Secure Primary Transmission Assisted by a Secondary Full-Duplex NOMA Relay

Bingcai Chen, *Member, IEEE,* Yu Chen, Yunfei Chen, *Senior Member, IEEE,* Yang Cao, Zhiguo Ding, *Senior Member, IEEE,* Nan Zhao, *Senior Member, IEEE,* Xianbin Wang, *Fellow, IEEE*

***Abstract*—In this correspondence, secure primary transmission is proposed by using a multi-antenna secondary full-duplex non-orthogonal multiple access (NOMA) relay in cognitive radio (CR) networks. First, the primary signal is transmitted from the primary transmitter to the relay. Artificial noise is generated by using part of the antennas at the relay to disrupt eavesdropping, without affecting the primary transmission. Then, superimposed signals are transmitted from the relay to the primary receiver (PR) and secondary receivers (SRs) via NOMA. The primary security is guaranteed by the modified decoding order and beamforming optimization, which is converted to convex and solved by an iterative algorithm. Simulation results are presented to show the effectiveness of the proposed scheme in guaranteeing the primary security in CR networks.**

***Index Terms*—Artificial noise, cognitive radio, non-orthogonal multiple access, physical layer security, full-duplex relay.**

I. Introduction

Non-orthogonal multiple access (NOMA) is considered as a promising technique for radio resource constrained 5G mobile networks [1]. Among several possible implementation schemes, power-domain NOMA remains the most popular one, in which different transmit power is allocated to users according to their channel strength, and the transmitted information is recovered by successive interference cancellation (SIC) at each receiver [2]. Recently, relay-aided NOMA has been widely studied due to its superior performance in improving spectrum efficiency and network coverage concurrently [3]–[6]. In [3], Wu *et al.* optimized the power allocation (PA) to maximize the throughput for NOMA relay-assisted networks. Energy efficiency was maximized through PA by Liu *et al.* in [4], for cooperative networks using NOMA. In [5], Lv *et al.* presented a novel NOMA-based transmission scheme to deliver the primary and secondary messages via a secondary relay in cognitive radio (CR) networks. Long-distance primary transceivers were connected via a secondary NOMA relay to achieve spectrum sharing by Chen *et al.* in [6].

Although NOMA can enhance spectrum efficiency, its communication security and confidentiality remain as major challenges [7]–[10]. In [9], Liu *et al.* analyzed the security performance of NOMA in large-scale networks. Lv *et al.* proposed a novel beamforming scheme in [10], in which artificial noise (AN) is adopted to improve the transmission confidentiality of NOMA users. However, very few works have been focused on the security of relay-aided NOMA networks [11] [12]. In [11], an effective downlink cascaded beamforming scheme was proposed by Nandan *et al.* to guarantee the secure transmission for a two-cell MIMO-NOMA based CR network. In [12], Zheng *et al.* proposed a two-way secure transmission scheme via a full-duplex NOMA relay and AN, in which the relay with multiple antennas is exploited to ensure the security of signal transmission between two users. Different from [12], we propose a two-slot secure transmission scheme assisted by a secondary full-duplex NOMA relay for CR networks in this correspondence. The key motivation and contribution of this paper are summarized as follows.

- We consider the scenario where the primary[1] receiver is far from its transmitter without direct channel, and the primary user requires secure transmission, which is very challenging. To solve this problem, the secondary users aim to perform transmission via NOMA in the primary spectrum, on the condition that they can help the primary user to perform secure transmission. Thus, we propose this secure primary transmission scheme assisted by a secondary NOMA relay in this paper.
- The proposed scheme can be achieved in two time slots. First, the primary signal is transmitted from the primary transmitter (PT) to the relay, which is easy to be eavesdropped. Thus, we use the full-duplex relay to generate AN to disrupt the eavesdropping while receiving the signal from PT, and the AN will not affect the legitimate transmission.
- The distance between the relay and the primary receiver

[1]In this paper, "primary" and "secondary" refer to the transmission for the primary user and secondary users in the CR network, respectively.

Manuscript received November 3, 2018; revised January 24, 2019, March 20, 2019 and May 9, 2019; accepted May 26, 2019. The work of B. Chen was supported by the National Natural Science Foundation of China (NSFC) under Grant 61871065 and 61871139. The work of Z. Ding was supported by the UK EPSRC under grant number EP/L025272/2, NSFC under grant number 61728101 and H2020-MSCA-RISE-2015 under grant number 690750. The associate editor coordinating the review of this paper and approving it for publication was S. Majhi. *(Corresponding author: Nan Zhao.)*

B. Chen, Y. Chen, Y. Cao and N. Zhao are with the Faculty of Electronic Information and Electrical Engineering, Dalian University of Technology, Dalian 116024, China, and also with the School of Information Science and Technology, Qingdao University of Science and Technology, Qingdao, 266000, P. R. China. B. Chen is also with School of Computer Science and Technology, Xinjiang Normal University, Urumqi 830054, China. (email: china@dlut.edu.cn, chenyu2017@mail.dlut.edu.cn, cy216@mail.dlut.edu.cn, zhaonan@dlut.edu.cn).

Y. Chen is with the School of Engineering, University of Warwick, Coventry CV4 7AL, U.K. (e-mail: Yunfei.Chen@warwick.ac.uk).

Z. Ding is with the School of Electrical and Electronic Engineering, the University of Manchester, Manchester, M13 9PL, U.K. (e-mail: zhiguo.ding@manchester.ac.uk).

X. Wang is with the Department of Electrical and Computer Engineering, University of Western Ontario, London, ON N6A 5B9, Canada (e-mail: xianbin.wang@uwo.ca).

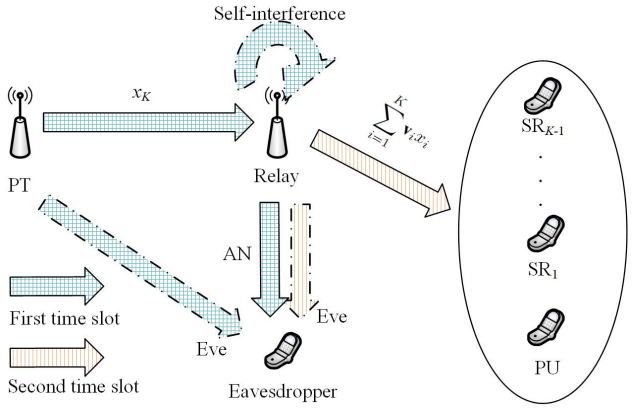

Fig. 1. System model of the secure primary transmission scheme assisted by a multi-antenna secondary full-duplex NOMA relay.

(PR) is longer than the distances between the relay and secondary receivers (SRs). According to the conventional NOMA, the transmit power allocated to the PR is the highest, which makes primary transmission easy to be eavesdropped. Thus, in the second time slot, we modify the decoding order of NOMA via beamforming optimization to guarantee the primary secure transmission.

- The beamforming optimization problem in the second time slot is non-convex and difficult to solve. Thus, the problem is first transformed into a convex one, and then solved by an iterative algorithm with reliable performance.

$Notation$: $\|\mathbf{v}\|$ represents the the Euclidean norm of vector $\mathbf{v}$. $\mathbf{A}^\dagger$ denotes the Hermitian transpose of matrix $\mathbf{A}$. $\bigtriangledown f(x)$ is the differential operator of $f(x)$. $Re(x)$ denotes the real operator of x. $\mathbb{C}^{M\times N}$ denotes the space of complex $M \times N$ matrices. $\mathbf{I}$ is the identity matrix. $\mathcal{CN}(\mathbf{a},\mathbf{A})$ denotes the complex Gaussian distribution with mean $\mathbf{a}$ and covariance $\mathbf{A}$. $\mathbb{E}[x]$ denotes the expectation of x.

II. System Model

Consider a cooperative CR network in Fig. 1, in which the PT with a single antenna transmits x_K to a single-antenna PR with the help of a N-antenna full-duplex relay. For the relay, it serves the PR and $K-1$ single-antenna SRs via NOMA. The unitary transmitted signal for the ith SR can be denoted by x_i, $i \in \mathcal{K} = \{1, 2, ..., K-1\}$. Assume that the primary signal x_K is overheard by a single-antenna eavesdropper. It is assumed that there is no direct link between PT and PR, due to the strong blockage and path loss between the two far-separated nodes. The channel strength from the relay to PR is weaker than those from the relay to SRs, which will lead to severe security threat to the primary transmission. Accordingly, assume that the distances from the relay to the PR and SRs satisfy[2]

$$d_K \geq d_1 \geq ... \geq d_{K-1}, \tag{1}$$

[2]In this paper, we assume that d_K is larger than $d_i, i \in \mathcal{K}$, which is the most challenging case. Nevertheless, the proposed scheme can be easily extended to the case where d_K is not the largest one.

where d_i is the distance from the relay to the PR ($i = K$) or SRs ($i \in \mathcal{K}$). Thus, the order of the channel-gain expectations can be expressed as[3]

$$\mathbb{E}\left[\|\mathbf{h}_K\|^2\right] \leq \mathbb{E}\left[\|\mathbf{h}_1\|^2\right] \leq ... \leq \mathbb{E}\left[\|\mathbf{h}_{K-1}\|^2\right], \tag{2}$$

where $\mathbf{h}_i = \sqrt{\beta d_i^{-\alpha}}\mathbf{g}_i \in \mathbb{C}^{1\times N}$, $i \in \mathcal{M} = \{1, 2, ..., K\}$, is the channel vector from the relay to PR ($i = K$) or SRs ($i \in \mathcal{K}$). α is the path-loss exponent, β is the path loss at unit distance, and $\mathbf{g}_i \sim \mathcal{CN}(\mathbf{0}, \mathbf{I})$ is the Rayleigh fading vector.

The transmit power of PT and the relay can be denoted by P_p and P_s, respectively.

In this correspondence, we propose a secure primary transmission scheme assisted by a secondary NOMA relay operating in two time slots. In the first time slot, PT sends x_K to the relay, and we use N_t antennas to generate AN at the relay while a single antenna to receive x_K, where $N_t + 1 = N$. In this way, the security of x_K can be guaranteed, with the self-interference at the relay eliminated. In the second time slot, the relay transmits the superimposed signals to both PR and SRs via NOMA, with the modified SIC order and beamforming optimization to guarantee the security of primary transmission.

III. Secure Primary Transmission via a Secondary Full-Duplex NOMA Relay

In this section, we describe the secure primary transmission scheme via the secondary NOMA relay with two time slots.

A. First Time Slot

In the first time slot, the PT sends x_K to the relay. The relay uses $N_t = N - 1$ antennas to generate the AN signal x_{AN} to disrupt eavesdropping simultaneously. Thus, the received signal at the single antenna of the relay can be expressed as

$$y_{ps} = \sqrt{P_p}h_{ps}x_K + \mathbf{h}_{ss}\mathbf{v}_{AN}x_{AN} + n_s, \tag{3}$$

where $h_{ps} = \sqrt{\beta d_{ps}^{-\alpha}}g_{ps}$ is the channel fading from PT to the relay. d_{ps} and g_{ps} are the corresponding distance and Rayleigh fading coefficient, respectively. n_s is the additive white Gaussian noise with mean zero and variance σ^2 at the relay. $\mathbf{v}_{AN} \in \mathbb{C}^{N_t\times 1}$ is the precoding vector for AN, with $\|\mathbf{v}_{AN}\|^2 = P_s$. $\mathbf{h}_{ss} \in \mathbb{C}^{1\times N_t}$ is the self-interference channel vector.

In order to eliminate the self-interference caused by the AN, the following condition

$$\mathbf{h}_{ss}\mathbf{v}_{AN} = 0 \tag{4}$$

should be satisfied. Since (4) and $\|\mathbf{v}_{AN}\|^2 = P_s$ are two different equations with N_t variables, we can derive that they can only be satisfied when $N_t \geq 2$.

Thus, we can obtain the achievable data rate at the relay as

$$R_{ps} = \log_2\left(1 + \frac{P_p|h_{ps}|^2}{\sigma^2}\right), \tag{5}$$

[3]In the proposed scheme, cooperation between the primary user and secondary users is needed to synchronize the transmission and exchange the channel state information (CSI) [13], because the secondary users can assist the primary user to perform long-distance secure transmission.

which should satisfy

$$R_{K1} = R_{ps} \geq r_K, \tag{6}$$

where r_K denotes the minimum rate to decode x_K. From (6), we can obtain

$$P_p \geq \frac{\sigma^2(2^{r_K}-1)}{|h_{ps}|^2}. \tag{7}$$

On the other hand, the received signal at the eavesdropper can be expressed as[4]

$$y_{e1} = \sqrt{P_p} h_{pe} x_K + \mathbf{h}_{se1}\mathbf{v}_{AN}x_{AN} + n_e, \tag{8}$$

where $h_{pe} = \sqrt{\beta d_{pe}^{-\alpha}} g_{pe}$ is the channel coefficient from PT to eavesdropper, in which d_{pe} and g_{pe} are the corresponding distance and Rayleigh fading coefficient, respectively. n_e is the additive white Gaussian noise with mean zero and variance σ^2 at the eavesdropper. $\mathbf{h}_{se1} = \sqrt{\beta d_{se}^{-\alpha}}\mathbf{g}_{se1} \in \mathbb{C}^{1\times N_t}$ is the channel vector from the relay to eavesdropper in the first time slot, in which d_{se} and $\mathbf{g}_{se1} \sim \mathcal{CN}(\mathbf{0}, \mathbf{I})$ are the corresponding distance and Rayleigh fading vector, respectively.

In this paper, we assume that the eavesdropper has the knowledge of the signal format of the legitimate users, which is possible as the eavesdropper could be a legitimate but malicious user in the same network. Hence, when the PT and the relay start to use the training period in the data packet to achieve synchronization, the eavesdropper can use the same training period for synchronization too. In this case, both x_K and x_{AN} can be synchronized to the eavesdropper. In the case when synchronization cannot be achieved by the eavesdropper, who is either not a legitimate user of the same network or does not want to implement complicated synchronization for eavesdropping, there will be a SINR penalty ρ, as the eavesdropper will start eavesdropping either too early or too late. Thus, the achievable signal-to-interference-plus-noise-ratio (SINR) at the eavesdropper can be obtained as

$$\mathrm{SINR}_{pe} = \frac{\rho_1 P_p |h_{pe}|^2}{|\mathbf{h}_{se1}\mathbf{v}_{AN}|^2 + \sigma^2}, \tag{9}$$

where ρ_1 is the SINR penalty caused by the asynchronization at the eavesdropper in the first time slot.

B. Second Time Slot

In the second time slot, the relay transmits the superimposed signal to the PR and SRs via NOMA, which is expressed as

$$\mathbf{x} = \sum_{j=1}^{K} \mathbf{v}_j x_j, \tag{10}$$

where $\mathbf{v}_j \in \mathbb{C}^{N\times 1}$ is the precoding vector of the PR or SR_j. Thus, the received signal at the PR or SR_i can be obtained as

$$y_i = \mathbf{h}_i \sum_{j=1}^{K} \mathbf{v}_j x_j + n_i, \tag{11}$$

where n_i is the additive white Gaussian noise with mean zero and variance σ^2 at the PR or SR_i. Due to the fact that the eavesdropping CSI is not available, we cannot optimize the secrecy rate directly. Instead, we can minimize the transmit power allocated to PR.

According to the principle of SIC, the conventional decoding order of NOMA at the PR and SRs can be expressed as

$$\begin{cases} |\mathbf{h}_1\mathbf{v}_{K-1}|^2 \leq ... \leq |\mathbf{h}_1\mathbf{v}_1|^2 \leq |\mathbf{h}_1\mathbf{v}_K|^2, \\ ... \\ |\mathbf{h}_{K-1}\mathbf{v}_{K-1}|^2 \leq ... \leq |\mathbf{h}_{K-1}\mathbf{v}_1|^2 \leq |\mathbf{h}_{K-1}\mathbf{v}_K|^2, \\ |\mathbf{h}_K\mathbf{v}_{K-1}|^2 \leq ... \leq |\mathbf{h}_K\mathbf{v}_1|^2 \leq |\mathbf{h}_K\mathbf{v}_K|^2, \end{cases} \tag{12}$$

from which we can observe that the power allocated to the PR is much higher, which will cause potential eavesdropping towards the PR. Thus, we should minimize the power allocated to the PR, through which the primary signal will be hidden in the strong secondary signals. Thus, the SIC order of NOMA at the PR and SRs can be modified as

$$\begin{cases} |\mathbf{h}_1\mathbf{v}_K|^2 \leq |\mathbf{h}_1\mathbf{v}_{K-1}|^2 \leq ... \leq |\mathbf{h}_1\mathbf{v}_1|^2, \\ ... \\ |\mathbf{h}_{K-1}\mathbf{v}_K|^2 \leq |\mathbf{h}_{K-1}\mathbf{v}_{K-1}|^2 \leq ... \leq |\mathbf{h}_{K-1}\mathbf{v}_1|^2, \\ |\mathbf{h}_K\mathbf{v}_K|^2 \leq |\mathbf{h}_K\mathbf{v}_{K-1}|^2 \leq ... \leq |\mathbf{h}_K\mathbf{v}_1|^2. \end{cases} \tag{13}$$

Using SIC according to (13), the received SINR at the PR or SRs to decode x_j from SR_j can be expressed as

$$\mathrm{SINR}_{ij} = \frac{|\mathbf{h}_i\mathbf{v}_j|^2}{\sum_{m=j+1}^{K} |\mathbf{h}_i\mathbf{v}_m|^2 + \sigma^2}, i \in \mathcal{M}, j \in \mathcal{K}, i \geq j. \tag{14}$$

Thus, the transmission rate of SR_j can be expressed as

$$R_j = \log_2\left(1 + \min_{i=j}^{K} \mathrm{SINR}_{ij}\right), j \in \mathcal{K}, \tag{15}$$

which should satisfy

$$R_j \geq r_j, j \in \mathcal{K}, \tag{16}$$

where r_j denotes the rate threshold of x_j. We can also obtain the SINR at PR for the decoding of x_K in the second time slot as

$$\mathrm{SINR}_{KK} = \frac{|\mathbf{h}_K\mathbf{v}_K|^2}{\sigma^2}, \tag{17}$$

and the rate for x_K in the second slot can be obtained as

$$R_{K2} = \log_2(1 + \mathrm{SINR}_{KK}). \tag{18}$$

According to (6) and (18), the overall transmission rate of x_K over the two time slots can be expressed as

$$R_K = \min\{R_{K1}, R_{K2}\} \geq r_K. \tag{19}$$

For the eavesdropper, it receives the superimposed signal containing both x_K and x_i, $i \in \mathcal{K}$, which can be expressed as

$$y_{e2} = \sum_{i=1}^{K} \mathbf{h}_{se2}\mathbf{v}_i x_i + n_0. \tag{20}$$

$\mathbf{h}_{se2} = \sqrt{\beta d_{se}^{-\alpha}}\mathbf{g}_{se2} \in \mathbb{C}^{1\times N}$ is the channel vector from the relay to eavesdropper in the second time slot, in which $\mathbf{g}_{se2} \sim \mathcal{CN}(\mathbf{0}, \mathbf{I})$ is the Rayleigh fading vector. The received SINR at

[4]In the proposed scheme, we do not need the eavesdropping CSI, instead, we use it only for security analysis.

the eavesdropper towards x_K can be expressed as

$$\mathrm{SINR}_{se} = \frac{\rho_2 |\mathbf{h}_{se2}\mathbf{v}_K|^2}{\sum_{i=1}^{K-1} |\mathbf{h}_{se2}\mathbf{v}_i|^2 + \sigma^2}, \tag{21}$$

where ρ_2 is the SINR penalty caused by the asynchronization at the eavesdropper in the second time slot.

Based on (9) and (21), we can obtain the eavesdropping rate by using the maximal-ratio combining (MRC) method as

$$R_e = \log_2(1 + \mathrm{SINR}_{pe} + \mathrm{SINR}_{se}), \tag{22}$$

Thus, we can obtain the primary secrecy rate as

$$R_s = [R_K - R_e]^+, \tag{23}$$

where $[x]^+ \triangleq \max(x, 0)$.

To further improve the security performance of primary transmission in the second time slot, we minimize the primary transmit power with the rate threshold of all the users guaranteed as

$$\begin{aligned} &\min_{\mathbf{v}_i} \ \|\mathbf{v}_K\|^2 \\ &s.t. \ \sum_{i=1}^{K} \|\mathbf{v}_i\|^2 = P_s, \\ &\quad (13), \ (16), \ \text{and} \ (19), \end{aligned} \tag{24}$$

which is non-convex and difficult to solve.

IV. Low-Conplexity Solution to (24)

To make (24) convex, a lemma in [14] is first reviewed.

Lemma 1: If $f(x)$ is convex and differentiable, then

$$f(x) \geq f(x^{(m)}) + \bigtriangledown f(x^{(m)})^\dagger (x - x^{(m)}), \tag{25}$$

where $f(x^{(m)}) + \bigtriangledown f(x^{(m)})^\dagger (x - x^{(m)})$ is the first-order Taylor expansion around $x^{(m)}$. When $x = x^{(m)}$, the equality holds.■

Thus, we can transform (24) into a convex one using Lemma 1. For convenience, we define

$$L_{i,j}(\mathbf{v}_j) = |\mathbf{h}_i \mathbf{v}_j|^2, \tag{26}$$

$$F_{i,j}(\mathbf{v}_j) = \frac{|\mathbf{h}_i \mathbf{v}_j|^2}{2^{r_j} - 1}. \tag{27}$$

According to [14], the first-order Taylor approximations of (26) and (27) over a certain $\mathbf{v}'_j$ can be obtained as

$$\mathcal{L}_{i,j}(\mathbf{v}_j, \mathbf{v}'_j) = 2Re(\mathbf{v}'^\dagger_j h_i^\dagger h_i \mathbf{v}_j) - Re(\mathbf{v}'^\dagger_j h_i^\dagger h_i \mathbf{v}'_j), \tag{28}$$

$$\mathcal{F}_{i,j}(\mathbf{v}_j, \mathbf{v}'_j) = \frac{\mathcal{L}_{i,j}(\mathbf{v}_j, \mathbf{v}'_j)}{2^{r_{ij}} - 1}. \tag{29}$$

In addition, the condition (13) is equivalent to

$$\begin{cases} |\mathbf{h}_i \mathbf{v}_K|^2 \leq |\mathbf{h}_i \mathbf{v}_{K-1}|^2, \\ |\mathbf{h}_i \mathbf{v}_{K-1}|^2 \leq |\mathbf{h}_i \mathbf{v}_{K-2}|^2, \\ \cdots\cdots, \\ |\mathbf{h}_i \mathbf{v}_2|^2 \leq |\mathbf{h}_i \mathbf{v}_1|^2, \end{cases} \tag{30}$$

which can be approximated as

$$\begin{cases} |\mathbf{h}_i \mathbf{v}_K|^2 \leq \mathcal{L}_{i,K-1}\left(\mathbf{v}_{K-1}, \mathbf{v}'_{K-1}\right), \\ |\mathbf{h}_i \mathbf{v}_{K-1}|^2 \leq \mathcal{L}_{i,K-2}\left(\mathbf{v}_{K-2}, \mathbf{v}'_{K-2}\right), \\ \cdots\cdots, \\ |\mathbf{h}_i \mathbf{v}_2|^2 \leq \mathcal{L}_{i,1}\left(\mathbf{v}_1, \mathbf{v}'_1\right), \end{cases} \tag{31}$$

where $i \in \mathcal{M}$. The condition (16) can be expressed as

$$\mathrm{SINR}_{ij} \geq 2^{r_j} - 1, \quad i \in \mathcal{M}, j \in \mathcal{K}, i \geq j, \tag{32}$$

which can be approximated as

$$\sum_{m=j+1}^{K} |\mathbf{h}_i \mathbf{v}_m|^2 + \sigma^2 \leq \mathcal{F}_{i,j}\left(\mathbf{v}_j, \mathbf{v}'_j\right), \tag{33}$$

where $i \in \mathcal{M}, j \in \mathcal{K}, i \geq j$. The condition (19) can be expressed as

$$\mathrm{SINR}_{KK} \geq 2^{r_K} - 1, \tag{34}$$

and (7). The condition (34) can be approximated to

$$\sigma^2 \leq \mathcal{F}_{K,K}\left(\mathbf{v}_K, \mathbf{v}'_K\right), \tag{35}$$

Thus, the problem (24) can be approximately converted to

$$\begin{aligned} &\min_{\mathbf{v}_i} \ \|\mathbf{v}_K\|^2 \\ &s.t. \ \sum_{i=1}^{K} \|\mathbf{v}_i\|^2 = P_s, \\ &\quad (31), \ (33) \ \text{and} \ (35), \end{aligned} \tag{36}$$

which is convex and can be easily solved. Thus, Algorithm 1 is proposed to calculate the suboptimal solutions to (24).

Algorithm 1 Iterative Algorithm for Problem (24)

1: Initialization: Randomly set the initial values $\mathbf{v}'_j$, $j \in \mathcal{M}$.
2: **Repeat**
3: Solve the problem (36) and get the result $\mathbf{v}^*_j$.
4: Let $\mathbf{v}'_j = \mathbf{v}^*_j$.
5: **Until** $\mathbf{v}^*_j$ is convergent.
6: Output $\mathbf{v}^*_j$.

In addition, the feasibility of Algorithm 1 for (24) can be proved in Proposition 1.

Proposition 1: The feasible set of solutions to (36) is within that to the original (24).

Proof: Define

$$f(\mathbf{v}_m) = \sum_{m=j+1}^{K} |\mathbf{h}_i \mathbf{v}_m|^2 + \sigma^2. \tag{37}$$

Thus, the condition (16) can be expressed as

$$f(\mathbf{v}_m) - F_{i,j}(\mathbf{v}_j) \leq 0. \tag{38}$$

According to Lemma 1 and (33), we can obtain

$$f(\mathbf{v}_m) - F_{i,j}(\mathbf{v}_j) \leq f(\mathbf{v}_m) - \mathcal{F}_{i,j}(\mathbf{v}_j, \mathbf{v}'_j) \leq 0. \tag{39}$$

The following expression can be obtained in the nth iteration.

$$f\left(\mathbf{v}_m^{(n)}\right) - F_{i,j}\left(\mathbf{v}_j^{(n)}\right) \leq f\left(\mathbf{v}_m^{(n)}\right) - \mathcal{F}_{i,j}\left(\mathbf{v}_j^{(n)}, \mathbf{v}_j^{(n-1)}\right) \leq 0. \tag{40}$$

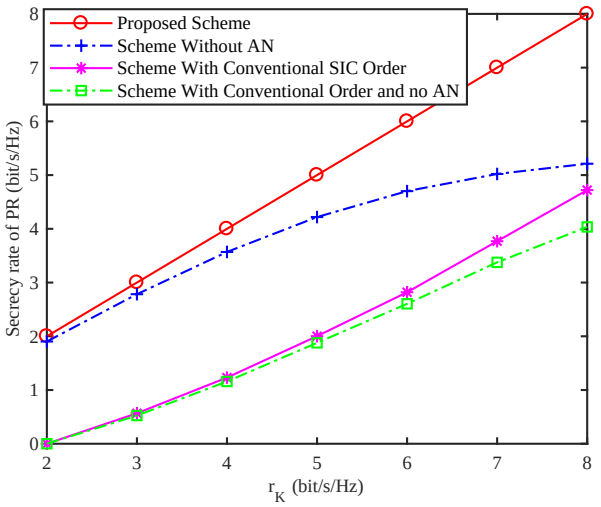

Fig. 2. Comparison of secrecy rate for the proposed scheme, the scheme without AN, the scheme conventional SIC order and the scheme with conventional SIC order and no AN, for different values of r_K. ρ_1=ρ_2=1.

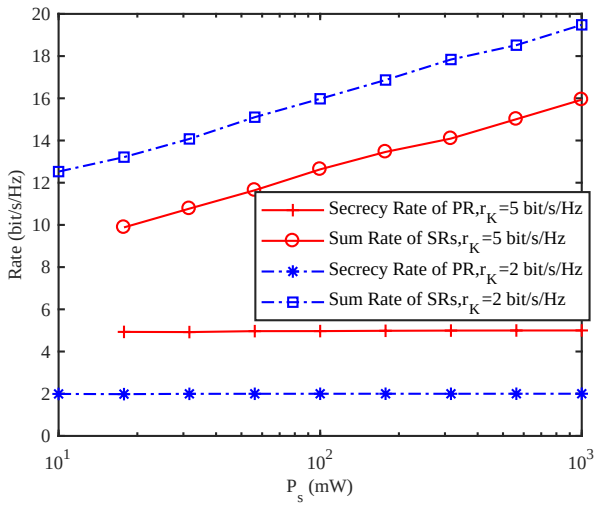

Fig. 3. Comparison of the primary secrecy rate and secondary sum rate of the proposed scheme for different values of P_s and r_K. ρ_1=ρ_2=1.

When $\mathbf{v}_j^{(n)} = \mathbf{v}_j^{(n-1)}$, the equality in (40) holds. According to [15], Algorithm 1 is convergent. Thus, $\mathbf{v}_j^{(n)} = \mathbf{v}_j^{(n-1)}$ can be achieved. Similar conclusions can be obtained by analyzing other conditions, and we can conclude that the feasible set of solutions to (34) is within that to the original (22). ■

When the number of users becomes larger, the limited antennas cannot satisfy the requirement. In this case, we can utilize the idea of opportunistic communication to select some proper users to perform the NOMA transmission in each time slot [16], and all the secondary users will have the chance to access the network over several slots.

V. Simulation Results

In the simulation, we consider one PR and three SRs, i.e., $K = 4$. We set N=3. d_1=25 m, d_2=20 m, d_3=15 m and d_4=30 m. d_{ps}=20 m, d_{pe}=30 m and d_{se}=30 m. $r_1 = r_2 = r_3 = 2$ bit/s/Hz. $\sigma^2 = -110$ dBm. $\alpha = 2.6$ and $\beta = 10^{-4}$.

First, the secrecy rate of PR is compared in Fig. 2 for different values of r_K for the proposed scheme, the scheme without AN, the scheme with conventional SIC order and the scheme with conventional SIC order and no AN. ρ_1=ρ_2=1. The conventional SIC order has been defined as (12). Specifically, the scheme without AN is actually the scheme exploiting a half-duplex relay. We use P_s=50 mW for all these schemes. From the results, we can see that the secrecy rate of PR increases with r_K in all these schemes. Furthermore, the secrecy rate of the proposed scheme is much higher than those of the other schemes, which reflects the effectiveness of the proposed scheme in improving the primary security performance.

Then, the secrecy rate of PR and the sum rate of SRs in the proposed scheme are compared in Fig. 3 with different values of P_s and r_K. ρ_1=ρ_2=1. From the results, we can see that the secrecy rate of PR can be guaranteed, which is close to r_K, while the sum rate of SRs increase with P_s. Furthermore, the secrecy rate of PR increases and the sum rate of SRs decreases, when r_K increases, which indicates that more resources will be allocated to PR to improve its secrecy rate.

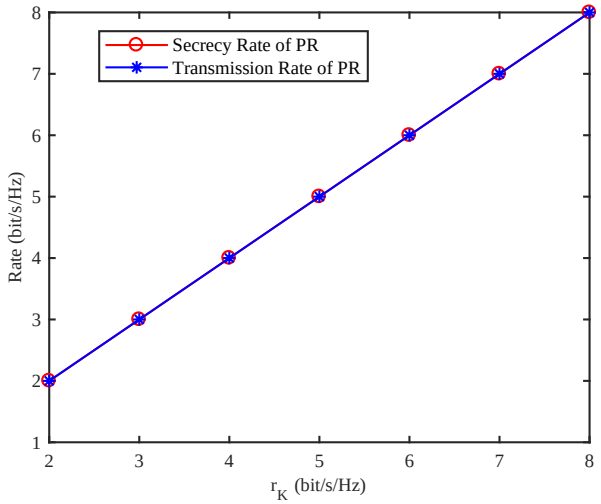

Fig. 4. Comparison of secrecy rate and transmission rate of PR for different values of r_K. P_s=50 mW. ρ_1=ρ_2=1.

Furthermore, we compare the secrecy rate and transmission rate of PR for different values of r_K in Fig. 4. ρ_1=ρ_2=1. P_s=50 mW. From the results, we can see that the secrecy rate of PR is close to its transmission rate, which means that the eavesdropping rate towards the PR is close to 0. Thus, zero eavesdropping rate indicates that the transmit power of PR can be effectively minimized in (24) to prevent eavesdropping.

Last, the eavesdropping rate towards the primary user for different values of ρ_1, ρ_2 and r_K in the proposed scheme is compared in Fig. 5. From the results, we can see that the eavesdropping rate increases with r_K, this is because more transmit power should be allocated to the primary user to satisfy its rate requirement. In addition, we can also observe that the eavesdropping rate increases with ρ_1 and ρ_2, due to the fact that the asynchronization at the eavesdropper will degrade the eavesdropping performance.

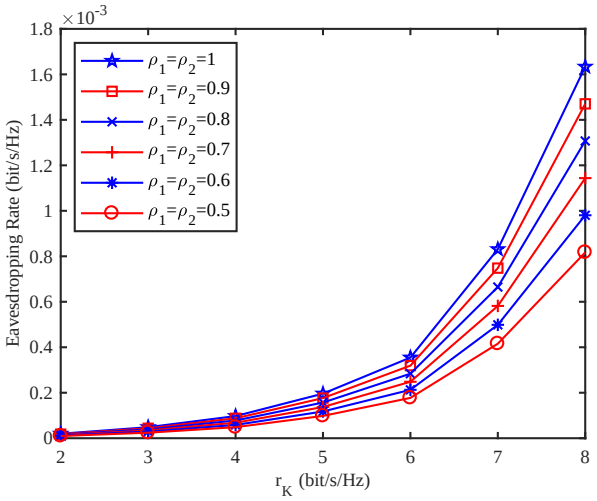

Fig. 5. Comparison of the eavesdropping rate towards the primary user for different values of ρ_1, ρ_2 and r_K in the proposed scheme.

VI. Conclusions and Future Work

In this correspondence, we have proposed a secure primary transmission scheme assisted by a secondary NOMA relay. In the first time slot, the secure information is transmitted from PT to the relay, while AN is generated by the relay to disrupt the eavesdropping without affecting the legitimate transmission. In the second time slot, the information for the PR and SRs are transmitted from the relay to PR and SRs via NOMA, and the security of PR is guaranteed through the modified SIC order and joint beamforming optimization. Furthermore, the beamforming optimization problem is converted to convex and solved by an iterative algorithm. Finally, simulation results are presented to show the effectiveness of the proposed scheme. In our future work, we will still focus on other methods to solve (24) with solutions close to the optimal ones.

Acknowledgment

We thank the editor and reviewers for their detailed reviews and constructive comments, which have greatly improved the quality of this paper.

References

[1] Z. Ding, X. Lei, G. K. Karagiannidis, R. Schober, J. Yuan, and V. Bhargava, "A survey on non-orthogonal multiple access for 5G networks: Research challenges and future trends," *IEEE J. Sel. Areas Commun.*, vol. 35, no. 10, pp. 2181–2195, Oct. 2017.

[2] N. Zhao, X. Pang, Z. Li, Y. Chen, F. Li, Z. Ding, and M. Alouini, "Joint trajectory and precoding optimization for UAV-assisted NOMA networks," *IEEE Trans. Commun.*, vol. 67, no. 5, pp. 3723–3735, May 2019.

[3] Y. Wu, L. P. Qian, H. Mao, X. Yang, H. Zhou, and X. Shen, "Optimal power allocation and scheduling for non-orthogonal multiple access relay-assisted networks," *IEEE Trans. Mobile Comput.*, vol. 17, no. 11, pp. 2591–2606, Nov. 2018.

[4] Q. Liu, T. Lv, and Z. Lin, "Energy-efficient transmission design in cooperative relaying systems using NOMA," *IEEE Commun. Lett.*, vol. 22, no. 3, pp. 594–597, Mar. 2018.

[5] L. Lv, Q. Ni, Z. Ding, and J. Chen, "Application of non-orthogonal multiple access in cooperative spectrum-sharing networks over nakagami-m fading channels," *IEEE Trans. Veh. Technol.*, vol. 66, no. 6, pp. 5506–5511, Jun. 2017.

[6] B. Chen, Y. Chen, Y. Chen, Y. Cao, N. Zhao, and Z. Ding, "A novel spectrum sharing scheme assisted by secondary NOMA relay," *IEEE Wireless Commun. Lett.*, vol. 7, no. 5, pp. 732–735, Oct. 2018.

[7] N. Nandan, S. Majhi, and H.-C. Wu, "Maximizing secrecy capacity of underlay MIMO-CRN through bi-directional zero-forcing beamforming," *IEEE Trans. Wireless Commun.*, vol. 17, no. 8, pp. 5327–5337, Aug. 2018.

[8] N. Zhao, F. R. Yu, M. Li, Q. Yan, and V. C. M. Leung, "Physical layer security issues in interference-alignment-based wireless networks," *IEEE Commun. Mag.*, vol. 54, no. 8, pp. 162–168, Aug. 2016.

[9] Y. Liu, Z. Qin, M. Elkashlan, Y. Gao, and L. Hanzo, "Enhancing the physical layer security of non-orthogonal multiple access in large-scale networks," *IEEE Trans. Wireless Commun.*, vol. 16, no. 3, pp. 1656–1672, Mar. 2017.

[10] L. Lv, Z. Ding, Q. Ni, and J. Chen, "Secure MISO-NOMA transmission with artificial noise," *IEEE Trans. Veh. Technol.*, vol. 67, no. 7, pp. 6700–6705, Mar. 2018.

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

[12] B. Zheng, M. Wen, C. Wang, X. Wang, F. Chen, J. Tang, and F. Ji, "Secure NOMA based two-way relay networks using artificial noise and full duplex," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 7, pp. 1426–1440, Jul. 2018.

[13] J. M. Peha, "Sharing spectrum through spectrum policy reform and cognitive radio," *Proc. IEEE*, vol. 97, pp. 708–719, Apr. 2009.

[14] D. R. Hunter and K. Lange, "A tutorial on MM algorithms," *Amer. Statist.*, vol. 58, no. 1, pp. 30–37, Feb. 2004.

[15] B. K. Sriperumbudur and G. R. G. Lanckriet, "On the convergence of the concave-convex procedure," in *Proc. International Conference on Neural Information Processing Systems*, pp. 1759–1767, 2009.

[16] N. Zhao, F. R. Yu, and V. C. M. Leung, "Opportunistic communications in interference alignment networks with wireless power transfer," *IEEE Wireless Commun.*, vol. 22, no. 1, pp. 88–95, Feb. 2015.