mathbf{I}_{N_t} - \mathbf{B}_1^* \succeq \mathbf{0}$ is positive semi-definite for (41), $\upsilon^* \geq \lambda_{\mathbf{B}_1^*}^{\max} \geq 0$ must hold, where $\lambda_{\mathbf{B}_1^*}^{\max}$ is the real-valued maximum eigenvalue of matrix $\mathbf{B}_1^*$. Consider the KKT condition related to matrix $\mathbf{W}_1^*$ in (42), we can show that if $\upsilon^* > \lambda_{\mathbf{B}_1^*}^{\max}$, matrix $\mathbf{Y}_1^*$ will become positive definite and full rank. However, this will yield the solution $\mathbf{W}_1^* = \mathbf{0}$ where the corresponding SINR of the private message intended to the 1-th user will equal 0. On the other hand, when we have $\upsilon^* = \lambda_{\mathbf{B}_1^*}^{\max}$ and $\mathrm{Rank}(\mathbf{Y}_1^*) = N_t - 1$, the rank of matrix $\mathbf{W}_1^*$ equal to 1. By the same method, it is easy to prove that both $\mathbf{W}_c^*$ and $\mathbf{W}_2^*$ also satisfy Theorem 1. This completes the proof.

APPENDIX C
PROOF OF PROPOSITION 2

Noted that, by invoking the equations in (17) and (22), problem (33) can be solved by using the alternating optimization (AO) principle. First, $\{a_{k,1}\}_{k\in\mathcal{K}}$ and $\{a_{k,2}\}_{k\in\mathcal{K}}$ were optimized by solving (15) and (18), respectively. Then, $\{\mathbf{W}_m\}_{m\in\mathcal{M}}$ were updated by solving problem (33), which is formulated by fixing $\{a_{k,1}\}_{k\in\mathcal{K}}$ and $\{a_{k,2}\}_{k\in\mathcal{K}}$. Obviously, problem (33) is a SDP problem, and can be solved by interior-point methods. This procedure is repeated in an iterative manner as described in Algorithm 1. In other words, updating the sequence $\mathbf{\Gamma} = (\{a_{k,1}\}, \{a_{k,2}\}, \{\mathbf{W}_m\}), \forall k \in \mathcal{K}, m \in \mathcal{M}$, applied the successive convex approximation (SCA) method [38], [56]. Besides, the Slater's condition also holds for the convex approximated problem (33) [56]. Furthermore, since the iterations in Algorithm 1 lie in a nonempty, compact, and convex set, according to the Lemma in [46], any limit point of the AO procedure in Algorithm 1 is a KKT stationary point of problem (33) [56]. Hence, the convergence of problem (33) to the set of KKT points is proved.

In addition, since problem (33) is the convex approximated version of the original problem (9), we will prove that every stationary point of problem (33) in Algorithm 1 is also a stationary point of the original problem (9). Problem (33) can be rewritten as below:

$$\underset{\substack{\{\mathbf{W}_m^{(n)}\},\{a_{k,1}^{(n)}\},\{a_{k,2}^{(n)}\}\\ m\in\mathcal{M},k\in\mathcal{K}}}{\text{maximize}} \quad \Phi_1(\mathbf{\Gamma}^{(n)}) \qquad (48)$$

$$\begin{aligned}\text{s.t.}\ \ &\text{C1: } \mathbf{W}_m^{(n)} \succeq \mathbf{0},\ m \in \mathcal{M}, \\ &\text{C2: } \gamma_c^{(n)}\sum_{i\in\mathcal{K}}\mathrm{Tr}(\mathbf{R}_{\mathbf{h}_k}\mathbf{W}_i^{(n)}) + \gamma_c^{(n)}\sigma_k^2 - \mathrm{Tr}(\mathbf{R}_{\mathbf{h}_k}\mathbf{W}_c^{(n)}) \\ &\qquad \leq 0,\ k \in \mathcal{K}, \\ &\text{C3: } \mathbf{S}_{\mathrm{C3}} \succeq \mathbf{0}, \quad \text{C4: } \sum_{m\in\mathcal{M}}\mathrm{Tr}(\mathbf{W}_m^{(n)}) - P_t \leq 0, \\ &\text{C5: } \mathbf{S}_{e_m} \succeq \mathbf{0}, m \in \mathcal{M}, \\ &\text{C6: } \tau_3 - \mathbf{h}_1^H\mathbf{W}_1^{(n)}\mathbf{h}_1 \leq 0, \quad \text{C7: } \tau_4 - \mathbf{h}_1^H\mathbf{W}_2^{(n)}\mathbf{h}_1 \geq 0, \\ &\text{C8: } \tau_5 - \mathbf{h}_2^H\mathbf{W}_1^{(n)}\mathbf{h}_2 \geq 0, \quad \text{C9: } \tau_6 - \mathbf{h}_2^H\mathbf{W}_2^{(n)}\mathbf{h}_2 \leq 0,\end{aligned}$$

where the objective function can be expressed as below:

$$\Phi_1(\mathbf{\Gamma}^{(n)}) = \min_{k\in\mathcal{K}}\{PT_k^{(n)} + NT_{k,1}^{\mathrm{L}\,(n)} + NT_{k,2}^{\mathrm{L}\,(n)}(\alpha_k + 1)\}, \qquad (49)$$

where $NT_{k,1}^{\mathrm{L}\,(n)}$ and $NT_{k,2}^{\mathrm{L}\,(n)}$ are deduced by (13) and (14) for the n-th iteration.

Obviously, problem (48) is the equivalent reformulated version of the original problem (9) under the imperfect CSIT, where the rank-one constraints on $\{\mathbf{W}_m\}_{m\in\mathcal{M}}$ have been relaxed by Theorem 1, and the non-concave parts in the objective function of (9) have been reformulated by Proposition 1 for each iteration. Besides, the semi-infinite constraints for the imperfect CSIT have been tackled by Lemma 1. Similarly, we denote the objective function of problem (9) as

$$\Phi_2(\mathbf{\Gamma}) = \min_{k\in\mathcal{K}}\{R_{k,\mathrm{tot}}^{\mathrm{sec}}\}, \qquad (50)$$

where $R_{k,\mathrm{tot}}^{\mathrm{sec}}$ is given by (8). Since the objective function of (48) is concave, if $\mathbf{\Gamma}^*$ is a stationary point of (48), we will have

$$\mathrm{Tr}[\Delta_{\mathbf{W}_m}\Phi_1^H(\mathbf{\Gamma}^*)(\mathbf{W}_m - \mathbf{W}_m^*)] \leq 0,\ \forall m,\ (\text{C1}) - (\text{C9}), \qquad (51)$$

$$\nabla_{a_{k,1}}\Phi_1^H(\mathbf{\Gamma}^*)(a_{k,1} - a_{k,1}^*) \leq 0,\ \forall\ a_{k,1} \geq 0, \forall k, m, \quad (52)$$

$$\nabla_{a_{k,2}}\Phi_1^H(\mathbf{\Gamma}^*)(a_{k,2} - a_{k,2}^*) \leq 0,\ \forall\ a_{k,2} \geq 0, \forall k, m. \quad (53)$$

From Proposition 1, (17), (22), (52), and (53), we have

$$a_{k,1}^* = (\mathbf{h}_k^H \mathbf{W}_i^* \mathbf{h}_k + \sigma_k^2)^{-1},\ i \neq k, k \in \mathcal{K}, \tag{54}$$

$$a_{k,2}^* = (\mathbf{g}^H \sum_{m\in\mathcal{M}} \mathbf{W}_m^* \mathbf{g} + \sigma_e^2)^{-1},\ k \in \mathcal{K}. \tag{55}$$

By substituting (54) and (55) into (51), we achieve that

$$\nabla_{\mathbf{W}_m} \Phi_1(\mathbf{\Gamma}^*) = \nabla_{\mathbf{W}_m} \Phi_2(\{\mathbf{W}_m^*\}_{m\in\mathcal{M}})^H,\ k \in \mathcal{K}, m \in \mathcal{M}. \tag{56}$$

Based on (51) and (56), we conclude that

$$\begin{aligned}&\mathrm{Tr}[\nabla_{\mathbf{W}_m} \Phi_2(\{\mathbf{W}_m^*\}_{m\in\mathcal{M}})^H (\mathbf{W}_m - \mathbf{W}_m^*)] \leq 0,\ m \in \mathcal{M},\\ &(\mathrm{C1}) - (\mathrm{C9}),\end{aligned} \tag{57}$$

where (C1)−(C9) are the same as the ones in (48). In other words, the solution, i.e., $\{\mathbf{W}_m^*\}_{m\in\mathcal{M}}$, existed in $\mathbf{\Gamma}^*$ for problem (48), is also an optimal solution of the following problem:

$$\begin{aligned}&\underset{\{\mathbf{W}_m^{(n)}\}}{\mathrm{maximize}}\ \nabla_{\mathbf{W}_m} \Phi_2(\{\mathbf{W}_m^*\}_{m\in\mathcal{M}})^H (\mathbf{W}_m - \mathbf{W}_m^*)\\ &\mathrm{s.t.}\quad (\mathrm{C1}) - (\mathrm{C9}),\end{aligned} \tag{58}$$

where (C1)−(C9) are the same as the ones in (48). Hence, $\{\mathbf{W}_m^*\}_{m\in\mathcal{M}}$ also satisfy the KKT conditions of (58) which are listed as follows:

$$\begin{aligned}&\mathbf{W}_m^* \succeq \mathbf{0},\ \mathbf{S}_{e_m}(\mathbf{W}_m^*) \succeq \mathbf{0},\ \mathbf{S}_{\mathrm{C3}}(\{\mathbf{W}_m^*\}) \succeq \mathbf{0},\ \forall m,\\
&\hat{\mathbf{Y}}_m \succeq \mathbf{0},\ \hat{\mathbf{M}}_{e_m} \succeq \mathbf{0},\ \forall m,\ \hat{\mathbf{M}}_{\mathrm{C3}} \succeq \mathbf{0},\ \forall m,\\
&\hat{\lambda}_{\mathrm{C}_i} \geq 0,\ f_{\mathrm{C}_i}(\{\mathbf{W}_m^*\}_{m\in\mathcal{M}}) \leq 0,\ \forall i \in \mathcal{I},\\
&\mathbf{Y}_m \mathbf{W}_m^* = \mathbf{0},\ \hat{\mathbf{M}}_{e_m} \mathbf{S}_{e_m}(\mathbf{W}_m^*) = \mathbf{0},\ \hat{\mathbf{M}}_{\mathrm{C3}} \mathbf{S}_{\mathrm{C3}}(\{\mathbf{W}_m^*\}) = \mathbf{0},\\
&\hat{\lambda}_{\mathrm{C}_i} f_{\mathrm{C}_i}(\{\mathbf{W}_m^*\}_{m\in\mathcal{M}}) = 0,\ \forall i, m,\\
&\nabla_{\mathbf{W}_m} \Phi_2(\{\mathbf{W}_m^*\}_{m\in\mathcal{M}}) + \sum_{i=4}^{9} \hat{\lambda}_{\mathrm{C}_i} \nabla_{\mathbf{W}_m} f_{\mathrm{C}_i}(\{\mathbf{W}_m^*\}_{m\in\mathcal{M}})\\
&- \mathbf{Y}_m - \sum_{m\in\mathcal{M}} \hat{\mathbf{M}}_{e_m} \nabla_{\mathbf{W}_m} \mathbf{S}_{e_m} - \hat{\mathbf{M}}_{\mathrm{C3}} \nabla_{\mathbf{W}_m} \mathbf{S}_{\mathrm{C3}}(\{\mathbf{W}_m^*\}) = \mathbf{0},\\
&\forall m \in \mathcal{M},\ i \in \mathcal{I},\ \mathcal{I} = \{4,5,6,7,8,9\},\end{aligned} \tag{59}$$

where $\{\hat{\mathbf{Y}}_m\}_{m\in\mathcal{M}}$, $\{\mathbf{S}_{e_m}\}_{m\in\mathcal{M}}$, $\mathbf{S}_{\mathrm{C3}}$, and $\{\hat{\lambda}_{\mathrm{C}_i}\}_{i\in\mathcal{I}}$ are Lagrangian multipliers. Unquestionably, the conditions in (59) are also exactly the KKT conditions of the original problem (9) with the imperfect CSIT of the PE. Hence, Proposition 2 is proved.

References

[1] C. Lim, T. Yoo, B. Clerckx, B. Lee, and B. Shim, "Recent trend of multiuser MIMO in LTE-advanced, "*IEEE Commun. Maga.*, vol. 51, no. 3, pp. 127-135, Mar. 2013.

[2] J. Zhang, et al., "Prospective multiple antenna technologies for beyond 5G," *IEEE J. Sel. Areas Commun.*, vol. 38, no. 8, pp. 1637-1660, Aug. 2020.

[3] Z. Wei, L. Yang, D. W. K. Ng, J. Yuan, and L. Hanzo, "On the performance gain of NOMA over OMA in uplink communication systems," *IEEE Trans. Commun.*, vol. 68, no. 1, pp. 536-568, Jan. 2020.

[4] M. Bloch and J.Barros, "Physical-layer security: from information theory to security engineering", *1st ed. Cambridge, U.K.: Cambridge Univ. Press*, 2011.

[5] T. Lv, J. Yin, Y. Lu, S. Yang, E. Liu, and G. Clapworthy, "Physical detection of misbehavior in relay systems with unreliable channel state information," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 7, pp. 1517-1530, Jul. 2018.

[6] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no.8, pp. 1355-387, Oct. 1975, Tech. Rep.

[7] L. Jiang, H. Tian, C. Qin, S. Gjessing, and Y. Zhang, "Secure beamforming in wireless-powered cooperative cognitive radio networks," *IEEE Commun. Lett.*, vol. 20, no. 3, pp. 522-525, Mar. 2016.

[8] M. Zhang and Y. Liu, "Secure beamforming for untrusted MISO cognitive radio networks," *IEEE Trans. Wireless Commun.*, vol. 17, no. 7, pp. 4861-4872, Jul. 2018.

[9] Q. Li, Q. Zhang, and J. Qin, "Secure relay beamforming for SWIPT in amplify-and-forward two-way relay networks," *IEEE Trans. Veh. Technol.*, vol. 65, no. 11, pp. 9006-9019, Nov. 2016.

[10] D. W. K. Ng, E. S. Lo, and R. Schober, "Robust beamforming for secre communication in systems with wireless information and power transfer," *IEEE Trans. Wireless Commun.*, vol. 13, no. 8, pp. 4599-4615, Aug. 2014.

[11] T. Lv, H. Gao, and S. Yang, "Secrecy transmit beamforming for heterogeneous networks," *IEEE J. Sel. Areas Commun.*, vol. 33, no. 6, pp. 1154-1170, Jun. 2015.

[12] S. Gong, C. Xing, S. Ma, Z. Zhang, and Z. Fei, "Secure wideband beamforming design for two-way MIMO relaying systems," *IEEE Trans. Veh. Technol.*, vol. 68, no. 4, pp. 3472-3486, Apr. 2019.

[13] Y. Sun, D. W. K. Ng, J. Zhu, and R. Schober, "Multi-objective optimization for robust power efficient and secure full-duplex wireless communication systems," *IEEE Trans. Wireless Commun.*, vol. 15, no. 8, pp. 5511-5526, Aug. 2016.

[14] Y. Li, M. Jiang, Q. Zhang, Q. Li, and J. Qin, "Secure beamforming in downlink MISO non-orthogonal multiple access systems," *IEEE Trans. Veh. Technol.*, vol. 66, no. 8, pp. 7563-7567, Aug. 2017.

[15] M. Jiang, Y. Li, Q. Zhang, Q. Li, and J. Qin, "Secure beamforming in downlink MIMO non-orthogonal multiple access networks," *IEEE Signal Process Lett.*, vol. 24, no. 12, pp. 1852-1856, Dec. 2017.

[16] M. Tian, Q. Zhang, S. Zhao, Q. Li, and J. Qin, "Secrecy sum rate optimization for downlink MIMO non-orthogonal multiple access systems," *IEEE Signal Process Lett.*, vol. 24, no. 8, pp. 1113-1117, Aug. 2017.

[17] Y. Sun, D. W. K. Ng, J. Zhu, and R. Schober, "Robust and secure resource allocation for full-duplex MISO multicarrier NOMA systems," *IEEE Trans. Commun.*, vol. 66, no. 9, pp. 4119-4137, Sep. 2018.

[18] R. Negi and S. Goel, "Secret communication using artificial noise," in *Proc. IEEE Veh. Technol. Conf. (VTC)*, Sep. 2005, pp. 1906-1910.

[19] S. Fakoorian and A. Swindlehurst, "Solution for the MIMO gaussian wiretap channel with a cooperative jammer," *IEEE Trans. Signal Process.*, vol. 59, no. 10, pp. 5013-5022, Oct. 2011.

[20] W. Liao, T. Chang, W. Ma, and C. 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.

[21] Q. Li, W. Ma, and A. M. So, "Safe convex approximation to outage based MISO secrecy rate optimization under imperfect CSI and with artificial noise," in *Proc. ASILOMAR Conf. Comput. Commun. Signals, Syst. Comput.*, Nov. 2011, pp. 207-211.

[22] J. Zhu, R. Schober, and V. Bhargava, "Linear precoding of data and artificial noise in secure massive MIMO systems," *IEEE Trans. Wireless Commun.*, vol. 15, no. 3, pp. 2245-2261, Mar. 2016.

[23] W. Tang, S. Feng, Y. Ding, and L. Yuan, "Physical layer security in heterogeneous networks with jammer selection and full-duplex users," *IEEE Trans. Wireless Commun.*, vol. 16, no. 12, pp. 7982-7995, Dec 2017.

[24] M. Zhang, Y. Liu, and R. Zhang, "Artificial noise aided secrecy information and power transfer in OFDMA systems," *IEEE Trans. Wireless Commun.*, vol. 15, no. 4, pp. 3085-3096, Apr. 2016.

[25] A. Wolf and E. Jorswieck, "Maximization of worst-case secrecy rates in MIMO wiretap channels," presented at the *Asilomar Conf. Signals, Syst., Comput.*, Pacific Grove, CA, USA, Nov. 2010.

[26] Q. Li and W. 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.

[27] J. Huang and A. 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.

[28] Q. Li and W. Ma, "Spatially selective artificial-noise aided transmit optimization for MISO multi-eves secrecy rate maximization," *IEEE Trans. Signal Process*, vol. 61, no. 10, pp. 2704-2717, May 2013.

[29] S. Gerbracht, C. Scheunert, and E. Jorswieck, "Secrecy outage in MISO systems with partial channel information," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 2, pp. 704-716, Apr. 2012.

[30] S. Luo, J. Li, and A. Petropulu, "Outage constrained secrecy rate maximization using cooperative jamming," *IEEE Statist. Signal Process*, Workshop (SSP), Aug. 2012.

[31] B. Clerckx, H. Joudeh, C. Hao, M. Dai, and B. Rassouli, "Rate splitting for MIMO wireless networks: a promising PHY-layer strategy for LTE evolution," *IEEE Commun. Maga.*, vol. 54, no. 5, pp. 98-105, May 2016.

[32] A. El Gamal and Y. H. Kim, "Network Information Theory," *Cambridge Univ. Press*, 2011.

[33] C. Hao, Y. Wu, and B. Clerckx, "Rate analysis of two-receiver MISO broadcast channel with finite rate feedback: A rate-splitting approach," *IEEE Trans. Commun*, vol. 63, no. 9, pp. 3232-3246, Sep. 2015.

[34] M. Dai, B. Clerckx, D. Gesbert, and G. Caire, "A rate splitting strategy for massive MIMO with imperfect CSIT," *IEEE Trans. Wireless Commun.*, vol. 15, no. 7, pp. 4611-4624, Jul. 2016.

[35] H. Joudeh and B. Clerckx, "Sum-rate maximization for linearly precoded downlink multiuser MISO systems with partial CSIT: A rate splitting approach," *IEEE Trans. Commun.*, vol. 64, no. 11, pp. 4847-4861, Nov. 2016.

[36] A. R. Flores, B. Clerckx, and R. C. de Lamare, "Tomlinson-Harashima precoded rate-splitting for multiuser multiple-antenna systems," *15th International Symposium on Wireless Communication Systems*, 2018.

[37] H. Joudeh and B. Clerckx, "Rate-splitting for max-min fair multigroup multicast beamforming in overloaded systems," *IEEE Trans. Wireless Commun.*, vol. 16, no. 11, pp. 7276-7289, Nov. 2017.

[38] H. Joudeh and B. Clerckx, "Robust transmission in downlink multiuser MISO systems: A rate-splitting approach," *IEEE Trans. Signal Process*, vol. 64, no. 23, pp. 6227-6242, Dec. 2016.

[39] A. Papazafeiropoulos and T. Ratnarajah, "Rate-splitting robustness in multi-pair massive MIMO relay systems," *IEEE Trans. Wireless Commun.*, vol. 17, no. 8, pp. 5623-5636, Aug. 2018.

[40] A. Papazafeiropoulos, B. Clerckx, and T. Ratnarajah, "Rate-splitting to mitigate residual transceiver hardware impairments in massive MIMO systems," *IEEE Trans. Veh. Technol.*, vol. 66, no. 9, pp. 8196-8211, Sep. 2017.

[41] Y. Mao, B. Clerckx, and V. Li, "Rate-splitting for multi-antenna non-orthogonal unicast and multicast transmission: spectral and energy efficiency analysis," *IEEE Trans. Commun.*, vol. 67, no. 12, pp. 8754-8770, Dec. 2019.

[42] Y. Mao, B. Clerckx, and V. Li, "Rate-splitting multiple access for downlink communication systems: Bridging, generalizing and outperforming SDMA and NOMA," *Eurasip Journal on Wireless Communications and Networking*, in press.

[43] B. Clerckx, Y. Mao, R. Schober, and H. V. Poor, "Rate-splitting unifying SDMA, OMA, NOMA, and multicasting in MISO broadcast channel: a simple two-user rate analysis," *IEEE Wireless Commun. Lett.*, vol. 9, no. 3, pp. 349-353, Mar. 2020.

[44] Y. Zhang, H. 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, May 2016.

[45] N. Nandan, S. Majhi, and H. C. Wu, "Secure beamforming for MIMO-NOMA based cognitive radio network," *IEEE Commun. Lett.*, vol. 22, no. 8, pp. 1708-1711, Aug. 2018.

[46] R. Feng, Q. Li, Q. Zhang, and J. Qin, "Robust secure beamforming in MISO full-duplex two-way secure communications," *IEEE Trans. Veh. Technol.*, vol. 65, no. 1, pp. 408-414, Jan. 2016.

[47] S. Boyd and L. Vanderberghe, "Convex Optimization," *Cambridge, U.K.: Cambridge Univ. Press*, 2004.

[48] M. Grant and S. Boyd. (2016). "CVX: MATLAB Software for Disciplined Convex Programming," [Online]. Available: http://cvxr.com/cvx.

[49] D. W. K. Ng and R. Schober, "Max-min fair wireless energy transfer for secure multiuser communication systems," in *2014 IEEE Information Theory Workshop (ITW 2014)*, 2014, pp. 326-330.

[50] I. Polik and T. Terlaky, "Interior point methods for nonlinear optimization," in *Nonlinear Optimization*, 1st ed. G. Di Pillo and F. Schoen, Eds. New York, NY, USA: Springer, 2010.

[51] M. Costa, "Writing on dirty paper," *IEEE Trans. Inf. Theory*, vol. IT-29, pp. 439-441, May 1983.

[52] R. Liu, T. Liu, H. V. Poor, and S. Shamai, "MIMO Gaussian broadcast channels with confidential and common messages," *IEEE International Symposium on Information Theory*, Austin, TX, 2010, pp. 2578-2582.

[53] Z. Tu et al., "Multiuser diversity for a dirty paper approach," *IEEE Commun. Lett.*, vol. 7, no. 8, pp. 370-372, Aug. 2003.

[54] G. Caire and S. Shamai, "On the achievable throughput of a multiantenna Gaussian broadcast channel," *IEEE Trans. Inf. Theory*, vol. 49, no. 7, pp. 1691-1706, Jul. 2003.

[55] W. Liao, et al., "Joint transmit beamforming and artificial noise design for QoS discrimination in wireless downlink," *2010 IEEE International Conference on Acoustics, Speech and Signal Processing*, pp. 2562-2565, 2010.

[56] M. Razaviyayn, "Successive convex approximation: analysis and applications," Ph.D. dissertation, Univ. of Minnesota, Minneapolis, MN, USA, 2014.

Hao Fu received the B.E. degree in electrical engineering and automation from He Fei University of Technology, Hefei, China, and the M.E. degree in electronics and communications engineering from South China University of Technology, Guangzhou, China, in 2012 and 2016, respectively. He is currently pursuing the Ph.D. degree with the School of Electronic and Information Engineering, South China University of Technology, Guangzhou, China. His research interests include physical layer security, rate splitting multiple access, and the application of convex optimization in wireless communications.

Suili Feng (M'05) received the B.S. degree in electrical engineering from South China Institute of Technology, Guangzhou, China, and the M.S. and Ph.D. degrees in electronic and communication system from South China University of Technology, Guangzhou, China, in 1982, 1989, and 1998, respectively. He was a Research Assistant with Hong Kong Polytechnic University, Hung Hom, Hong Kong, from 1991 to 1992, and a Visiting Scholar at the University of South Florida, Tampa, FL, USA, from 1998 to 1999. He has been with South China University of Technology since 1989, where he currently works as a Professor with the School of Electronic and Information Engineering. His research interests include wireless networks, computer networks, and communication signal processing.

Weijun Tang received the B.E. degree in information engineering, and the Ph.D. degree in information and communication engineering from South China University of Technology, Guangzhou, China, in 2012 and 2018, respectively. He is currently a Postdoctoral Fellow in the School of Electronic and Information Engineering, South China University of Technology, Guangzhou, China. His research interests include future cellular networks, full duplex, low latency and ultra-reliable communications, IoT, stochastic geometry and resource allocation in wireless networks.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TWC.2020.3021725, IEEE Transactions on Wireless Communications

Derrick Wing Kwan Ng (S'06-M'12-SM'17) received the bachelor degree with first-class honors and the Master of Philosophy (M.Phil.) degree in electronic engineering from the Hong Kong University of Science and Technology (HKUST) in 2006 and 2008, respectively. He received his Ph.D. degree from the University of British Columbia (UBC) in 2012. He was a senior postdoctoral fellow at the Institute for Digital Communications, Friedrich-Alexander-University Erlangen-Nürnberg (FAU), Germany. He is now working as a Senior Lecturer and a Scientia Fellow at the University of New South Wales, Sydney, Australia. His research interests include convex and non-convex optimization, physical layer security, IRS-assisted communication, UAV-assisted communication, wireless information and power transfer, and green (energy-efficient) wireless communications.

Dr. Ng received the Australian Research Council (ARC) Discovery Early Career Researcher Award 2017, the Best Paper Awards at the IEEE TCGCC Best Journal Paper Award 2018, INISCOM 2018, IEEE International Conference on Communications (ICC) 2018, IEEE International Conference on Computing, Networking and Communications (ICNC) 2016, IEEE Wireless Communications and Networking Conference (WCNC) 2012, the IEEE Global Telecommunication Conference (Globecom) 2011, and the IEEE Third International Conference on Communications and Networking in China 2008. He has been serving as an editorial assistant to the Editor-in-Chief of the IEEE Transactions on Communications from Jan. 2012 to Dec. 2019. He is now serving as an editor for the IEEE Transactions on Communications, the IEEE Transactions on Wireless Communications, and an area editor for the IEEE Open Journal of the Communications Society. Also, he is listed as a Highly Cited Researcher by Clarivate Analytics in 2018 and 2019.