Hindawi
Security and Communication Networks
Volume 2021, Article ID 5526485, 9 pages
https://doi.org/10.1155/2021/5526485

Research Article

Robust Secure Beamforming Design for Cooperative Cognitive Radio Nonorthogonal Multiple Access Networks

Quanzhong Li [1] **and Sai Zhao** [2]

[1] *The School of Computer Science and Engineering, Sun Yat-sen University, Guangzhou 510006, China*
[2] *The School of Electronics and Communication Engineering, Guangzhou University, Guangzhou 510006, China*

Correspondence should be addressed to Quanzhong Li; liquanzh@mail.sysu.edu.cn

Received 20 January 2021; Revised 23 February 2021; Accepted 2 March 2021; Published 19 March 2021

Academic Editor: Mamoun Alazab

By the integration of cooperative cognitive radio (CR) and nonorthogonal multiple access (NOMA), cooperative CR NOMA networks can improve the spectrum efficiency of wireless networks significantly. Due to the openness and exposure of wireless signals, secure communication is an important issue for cooperative CR NOMA networks. In this paper, we investigate the physical layer security design for cooperative CR NOMA networks. Our objective is to achieve maximum secrecy rate of the secondary user by designing optimal beamformers and artificial noise covariance matrix at the multiantenna secondary transmitter under the quality-of-service at the primary user and the transmit power constraint at the secondary transmitter. We consider the practical case that the channel state information (CSI) of the eavesdropper is imperfect, and we model the imperfect CSI by the worst-case model. We show that the robust secrecy rate maximization problem can be transformed to a series of semidefinite programmings based on *S*-procedure and rank-one relaxation. We also propose an effective method to recover the optimal rank-one solution. Simulations are provided to show the effectiveness of our proposed robust secure algorithm with comparison to the nonrobust secure design and traditional orthogonal multiple access schemes.

1. Introduction

Cooperative cognitive radio (CR) is a promising technique for easing the strain on the spectrum resources, where the secondary user (SU) works as a relaying station and assists the primary user (PU) to transmit the signals, and as a return, the SU can use the spectrum occupied by the PU to serve its own cognitive user [1–5]. Nonorthogonal multiple access (NOMA) is an effective and new technique over conventional orthogonal multiple access (OMA) to enhance the spectrum efficiency, through transmitting the superposition of the weighted version of the strong (central) and weak (edge) users' signals and employing successive interference cancellation (SIC) at the strong user [6–11]. By the integration of cooperative CR and NOMA techniques, cooperative CR NOMA networks can improve spectrum utilization efficiency and information rate significantly [12–14].

In the early days, information security was mainly focused on wired communication, where gateway selection algorithm [15], multilayer botnet detection technique [16], and intelligent spam e-mail detection [17] could be used to improve the communication security. For wireless communication, because of the openness of the wireless transmission medium, wireless information is susceptible to eavesdropping. Then, more attention is paid to the information security of wireless communication where clone node detection [18], machine learning [19], physical layer security [20], and so on can be employed to enhance the information security. Secure communication is also a critical issue for cooperative CR NOMA networks. Recently, physical layer security has been proposed in [21–27] for cooperative CR NOMA networks, where the security performance of communication networks can be greatly improved by the cooperation of the relay node (i.e., SU). The authors in [21] studied the physical layer security in a cooperative CR NOMA network where all the nodes had a single antenna and the SU employed amplify-and-forward (AF) relaying to forward the PU's signal, aiming to analyze the security performance of the PU and throughput of the SU. In the study by Chen et al. [22], the authors considered a cooperative CR NOMA network with decode-and-forward (DF) relaying and designed the relay beamforming to improve the security of the PU. In the study by She et al. [23], the authors investigated the optimization of power allocation and transmit covariance matrix to improve the security energy efficiency of the SU for a DF-relaying cooperative CR NOMA network. The works [25–27] also focused on the DF-relaying cooperative CR NOMA network in order to analyze the security performance of the network.

Most existing works for physical layer security in cooperative CR NOMA networks consider the analysis of the security performance, e.g., [21, 24–27], but only few works consider the physical layer security optimization, e.g., [22, 23]. Besides, physical layer security optimization for conventional cooperative CR NOMA networks is investigated in [28]. It is worth noting that the optimization design to improve the physical layer security of cooperative CR NOMA networks highly depends on the channel state information (CSI) of the eavesdropper. However, the works [22, 23, 28] consider that the CSI of the eavesdropper is perfect, which is impractical. In fact, getting the perfect CSI of the eavesdropper is very hard or even impossible. Under such cases, the imperfect CSI of the eavesdropper may be obtained in practice, based on the past channel observations or a priori knowledge of the particular propagation environment [29].

In this paper, we focus on secure beamforming and artificial noise (AN) covariance matrix design problem for a cooperative CR NOMA network, where the CSI of the eavesdropper is considered to be imperfect. We investigate AF relaying in the cooperative CR NOMA network, where the multiantenna secondary transmitter (ST) helps relaying the information from the primary transmitter (PT) to the PU and serves its own SU, while an eavesdropper located near the SU intends to overhear the signal intended for the SU. By employing the worst model to model the imperfect CSI of the eavesdropper, we aim to achieve maximum secrecy rate of the SU under the quality-of-service (QoS) at the PU and the transmit power constraint at the ST. We transform the robust secrecy rate maximization to a series of semidefinite programmings (SDPs) with the help of S-procedure and rank-one relaxation. An effective method is also proposed to recover the optimal rank-one solution. Simulation results show the superiority of our proposed robust secure algorithm with comparison to the existing secure design schemes. The main contributions of this paper are summarized as follows:

(i) We propose a robust secure optimization algorithm for a cooperative CR NOMA network based on the semidefinite relaxation scheme, where the CSI of the eavesdropper is imperfect.

(ii) An effective method is designed to find an optimal rank-one solution for the proposed semidefinite relaxation scheme, which offers a global optimal solution for the robust secrecy rate maximization problem.

(iii) We provide simulation results to show the effectiveness of our proposed robust secure algorithm with comparison to the nonrobust secure design and traditional orthogonal multiple access schemes.

Note that our work is very different from the previous works in [21–28]. First, we assume that the CSI of the eavesdropper is imperfect, which is more practical than the assumption of the perfect CSI in [21–28]. Second, we focus on the optimization design to improve the security performance, while [21] and [24–27] just provide the analysis of the security performance. Third, we propose a global optimal solution for the secure optimization problem, while only suboptimal solutions are provided in [22, 23]. Last, we employ NOMA transmission to improve the spectrum efficiency, while the conventional OMA scheme is adopted in [28].

The rest of this paper is organized as follows. In Section 2, the system model is described. In Section 3, the robust secrecy rate maximization problem is formulated, and an efficient optimization algorithm and an optimal rank-one solution recovering method are proposed. Simulation results are provided in Section 4, and we summary this paper in Section 5.

Notations. Boldface lowercase and uppercase letters denote vectors and matrices, respectively. $\mathbf{A}^T$, $\mathbf{A}^*$, $\mathbf{A}^\dagger$, $\|\mathbf{A}\|$, and $\mathrm{tr}(\mathbf{A})$ denote the transpose, conjugate, conjugate transpose, Frobenius norm, and trace of the matrix $\mathbf{A}$, respectively. $\otimes$ denotes the Kronecker product. $\odot$ denotes the Hadamard product. $\mathrm{vec}(\mathbf{A})$ denotes to stack the columns of a matrix $\mathbf{A}$ into a single vector $\mathbf{a}$. $\mathrm{Re}\{\mathbf{a}\}$ denotes the real part of $\mathbf{a}$. By $\mathbf{A} \succcurlyeq 0$, we mean that $\mathbf{A}$ is positive semidefinite. $\mathbf{e}_k$ denotes an elementary vector with the kth element being one and others zero. 1 denotes the vector/matrix with all elements being one. $\mathbf{E}$ denotes $\mathrm{diag}(1, 1, \ldots, 1)$.

2. System Model

As shown in Figure 1, we consider an AF-relaying cooperative CR NOMA network. The primary network consists of a PT and a PU, where the PT wants to transmit the signal to the PU. Due to impairments such as long distance and obstacles, the direct communication between the PT and PU cannot satisfy the rate demand. They thus need the help of the secondary user to meet the PU's QoS requirement. The secondary network has a secondary transmitter (ST) with N antennas, which assists the transmission of the PT and serves an SU by using the principle of NOMA. Meanwhile, an eavesdropper (EV) which is located near the SU intends to overhear the signal sent for the SU. The potential application scenarios include device-to-device communications [30], where two mobile phones directly communicate with the help of a femto cell or a laptop, which also transmits its private information to another mobile phone simultaneously.

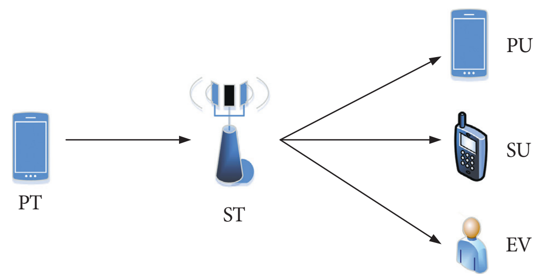

Figure 1: The model for secure communication in an AF-relaying cooperative CR NOMA network.

The transmission consists of two consecutive equal-duration time slots. In the first time slot, the PT transmits symbol x_p to the ST, and the received signal at the ST is given by

$$\mathbf{y}_r = \mathbf{h}_p x_p + \mathbf{n}_r, \tag{1}$$

where $\mathbf{h}_p \in \mathbb{C}^{N\times 1}$ denotes the channel response between the PT and ST, $\mathbf{n}_r \sim \mathscr{CN}(0, \sigma_r^2\mathbf{I})$ is the Gaussian noise at the ST, and the transmit power of x_p is $\mathbb{E}[|x_p|^2] = P_t$.

In the second time slot, the ST employs the NOMA principle to transmit the signals, which multiplies the received signal $\mathbf{y}_r$ by a beamforming matrix, denoted as $\mathbf{F} \in \mathbb{C}^{N\times N}$, and superimposes $\mathbf{F}\mathbf{y}_r$ with its own signal x_s using the cognitive beamforming vector $\mathbf{w} \in \mathbb{C}^{N\times 1}$. To ensure the secure communication of the SU, the ST employs the artificial noise to interfere the eavesdropper. Thus, from (1), the transmit signal at the ST is expressed as

$$\mathbf{x}_r = \mathbf{F}\mathbf{h}_p x_p + \mathbf{F}\mathbf{n}_r + \mathbf{w}x_s + \mathbf{v}, \tag{2}$$

where $\mathbf{v} \in \mathbb{C}^{N\times 1}$ is the artificial noise with covariance $\mathbb{E}(\mathbf{v}\mathbf{v}^\dagger) = \mathbf{V}$ and the signal x_s is normalized to $\mathbb{E}[|x_s|^2] = 1$. From (2), the average transmit power at the ST is

$$P_{\mathbf{x}_r} = \mathbb{E}\left[\left\|\mathbf{x}_r\right\|^2\right] = P_t\left\|\mathbf{F}\mathbf{h}_p\right\|^2 + \sigma_r^2\|\mathbf{F}\|^2 + \|\mathbf{w}\|^2 + \operatorname{tr}(\mathbf{V}). \tag{3}$$

The received signal at the PU, SU, and EV is, respectively,

$$y_p = \mathbf{g}_p^T\mathbf{F}\mathbf{h}_p x_p + \mathbf{g}_p^T\mathbf{F}\mathbf{n}_r + \mathbf{g}_p^T\mathbf{w}x_s + \mathbf{g}_p^T\mathbf{v} + n_p, \tag{4}$$

$$y_s = \mathbf{g}_s^T\mathbf{F}\mathbf{h}_p x_p + \mathbf{g}_s^T\mathbf{F}\mathbf{n}_r + \mathbf{g}_s^T\mathbf{w}x_s + \mathbf{g}_s^T\mathbf{v} + n_s, \tag{5}$$

$$y_e = \mathbf{g}_e^T\mathbf{F}\mathbf{h}_p x_p + \mathbf{g}_e^T\mathbf{F}\mathbf{n}_r + \mathbf{g}_e^T\mathbf{w}x_s + \mathbf{g}_e^T\mathbf{v} + n_e, \tag{6}$$

where $\mathbf{g}_p, \mathbf{g}_s$, and $\mathbf{g}_e \in \mathbb{C}^{N\times 1}$ denote the channel response from the ST to PU, SU, and EV, respectively. $n_p \sim \mathscr{CN}(0, \sigma_p^2)$, $n_s \sim \mathscr{CN}(0, \sigma_s^2)$, and $n_e \sim \mathscr{CN}(0, \sigma_e^2)$ is the Gaussian noise at the PU, SU, and EV, respectively.

To support the QoS requirement at the PU, it is natural to treat the PU as a strong user and the SU as a weak user [12, 13]. At the PU, the signal x_s intended for the SU is first detected, and from (4), the signal-to-interference-and-noise ratio (SINR) for detecting x_s is given by

$$\Gamma_{p,s} = \frac{\left|\mathbf{g}_p^T\mathbf{w}\right|^2}{P_t\left|\mathbf{g}_p^T\mathbf{F}\mathbf{h}_p\right|^2 + \sigma_r^2\left\|\mathbf{g}_p^T\mathbf{F}\right\|^2 + \mathbf{g}_p^T\mathbf{V}\mathbf{p}_s^* + \sigma_p^2}. \tag{7}$$

Suppose $1/2\log_2(1+\Gamma_{p,s}) \geq r_s$, where r_s denotes the transmission rate requirement for correctly decoding x_s, i.e., $\Gamma_{p,s} \geq \gamma_s$ where $\gamma_s = 2^{2r_s} - 1$, and the PU is able to detect the signal x_s. From the NOMA principle, the PU first removes x_s by successive interference cancellation to obtain the following signal:

$$\tilde{y}_p = \mathbf{g}_p^T\mathbf{F}\mathbf{h}_p x_p + \mathbf{g}_p^T\mathbf{F}\mathbf{n}_r + \mathbf{g}_p^T\mathbf{v} + n_p. \tag{8}$$

Then, the PU can detect its own signal x_p with the following signal-to-noise ratio (SNR):

$$\Gamma_{p,p} = \frac{P_t\left|\mathbf{g}_p^T\mathbf{F}\mathbf{h}_p\right|^2}{\sigma_r^2\left\|\mathbf{g}_p^T\mathbf{F}\right\|^2 + \mathbf{g}_p^T\mathbf{V}\mathbf{g}_p^* + \sigma_p^2}. \tag{9}$$

From (5) and (6), the SINR at the SU and EV to detect signal x_s is, respectively, given by

$$\Gamma_s = \frac{\left|\mathbf{g}_s^T\mathbf{w}\right|^2}{P_t\left|\mathbf{g}_s^T\mathbf{F}\mathbf{h}_p\right|^2 + \sigma_r^2\left\|\mathbf{g}_s^T\mathbf{F}\right\|^2 + \mathbf{g}_s^T\mathbf{V}\mathbf{g}_s^* + \sigma_s^2}, \tag{10}$$

$$\Gamma_e = \frac{\left|\mathbf{g}_e^T\mathbf{w}\right|^2}{P_t\left|\mathbf{g}_e^T\mathbf{F}\mathbf{h}_p\right|^2 + \sigma_r^2\left\|\mathbf{g}_e^T\mathbf{F}\right\|^2 + \mathbf{g}_e^T\mathbf{V}\mathbf{g}_e^* + \sigma_e^2}. \tag{11}$$

Using (10) and (11), the achievable secrecy rate for the SU, which is denoted by R_s, is given by [31]:

$$R_s = \frac{1}{2}\log_2(1+\Gamma_s) - \frac{1}{2}\log_2(1+\Gamma_e). \tag{12}$$

3. Robust Secure Design with Imperfect CSI

In this paper, we assume that the perfect CSI of the eavesdropper is not available, which is the practical case in cooperative CR NOMA networks. As in [32, 33], we assume that the actual channel is within the neighborhood of a nominal channel which, specifically, only the noisy version of actual channel response $\mathbf{g}_e$ is known, is denoted as $\overline{\mathbf{g}}_e$:

$$\mathbf{g}_e = \overline{\mathbf{g}}_e + \Delta\mathbf{g}_e, \tag{13}$$

where $\overline{\mathbf{g}}_e$ is the estimated channel vector and $\Delta\mathbf{g}_e$ is the CSI uncertainty and is norm-bounded by the elliptical region:

$$\mathscr{G}_e \triangleq \left\{\Delta\mathbf{g}_e | \Delta\mathbf{g}_e^\dagger\mathbf{T}\Delta\mathbf{g}_e \leq 1\right\}, \tag{14}$$

where the matrix $\mathbf{T} \succ 0$, assumed to be known, determines the quality of CSI.

Based on (3) and (7)–(14), the robust secure design with aiming to maximize the worst-case achievable secrecy rate for the SU subject to the QoS constraints at the PU and the transmit power constraint at the ST can be expressed as

$$\max_{\mathbf{F},\mathbf{w},\mathbf{V}\succeq 0}\ \min_{\Delta\mathbf{g}_e\in\mathscr{G}_e}\ \frac{1}{2}\log_2(1+\Gamma_s) - \frac{1}{2}\log_2(1+\Gamma_e), \tag{15a}$$

$$\text{s.t. } \Gamma_{p,s} \geq \gamma_s, \tag{15b}$$

$$\Gamma_{p,p} \geq \gamma_p, \tag{15c}$$

$$P_t\left\|\mathbf{F}\mathbf{h}_p\right\|^2 + \sigma_r^2\|\mathbf{F}\|^2 + \|\mathbf{w}\|^2 + \operatorname{tr}(\mathbf{V}) \leq P_r, \tag{15d}$$

where $\gamma_p = 2^{2r_p} - 1$ with r_p being the rate requirement at the PU and P_r is the transmit power constraint at the ST. The robust optimization (15a)–(15d) is nonconvex, and the global optimal solution is very difficult to find. In the following, we propose an effective scheme to solve (15a)–(15d) globally.

3.1. Convex Reformulation. Introducing the slack variable β such that $(1/2)\log_2(1+\Gamma_e) \leq \beta$, problem (15a)–(15d) can be rewritten as

$$\begin{aligned} \max_{\mathbf{F},\mathbf{w},\mathbf{V}\succcurlyeq 0,\beta} \quad & \frac{1}{2}\log_2(1+\Gamma_s) - \beta, \\ \text{s.t.} \quad & \frac{1}{2}\log_2(1+\Gamma_e) \leq \beta, \quad \forall \Delta g_e \in \mathcal{G}_e, \\ & (15b), (15c), (15d). \end{aligned} \tag{16}$$

To proceed, we need the following result.

Lemma 1. *Define* $\mathbf{f} = vec(\mathbf{F})$, *and we have*

$$\mathbf{q}^T\mathbf{F}\mathbf{p} = \mathbf{q}^T\left(\mathbf{p}^T \otimes \mathbf{I}\right)\mathbf{f}, \tag{17}$$

$$\mathbf{q}^T\mathbf{F}\mathbf{F}^\dagger\mathbf{p}^* = \mathbf{q}^T\left(1^T \otimes \mathbf{I}\right)\left(\mathbf{E}\odot\left(\mathbf{f}\mathbf{f}^\dagger\right)\right)(1\otimes\mathbf{I})\mathbf{p}^*. \tag{18}$$

Proof. Please see the Appendix.

Let us define

$$\mathbf{f} = \operatorname{vec}(\mathbf{F}), \tag{19}$$

$$\mathbf{X} = \mathbf{f}\mathbf{f}^\dagger, \tag{20}$$

$$\mathbf{Y} = \mathbf{w}\mathbf{w}^\dagger, \tag{21}$$

$$\mu(\mathbf{X}) = P_t\left(\mathbf{h}_p^T \otimes \mathbf{I}\right)\mathbf{X}\left(\mathbf{h}_p^* \otimes \mathbf{I}\right) + \sigma_r^2\left(1^T \otimes \mathbf{I}\right)(\mathbf{E}\odot\mathbf{X})(1\otimes\mathbf{I}). \tag{22}$$

Using Lemma 1 and equations (17)–(22), we can rewrite problem (16) with a given β as

$$\max_{\mathbf{X},\mathbf{Y},\mathbf{V}} \frac{\operatorname{tr}(\mathbf{B}_1\mathbf{Y})}{\operatorname{tr}(\mathbf{A}_1\mathbf{X}) + \operatorname{tr}(\mathbf{B}_1\mathbf{V}) + \sigma_s^2}, \tag{23a}$$

$$\text{s.t. } \Delta\mathbf{g}_e^T\mathbf{D}\Delta\mathbf{g}_e^* + 2\operatorname{Re}\left\{\mathbf{d}^\dagger\Delta\mathbf{g}_e^*\right\} + d \leq 0, \quad \forall \Delta\mathbf{g}_e \in \mathcal{G}_e, \tag{23b}$$

$$\operatorname{tr}(\mathbf{B}_2\mathbf{Y}) - \gamma_s\operatorname{tr}(\mathbf{A}_2\mathbf{X}) - \gamma_s\operatorname{tr}(\mathbf{B}_2\mathbf{V}) - \gamma_s\sigma_p^2 \geq 0, \tag{23c}$$

$$\operatorname{tr}(\mathbf{A}_3\mathbf{X}) - \gamma_p\operatorname{tr}(\mathbf{B}_2\mathbf{V}) - \gamma_p\sigma_p^2 \geq 0, \tag{23d}$$

$$\operatorname{tr}(\mathbf{A}_4\mathbf{X}) + \operatorname{tr}(\mathbf{Y}) + \operatorname{tr}(\mathbf{V}) \leq P_r, \tag{23e}$$

$$\mathbf{X} \succcurlyeq 0, \mathbf{Y} \succcurlyeq 0, \mathbf{V} \succcurlyeq 0, \tag{23f}$$

$$\begin{aligned} &\operatorname{Rank}(\mathbf{X}) = 1, \\ &\operatorname{Rank}(\mathbf{Y}) = 1, \end{aligned} \tag{23g}$$

where $\overline{\beta} = 2^{2\beta} - 1$ and

$$\begin{aligned} \mathbf{A}_1 &= P_t\left(\mathbf{h}_p^*\mathbf{h}_p^T\right)\otimes\left(\mathbf{g}_s^*\mathbf{g}_s^T\right) + \sigma_r^2\mathbf{I}\otimes\left(\mathbf{g}_s^*\mathbf{g}_s^T\right), \\ \mathbf{A}_2 &= P_t\left(\mathbf{h}_p^*\mathbf{h}_p^T\right)\otimes\left(\mathbf{g}_p^*\mathbf{g}_p^T\right) + \sigma_r^2\mathbf{I}\otimes\left(\mathbf{g}_p^*\mathbf{g}_p^T\right), \\ \mathbf{A}_3 &= P_t\left(\mathbf{h}_p^*\mathbf{h}_p^T\right)\otimes\left(\mathbf{g}_p^*\mathbf{g}_p^T\right) - \sigma_r^2\gamma_p\mathbf{I}\otimes\left(\mathbf{g}_p^*\mathbf{g}_p^T\right), \\ \mathbf{A}_4 &= P_t\left(\mathbf{h}_p^*\mathbf{h}_p^T\right)\otimes\mathbf{I} + \sigma_r^2\mathbf{I}, \\ \mathbf{B}_1 &= \mathbf{g}_s^*\mathbf{g}_s^T, \\ \mathbf{B}_2 &= \mathbf{g}_p^*\mathbf{g}_p^T, \\ \mathbf{D} &= \mathbf{Y} - \overline{\beta}\mu(\mathbf{X}) - \overline{\beta}\mathbf{V}, \\ \mathbf{d}^\dagger &= \overline{\mathbf{g}}_e^T\mathbf{D}, \\ d &= \overline{\mathbf{g}}_e^T\mathbf{D}\overline{\mathbf{g}}_e^* - \overline{\beta}\sigma_e^2. \end{aligned} \tag{24}$$

Dropping the rank-one constraints in (23g) and employing the Charnes–Cooper transformation [14], i.e.,

$$\begin{aligned} t &= \frac{1}{\operatorname{tr}(\mathbf{A}_1\mathbf{X}) + \operatorname{tr}(\mathbf{B}_1\mathbf{V}) + \sigma_s^2}, \\ \widehat{\mathbf{X}} &= t\mathbf{X}, \\ \widehat{\mathbf{Y}} &= t\mathbf{Y}, \\ \widehat{\mathbf{V}} &= t\mathbf{V}, \end{aligned} \tag{25}$$

we can convert the robust problem (23a)–(23g) equivalently to

$$\max_{\widehat{\mathbf{X}},\widehat{\mathbf{Y}},\widehat{\mathbf{V}},t} \operatorname{tr}\left(\mathbf{B}_1\widehat{\mathbf{Y}}\right), \tag{26a}$$

$$s.t.\ \Delta\mathbf{g}_e^T\widehat{\mathbf{D}}\Delta\mathbf{g}_e^* + 2\operatorname{Re}\left\{\widehat{\mathbf{d}}^\dagger\Delta\mathbf{g}_e^*\right\} + \widehat{d} \leq 0, \quad \forall \Delta\mathbf{g}_e \in \mathcal{G}_e, \tag{26b}$$

$$\operatorname{tr}\left(\mathbf{A}_1\widehat{\mathbf{X}}\right) + \operatorname{tr}\left(\mathbf{B}_1\widehat{\mathbf{V}}\right) + \sigma_s^2 t = 1, \tag{26c}$$

$$\operatorname{tr}\left(\mathbf{B}_2\widehat{\mathbf{Y}}\right) - \gamma_s\operatorname{tr}\left(\mathbf{A}_2\widehat{\mathbf{X}}\right) - \gamma_s\operatorname{tr}\left(\mathbf{B}_2\widehat{\mathbf{V}}\right) - \gamma_s\sigma_p^2 t \geq 0, \tag{26d}$$

$$\operatorname{tr}\left(\mathbf{A}_3\widehat{\mathbf{X}}\right) - \gamma_p\operatorname{tr}\left(\mathbf{B}_2\widehat{\mathbf{V}}\right) - \gamma_p\sigma_p^2 t \geq 0, \tag{26e}$$

$$\operatorname{tr}\left(\mathbf{A}_4\widehat{\mathbf{X}}\right) + \operatorname{tr}(\widehat{\mathbf{Y}}) + \operatorname{tr}(\widehat{\mathbf{V}}) \leq P_r t, \tag{26f}$$

$$\widehat{\mathbf{X}} \succcurlyeq 0, \widehat{\mathbf{Y}} \succcurlyeq 0, \widehat{\mathbf{V}} \succcurlyeq 0, \quad t \geq 0, \tag{26g}$$

where

$$\widehat{\mathbf{D}} = \widehat{\mathbf{Y}} - \overline{\beta}\mu(\widehat{\mathbf{X}}) - \overline{\beta}\widehat{\mathbf{V}}, \tag{27}$$

$$\widehat{\mathbf{d}}^{\dagger} = \overline{\mathbf{g}}_e^T \widehat{\mathbf{D}}, \tag{28}$$

$$\widehat{d} = \overline{\mathbf{g}}_e^T \widehat{\mathbf{D}} \overline{\mathbf{g}}_e^* - \overline{\beta}\sigma_e^2 t. \tag{29}$$

Due to semi-infinite constraints caused by the channel uncertainty, the robust optimization (26a)–(26g) is difficult to solve. Thus, we need to eliminate the semi-infinite constraints. To make the problem (26a)–(26g) tractable, we convert the semi-infinite constraints into linear matrix inequalities (LMIs) equivalently, using the following S-procedure [34]. □

Lemma 2. *Define the functions:*

$$f_j(\mathbf{x}) = \mathbf{x}^{\dagger}\mathbf{A}_j\mathbf{x} + 2\mathrm{Re}\left\{\mathbf{b}_j^{\dagger}\mathbf{x}\right\} + c_j, \quad j = 1, 2, \tag{30}$$

where $\mathbf{A}_j = \mathbf{A}_j^{\dagger} \in \mathbb{C}^{n\times n}$, $\mathbf{b}_j \in \mathbb{C}^n$, *and* $c_j \in \mathbb{R}$. *The implication* $f_1(\mathbf{x}) \le 0 \Longrightarrow f_2(\mathbf{x}) \le 0$ *holds if and only if there exists* $\lambda \ge 0$ *such that*

$$\lambda \begin{bmatrix} \mathbf{A}_1 & \mathbf{b}_1 \\ \mathbf{b}_1^{\dagger} & c_1 \end{bmatrix} - \begin{bmatrix} \mathbf{A}_2 & \mathbf{b}_2 \\ \mathbf{b}_2^{\dagger} & c_2 \end{bmatrix} \succcurlyeq 0, \tag{31}$$

provided that there exists a point $\mathbf{x}_0$ *such that* $f_1(\mathbf{x}_0) < 0$.

Using Lemma 2, the robust optimization (26a)–(26g) can be converted into the following convex SDP:

$$\begin{aligned} \max_{\widehat{\mathbf{X}},\widehat{\mathbf{Y}},\widehat{\mathbf{V}},t,\lambda\ge 0} \quad & (26a), \\ \text{s.t.} \quad & \begin{bmatrix} \lambda\mathbf{T}^T - \widehat{\mathbf{D}} & -\widehat{\mathbf{d}} \\ -\widehat{\mathbf{d}}^{\dagger} & -\lambda - \widehat{d} \end{bmatrix} \succcurlyeq 0, \\ & (26c)\text{–}(26g). \end{aligned} \tag{32}$$

It is easy to see that if the optimal $(\widehat{\mathbf{X}}^*, \widehat{\mathbf{Y}}^*)$ to the SDP (32) is rank-one, it is also optimal to the problem (16) with a given β. However, the solution to the SDP (32) is not always rank-one. In the next subsection, we propose an effective method to construct the optimal rank-one solution to the problem (16) based on $(\widehat{\mathbf{X}}^*, \widehat{\mathbf{Y}}^*, \widehat{\mathbf{V}}^*, t^*, \lambda^*)$, which is optimal to (32).

3.2. Rank-One Solution Recovering. First, the worst-case $\Delta\mathbf{g}_e$, denoted as $\Delta\mathbf{g}_e^*$, can be computed by solving the following feasibility problem:

$$\begin{aligned} \text{Find} \quad & \Delta\mathbf{g}_e \\ \text{s.t.} \quad & \Delta\mathbf{g}_e^T \widehat{\mathbf{D}}^* \Delta\mathbf{g}_e^* + 2\mathrm{Re}\left\{\widehat{\mathbf{d}}^{*\dagger}\Delta\mathbf{g}_e^*\right\} + \widehat{d}^* \le 0, \\ & \Delta\mathbf{g}_e^{\dagger}\mathbf{T}\Delta\mathbf{g}_e \le 1. \end{aligned} \tag{33}$$

where $\widehat{\mathbf{D}}^*$, $\widehat{\mathbf{d}}^*$, and $\widehat{d}^*$ are obtained by replacing $(\widehat{\mathbf{X}}, \widehat{\mathbf{Y}}, \widehat{\mathbf{V}}, t)$ by $(\widehat{\mathbf{X}}^*, \widehat{\mathbf{Y}}^*, \widehat{\mathbf{V}}^*, t^*)$ in (27)–(29). The feasibility problem (33) is also a nonconvex problem; however, its optimal solution can be found by the following Lemma.

Lemma 3. *The optimal solution to problem (33) can be found by solving the following convex SDP:*

$$\begin{aligned} \min_{\mathbf{Z}\succcurlyeq 0} \quad & 0, \\ \text{s.t.} \quad & \mathrm{tr}(\mathbf{C}_1\mathbf{Z}) = 1, \\ & \mathrm{tr}(\mathbf{C}_i\mathbf{Z}) \le 0, \quad i = 2, 3, \end{aligned} \tag{34}$$

where

$$\begin{aligned} \mathbf{C}_1 &= \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}, \\ \mathbf{C}_2 &= \begin{bmatrix} \widehat{\mathbf{D}}^* & \widehat{\mathbf{d}}^* \\ \widehat{\mathbf{d}}^{*\dagger} & \widehat{d}^* \end{bmatrix}, \\ \mathbf{C}_3 &= \begin{bmatrix} \mathbf{T}^T & 0 \\ 0 & -1 \end{bmatrix}. \end{aligned} \tag{35}$$

Proof. Introducing the slack variable t, we can equivalently rewrite (33) as a homogeneous quadratically constrained quadratic program (QCQP) [35]:

$$\begin{aligned} \text{Find} \quad & \{\Delta\mathbf{g}_e, t\} \\ \text{s.t.} \quad & \left[\Delta\mathbf{g}_e^T, t\right]\mathbf{C}_1\left[\Delta\mathbf{g}_e^T, t\right]^T = 1, \\ & \left[\Delta\mathbf{g}_e^T, t\right]\mathbf{C}_i\left[\Delta\mathbf{g}_e^T, t\right]^T \le 0, \quad i = 2, 3. \end{aligned} \tag{36}$$

Let $\mathbf{Z} = [\Delta\mathbf{g}_e^T, t]^T[\Delta\mathbf{g}_e^T, t]$. The rank-one relaxation of (36) is

$$\begin{aligned} \min_{\mathbf{Z}\succcurlyeq 0} \quad & 0, \\ \text{s.t.} \quad & \mathrm{tr}(\mathbf{C}_1\mathbf{Z}) = 1, \\ & \mathrm{tr}(\mathbf{C}_i\mathbf{Z}) \le 0, \quad i = 2, 3. \end{aligned} \tag{37}$$

Since there are three linear constraints in (37), according to the rank-one decomposition theorem in [36], there is a rank-one optimal solution to problem (37).

From Lemma 3, the optimal rank-one solution to the SDP (32) can be constructed by considering the following convex SDP:

$$\begin{aligned} \max_{\widehat{\mathbf{X}},\widehat{\mathbf{Y}},\widehat{\mathbf{V}},t} \quad & (26a), \\ \text{s.t.} \quad & \Delta\mathbf{g}_e^{*\,T}\widehat{\mathbf{D}}\Delta\mathbf{g}_e^{**} + 2\mathrm{Re}\left\{\widehat{\mathbf{d}}^{\dagger}\Delta\mathbf{g}_e^{**}\right\} + \widehat{d} \le 0, \\ & (26c)\text{–}(26g), \end{aligned} \tag{38}$$

with the optimal solution $(\widehat{\mathbf{X}}^*, \widehat{\mathbf{Y}}^*, \widehat{\mathbf{V}}^*, t^*)$, since for the SDP (38), we have Theorem 1. □

Theorem 1. *There exists a rank-one optimal solution to the SDP (38).*

Proof. Since there are five linear constraints and three matrix variables in the SDP (38), according to Theorem 3.2 in [37], there exists an optimal solution $(\mathbf{X}^o, \mathbf{Y}^o, \mathbf{V}^o)$ to the SDP (38) such that

$$\mathrm{Rank}^2(\mathbf{X}^o) + \mathrm{Rank}^2(\mathbf{Y}^o) + \mathrm{Rank}^2(\mathbf{V}^o) \le 5. \tag{39}$$

```
(1) Choose some large $L$. Define $\Delta\beta = (\beta_u - \beta_l)/L$. Initialize $\varphi^* = 0$.
(2) **For** $j = 0: L$
            Set $\beta = \beta_l + j\Delta\beta$;
            Solve SDP (32);
            **If** the **optimal value** $\varphi^o > \varphi^*$
                Update $\varphi^* = \varphi^o$;
                Save the **optimal solution** as $(\widehat{\mathbf{X}}^*, \widehat{\mathbf{Y}}^*, \widehat{\mathbf{V}}^*, t^*, \lambda^*)$;
            **End**
(3) **End**
(4) **If** $\text{rank}(\widehat{\mathbf{X}}^*) \geq 2$ or $\text{rank}(\widehat{\mathbf{Y}}^*) \geq 2$
            Employ the proposed method in section 3.B to find an optimal rank-one solution to SDP (32).
    **End**
```

Algorithm 1: Find the optimal solution to robust secure problem (15a)–(15d).

Since the optimal solution is nonzero, we have $\text{Rank}(\mathbf{X}^o) = \text{Rank}(\mathbf{Y}^o) = \text{Rank}(\mathbf{V}^o) = 1$. □

3.3. Algorithm and Complexity. Based on Theorem 1, if the optimal solution $(\mathbf{X}^*, \mathbf{Y}^*)$ we have found has a higher rank than one, we can find another optimal rank-one solution $(\mathbf{X}^o, \mathbf{Y}^o)$. Therefore, the optimal solution to robust problem (15a)–(15d) can be found by 1-D search over β, where during each search, the SDP (32) is solved, which is summarized in Algorithm 1.

The **optimal value** and **optimal solution** in Algorithm 1 refer to the optimal value and solution to SDP (32), respectively. The upper and lower bounds of β in Algorithm 1 can be chosen as $\beta_u = (1/2)\log_2(1 + P_r(\|\overline{\mathbf{g}}_e\|^2 + 1/\nu))$ and $\beta_l = 0$, where ν is the minimum eigenvalue of $\mathbf{T}$.

The computational complexity of Algorithm 1 is mainly from the computation of the SDP (32). From [38], the computational complexity for solving an SDP within a tolerance ϵ is $\mathcal{O}((m_{\text{sdp}} n_{\text{sdp}}^{3.5} + m_{\text{sdp}}^2 n_{\text{sdp}}^{2.5} + m_{\text{sdp}}^3 n_{\text{sdp}}^{0.5}) \cdot \log(1/\in))$, where n_{sdp} is the dimension of the semidefinite cone and m_{sdp} is the number of linear constraints. Thus, the computational complexity of the SDP (32) is about $\mathcal{O}(N^7 \log(1/\in))$, which leads to the complexity of the proposed algorithm which is about $\mathcal{O}(\text{LN}^7 \log(1/\in))$. Similarly, the computational complexity of the nonrobust design scheme proposed in [22] is about $\mathcal{O}(\text{LKN}^{3.5} \log(1/\in))$ with K SUs, and that of the conventional OMA scheme proposed in [28] is about $\mathcal{O}(\text{LN}^6 \log(1/\in))$.

4. Simulation Results

In this section, we present the simulation results of our proposed robust secure design scheme, where the average worst-case achievable secrecy rate of the SU will be evaluated under various system parameters. We consider a scenario that, in the AF-relaying cooperative CR NOMA network, all the entries in the channel responses $\mathbf{h}_p$, $\mathbf{g}_p$, $\mathbf{g}_s$, and $\overline{\mathbf{g}}_e$ are independent and identically distributed complex Gaussian random variables with zero mean and unit variance. We assume that the number of antennas equipped at the ST is $N = 3$ and all the noise variances are equal, i.e., $\sigma_i^2 = \sigma^2$, $i \in \{r, p, s, e\}$, the transmission rate requirement is $r_s = 0.5$ bps/Hz, and the transmit power of the PT is fixed to be $P_t/\sigma^2 = 15$ dB. For simplicity, the uncertainty region of the eavesdropper's CSI is assumed to be the norm-bounded, i.e., $\mathbf{T} = (1/\omega)\mathbf{I}$, where ω determines the quality of the CSI of the eavesdropper. In simulations, we compare the proposed robust secure design scheme, denoted as "Proposed Robust," with the nonrobust design scheme proposed in [22], denoted as "NonRobust," and the conventional OMA scheme proposed in [28], denoted as "OMA."

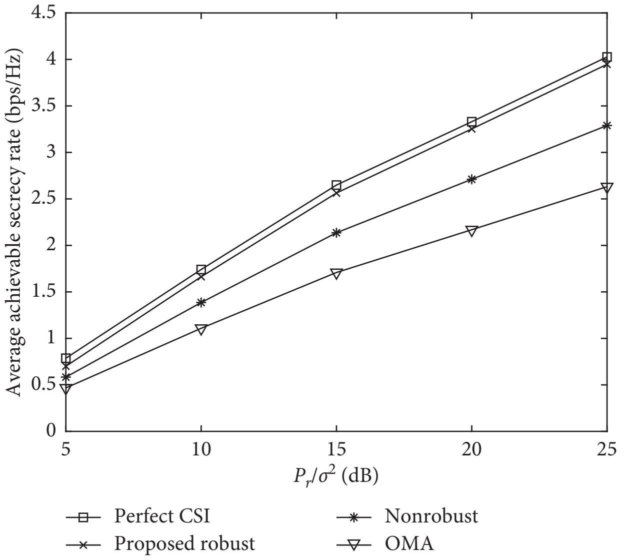

Figure 2: Average worst-case achievable secrecy rate of the SU versus the transmit power of the ST to the noise power ratio P_r/σ^2.

In Figure 2, we present the average worst-case achievable secrecy rate of the SU versus the transmit power of the ST to the noise power ratio, i.e., P_r/σ^2, where the QoS target of the PU is $r_p = 1$ bps/Hz and the channel error is $\omega = 0.001$. The average achievable secrecy rate using the perfect CSI is also presented, denoted as "Perfect CSI." From Figure 2, it is observed that when the channel error is small, i.e., $\omega = 0.001$, the average achievable secrecy rate of the SU by the proposed robust scheme is very close to that by the scheme of "Perfect CSI." We can also see from Figure 2 that the proposed robust

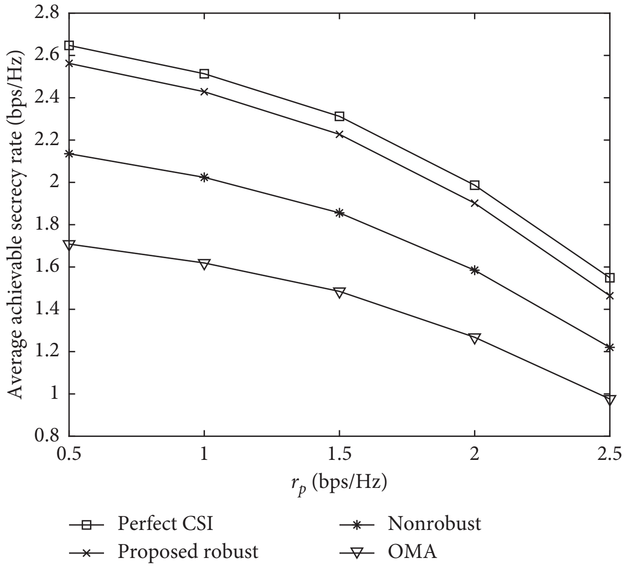

Figure 3: Average worst-case achievable secrecy rate of the SU versus the QoS target of the PU r_p.

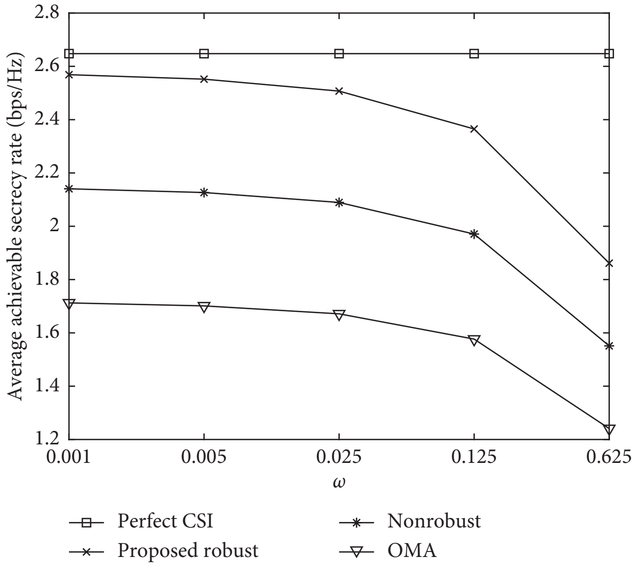

Figure 4: Average worst-case achievable secrecy rate of the SU versus the channel error ω.

secure design scheme outperforms the nonrobust and OMA schemes.

In Figure 3, we present the average worst-case achievable secrecy rate of the SU versus the QoS target of the PU r_p, where the transmit power of the ST to the noise power ratio is $P_r/\sigma^2 = 15$ dB and the channel error is $\omega = 0.001$. From Figure 3, it is seen that the average achievable secrecy rate of the SU by the proposed robust scheme performs close to that by the scheme of "Perfect CSI" and is better than those by the nonrobust and OMA schemes under different values of r_p. We can also see from Figure 3 that, as the QoS target of the PU becomes higher, the average achievable secrecy rate by all the schemes decreases.

In Figure 4, we present the average worst-case achievable secrecy rate of the SU versus the channel error ω, where the transmit power of the ST to the noise power ratio is $P_r/\sigma^2 = 15$ dB and the QoS target of the PU is $r_p = 1$ bps/Hz. From Figure 4, we see that when the channel error ω is small, the average achievable secrecy rate of the SU by the proposed robust scheme performs close to that by the scheme of "Perfect CSI." As ω increases, the average achievable secrecy rate decreases and the gap between the proposed robust scheme and the scheme of "Perfect CSI" becomes larger. From Figure 4, we also see that the proposed robust scheme performs better than the nonrobust and OMA schemes for different values of ω.

5. Conclusions

In this paper, we have proposed a robust physical layer security design algorithm for AF-relaying cooperative CR NOMA networks, where imperfect CSI of the eavesdropper is considered. We transform the robust secrecy rate maximization optimization problem to a series of convex semidefinite programmings with the help of S-procedure and rank-one relaxation and propose an effective method to recover the optimal rank-one solution. Simulation results have shown the effectiveness of our proposed secure design scheme. One possible limitation of the proposed robust physical layer security design algorithm is that it is designed for single-antenna users and eavesdropper. Thus, a generalization of the proposed robust algorithm for cooperative CR NOMA networks with multiantenna users and eavesdropper is an interesting topic for future investigation.

Appendix

A.1. Proof of Lemma 1

Using the identity $\mathrm{tr}(\mathbf{ABC}) = (\mathbf{C}^T \otimes \mathbf{A})\mathrm{vec}(\mathbf{B})$ [39], we have

$$\mathbf{Fp} = \left(\mathbf{p}^T \otimes \mathbf{I}\right)\mathbf{f}, \tag{A.1}$$

which results in (17).

Since $\mathbf{I} = \sum_{i=1}^{N} \mathbf{e}_i \mathbf{e}_i^T$, we have

$$\begin{aligned} \mathbf{q}^T \mathbf{F}\mathbf{F}^\dagger \mathbf{p}^* &= \mathbf{q}^T \mathbf{F}\left(\sum_{i=1}^{N} \mathbf{e}_i \mathbf{e}_i^T\right)\mathbf{F}^\dagger \mathbf{p}^* \\ &= \mathbf{q}^T \left(\sum_{i=1}^{N} \left(\mathbf{e}_i^T \otimes \mathbf{I}\right)\mathbf{f}\mathbf{f}^\dagger \left(\mathbf{e}_i \otimes \mathbf{I}\right)\right)\mathbf{p}^*. \end{aligned} \tag{A.2}$$

It is easy to verify that

$$\sum_{i=1}^{N} \left(\mathbf{e}_i^T \otimes \mathbf{I}\right)\mathbf{f}\mathbf{f}^\dagger \left(\mathbf{e}_i \otimes \mathbf{I}\right) = \left(1^T \otimes \mathbf{I}\right)\left(\mathbf{E} \odot \left(\mathbf{f}\mathbf{f}^\dagger\right)\right)\left(1 \otimes \mathbf{I}\right). \tag{A.3}$$

Thus, from (A.2) and (A.3), we have proved (18).

Data Availability

No data were used to support this study.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

This work was supported in part by the National Natural Science Foundation of China under Grant nos. 61802447 and 61902084 and Featured Innovation Project of the Guangdong Education Department under Grant no. 2018KTSCX174.

References

[1] R. Manna, R. H. Y. Louie, Y. Yonghui Li, and B. Vucetic, "Cooperative spectrum sharing in cognitive radio networks with multiple antennas," *IEEE Transactions on Signal Processing*, vol. 59, no. 11, pp. 5509–5522, 2011.

[2] R. Wang, M. Tao, and Y. Liu, "Optimal linear transceiver designs for cognitive two-way relay networks," *IEEE Transactions on Signal Processing*, vol. 61, no. 4, pp. 992–1005, 2013.

[3] G. Zheng, I. Krikidis, and B. o. Ottersten, "Full-duplex cooperative cognitive radio with transmit imperfections," *IEEE Transactions on Wireless Communications*, vol. 12, no. 5, pp. 2498–2511, May 2013.

[4] G. Zheng, S. Song, K.-K. Wong, and B. Ottersten, "Cooperative cognitive networks: optimal, distributed and low-complexity algorithms," *IEEE Transactions on Signal Processing*, vol. 61, no. 11, pp. 2778–2790, 2013.

[5] J.-H. Noh and S.-J. Oh, "Cognitive radio channel with cooperative multi-antenna secondary systems," *IEEE Journal on Selected Areas in Communications*, vol. 32, no. 3, pp. 539–549, 2014.

[6] L. Dai, B. Wang, Y. Yuan, S. Han, I. Chih-lin, and Z. Wang, "Non-orthogonal multiple access for 5G: solutions, challenges, opportunities, and future research trends," *IEEE Communications Magazine*, vol. 53, no. 9, pp. 74–81, Sep. 2015.

[7] Z. Ding, Z. Yang, P. Fan, and H. V. Poor, "On the performance of non-orthogonal multiple access in 5G systems with randomly deployed users," *IEEE Signal Processing Letters*, vol. 21, no. 12, pp. 1501–1505, 2014.

[8] Z. Ding, J. Xu, O. A. Dobre, and H. V. Poor, "Joint power and time allocation for NOMA-MEC offloading," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 6, pp. 6207–6211, 2019.

[9] N. Zhao, D. Li, M. Liu et al., "Secure transmission via joint precoding optimization for downlink MISO NOMA," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 8, pp. 7603–7615, 2019.

[10] Q.-V. Pham, T. Huynh-The, M. Alazab, J. Zhao, and W.-J. Hwang, "Sum-rate maximization for UAV-assisted visible light communications using NOMA: swarm intelligence meets machine learning," *IEEE Internet of Things Journal*, vol. 7, no. 10, pp. 10375–10387, 2020.

[11] I. Budhiraja, N. Kumar, M. Alazab, S. Tyagi, S. Tanwar, and G. Srivastava, "Energy management scheme for wireless powered D2D users with NOMA underlaying full duplex UAV," in *Proceedings of the 2nd ACM MobiCom Workshop on Drone Assisted Wireless Communications for 5G and beyond*, pp. 7–12, New York, NY, USA, September 2020.

[12] L. Lv, J. Chen, Q. Ni, Z. Ding, and H. Jiang, "Cognitive non-orthogonal multiple access with cooperative relaying: a new wireless frontier for 5G spectrum sharing," *IEEE Communications Magazine*, vol. 56, no. 4, pp. 188–195, 2018.

[13] F. Zhou, Y. Wu, Y.-C. Liang, Z. Li, Y. Wang, and K.-K. Wong, "State of the art, taxonomy, and open issues on cognitive radio networks with NOMA," *IEEE Wireless Communications*, vol. 25, no. 2, pp. 100–108, 2018.

[14] M. Zeng, W. Hao, O. A. Dobre, and Z. Ding, "Cooperative NOMA: state of the art, key techniques, and open challenges," *IEEE Net.*vol. 34, no. 5, pp. 205–211, 2020.

[15] C. Chakraborty and R. Roy, "Markov decision process based optimal gateway selection algorithm," *Int. Journal of Systems, Algorithms & Applications (IJSAA)*, vol. 2, pp. 48–52, 2012.

[16] R. U. Khan, X. Zhang, R. Kumar, A. Sharif, N. A. Golilarz, and M. Alazab, "An adaptive multi-layer botnet detection

technique using machine learning classifiers," *Applied Sciences*, vol. 9, no. 11, p. 2375, 2019.

[17] A. Karim, S. Azam, B. Shanmugam, K. Kannoorpatti, and M. Alazab, "A comprehensive survey for intelligent spam email detection," *IEEE Access*, vol. 7, pp. 168261–168295, 2019.

[18] M. Numan, F. Subhan, W. Z. Khan et al., "A systematic review on clone node detection in static wireless sensor networks," *IEEE Access*, vol. 8, pp. 65450–65461, 2020.

[19] M. H. Abidia, H. Alkhalefah, K. Moiduddin et al., "Optimal 5G network slicing using machine learning and deep learning concepts," *Computer Standards & Interfaces*, vol. 76, 2021.

[20] L. Yang, J. Yang, W. Xie, M. O. Hasna, T. Tsiftsis, and M. D. Renzo, "Secrecy performance analysis of RIS-aided wireless communication systems," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 10, pp. 12296–12300, 2020.

[21] Z. Xiang, W. Yang, G. Pan, Y. Cai, and Y. Song, "Physical layer security in cognitive radio inspired NOMA network," *IEEE Journal of Selected Topics in Signal Processing*, vol. 13, no. 3, pp. 700–714, 2019.

[22] B. Chen, Y. Chen, Y. Chen et al., "Secure primary transmission assisted by a secondary full-duplex NOMA relay," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 7, pp. 7214–7219, 2019.

[23] W. Zhao, R. She, and H. Bao, "Security energy efficiency maximization for two-way relay assisted cognitive radio NOMA network with self-interference harvesting," *IEEE Access*, vol. 7, pp. 74401–74411, 2019.

[24] S. Bhattacharjee, "Friendly jamming assisted secure cooperative multicasting in cognitive radio-NOMA networks," in *Proceedings of 2019 IEEE Globecom Workshops (GC Wkshps)*, Waikoloa, HI, USA, December 2019.

[25] M. Zhu, Z. Yang, and Y. Feng, "Physical layer security of NOMA with decode-and-forward relaying in underlay CR network," in *Proceedings of 2020 International Conference On Wireless Communications and Signal Processing (WCSP)*, pp. 783–788, Nanjing, China, October 2020.

[26] B. Li, X. Qi, K. Huang, Z. Fei, F. Zhou, and R. Q. Hu, "Security-reliability tradeoff analysis for cooperative NOMA in cognitive radio networks," *IEEE Transactions on Communications*, vol. 67, no. 1, pp. 83–96, 2019.

[27] H.-N. Nguyen, N.-L. Nguyen, N.-T. Nguyen et al., "Reliable and secure transmission in multiple antennas hybrid satellite-terrestrial cognitive networks relying on NOMA," *IEEE Access*, vol. 8, pp. 215044–215056, 2020.

[28] Q. Li and L. Yang, "Beamforming for cooperative secure transmission in cognitive two-way relay networks," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 130–143, 2020.

[29] D. Wang, B. Bai, W. Zhao, and Z. Han, "A survey of optimization approaches for wireless physical layer security," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1878–1911, 2019.

[30] P. Janis, C.-H. YU, K. Doppler et al., "Device-to-device communication underlaying cellular communications systems," *International Journal of Communications, Network and System Sciences*, vol. 2, no. 3, pp. 169–178, 2009.

[31] Y. Pei, Y.-C. Liang, L. Zhang, K. Teh, and K. Li, "Secure communication over MISO cognitive radio channels," *IEEE Transactions on Wireless Communications*, vol. 9, no. 4, pp. 1494–1502, 2010.

[32] L. Zhang, Y. C. Liang, Y. Xin, and H. V. Poor, "Robust cognitive beamforming with partial channel state information," *IEEE Transactions on Wireless Communications*, vol. 8, no. 8, pp. 4143–4153, 2009.

[33] J. Wang, G. Scutari, and D. P. Palomar, "Robust MIMO cognitive radio via game theory," *IEEE Transactions on Signal Processing*, vol. 59, no. 3, pp. 1183–1201, 2011.

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

[35] Z.-Q. Luo, W.-K. Ma, A. So, Y. Ye, and S. Zhang, "Semidefinite relaxation of quadratic optimization problems," *IEEE Signal Processing Magazine*, vol. 27, no. 3, pp. 20–34, 2010.

[36] W. Ai, Y. Huang, and S. Zhang, "New results on Hermitian matrix rank-one decomposition," *Mathematical Programming*, vol. 128, no. 1-2, pp. 253–283, 2011.

[37] Y. Huang and D. P. Palomar, "Rank-constrained separable semidefinite programming with applications to optimal beamforming," *IEEE Transactions on Signal Processing*, vol. 58, no. 2, pp. 664–678, 2010.

[38] I. Polik and T. Terlaky, "Interior Point Methods for Nonlinear Optimization," in *Nonlinear Optimization*, G. Di Pillo and F. Schoen, Eds., Springer, Berlin, Germany, 1st edition, 2010.

[39] H. Lutkepohl, *Handbook of Matrices*, John Wiley & Sons, Chichester, UK, 1996.