A Unified Rate-Splitting Framework for Secure Spectrum Sharing via Joint Precoding Optimization

Dongdong Li, Zhutian Yang, *Senior Member, IEEE,* Nan Zhao, *Senior Member, IEEE,* Yunfei Chen, *Senior Member, IEEE,* Zhilu Wu, and Yonghui Li, *Fellow, IEEE*

***Abstract*—To handle the security problem of cognitive radio (CR) systems, secondary users (SUs) are able to be designed to assist the primary user (PU) in secure transmission. To realize the spectrum sharing among CR users, we adopt the rate-splitting multiple access (RSMA) properly, with non-orthogonal multiple access (NOMA) and space division multiple access (SDMA) as its special cases. In this paper, we set up a unified rate-splitting framework to guarantee the safe spectrum sharing through multiple multi-access strategies, without the knowledge of wiretap channels. The precoding vectors at the transmitter are conjointly designed to boost the transmission of common stream, which is from both PU and SU. Besides, the private stream of the downlink CR system can be well secreted in the high-power common signal. As for NOMA and SDMA, when the message of SU is regarded as the friendly jamming signal, the security transmission requirement of PU can be similarly guaranteed via precoding design. Simulations validate that the rate-splitting framework we established can be effective in ensuring the spectrum sharing security for the secure users through RSMA, and the security for NOMA and SDMA is also able to be promoted through adjusting our designed framework.**

***Index Terms*—Precoding optimization, RSMA, NOMA, SDMA, secure spectrum sharing.**

I. Introduction

Evolving multiple access schemes can be one key action for encouraging spectrum sharing for the next generation wireless communications [2], [3]. To promote the transmission performance, the multi-access strategies have been widely researched and advanced [4]. For multi-antenna networks, through antenna arrangements, users' signals are sent with the same time-frequency resource. Then, the appropriate spatial dimensions can be used to separate different messages. This strategy is known as space-division multiple access (SDMA). Other nodes' signal can be regarded as interference for the SDMA node to achieve spectrum sharing via multi-antenna beamforming. In addition, SDMA can be connected with orthogonal frequency-division multiplexing (OFDM) to exploit frequency resource and settle the limited bandwidth [5], [6]. Other multi-access strategies, such as non-orthogonal multiple access (NOMA) and code division multiple access (CDMA), are also able to assist with SDMA [7], [8].

Besides SDMA, NOMA is also a superimposed transmission method for multi-user access [9]. However, at the receivers, successive interference cancellation (SIC) should be exploited for separating different NOMA users, indicating that other nodes' message should be completely recovered and eliminated [10]. NOMA can be connected with multiple-input and multiple-output (MIMO) networks to achieve better performance [11], [12]. In addition, the combination of cognitive radio (CR) and NOMA can achieve effective spectrum sharing, and different transmission indicators can be better balanced and improved [13]–[16]. Furthermore, the private transmission problem for NOMA systems has also received enormous consideration [17]–[20]. For NOMA-aided CR system, Nandan *et al.* designed one beamforming plan against the illegitimate eavesdroppers [17]. In [18], Cao *et al.* considered several strategies for guaranteeing secure communication for private message of NOMA systems with the existence of potential eavesdroppers. In downlink NOMA systems [19], Zhao *et al.* designed the precoders to strengthen the secure transmission for private nodes. In the NOMA-aided mobile-edge computing networks, Wu *et al.* considered the improvement of the minimum anti-eavesdropping ability [20].

Latterly, a more flexible and broader multi-access scheme of rate-splitting multiple access (RSMA), was proposed to be the connection for SDMA and NOMA [21]. For the base station (BS) of RSMA system, the messages required by receivers should be split into the private and common parts. Next, common messages can be encoded as a common stream to broadcast [22]–[24]. Just like NOMA, the receiving nodes in RSMA also adopts SIC. The difference is that, the RSMA users first apply the method of NOMA to demodulate the common information and divide it. Then, they consider the method of SDMA to decode the private messages. Owing to RSMA's adaptability and superiority, several relevant works for RSMA have been studied [25]–[32]. In view of energy transmission, the superiority of rate-splitting under the constraint of energy receivers was proved by Mao *et al.* in [25]. According to linearly precoded rate splitting, Acosta *et al.* studied the power minimization problem, which was separated into outer or inner ones to be solved [26]. In multi-antenna CR networks, the

Manuscript received September 23, 2022; revised January 21, 2023 and March 01, 2023; accepted March 06, 2023. The work was supported by the National Natural Science Foundation of China (NSFC) under Grant 62071143 and 62271099. Part of this work was presented in IEEE ICC'22 [1]. *(Corresponding author: Zhutian Yang.)*

D. Li, Z. Yang and Z. Wu are with the School of Electronics and Information Engineering, Harbin Institute of Technology, Harbin 150001, China (e-mail: dongdongli@stu.hit.edu.cn, yangzhutian@hit.edu.cn, wuzhilu@hit.edu.cn).

N. Zhao is with the School of Information and Communication Engineering, Dalian University of Technology, Dalian 116024, China (email: zhaonan@dlut.edu.cn).

Y. Chen is with the Department of Engineering, University of Durham, Durham, UK, DH1 3LE (Yunfei.Chen@durham.ac.uk).

Y. Li is with the School of Electrical and Information Engineering, University of Sydney, Sydney, NSW 2006, Australia (e-mail: yonghui.li@sydney.edu.au).

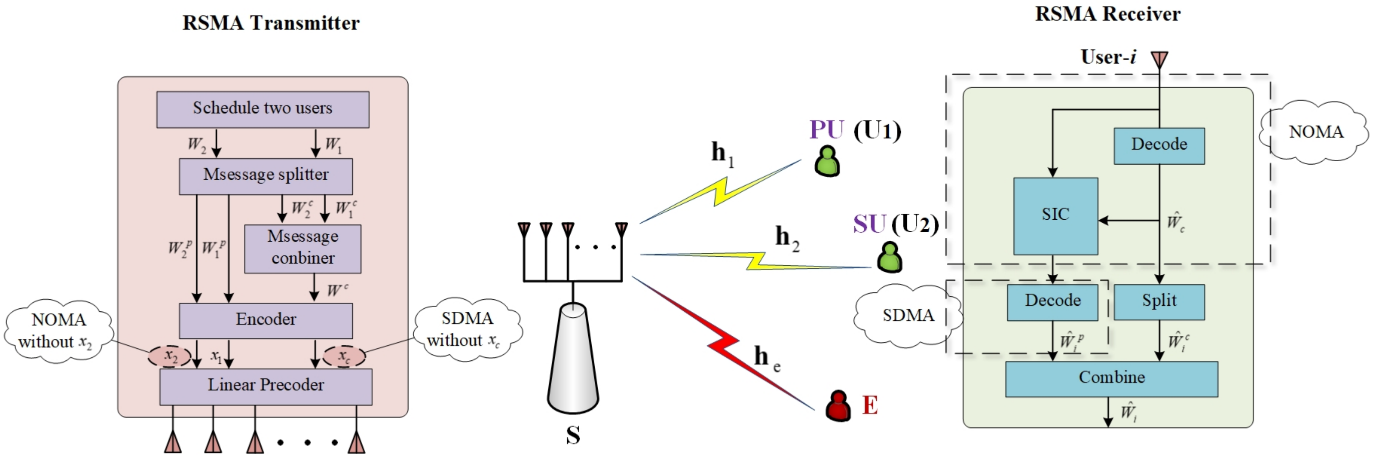


Fig. 1. A downlink RSMA-CR system for secure spectrum sharing with PU, SU, and potential eavesdropper.

superiority of rate-splitting was proved in [27], which was employed for the secondary transmitter. Moreover, the rate for uplink RSMA was considered in [28], and Yang *et al.* found that under proportional rate constraints, more sum rate could be achieved for the proposed circumstance. An aerial rate splitting scheme, which is especially suitable for unmanned aerial vehicle (UAV) systems, was considered by Jaafar *et al.* to analyze the rate of ground nodes [29]. For satellite and aerial integrated networks, the UAV subnetwork can significantly suppress the mutual interference via RSMA [30]. Through managing the BS clustering and designing the precoders in [31], the minimum weighted rate was maximized by Zhou *et al.*, indicating the benefits of RSMA scheme. A sum-rate maximization scheme for RSMA systems was proposed, in which successive convex approximation was implemented for settling the original optimization [32].

Actually, there are a few works that take the privacy of RSMA nodes or the security of RSMA communication into account, in order to maximize secrecy sum rate [33], weighted sum rate [34], minimum secrecy rate [35]–[37], or secrecy energy efficiency [38]. Specifically, by letting the legal node to send the decoded information to another node, cooperative rate-splitting was implemented and the secure sum rate was maximized [33]. While constraining the security rate of all users, Xia *et al.* found that RSMA's weighted sum rate can be superior to that of general multi-user linear precoding [34]. A RSMA-aided cognitive satellite terrestrial network was considered by Lin *et al.* in [38], and the proposed design can also obtain acceptable performance of cellular users. Moreover, Salem *et al.* in [39] investigated the tradeoff between sum rate and secrecy rate for multi-user RSMA networks.

Different from the aforementioned works, concentrating on the security issues without eavesdropping channel state information (CSI), we guarantee the secure spectrum sharing among CR users via three different multiple access methods of RSMA, NOMA and SDMA, and integrate these strategies into a unified rate-splitting framework. The main contributions are listed as follows.

- To deal with security challenge of being eavesdropped, the secondary user (SU) is designed to connect CR network to assist the primary user (PU) in secure transmission. We also set up a unified rate-splitting framework to insure the secure spectrum sharing among users in RSMA, NOMA and SDMA networks without the eavesdropping CSI.
- By adopting the RSMA strategy, the secure spectrum sharing of the private message intended to both PU and SU is enhanced through joint precoding optimization. In addition, the performance for other broadcasting information of PU and SU is enhanced. While the optimization problem is non-convex, it is transformed into convex and solved iteratively.
- For NOMA and SDMA, the considered secure strategy is also able to meet the requirements for secure spectrum sharing through regarding SU's message as the friendly jamming signal. Moreover, the convex conversion process of these two cases can be addressed similar to the RSMA scheme. The relevance and difference of these three multiple access technologies are also compared.

The rest of the paper is organized as follows. Section II introduces the system model. The security scheme for RSMA-CR users is proposed in Section III. The cases for NOMA and SDMA and their corresponding secure schemes are demonstrated in Section IV, respectively. Section V introduces the simulations. Finally, Section VI concludes the paper.

Notation: Boldface $\mathbf{A}$ and boldface $\mathbf{a}$ denote matrix and vector, respectively. $\mathbf{I}$ and $\mathbf{0}$ respectively represent the identity matrix and the zero matrix. $\mathbf{A}^{\dagger}$ corresponds to the Hermitian-transpose operator. $\|\mathbf{a}\|$ refers to the Euclidean norm. $\mathcal{CN}(\mathbf{n},\mathbf{N})$ means a complex Gaussian distribution with the covariance matrix $\mathbf{N}$ and mean $\mathbf{n}$. $\mathfrak{Re}(\cdot)$ stands for the real operator.

II. System Model

For a CR network, the SU can have chance to share the spectrum only when the PU's transmission will not be hindered. According to this principle, we propose that SU is designed to help PU for secure transmission, so as to have more chance to access the spectrum. Then, the friendly interference, which consists of the signal of SU, can be utilized to disrupt the eavesdropping. Specifically, as shown in Fig. 1, for both of PU and SU, its message W_i, $\forall i \in \{1, 2\}$, should be split into private part W_i^p and remaining common part W_i^c through RSMA strategy [23], [24]. The private message W_i^p is naturally suitable to be transmitted securely, for the reason that W_i^p can be secreted with the help of high-power common signal in accordance with SIC. Therefore, we put the secure message that needs secure transmission into the private part W_i^p, and focus on the protection of the secure message. Thus, a unified framework is established to guarantee the secure spectrum sharing for the broadcasting RSMA system, as well as the special cases, i.e., NOMA and SDMA.

Then, W_i^c is cooperatively encoded into common stream x_c for PU and SU, and the private message W_i^p is encoded into x_i. $\mathbb{E}\{\|x_i\|^2\} = \mathbb{E}\{\|x_c\|^2\} = 1$. Therefore, its transmitted signal can be given by

$$\mathbf{s}_R = \sum_{i=1}^{2} \mathbf{v}_i x_i + \mathbf{v}_c x_c, \tag{1}$$

where $\mathbf{v}_i, \mathbf{v}_c \in \mathbb{C}^{M\times 1}$ are precoders for x_i and x_c.

Moreover, NOMA and SDMA are also illustrated. When the information desired by SU is only x_c, the RSMA network is turned as a NOMA network, with the transmitted signal denoted as

$$\mathbf{s}_N = \mathbf{v}_1 x_1 + \mathbf{v}_c x_c. \tag{2}$$

Differently, the RSMA network can be transformed as a SDMA network when there is no x_c, with the transmitted signal expressed as

$$\mathbf{s}_S = \mathbf{v}_1 x_1 + \mathbf{v}_2 x_2. \tag{3}$$

In the CR system, the received signal for the ith user is

$$y_i = \mathbf{h}_i \sum_{k=1}^{2} \mathbf{v}_k x_k + \mathbf{h}_i \mathbf{v}_c x_c + n_i,\ i \in \{1, 2\}, \tag{4}$$

where $n_i \sim \mathcal{CN}\left(0, \sigma^2\right)$ represents the additive white Gaussian noise at the ith node. The channel to the ith node is

$$\mathbf{h}_i = \sqrt{\beta d_{SU_i}^{-\alpha}}\, \mathbf{g}_{SU_i} \in \mathbb{C}^{1\times M},\ i \in \{1, 2\}, \tag{5}$$

where d_{SU_i} denotes the distance between BS and the ith user, β represents the unit channel gain, α denotes the path-loss exponent, and $\mathbf{g}_{SU_i} \sim \mathcal{CN}(\mathbf{0}, \mathbf{I})$ denotes the normalized Rayleigh fading vector.

At the beginning, PU and SU demodulate x_c while regarding x_i as interference. The signal-to-interference-plus-noise ratio (SINR) to demodulate x_c for the ith user $r_c^{[i]}$ is written as

$$r_c^{[i]} = \frac{|\mathbf{h}_i \mathbf{v}_c|^2}{\sum\limits_{k=1}^{2} |\mathbf{h}_i \mathbf{v}_k|^2 + \sigma^2},\ i \in \{1, 2\}. \tag{6}$$

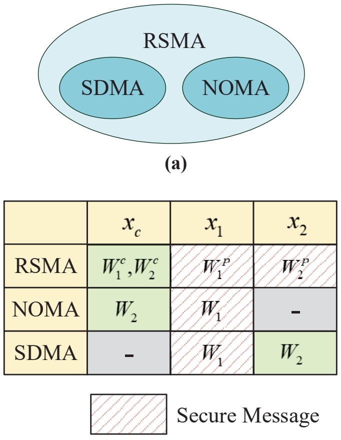
To ensure that PU and SU demodulate x_c favorably, the transmission rate of x_c is obtained as

$$R_c = \log_2 \left(1 + \min\left\{r_c^{[1]}, r_c^{[2]}\right\}\right), \tag{7}$$

and

$$R_c = C_1 + C_2, \tag{8}$$

in which C_i is the portion of common rate of the ith user.



(a)

	x_c	x_1	x_2
RSMA	W_1^c, W_2^c	▨ W_1^p	▨ W_2^p
NOMA	W_2	▨ W_1	-
SDMA	-	▨ W_1	W_2

▨ Secure Message

(b)

Fig. 2. (a) RSMA is a bridge for SDMA and NOMA [21]; (b) the secure message in three systems.

Next, x_c is eliminated at the ith user, and its own private signal is demodulated. For the ith user, the SINR of demodulating x_i is given by

$$r_p^{[i]} = \frac{|\mathbf{h}_i \mathbf{v}_i|^2}{|\mathbf{h}_i \mathbf{v}_k|^2 + \sigma^2},\ i, k \in \{1, 2\}, k \neq i. \tag{9}$$

Hence, for the ith user, the transmission rate for x_i can be given by

$$R_p^{[i]} = \log_2 \left(1 + r_p^{[i]}\right), i \in \{1, 2\}. \tag{10}$$

We should notice that, for NOMA systems, PU and SU recover x_c firstly, and then remove it through SIC to demodulate x_1 at PU. While for SDMA, PU and SU directly demodulate its own message x_1 or x_2.

For traditional RSMA networks, the sum rate should be optimized to enhance the transmission capability. Nevertheless, we can also make use of the high-power x_c to ensure the security of x_1 or x_2 and resist the malicious wiretapper.

Since the eavesdropper cannot have enough information to perform SIC, the eavesdropping SINR towards x_i is denoted by[1]

$$r_e^{[i]} = \frac{|\mathbf{h}_e \mathbf{v}_i|^2}{|\mathbf{h}_e \mathbf{v}_k|^2 + |\mathbf{h}_e \mathbf{v}_c|^2 + \sigma^2},\ i, k \in \{1, 2\}, k \neq i, \tag{11}$$

where $\mathbf{h}_e$ denotes the channel between the BS and eavesdropper. Hence, the eavesdropping rate towards x_i is obtained as

$$R_e^{[i]} = \log_2 \left(1 + r_e^{[i]}\right),\ i, k \in \{1, 2\}, k \neq i. \tag{12}$$

We should notice that the $|\mathbf{h}_e \mathbf{v}_c|^2$ in (11) could be increased to counter the eavesdropping toward x_i.

[1] While the eavesdropper is neither a user who is communicating with BS nor a valued CR user, she cannot perform SIC decoding on $\mathbf{v}_c$ because she cannot have enough information.

According to the mutual message between the BS and the ith user as well as the eavesdropper [40], the achievable secrecy rate of x_i intended to user-i is given by[2]

$$R_s^{[i]} = \left[R_p^{[i]} - R_e^{[i]}\right]^+, \ i \in \{1, 2\}, \tag{13}$$

in which $[\cdot]^+$ represents that while $R_p^{[i]} < R_e^{[i]}$, the achievable secrecy rate $R_s^{[i]}$ becomes zero.

For the NOMA network, the signal of SU can be also utilized to protect the private message intended to PU, because it is also part of the denominator in $r_e^{[i]}$. Thus, similar methods is adopted in NOMA to improve the spectrum sharing security of PU. However, no common signal is existed in SDMA system. Therefore, we can enhance the security for PU with the assistance of SU as a friendly jammer through precoding optimization.

Based on these discussions, a unified rate-spitting framework for communication security can be organized. In Fig. 2, the connection among RSMA, NOMA and SDMA is displayed. While the private message x_2 is not required for SU, RSMA is turned into NOMA. In addition, while x_c is not required for both of PU and SU, RSMA is transformed into SDMA.

In the following sections, a joint precoding optimization is first proposed for secure RSMA system. Then, the security strategies for NOMA and SDMA are also discussed.

III. Security Optimization for RSMA Networks

In this section, we first develop the security optimization in RSMA systems. Next, the non-convex optimization is converted into convex, with the iterative algorithm designed to tackle it. The computational complexity is further analyzed.

A. Problem Formulation

For RSMA, the message of PU and SU is first split into W_i^p and W_i^c, and then they can be encoded, individually. The private parts are inherently suitable to be transmitted securely, because it could be secreted by the great-power common signal. Therefore, the precoding vectors optimization at the transmitter is designed to guarantee the privacy for the RSMA system without knowing the eavesdropping CSI.

Through maximizing the transmission rate of x_c, the transmission performance of this non-confidential message can be improved. Then, the transmit power of x_c becomes higher, which can act as an undecodable and controllable interference at the eavesdropper, and the private part can be secreted by this high-power common part in accordance with (11). Therefore, for a given pair of weight coefficients α_i, the precoding optimization problem is established as

$$\max_{\mathbf{v}_i, \mathbf{v}_c, C_i} \ \sum_{i \in \{1,2\}} \alpha_i C_i \tag{14a}$$

$$s.t. \ R_p^{[i]} \geq r_i^{th}, \ \forall i \in \{1, 2\}, \tag{14b}$$

$$\sum_{j=1}^{2} C_j \leq \log_2\left(1 + r_c^{[i]}\right), \ \forall i \in \{1, 2\}, \tag{14c}$$

$$C_i \geq c_i^{th}, \ \forall i \in \{1, 2\}, \tag{14d}$$

$$\|\mathbf{v}_c\|^2 + \sum_{i=1}^{2} \|\mathbf{v}_i\|^2 \leq P_s, \tag{14e}$$

in which α_i represents the weight coefficient of the achievable rate of the common part of W_i^c, r_i^{th} is the rate threshold of $R_p^{[i]}$, c_i^{th} denotes the rate threshold for the common message of user-i, and P_s denotes the total transmitted power. (14b) is to ensure that $R_p^{[i]}$ for x_i can meet its threshold. (14c) comes from (7) and (8). C_i is required to meet the threshold in (14d). (14e) is the upper limit of transmit power. Due to the non-convexity of (14b) and (14c), problem (14) need to be converted into convex.

B. Approximate Transformations

First, a_i, $i \in \{1, 2\}$ are introduced, and (14b) is reformulated into

$$\begin{cases} a_i \geq 2^{r_i^{th}}, \ i \in \{1, 2\}, & (15) \\ 1 + \dfrac{|\mathbf{h}_i \mathbf{v}_i|^2}{|\mathbf{h}_i \mathbf{v}_k|^2 + \sigma^2} \geq a_i, \ i \in \{1, 2\}. & (16) \end{cases}$$

Subsequently, b_i is introduced to denote the denominator of $r_p^{[i]}$. Therefore, the constraint (16) is transformed as

$$\begin{cases} \dfrac{|\mathbf{h}_i \mathbf{v}_i|^2}{b_i} \geq a_i - 1, \ i \in \{1, 2\}, & (17) \\ b_i \geq |\mathbf{h}_i \mathbf{v}_k|^2 + \sigma^2, \ i \in \{1, 2\}. & (18) \end{cases}$$

Then, the variables ν and μ are introduced. Based on the first-order lower approximation at $\overline{\nu}$ and $\overline{\mu}$, we can obtain

$$\frac{\nu^2}{\mu} \geq \frac{2\overline{\nu}}{\overline{\mu}} \cdot \nu - \left(\frac{\overline{\nu}}{\overline{\mu}}\right)^2 \cdot \mu. \tag{19}$$

In accordance with the above method, we have

$$\begin{aligned} \frac{|\mathbf{h}_i \mathbf{v}_i|^2}{b_i} \geq & \frac{2\mathfrak{Re}\left(\overline{\mathbf{v}}_i^\dagger \mathbf{h}_i^\dagger \mathbf{h}_i \mathbf{v}_i\right)}{\overline{b}_i} \\ & - \left(\frac{|\mathbf{h}_i \overline{\mathbf{v}}_i|}{\overline{b}_i}\right)^2 b_i = \mathcal{T}_i(\mathbf{v}_i, b_i), \ i \in \{1, 2\}. \end{aligned} \tag{20}$$

Thus, (14b) is rewritten as

$$(14b) \Leftrightarrow \begin{cases} a_i \geq 2^{r_i^{th}}, \ i \in \{1, 2\}, \\ b_i \geq |\mathbf{h}_i \mathbf{v}_k|^2 + \sigma^2, \ i \in \{1, 2\}, \\ \mathcal{T}_i(\mathbf{v}_i, b_i) \geq a_i - 1, \ i \in \{1, 2\}. \end{cases} \tag{21}$$

Moreover, Proposition 1 is proposed to restrict and transform C_i.

[2] Among the proposed optimization schemes, the eavesdropping CSI is unknown at the BS. We only require $\mathbf{h}_e$ and calculate $R_s^{[i]}$ when simulating and analyzing the system performance.

Proposition 1: (14c) can be derived as

$$\begin{cases} \sum\limits_{j=1}^{2} C_j \leq \epsilon_i, \ i \in \{1,2\}, \\ \theta_i \geq 2^{\epsilon_i}, \ i \in \{1,2\}, \\ z_i \geq \sum\limits_{k=1}^{2} |\mathbf{h}_i \mathbf{v}_k|^2 + \sigma^2, \ i \in \{1,2\}, \\ \mathcal{L}_i(\mathbf{v}_c, z_i) \geq \theta_i - 1, \ i \in \{1,2\}. \end{cases} \tag{22}$$

Proof: Defining ϵ_i to denote the rate of decoding x_c at user-i, (14c) is changed into

$$\begin{cases} \sum\limits_{j=1}^{2} C_j \leq \epsilon_i, \ i \in \{1,2\}, & (23) \\ \log_2 \left(1 + r_c^{[i]}\right) \geq \epsilon_i, \ i \in \{1,2\}. & (24) \end{cases}$$

To deal with the non-convexity of (24), θ_i are introduced to express $r_c^{[i]}$, $i \in \{1,2\}$. Therefore, (24) is transformed as

$$\begin{cases} \theta_i \geq 2^{\epsilon_i}, \ i \in \{1,2\}, & (25) \\ 1 + \dfrac{|\mathbf{h}_i \mathbf{v}_c|^2}{\sum\limits_{k=1}^{2} |\mathbf{h}_i \mathbf{v}_k|^2 + \sigma^2} \geq \theta_i, \ i \in \{1,2\}. & (26) \end{cases}$$

Furthermore, using z_i to denote the denominator of the decoding SINR for x_c, (26) is expressed as

$$\begin{cases} \dfrac{|\mathbf{h}_i \mathbf{v}_c|^2}{z_i} \geq \theta_i - 1, \ i \in \{1,2\}, & (27) \\ z_i \geq \sum\limits_{k=1}^{2} |\mathbf{h}_i \mathbf{v}_k|^2 + \sigma^2, \ i \in \{1,2\}. & (28) \end{cases}$$

In accordance with (19), we further obtain

$$\begin{aligned} \frac{|\mathbf{h}_i \mathbf{v}_c|^2}{z_i} \geq & \frac{2\Re\left(\overline{\mathbf{v}}_c^\dagger \mathbf{h}_i^\dagger \mathbf{h}_i \mathbf{v}_c\right)}{\overline{z}_i} \\ & - \left(\frac{|\mathbf{h}_i \overline{\mathbf{v}}_c|}{\overline{z}_i}\right)^2 z_i = \mathcal{L}_i(\mathbf{v}_c, z_i), \ i \in \{1,2\}. \end{aligned} \tag{29}$$

According to these transformations, (14c) is rewritten as

$$(14c) \Leftrightarrow \begin{cases} (23),(25),(28), \\ \mathcal{L}_i(\mathbf{v}_c, z_i) \geq \theta_i - 1, \ i \in \{1,2\}, \end{cases} \tag{30}$$

and (22) is obtained. ■

Therefore, (14) can be converted into convex as (31) on the next page.

C. Iterative Algorithm

After all the conversions, the optimization problem (14) is converted into (31), which is solved through Algorithm 1.

Based on the algorithm, in the beginning, $\overline{\mathbf{v}}_i$ and $\overline{\mathbf{v}}_c$ should be initialized. $\overline{a}_i$, $\overline{b}_i$, $\overline{x}_i$, $\overline{y}_i$, and $\overline{z}_i$ are also initialized. Via CVX, $(\mathbf{v}_i^*, \mathbf{v}_c^*, a_i^*, b_i^*, x_i^*, y_i^*, z_i^*)$ can be calculated according to the constraints (31b)-(31g). Next, the solutions of current iteration can be adopted as the initial values in the next iteration. The problem (31) is solved iteratively. When t is equal to T, $\mathbf{v}_i^*$ can be obtained.

Algorithm 1 Iterative Algorithm for (14)

```
Set the maximum number of iterations $T$, $t = 0$, and randomly generate $(\overline{\mathbf{v}}_i, \overline{\mathbf{v}}_c, \overline{a}_i, \overline{b}_i, \overline{\epsilon}_i, \overline{\theta}_i, \overline{z}_i)$, $i \in \{1,2\}$.
Repeat
Calculate the solutions to (31) as $(\mathbf{v}_i^*, \mathbf{v}_c^*, a_i^*, b_i^*, \epsilon_i^*, \theta_i^*, z_i^*)$ via CVX, $i \in \{1,2\}$.
Update $(\overline{\mathbf{v}}_i, \overline{\mathbf{v}}_c, \overline{a}_i, \overline{b}_i, \overline{\epsilon}_i, \overline{\theta}_i, \overline{z}_i)$ with $(\mathbf{v}_i^*, \mathbf{v}_c^*, a_i^*, b_i^*, \epsilon_i^*, \theta_i^*, z_i^*)$, $i \in \{1,2\}$.
$t = t + 1$.
Until $t = T$.
Output $\mathbf{v}_i^*$ and $\mathbf{v}_c^*$, $i \in \{1,2\}$.
```

D. Computational Complexity

In (31), the number of constraints is calculated as $10K+2$. The number of iterations needed to reduce the duality gap to a small constant is upper bounded as

$$\mathcal{O}(\sqrt{10K+2}), \tag{32}$$

where K represents the number of users, and it equals 2 in the considered scenario. It is noteworthy that when the number of RSMA users exceeds 2, the expressions for the computational complexity are still applicable. Then, the number of operations for every iteration can be denoted by

$$\begin{aligned} \mathcal{O}(n(n^2 + 6nK + (K^2 + 4K + 1)M^2 \\ + (6K+2)M + 8K + 1)), \end{aligned} \tag{33}$$

where $n = (6K + 2MK + 2M)$ denotes the number of the optimized variables. Then, the worst-case computational complexity in (31) is denoted as

$$\begin{aligned} \mathcal{O}(n(n^2 + 6nK + (K^2 + 4K + 1)M^2 \\ + (6K+2)M + 8K + 1) \cdot (\sqrt{10K+2})). \end{aligned} \tag{34}$$

IV. Security Optimization for NOMA and SDMA

In this section, the cases of RSMA, i.e., NOMA and SDMA, and their corresponding secure schemes are demonstrated. Although NOMA and SDMA originate from RSMA, the proposed two schemes are quite different, which are demonstrated as follows.

A. Special Case of NOMA

In Fig. 2, based on RSMA framework, when the SU in the CR network only requires the common message x_c, and all the information sent by PU requires private transmission, the RSMA is transformed into NOMA. We should notice that NOMA can benefit the secure transmission, due to the SIC, i.e., the user decoded later can hide its information in the great-power signal first decoded.

In the NOMA network, the received signal for user-i is

$$y_i = \mathbf{h}_i \mathbf{v}_1 x_1 + \mathbf{h}_i \mathbf{v}_c x_c + n_i, \ i \in \{1,2\}. \tag{35}$$

The SINR of decoding x_c is written as

$$r_c^{[i]} = \frac{|\mathbf{h}_i \mathbf{v}_c|^2}{|\mathbf{h}_i \mathbf{v}_1|^2 + \sigma^2}, \ i \in \{1,2\}. \tag{36}$$

Similar to (7) and (8), R_c and C_i can be also obtained.

$$\max_{\substack{a_i,b_i,\epsilon_i,\theta_i,z_i\\ \mathbf{v}_i,\mathbf{v}_c,C_i}} \sum_{i\in\{1,2\}} \alpha_i C_i \tag{31a}$$

$$s.t.\ a_i \geq 2^{r_i^{th}},\ b_i \geq |\mathbf{h}_i\mathbf{v}_k|^2+\sigma^2,\ i\in\{1,2\},\ k\neq i, \tag{31b}$$

$$\mathcal{T}_i(\mathbf{v}_i,b_i)=\frac{2\mathfrak{Re}\left(\overline{\mathbf{v}}_i^{\dagger}\mathbf{h}_i^{\dagger}\mathbf{h}_i\mathbf{v}_i\right)}{\bar{b}_i}-\left(\frac{|\mathbf{h}_i\overline{\mathbf{v}}_i|}{\bar{b}_i}\right)^2 b_i,\ \mathcal{T}_i(\mathbf{v}_i,b_i)\geq a_i-1,\ i\in\{1,2\}, \tag{31c}$$

$$\sum_{j=1}^{2} C_j \leq \epsilon_i,\ \theta_i\geq 2^{\epsilon_i},\ z_i\geq \sum_{k=1}^{2}|\mathbf{h}_i\mathbf{v}_k|^2+\sigma^2,\ i\in\{1,2\}, \tag{31d}$$

$$\mathcal{L}_i(\mathbf{v}_c,z_i)=\frac{2\mathfrak{Re}\left(\overline{\mathbf{v}}_c^{\dagger}\mathbf{h}_i^{\dagger}\mathbf{h}_i\mathbf{v}_c\right)}{\bar{z}_i}-\left(\frac{|\mathbf{h}_i\overline{\mathbf{v}}_c|}{\bar{z}_i}\right)^2 z_i,\ \mathcal{L}_i(\mathbf{v}_c,z_i)\geq \theta_i-1,\ i\in\{1,2\}, \tag{31e}$$

$$C_i \geq c_i^{th},\ \forall i\in\{1,2\}, \tag{31f}$$

$$\|\mathbf{v}_c\|^2+\sum_{i=1}^{2}\|\mathbf{v}_i\|^2\leq P_s. \tag{31g}$$

In addition, SIC should be further applied at the PU. After removing x_c, the SINR of decoding x_1 is denoted by

$$r_p^{[1]}=\frac{|\mathbf{h}_1\mathbf{v}_1|^2}{\sigma^2}. \tag{37}$$

The eavesdropping rate to x_1 of PU can be denoted as

$$R_e^{[1]}=\log_2\left(1+\frac{|\mathbf{h}_e\mathbf{v}_1|^2}{|\mathbf{h}_e\mathbf{v}_c|^2+\sigma^2}\right). \tag{38}$$

Thus, for NOMA system, the achievable secrecy rate of PU can be given by

$$R_s^{[1]}=\left[\log_2\left(1+\frac{|\mathbf{h}_1\mathbf{v}_1|^2}{\sigma^2}\right)-R_e^{[1]}\right]^+. \tag{39}$$

Thus, in the NOMA system, while the private message x_2 is not required for SU, we let $\alpha_1=0$ and $r_2^{th}=0$. To enhance the security of private message without eavesdropping CSI, the original problem (14) is reformulated as

$$\max_{\mathbf{v}_1,\mathbf{v}_c,C_2} C_2 \tag{40a}$$

$$s.t.\ R_p^{[1]}\geq r_1^{th}, \tag{40b}$$

$$C_2\leq \log_2\left(1+r_c^{[i]}\right),\ \forall i\in\{1,2\}, \tag{40c}$$

$$C_2\geq c_2^{th}, \tag{40d}$$

$$\|\mathbf{v}_c\|^2+\|\mathbf{v}_1\|^2\leq P_s. \tag{40e}$$

Since (40) is also non-convex, it should be changed to convex.

Using the similar method in Subsection III-A, (40b) can be transformed as

$$\begin{cases} \widetilde{a}\geq 2^{r_1^{th}}, & (41)\\ \widetilde{b}\geq\sigma^2, & (42)\\ \dfrac{2\mathfrak{Re}\left(\overline{\mathbf{v}}_1^{\dagger}\mathbf{h}_1^{\dagger}\mathbf{h}_1\mathbf{v}_1\right)}{\bar{\widetilde{b}}}-\left(\dfrac{|\mathbf{h}_1\overline{\mathbf{v}}_1|}{\bar{\widetilde{b}}}\right)^2\widetilde{b}\geq\widetilde{a}-1. & (43)\end{cases}$$

Similarly, (40c) is equivalent to

$$\begin{cases} C_2\leq\widetilde{\epsilon}_i,\ \forall i\in\{1,2\}, & (44)\\ \widetilde{\theta}_i\geq 2^{\widetilde{\epsilon}_i},\ \forall i\in\{1,2\}, & (45)\\ \widetilde{z}_i\geq|\mathbf{h}_i\mathbf{v}_1|^2+\sigma^2,\ \forall i\in\{1,2\}, & (46)\\ \dfrac{2\mathfrak{Re}\left(\overline{\mathbf{v}}_c^{\dagger}\mathbf{h}_i^{\dagger}\mathbf{h}_i\mathbf{v}_c\right)}{\bar{\widetilde{z}}_i}-\left(\dfrac{|\mathbf{h}_i\overline{\mathbf{v}}_c|}{\bar{\widetilde{z}}_i}\right)^2\widetilde{z}_i\geq\widetilde{\theta}_i-1,\forall i\in\{1,2\}. & (47)\end{cases}$$

With a series of conversions, the problem (40) is eventually turned into a convex one as

$$\begin{aligned}
&\max_{\substack{\widetilde{a},\widetilde{b},\widetilde{\epsilon}_i,\widetilde{\theta}_i,\widetilde{z}_i\\ \mathbf{v}_1,\mathbf{v}_c,C_2}} C_2\\
&\quad s.t.\ \widetilde{a}\geq 2^{r_1^{th}},\ \ \widetilde{b}\geq\sigma^2,\\
&\qquad \frac{2\mathfrak{Re}\left(\overline{\mathbf{v}}_1^{\dagger}\mathbf{h}_1^{\dagger}\mathbf{h}_1\mathbf{v}_1\right)}{\bar{\widetilde{b}}}-\left(\frac{|\mathbf{h}_1\overline{\mathbf{v}}_1|}{\bar{\widetilde{b}}}\right)^2\widetilde{b}\geq\widetilde{a}-1,\\
&\qquad C_2\leq\widetilde{\epsilon}_i,\ \forall i\in\{1,2\},\\
&\qquad \widetilde{\theta}_i\geq 2^{\widetilde{\epsilon}_i},\ \forall i\in\{1,2\},\\
&\qquad \widetilde{z}_i\geq|\mathbf{h}_i\mathbf{v}_1|^2+\sigma^2,\ \forall i\in\{1,2\},\\
&\qquad \frac{2\mathfrak{Re}\left(\overline{\mathbf{v}}_c^{\dagger}\mathbf{h}_i^{\dagger}\mathbf{h}_i\mathbf{v}_c\right)}{\bar{\widetilde{z}}_i}-\left(\frac{|\mathbf{h}_i\overline{\mathbf{v}}_c|}{\bar{\widetilde{z}}_i}\right)^2\widetilde{z}_i\geq\widetilde{\theta}_i-1,\\
&\qquad\qquad\qquad\qquad\qquad\qquad \forall i\in\{1,2\},\\
&\qquad C_2\geq c_2^{th},\\
&\qquad \|\mathbf{v}_c\|^2+\|\mathbf{v}_1\|^2\leq P_s.
\end{aligned} \tag{48}$$

The convex problem (48) can be solved via CVX iteratively. Furthermore, similar to Subsection III-D, the number of constraints for (48) is $5K+6$. The iteration number to reduce the duality gap to a small constant is upper bounded as

$$\mathcal{O}(\sqrt{5K+6}), \tag{49}$$

where $K=2$ represents the amount of users. Then, the number of operations for every iteration can be denoted as

$$\begin{aligned}\mathcal{O}(n(n^2+(3K+4)n+(K+4)M^2\\ +(2K+4)M+4K+5)),\end{aligned} \tag{50}$$

where $n=(4M+3K+3)$ denotes the number of optimized variables. Then, the worst-case complexity in (48) is estimated as

$$\begin{aligned}&\mathcal{O}(n(n^2+(3K+4)n+(K+4)M^2\\&\quad+(2K+4)M+4K+5)\cdot(\sqrt{5K+6})).\end{aligned}\tag{51}$$

B. Special Case of SDMA

As shown in Fig. 2, when there is no common message, RSMA is then changed into SDMA. It is noteworthy that, compared with RSMA and NOMA, the characteristics of SDMA may be not suitable for the secure communication. When the common message x_c is not required for both of PU and SU in the SDMA system, by applying precoding to control the signal strength, the signal of SU can be amplified to hide the PU's private message, and the security of PU can be ensured with the access of SU.

In the SDMA network, the received signal at user-i is

$$y_i=\mathbf{h}_i\sum_{k=1}^{2}\mathbf{v}_k x_k+n_i,\ i\in\{1,2\}\,.\tag{52}$$

Moreover, at the receiving nodes of SDMA, the SINR for each user to decode its own information is

$$r_p^{[i]}=\frac{|\mathbf{h}_i\mathbf{v}_i|^2}{|\mathbf{h}_i\mathbf{v}_k|^2+\sigma^2},\ i,k\in\{1,2\}\,,k\neq i.\tag{53}$$

While PU denotes secure user, and SU accesses the network and serves as friendly jammer, the eavesdropping rate to PU is denoted by

$$R_e^{[1]}=\log_2\left(1+\frac{|\mathbf{h}_e\mathbf{v}_1|^2}{|\mathbf{h}_e\mathbf{v}_2|^2+\sigma^2}\right).\tag{54}$$

Similarly, in the SDMA system, the achievable secrecy rate for PU is expressed as

$$R_s^{[1]}=\left[\log_2\left(1+\frac{|\mathbf{h}_1\mathbf{v}_1|^2}{|\mathbf{h}_1\mathbf{v}_2|^2+\sigma^2}\right)-R_e^{[1]}\right]^+.\tag{55}$$

In order to resist the wiretapping to PU through increasing the power for SU, the precoding optimization problem (14) is reformulated for the SDMA case as

$$\max_{\mathbf{v}_i}\ R_p^{[2]}\tag{56a}$$

$$s.t.\ R_p^{[i]}\geq r_i^{th},\ \forall i\in\{1,2\}\,,\tag{56b}$$

$$\sum_{i=1}^{2}\|\mathbf{v}_i\|^2\leq P_s.\tag{56c}$$

Due to the non-convexity of (56a) and (56b), they should be transformed to convex.

First, the objective function (56a) can be rewritten as

$$\begin{aligned}&\log_2\left(1+\frac{|\mathbf{h}_2\mathbf{v}_2|^2}{|\mathbf{h}_2\mathbf{v}_1|^2+\sigma^2}\right)=\log_2\left(\frac{|\mathbf{h}_2\mathbf{v}_2|^2+|\mathbf{h}_2\mathbf{v}_1|^2+\sigma^2}{|\mathbf{h}_2\mathbf{v}_1|^2+\sigma^2}\right)\\&=\log_2\left(\frac{\sum_{j=1}^{2}\mathbf{h}_2\mathbf{v}_j\mathbf{v}_j^\dagger\mathbf{h}_2^\dagger+\sigma^2}{\mathbf{h}_2\mathbf{v}_1\mathbf{v}_1^\dagger\mathbf{h}_2^\dagger+\sigma^2}\right).\end{aligned}\tag{57}$$

Introducing variables m and n, we have

$$\sum_{j=1}^{2}\mathbf{h}_2\mathbf{v}_j\mathbf{v}_j^\dagger\mathbf{h}_2^\dagger+\sigma^2\geq e^m,\tag{58}$$

$$\mathbf{h}_2\mathbf{v}_1\mathbf{v}_1^\dagger\mathbf{h}_2^\dagger+\sigma^2\leq e^n.\tag{59}$$

Based on (58)-(59), we have

$$\begin{aligned}&\log_2\left(\frac{\sum_{j=1}^{2}\mathbf{h}_2\mathbf{v}_j\mathbf{v}_j^\dagger\mathbf{h}_2^\dagger+\sigma^2}{\mathbf{h}_2\mathbf{v}_1\mathbf{v}_1^\dagger\mathbf{h}_2^\dagger+\sigma^2}\right)\geq\log_2 e^m-\log_2 e^n\\&=(m-n)\cdot\log_2 e.\end{aligned}\tag{60}$$

Then, (56) is rewritten as

$$\max_{m,n,\mathbf{v}_i}\quad m-n\tag{61a}$$

$$s.t.\ \sum_{j=1}^{2}\mathbf{h}_2\mathbf{v}_j\mathbf{v}_j^\dagger\mathbf{h}_2^\dagger+\sigma^2\geq e^m,\tag{61b}$$

$$\mathbf{h}_2\mathbf{v}_1\mathbf{v}_1^\dagger\mathbf{h}_2^\dagger+\sigma^2\leq e^n,\tag{61c}$$

$$R_p^{[i]}\geq r_i^{th},\ \forall i\in\{1,2\}\,,\tag{61d}$$

$$\sum_{i=1}^{2}\|\mathbf{v}_i\|^2\leq P_s,\tag{61e}$$

in which the constraints still need to be further derived.

According to the Taylor' expansion, we have $T_1=e^{\overline{n}}(n-\overline{n}+1)$ at $\overline{n}$. Therefore, (61c) can be changed into

$$\mathbf{h}_2\mathbf{v}_1\mathbf{v}_1^\dagger\mathbf{h}_2^\dagger+\sigma^2\leq T_1.\tag{62}$$

Subsequently, using the second-order cone (SOC) constraint, we have

$$\zeta^2\leq\vartheta\omega\ (\vartheta\geq 0,\omega\geq 0)\Longrightarrow\|[2\zeta,\vartheta-\omega]^\dagger\|\leq\vartheta+\omega.\tag{63}$$

Thus, (62) can be expressed as

$$\left\|[2\mathbf{h}_2\mathbf{v}_1,2\sigma,T_1-1]^\dagger\right\|\leq T_1+1.\tag{64}$$

In addition, by adopting the first-order Taylor's approximation at $\overline{\mathbf{v}}_1$ and $\overline{\mathbf{v}}_2$, (61b) can be changed into

$$\begin{aligned}&2\mathfrak{Re}\left(\overline{\mathbf{v}}_1^\dagger\mathbf{h}_2^\dagger\mathbf{h}_2\mathbf{v}_1\right)-\mathfrak{Re}\left(\overline{\mathbf{v}}_1^\dagger\mathbf{h}_2^\dagger\mathbf{h}_2\overline{\mathbf{v}}_1\right)\\&+2\mathfrak{Re}\left(\overline{\mathbf{v}}_2^\dagger\mathbf{h}_2^\dagger\mathbf{h}_2\mathbf{v}_2\right)-\mathfrak{Re}\left(\overline{\mathbf{v}}_2^\dagger\mathbf{h}_2^\dagger\mathbf{h}_2\overline{\mathbf{v}}_2\right)+\sigma^2\geq e^m.\end{aligned}\tag{65}$$

Then, to ensure the transmission performance of the private information, especially to make the transmission rate of secure signal satisfy the threshold at PU, Proposition 2 is proposed to restrict and transform $R_p^{[i]}$.

Proposition 2: (61d) can be changed into

$$\begin{cases}\Gamma_i(\mathbf{v}_i,t_i,\overline{\mathbf{v}}_i,\overline{t}_i)=\dfrac{2\mathfrak{Re}\left(\overline{\mathbf{v}}_i^\dagger\mathbf{h}_i^\dagger\mathbf{h}_i\mathbf{v}_i\right)}{\overline{t}_i-1}\\\qquad-\dfrac{\mathfrak{Re}\left(\overline{\mathbf{v}}_i^\dagger\mathbf{h}_i^\dagger\mathbf{h}_i\overline{\mathbf{v}}_i\right)}{(\overline{t}_i-1)^2}(t_i-1),i\in\{1,2\}\,,\\\left\|[2\mathbf{h}_i\mathbf{v}_k,2\sigma,\Gamma_i-1]^\dagger\right\|\leq\Gamma_i+1,\ i\in\{1,2\}\,,\\t_i\geq 2^{r_i^{th}},\ i\in\{1,2\}\,.\end{cases}\tag{66}$$

TABLE I
COMPARISON OF RSMA, NOMA AND SDMA IN THE UNIFIED RATE-SPLITTING FRAMEWORK FOR SECURE SPECTRUM SHARING

	RSMA	**NOMA**	**SDMA**
Decoding method	Decode the common part via NOMA and recover the private messages via SDMA	Perform SIC at receiving ends	Treat the signal from the other user as noise
Secrecy capability	Secure transmission for both PU and SU	Secure transmission for PU	Secure transmission for PU
Security strategy	Hiding private message in the common signal	Hiding private message in the common signal	Hiding the private message in the signal of SU
Capability of accommodating more users	Good	Good	Limited

Proof: First, to deal with $R_p^{[i]} \geq r_i^{th}$, let

$$1+\frac{|\mathbf{h}_i\mathbf{v}_i|^2}{|\mathbf{h}_i\mathbf{v}_k|^2+\sigma^2} \geq t_i,\ i,k \in \{1,2\}, k \neq i, \tag{67}$$

which can be rewritten as

$$\frac{|\mathbf{h}_i\mathbf{v}_i|^2}{t_i-1} \geq |\mathbf{h}_i\mathbf{v}_k|^2+\sigma^2,\ i,k \in \{1,2\}, k \neq i. \tag{68}$$

The left part in (68) can be expressed as

$$L_i(\mathbf{v}_i, t_i) = \frac{\mathbf{h}_i\mathbf{v}_i\mathbf{v}_i^\dagger\mathbf{h}_i^\dagger}{t_i-1},\ i \in \{1,2\}. \tag{69}$$

Performing the first-order Taylor expansion of (69), we have

$$\begin{aligned}\Gamma_i(\mathbf{v}_i, t_i, \overline{\mathbf{v}}_i, \overline{t}_i) = & \frac{2\mathfrak{Re}\left(\overline{\mathbf{v}}_i^\dagger\mathbf{h}_i^\dagger\mathbf{h}_i\mathbf{v}_i\right)}{\overline{t}_i-1} \\ & - \frac{\mathfrak{Re}\left(\overline{\mathbf{v}}_i^\dagger\mathbf{h}_i^\dagger\mathbf{h}_i\overline{\mathbf{v}}_i\right)}{(\overline{t}_i-1)^2}(t_i-1), i \in \{1,2\}.\end{aligned} \tag{70}$$

Then, by using the SOC constraint (63), (68) can be changed into

$$\left\|\left[2\mathbf{h}_i\mathbf{v}_k, 2\sigma, \Gamma_i-1\right]^\dagger\right\| \leq \Gamma_i+1,\ i \in \{1,2\}. \tag{71}$$

After the above derivation, the rate constraint of the private message (61d) is eventually derived as

$$(70),\ (71),\ t_i \geq 2^{r_i^{th}},\ i \in \{1,2\}, \tag{72}$$

which is equivalent to (66). ■

Based on (64), (65) and Proposition 2, the optimization problem (61) is transformed as (73) at next page, which is convex.

Then, computational complexity of (73) can be estimated. The number of constraints in (73) is $3K+5$. The iteration number to reduce the duality gap to a small constant is upper bounded as

$$\mathcal{O}(\sqrt{3K+5}), \tag{74}$$

where $K=2$ represents users' number. Then, the number of operations for every iteration is

$$\begin{aligned}&\mathcal{O}(n(n^2+(K+1)n+(K^2+K+1)M^2 \\ &+(4K+2)M+2K+3)),\end{aligned} \tag{75}$$

where $n=(2MK+K+2)$ denotes the number of optimized variables. Thus, the worst-case complexity in (73) is derived as

$$\begin{aligned}&\mathcal{O}(n(n^2+(K+1)n+(K^2+K+1)M^2 \\ &+(4K+2)M+2K+3)\cdot(\sqrt{3K+5})).\end{aligned} \tag{76}$$

C. Comparison of Three Cases

The relevance and difference of the three cases in the RSMA framework for the secure transmission are compared in Table 1. Details are summarized as follows.

- *Decoding method:* RSMA first recovers the common signal and separates it from the private signal via NOMA. Next, it demodulates the private message of PU or SU via SDMA. In NOMA, SIC is performed, and PU should first decode the interference from SU and remove it. For SDMA, every user demodulates the desired information directly through regarding the interference from the other user as noise.
- *Secrecy capability:* RSMA can ensure the secure transmission for the private information of both PU and SU. For NOMA or SDMA networks, the private message of only PU can be safely transmitted.
- *Security strategy:* Both RSMA and NOMA can hide the private information in the common signal, while SDMA needs to hide the PU's private message in the signal of SU accessed to the network.
- *Capability of accommodating more users:* It is suitable for RSMA and NOMA to serve more users. For the SDMA, it becomes incapable when the communication system is overloaded.

V. SIMULATION RESULTS

To assess and compare the security achievement for the designed RSMA framework with its special instances of NOMA and SDMA, lots of simulations are presented. We focus on a downlink system including two CR nodes and one wiretapper. The distance between BS and PU and that between BS and SU is set to 250 m and 450 m, correspondingly. Besides, the noise power σ^2 is set to 10^{-11} mW, and α and β in (5) is set to 2.6 and 10^{-4} [41], respectively.

Fig. 3 presents the convergence for the common rate with different P_s in RSMA scheme, when $M=4$, $d_e=200$ m, and

$$\begin{aligned}
&\max_{m,n,t_i,\mathbf{v}_i} \quad m-n && \text{(73a)}\\
&s.t.\ \ 2\mathfrak{Re}\left(\overline{\mathbf{v}}_1^{\dagger}\mathbf{h}_2^{\dagger}\mathbf{h}_2\mathbf{v}_1\right)-\mathfrak{Re}\left(\overline{\mathbf{v}}_1^{\dagger}\mathbf{h}_2^{\dagger}\mathbf{h}_2\overline{\mathbf{v}}_1\right)+2\mathfrak{Re}\left(\overline{\mathbf{v}}_2^{\dagger}\mathbf{h}_2^{\dagger}\mathbf{h}_2\mathbf{v}_2\right)-\mathfrak{Re}\left(\overline{\mathbf{v}}_2^{\dagger}\mathbf{h}_2^{\dagger}\mathbf{h}_2\overline{\mathbf{v}}_2\right)+\sigma^2\geq e^{m}, && \text{(73b)}\\
&\quad T_1=e^{\overline{n}}(n-\overline{n}+1),\ \left\|\left[2\mathbf{h}_2\mathbf{v}_1,2\sigma,T_1-1\right]^{\dagger}\right\|\leq T_1+1, && \text{(73c)}\\
&\quad \Gamma_i(\mathbf{v}_i,t_i,\overline{\mathbf{v}}_i,\overline{t}_i)=\frac{2\mathfrak{Re}\left(\overline{\mathbf{v}}_i^{\dagger}\mathbf{h}_i^{\dagger}\mathbf{h}_i\mathbf{v}_i\right)}{\overline{t}_i-1}-\frac{\mathfrak{Re}\left(\overline{\mathbf{v}}_i^{\dagger}\mathbf{h}_i^{\dagger}\mathbf{h}_i\overline{\mathbf{v}}_i\right)}{(\overline{t}_i-1)^2}(t_i-1),\ i\in\{1,2\}, && \text{(73d)}\\
&\quad \left\|\left[2\mathbf{h}_i\mathbf{v}_k,2\sigma,\Gamma_i-1\right]^{\dagger}\right\|\leq\Gamma_i+1,\ t_i\geq 2^{r_i^{th}},\ \forall i\in\{1,2\}, && \text{(73e)}\\
&\quad \sum_{i=1}^{2}\|\mathbf{v}_i\|^2\leq P_s. && \text{(73f)}
\end{aligned}$$

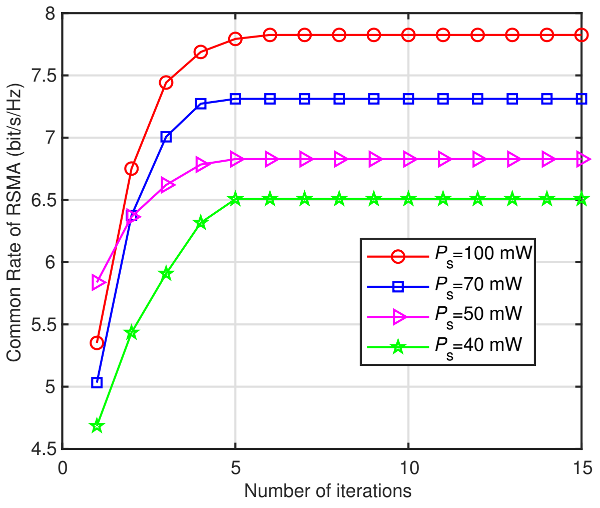


Fig. 3. Convergence of the common rate for RSMA with different P_s.

the transmission threshold for the private information $r_i^{th} = 0.5$ bit/s/Hz, $i = 1, 2$ [42]. After around six iterations, the common rate of RSMA tends to converge for various P_s. In addition, the achievable common rate increases from 6.5 to 7.8 bit/s/Hz as P_s varies from 40 mW to 100 mW. Therefore, we can see that the original optimization (14) can be effectively solved via the proposed algorithm, which is convergent.

Fig. 4 depicts a comparison for the common rate and the sum eavesdropping rate with various P_s and M, when $d_e = 200$ m, and $r_i^{th} = 1$ bit/s/Hz, $i = 1, 2$. The common rate for RSMA can be improved using more P_s and M, which suggest that more antennas or greater transmit power can improve transmission performance. RSMA's sum eavesdropping rate can approach 0 with varying M, especially at greater P_s. Through sheltering the secure part in larger common message, W_i^p is greatly protected. Moreover, it is noteworthy that sum eavesdropping rate in RSMA becomes smaller with P_s.

The weight coefficient α_1 and the threshold r_2^{th} have effect on the common rate, which is shown in Fig. 5. $P_s = 10$ mW, $M = 4$, $\alpha_2 = 1$, $r_1^{th} = 1$ bit/s/Hz, and $d_e = 200$ m. In detail, as r_2^{th} changes from 0 to 2 bit/s/Hz, the common rate declines consequently. This is because as the threshold for x_2 increases, more power should be utilized for the private part. Therefore,

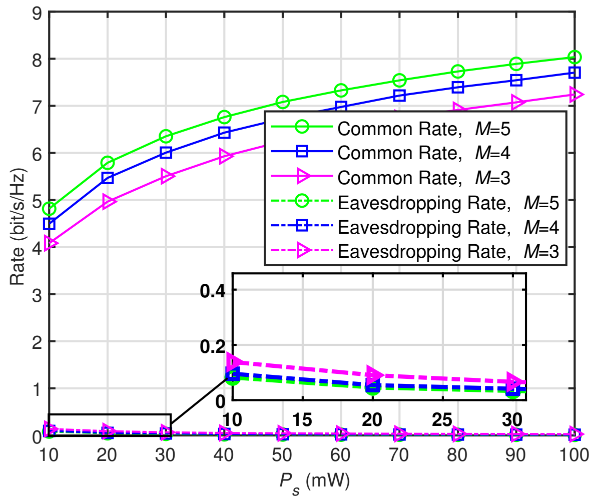


Fig. 4. Common rate and sum eavesdropping rate comparison for RSMA with different M and P_s.

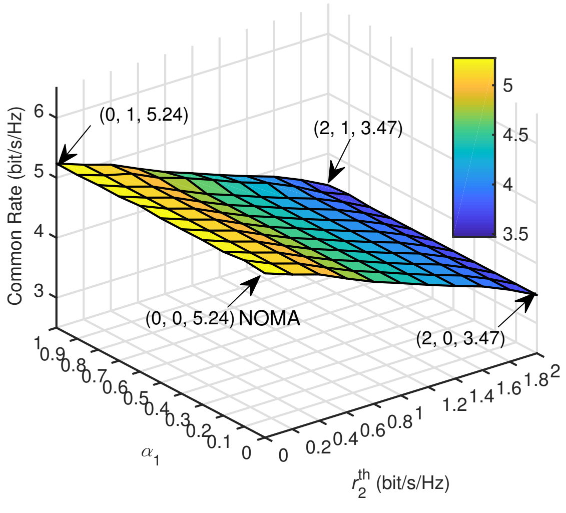


Fig. 5. Common rate comparison with different α_1 and r_2^{th}.

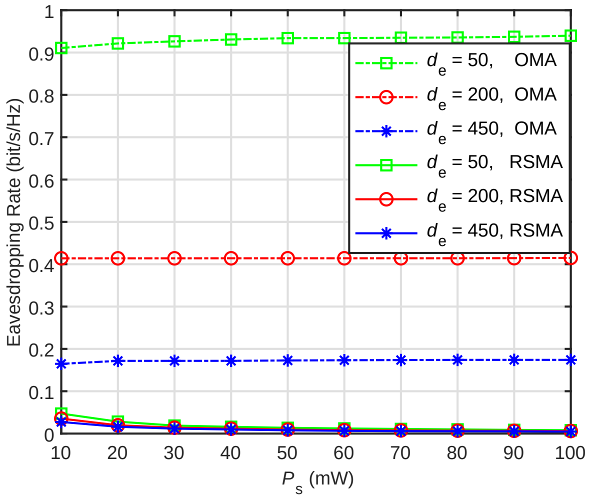


Fig. 6. Sum eavesdropping rate comparison for RSMA and OMA with different M, d_e and P_s.

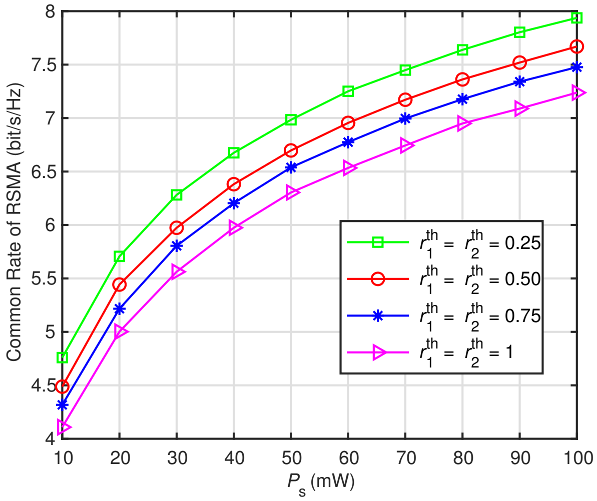


Fig. 7. Common rate comparison for RSMA with different r_i^{th} and P_s.

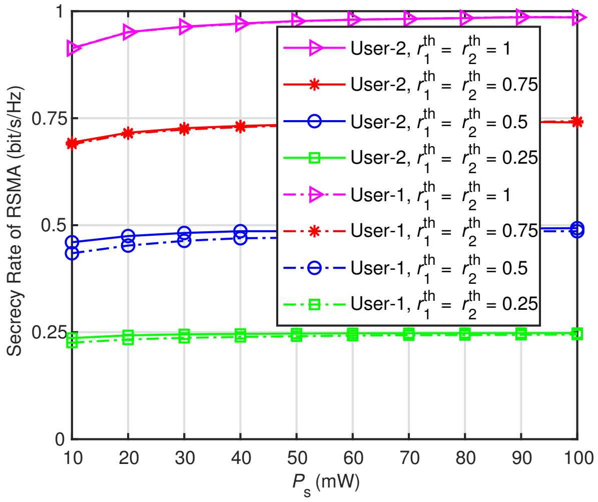


Fig. 8. Secrecy rate comparison for RSMA with different r_i^{th} and P_s.

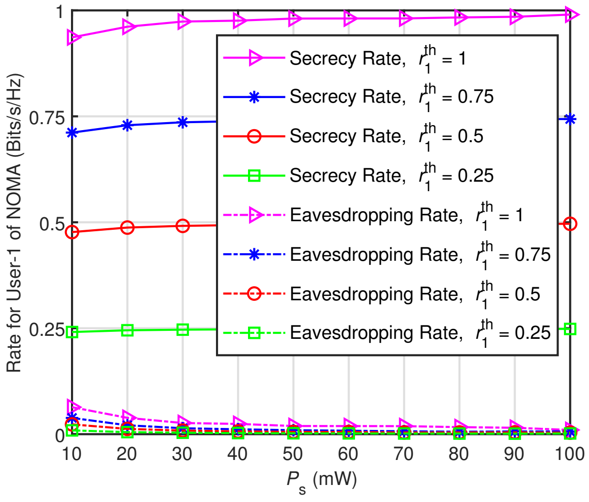


Fig. 9. Secrecy rate and eavesdropping rate comparison for NOMA with different r_1^{th} and P_s.

the allocated power for common message decreases, leading to the decrease of transmission rate of x_c. Moreover, changing α_1 will have little influence on the transmission performance of x_c with fixed allocated transmit power. Specifically, comparing (14) and (40), when both α_1 and r_2^{th} turn to 0, the proposed system switches from RSMA to NOMA.

Fig. 6 studies the impact of eavesdropping distance d_e and transmit power P_s on the sum eavesdropping rate in RSMA and OMA, when $M = 4$ and $r_1^{th} = r_2^{th} = 0.5$ bit/s/Hz. We can see that when d_e becomes larger, the security performance of the schemes can be better. It can also be noted that, through hiding the private message in the common signal, the eavesdropping rate to the private signals in RSMA is much smaller than that in OMA. Nevertheless, even when the eavesdropper is close to BS, the anti-eavesdropping for RSMA system can be also ensured through the proposed secure design.

Fig. 7 shows the impact of different threshold r_i^{th} and P_s on the common rate, when $M = 3$ and $d_e = 100$ m. It is shown that the common rate decreases with r_i^{th} in the RSMA scheme. This is because when the rate thresholds r_1^{th} and r_2^{th} become larger, more transmit power is allocated to the private signals, which will increase the transmission rate accordingly. Therefore, the transmit power allocated to x_c becomes lower, and the common transmission rate decreases.

Fig. 8 compares the secrecy rate in RSMA with different r_i^{th} and P_s, when $M = 3$ and $d_e = 100$ m. It is shown that secrecy rate of PU and SU is ensured to be close to r_i^{th} especially when P_s is higher. This indicates that via maximizing the common rate in (14), the eavesdropping to W_i^p can be interfered effectively. In addition, when the transmit power P_s is higher, its secrecy rate is closer to its transmission rate. It further proves that the wiretapping to x_i decreases with P_s.

Then, we compare the secrecy rate and the eavesdropping rate of PU in NOMA with different r_1^{th} and P_s in Fig. 9, when $M = 3$ and $d_e = 100$ m. It is shown that the eavesdropping towards the private message for PU can be disrupted in NOMA

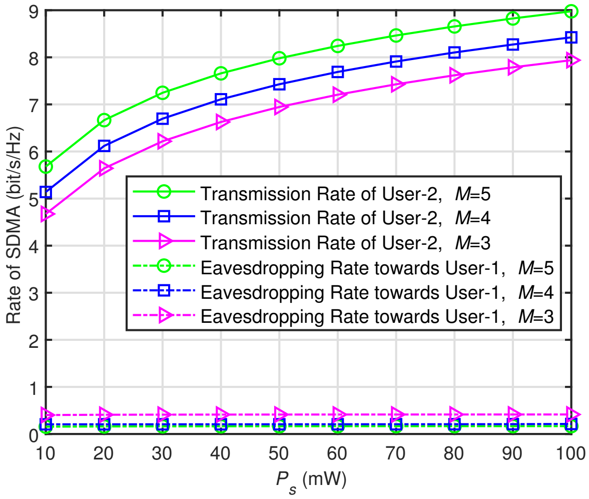


Fig. 10. Transmission rate of SU and eavesdropping rate towards the secure user comparison for SDMA with different M and P_s.

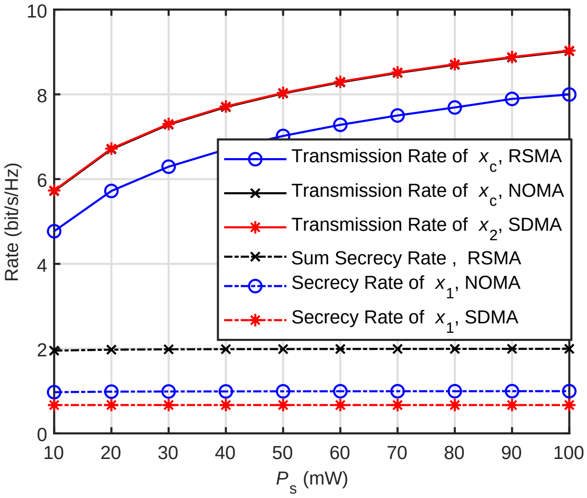


Fig. 11. Transmission rate and secrecy rate comparison for the three systems with different P_s.

design. Specifically, SU's common rate is maximized in (40) to disrupt the eavesdropping towards PU. When r_1^{th} is lower, more transmit power is saved to resist the wiretapper, and eavesdropping rate to PU is smaller. When P_s is high enough, PU's secrecy rate can be close to transmission rate, and the eavesdropping rate to PU in this network can approach zero.

Fig. 10 shows the transmission rate of SU and the eavesdropping rate to the secure user PU in the SDMA system with different P_s and M, when $d_e = 200$ m, and $r_i^{th} = 0.75$ bit/s/Hz, $i = 1, 2$. The results demonstrate that transmission performance of x_2 can be greatly improved in the proposed SDMA scheme, and SU's transmission rate increases with more antennas and higher transmit power. Furthermore, the eavesdropping rate towards the PU of SDMA will be lower when the number of antennas increases, but is not significantly affected by P_s. Thus, the communication privacy of the secure information in SDMA system can also be guaranteed.

Fig. 11 studies the transmission rate and secrecy rate for the three schemes under various P_s, when $M = 5$, $d_e = 150$ m, and $r_i^{th} = 0.5$ bit/s/Hz, $i = 1, 2$. The secrecy rate for NOMA and SDMA network is lower than that of RSMA, owing to our RSMA design can guarantee the security of all nodes' secure message. Furthermore, the secrecy rate for SDMA is the lowest in these three schemes, because SDMA nodes will interfere with each other when decoding. The secrecy rate for the private message of RSMA or NOMA can be nearer to the transmission threshold with higher transmit power. In addition, more resource is allocated to the private message in RSMA network, resulting in a smaller R_c than NOMA or SDMA.

VI. Conclusion

This research focuses on setting up a unified rate-splitting framework to ensure spectrum sharing security for CR networks via RSMA, NOMA, and SDMA strategies. By dividing the message of both PU and SU into private and common parts, RSMA is applied to decode the common information through SIC when taking the interference as noise while demodulating the private part. Via the precoding optimization and agile utilization of SIC, the private signal in RSMA can be secreted by the great-power common signal. In addition, regarding the signal of SU as friendly jamming, the secure spectrum sharing schemes for NOMA and SDMA can be similarly designed via precoding optimization, which has been transformed into a convex problem to be settled iteratively. Through the simulations, it is confirmed that the framework we established is capable of ensuring the privacy of private signal in RSMA. The security performance for NOMA and SDMA can be also effectively improved. Moreover, the imperfect SIC for the proposed rate-splitting framework will be studied in the future work.

References

[1] D. Li, Z. Yang, N. Zhao, Y. Chen, Z. Wu, and Y. Li, "Precoding optimization assisted secure transmission for rate-splitting multiple access," in *Proc. IEEE ICC'22*, pp. 1–6, Seoul, South Korea, May 2022.

[2] S. Haykin and P. Setoodeh, "Cognitive radio networks: The spectrum supply chain paradigm," *IEEE Trans. Cogn.. Commun. Netw.*, vol. 1, no. 1, pp. 3–28, Mar. 2015.

[3] 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 Commun. Mag.*, vol. 56, no. 4, pp. 188–195, Mar. 2018.

[4] Y. Cai, Z. Qin, F. Cui, G. Y. Li, and J. A. McCann, "Modulation and multiple access for 5G networks," *IEEE Commun. Surv. Tutor.*, vol. 20, no. 1, pp. 629–646, 1st Quart., 2018.

[5] A. I. Sulyman and M. Hefnawi, "Adaptive MIMO beamforming algorithm based on gradient search of the channel capacity in OFDM-SDMA systems," *IEEE Commun. Lett.*, vol. 12, no. 9, pp. 642–644, Sept. 2008.

[6] T. Zhou, M. Peng, W. Wang, and H. Chen, "Low-complexity coordinated beamforming for downlink multicell SDMA/OFDM systems," *IEEE Trans. Veh. Technol.*, vol. 62, no. 1, pp. 247–255, Jan. 2013.

[7] I. Khaled, C. Langlais, A. El Falou, M. Jezequel, and B. ElHasssan, "Joint SDMA and power-domain NOMA system for multi-user mm-wave communications," in *Proc. IEEE IWCMC'20*, pp. 1112–1117, Limassol, Cyprus, Jun. 2020.

[8] L. Yang, "MIMO-assisted space-code-division multiple-access: Linear detectors and performance over multipath fading channels," *IEEE J. Sel. Areas Commun.*, vol. 24, no. 1, pp. 121–131, Jan. 2006.

[9] Z. Ding, Y. Liu, J. Choi, Q. Sun, M. Elkashlan, I. Chih-Lin, and H. V. Poor, "Application of non-orthogonal multiple access in LTE and 5G networks," *IEEE Commun. Mag.*, vol. 55, no. 2, pp. 185–191, Feb. 2017.

[10] S. M. R. Islam, M. Zeng, O. A. Dobre, and K. Kwak, "Resource allocation for downlink NOMA systems: Key techniques and open issues," *IEEE Wireless Commun.*, vol. 25, no. 2, pp. 40–47, Apr. 2018.

[11] L. Liu, C. Yuen, Y. L. Guan, and Y. Li, “Capacity-achieving iterative lmmse detection for mimo-noma systems,” in *Proc. IEEE ICC’16*, pp. 1–6, May 2016.

[12] L. Liu, C. Yuen, Y. L. Guan, Y. Li, and C. Huang, “Gaussian message passing for overloaded massive mimo-noma,” *IEEE Trans. Wireless Commun.*, vol. 18, no. 1, pp. 210–226, Jan. 2019.

[13] B. M. ElHalawany, A. A. A. El-Banna, Q.-V. Pham, K. Wu, and E. M. Mohamed, “Spectrum sharing in cognitive-radio-inspired NOMA systems under imperfect SIC and cochannel interference,” *IEEE Syst. J.*, vol. 16, no. 1, pp. 1540–1547, Mar. 2022.

[14] 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 Trans. Commun.*, vol. 67, no. 1, pp. 83–96, Jan. 2019.

[15] L. Lv, J. Chen, and Q. Ni, “Cooperative non-orthogonal multiple access in cognitive radio,” *IEEE Commun. Lett.*, vol. 20, no. 10, pp. 2059–2062, Oct. 2016.

[16] L. Xu, W. Yin, X. Zhang, and Y. Yang, “Fairness-aware throughput maximization over cognitive heterogeneous NOMA networks for industrial cognitive IoT,” *IEEE Trans. Commun.*, vol. 68, no. 8, pp. 4723–4733, Aug. 2020.

[17] N. Nandan, S. Majhi, and H. Wu, “Secure beamforming for MIMO-NOMA-based cognitive radio network,” *IEEE Commun. Lett.*, vol. 22, no. 8, pp. 1708–1711, May 2018.

[18] Y. Cao, N. Zhao, Y. Chen, M. Jin, Z. Ding, Y. Li, and F. R. Yu, “Secure transmission via beamforming optimization for NOMA networks,” *IEEE Wireless Commun.*, vol. 27, no. 1, pp. 193–199, Aug. 2020.

[19] N. Zhao, D. Li, M. Liu, Y. Cao, Y. Chen, Z. Ding, and X. Wang, “Secure transmission via joint precoding optimization for downlink MISO NOMA,” *IEEE Trans. Veh. Technol.*, vol. 68, no. 8, pp. 7603–7615, May 2019.

[20] W. Wu, X. Wang, F. Zhou, K.-K. Wong, C. Li, and B. Wang, “Resource allocation for enhancing offloading security in NOMA-enabled MEC networks,” *IEEE Syst. J.*, vol. 15, no. 3, pp. 3789–3792, Sept. 2021.

[21] Y. Mao, B. Clerckx, and V. O. K. Li, “Rate-splitting multiple access for downlink communication systems: bridging, generalizing, and outperforming SDMA and NOMA,” *J. Wireless Com. Network*, vol. 133, no. 1, pp. 1687–1499, May 2018.

[22] 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, Jul. 2016.

[23] 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.

[24] 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. Mag.*, vol. 54, no. 5, pp. 98–105, May 2016.

[25] Y. Mao, B. Clerckx, and V. O. K. Li, “Rate-splitting for multi-user multi-antenna wireless information and power transfer,” in *Proc. IEEE SPAWC’19*, pp. 1–5, Cannes, France, Jul. 2019.

[26] M. R. C. Acosta, C. E. G. Moreta, and I. Koo, “Joint power allocation and power splitting for MISO-RSMA cognitive radio systems with SWIPT and information decoder users,” *IEEE Syst. J.*, vol. 15, no. 4, pp. 5289–5300, Dec. 2021.

[27] O. Dizdar and B. Clerckx, “Rate-splitting multiple access for communications and jamming in multi-antenna multi-carrier cognitive radio systems,” *IEEE Trans. Inf. Forensics Security*, vol. 17, pp. 628–643, Feb. 2022.

[28] Z. Yang, M. Chen, W. Saad, W. Xu, and M. Shikh-Bahaei, “Sum-rate maximization of uplink rate splitting multiple access (RSMA) communication,” *IEEE Trans. Mobile Comput.*, to be published, DOI:10.1109/TMC.2020.3037374.

[29] W. Jaafar, S. Naser, S. Muhaidat, P. C. Sofotasios, and H. Yanikomeroglu, “Multiple access in aerial networks: From orthogonal and non-orthogonal to rate-splitting,” *IEEE Open J. Veh. Technol.*, vol. 1, pp. 372–392, Oct. 2020.

[30] Z. Lin, M. Lin, T. de Cola, J.-B. Wang, W.-P. Zhu, and J. Cheng, “Supporting iot with rate-splitting multiple access in satellite and aerial-integrated networks,” *IEEE Internet Things J.*, vol. 8, no. 14, pp. 11123–11134, Jul. 2021.

[31] J. Zhou, Y. Sun, R. Chen, and C. Tellambura, “Rate splitting multiple access for multigroup multicast beamforming in cache-enabled C-RAN,” *IEEE Trans. Veh. Technol.*, vol. 70, no. 12, pp. 12758–12770, Dec. 2021.

[32] Z. Yang, M. Chen, W. Saad, and M. Shikh-Bahaei, “Optimization of rate allocation and power control for rate splitting multiple access (RSMA),” *IEEE Trans. Commun.*, vol. 69, no. 9, pp. 5988–6002, Sept. 2021.

[33] P. Li, M. Chen, Y. Mao, Z. Yang, B. Clerckx, and M. Shikh-Bahaei, “Cooperative rate-splitting for secrecy sum-rate enhancement in multi-antenna broadcast channels,” in *Proc. IEEE PIMRC’20*, pp. 1–6, London, UK, Sept. 2020.

[34] H. Xia, Y. Mao, B. Clerckx, X. Zhou, S. Han, and C. Li, “Weighted sum-rate maximization for rate-splitting multiple access based secure communication,” in *IEEE WCNC’22*, pp. 19–24, Austin, TX, USA, Apr. 2022.

[35] H. Bastami, M. Letafati, M. Moradikia, A. Abdelhadi, H. Behroozi, and L. Hanzo, “On the physical layer security of the cooperative rate-splitting-aided downlink in UAV networks,” *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 5018–5033, Oct. 2021.

[36] H. Fu, S. Feng, W. Tang, and D. W. K. Ng, “Robust secure beamforming design for two-user downlink miso rate-splitting systems,” *IEEE Trans. Wireless Commun.*, vol. 19, no. 12, pp. 8351–8365, Dec. 2020.

[37] Y. Gao, Q. Wu, W. Chen, and D. W. K. Ng, “Rate-splitting multiple access for intelligent reflecting surface-aided secure transmission,” *IEEE Commun. Lett.*, vol. 27, no. 2, pp. 482–486, Feb. 2023.

[38] Z. Lin, M. Lin, B. Champagne, W.-P. Zhu, and N. Al-Dhahir, “Secure and energy efficient transmission for RSMA-based cognitive satellite-terrestrial networks,” *IEEE Wireless Commun. Lett.*, vol. 10, no. 2, pp. 251–255, Feb. 2021.

[39] A. Salem, C. Masouros, and B. Clerckx, “Secure rate splitting multiple access: How much of the split signal to reveal?,” *IEEE Trans. Wireless Commun.*, to appear.

[40] A. Khisti and G. W. Wornell, “Secure transmission with multiple antennasłpart ii: The mimome wiretap channel,” *IEEE Trans. Inf. Theory*, vol. 56, no. 11, pp. 5515–5532, Nov. 2010.

[41] B. Chen, Y. Chen, Y. Chen, Y. Cao, Z. Ding, N. Zhao, and X. Wang, “Secure primary transmission assisted by a secondary full-duplex NOMA relay,” *IEEE Trans. Veh. Technol.*, vol. 68, no. 7, pp. 7214–7219, Jul. 2019.

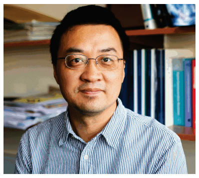
[42] Y. Cao, N. Zhao, G. Pan, Y. Chen, L. Fan, M. Jin, and M. Alouini, “Secrecy analysis for cooperative NOMA networks with multi-antenna full-duplex relay,” *IEEE Trans. Commun.*, vol. 67, no. 8, pp. 5574–5587, Aug. 2019.

Dongdong Li received the B.E. and M.E. degrees in information and communication engineering from Dalian University of Technology, Dalian, China, in 2018 and 2021, respectively. She is currently working toward the Ph.D. degree with the School of Electronics Information Engineering, Harbin Institute of Technology. Her research interests include nonorthogonal multiple access, physical layer security, integrated sensing and communications, and unmanned aerial vehicle communications.

Zhutian Yang (Senior Member, IEEE) received the Ph.D. degree in information and communication engineering from the Harbin Institute of Technology, Heilongjiang, China, in 2013.

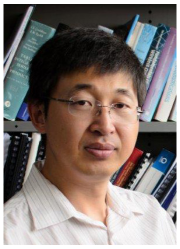
He was an Academic Visitor with King’s College London, in 2015. He is currently a Professor with the School of Electronics Information Engineering at the HIT, China. His current research interests include machine learning, signal processing, and smart city communications.

Nan Zhao (Senior Member, IEEE) is currently a Professor at Dalian University of Technology, China. He received the Ph.D. degree in information and communication engineering in 2011, from Harbin Institute of Technology, Harbin, China. Dr. Zhao is serving on the editorial boards of IEEE Wireless Communications and IEEE Wireless Communications Letters. He won the best paper awards in IEEE VTC 2017 Spring, ICNC 2018, WCSP 2018 and WCSP 2019. He also received the IEEE Communications Society Asia Pacific Board Outstanding Young Researcher Award in 2018.



Yunfei Chen (Senior Member, IEEE) received the B.E. and M.E. degrees in electronics engineering from Shanghai Jiaotong University, Shanghai, China, in 1998 and 2001, respectively, and the Ph.D. degree from the University of Alberta in 2006. He is currently working as a Professor with the Department of Engineering, University of Durham, U.K. His research interests include wireless communications, performance analysis, joint radar communications designs, cognitive radios, wireless relaying, and energy harvesting.

Zhilu Wu is currently a Professor with the School of Electronics Information Engineering, Harbin Institute of Technology. His research interests include space information acquisition and processing, formation flying satellite control, cognitive radio, and software radio.



Yonghui Li (Fellow, IEEE) received his PhD degree in November 2002 from Beijing University of Aeronautics and Astronautics. Since 2003, he has been with the Centre of Excellence in Telecommunications, the University of Sydney, Australia. He is now a Professor and Director of Wireless Engineering Laboratory in School of Electrical and Information Engineering, University of Sydney. He is the recipient of the Australian Queen Elizabeth II Fellowship in 2008 and the Australian Future Fellowship in 2012. He is a Fellow of IEEE.

His current research interests are in the area of wireless communications, with a particular focus on MIMO, millimeter wave communications, machine to machine communications, coding techniques and cooperative communications. He holds a number of patents granted and pending in these fields. He is now an editor for IEEE transactions on communications, IEEE transactions on vehicular technology. He also served as the guest editor for several IEEE journals, such as IEEE JSAC, IEEE Communications Magazine, IEEE IoT journal, IEEE Access. He received the best paper awards from IEEE International Conference on Communications (ICC) 2014, IEEE PIRMC 2017 and IEEE Wireless Days Conferences (WD) 2014.