Security Enhancement Using a Novel Two-Slot Cooperative NOMA Scheme

Abstract—**In this letter, we propose a novel cooperative non-orthogonal multiple access (NOMA) scheme to guarantee the secure transmission of a specific user via two time slots. During the first time slot, the base station (BS) transmits the superimposed signal to the first user and the relay via NOMA. Meanwhile, the signal for the first user is also decoded at the second user from the superimposed signal due to its high transmit power. In the second time slot, the relay forwards the signal to the second user while the BS retransmits the signal for the first user as interference to disrupt the eavesdropping. Due to the fact that the second user has obtained the signal for the first user in the first slot, the interference can be eliminated at the second user. To measure the performance of the proposed cooperative NOMA scheme, the outage probability for the first user and the secrecy outage probability for the second user are analyzed. Simulation results are presented to show the effectiveness of the proposed scheme.**

Index Terms—**Artificial noise, non-orthogonal multiple access, physical layer security, relay, secrecy outage probability.**

I. Introduction

Non-orthogonal multiple access (NOMA) can improve spectrum efficiency, reduce latency and support massive connectivity, which has attracted great attention [1], [2]. In NOMA networks, the receivers are allocated with different transmit power depending on their channel conditions, and the received signals are decoded at each receiver via successive interference cancellation (SIC).

Recently, cooperative NOMA has been widely studied to extend the coverage for NOMA [3]–[7]. In [3], the cooperative NOMA broadcasting/multicasting scheme was proposed by Liu *et al.* to achieve low-latency and high-reliability for V2X in 5G networks. A two-stage secondary NOMA relay assisted spectrum sharing scheme was proposed by Chen *et al.* in [4]. In [5], Liu *et al.* proposed an optimal power allocation scheme to maximize the global energy efficiency in a cooperative NOMA system. The cooperative NOMA system was proposed by Liu *et al.* to provide wireless transmission for two far users with decode-and-forward relaying in [6]. In [7], some excellent work was done by Jiao *et al.* to analyze the performance of cooperative NOMA networks over Rician fading channels.

Although NOMA plays an important role in improving spectrum efficiency, communication security in NOMA networks remains challenging [8]–[15]. In [9], Feng *et al.* developed a novel beamforming design with the aid of artificial noise to ensure the security of NOMA system. The secure cooperative NOMA scheme was proposed by Lv *et al.* in [10], in which jamming is leveraged to disrupt the untrusted relay via beamforming and adapting the rate. In [11], Chen *et al.* proposed a secure primary transmission scheme, which is guaranteed by a secondary full-duplex NOMA relay. The secrecy outage probability was derived by Lei *et al.* in [12] for NOMA networks with max-min transmit antenna selection. In [13], Cao *et al.* considered the security of a two-user cooperative NOMA system, in which the secrecy outage probability of the two users was analyzed. Tradeoff was made between the reliability and security by Li *et al.* of cooperative NOMA in cognitive radio networks [14].

Motivated by the above works, we propose a two-slot cooperative NOMA scheme in this paper. First, the BS sends superimposed signals to the first user (U1) and the relay via NOMA. U2 decodes the high-power signal of U1 and stores it locally. Then, the relay performs transmission for U2, while the BS transmits the signal of U1 to disrupt the eavesdropping. Since U2 has obtained the signal for U1, the interference can be eliminated at U2. To further analyze the performance of U1 and U2, the outage probability (OP) of U1 and the secrecy outage probability (SOP) of U2 are derived.

II. System Model

Consider a cooperative NOMA network as shown in Fig. 1, with a BS, a relay, two users of U1 and U2, and an eavesdropper. Assume that U2 requires secure transmission[1]. Each node is equipped with a single antenna and works in a

Manuscript received August 15, 2019; revised November 07, 2019 and December 25, 2019; accepted January 07, 2020. The work of B. Chen was supported by the National Natural Science Foundation of China (NSFC) under Grant 61771089, 61871065 and 61961040. The associate editor coordinating the review of this paper and approving it for publication was L. Dai.

[1] This is reasonable when U1 is a secondary user and U2 is a primary user in a cognitive radio network. The secondary user U1 can only access the licensed spectrum if it can help U1 to achieve secure transmission.

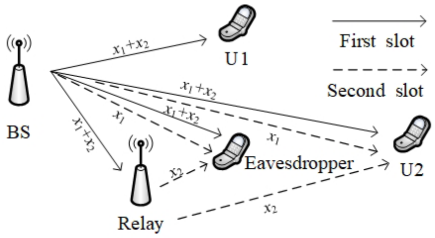

Fig. 1. Demonstration of the two-slot cooperative NOMA scheme.

half-duplex mode. The channels follow Rayleigh fading. The transmit power of BS and relay is denoted as P_B and P_R, respectively. Denote the transmitted signals for U1 and U2 as x_1 and x_2, respectively, and the eavesdropper only intends to intercept x_2. The distances from the BS to the relay, U1, and U2 can be denoted as d_{BR}, d_{B1} and d_{B2}, respectively, satisfying $d_{BR} < d_{B1} < d_{B2}$. Thus, the average channel gain can be ordered as $\mathbb{E}\left[|h_{BR}|^2\right] > \mathbb{E}\left[|h_{B1}|^2\right] > \mathbb{E}\left[|h_{B2}|^2\right]$, where $h_{BR} = \sqrt{\beta d_{BR}^{-\alpha}} g_{BR}$, $h_{B1} = \sqrt{\beta d_{B1}^{-\alpha}} g_{B1}$ and $h_{B2} = \sqrt{\beta d_{B2}^{-\alpha}} g_{B2}$ are the channel gains from the BS to the relay, U1, and U2, respectively. g_{BR}, g_{B1} and g_{B2} are the corresponding Rayleigh fading coefficients, α is the path-loss exponent, and β is the path loss at the reference distance 1 m.

Due to the weak channel strength from the BS to U2, the security of U2 is threatened[2]. To guarantee the security of U2, we propose a cooperative NOMA scheme with two time slots, which will be demonstrated in the next section.

III. Cooperative NOMA Scheme

In this section, we propose a novel cooperative NOMA scheme with two time slots as follows.

A. First Time Slot

In the first time slot, the superimposed signals of x_1 and x_2 are sent to the relay and U1 via NOMA. U1 decodes x_1, and relay decodes x_1 and x_2 with SIC. Perfect SIC is considered because the interference cancellation is performed only once. In addition, U2 decodes x_1 and stores it locally. The received signal at U1 can be expressed as

$$y_{B1} = \sqrt{P_1} h_{B1} x_1 + \sqrt{P_2} h_{B1} x_2 + n_1, \tag{1}$$

where $P_1 = \alpha_1 P_B$ and $P_2 = \alpha_2 P_B$ are the transmit power allocated to x_1 and x_2. α_1 and α_2 are the power allocation coefficients for x_1 and x_2, satisfying $\alpha_1 > \alpha_2$ and $\alpha_1 + \alpha_2 = 1$. n_1 is the additive white Gaussian noise (AWGN) with zero mean and variance σ^2 at U1. Thus, the received SINR for x_1 at U1 can be expressed as

$$\mathrm{SINR}_{11} = \frac{P_1 |h_{B1}|^2}{P_2 |h_{B1}|^2 + \sigma^2}. \tag{2}$$

The received signal at the relay can be obtained as

$$y_{BR} = \sqrt{P_1} h_{BR} x_1 + \sqrt{P_2} h_{BR} x_2 + n_r, \tag{3}$$

where n_r is the AWGN with zero mean and variance σ^2 at the relay. Thus, the received SINR at the relay to decode x_1 and x_2 can be written as

$$\mathrm{SINR}_{R1} = \frac{P_1 |h_{BR}|^2}{P_2 |h_{BR}|^2 + \sigma^2}, \tag{4}$$

$$\mathrm{SINR}_{R2} = \frac{P_2 |h_{BR}|^2}{\sigma^2}. \tag{5}$$

In the first time slot, U2 will try to decode x_1 and store it locally, and the received signal at U2 can be obtained as

$$y_{B2} = \sqrt{P_1} h_{B2} x_1 + \sqrt{P_2} h_{B2} x_2 + n_2, \tag{6}$$

where n_2 is the AWGN with zero mean and variance σ^2 at U2. Thus, the received SINR at U2 to decode x_1 and x_2 can be denoted as

$$\mathrm{SINR}_{21} = \frac{P_1 |h_{B2}|^2}{P_2 |h_{B2}|^2 + \sigma^2}, \tag{7}$$

$$\mathrm{SINR}_{22} = \frac{P_2 |h_{B2}|^2}{\sigma^2}. \tag{8}$$

SINR_{22} in (8) is very small and can be ignored because the distance from BS to U2 is the longest.

The received signal at the eavesdropper can be obtained as

$$y_{BE} = \sqrt{P_1} h_{BE} x_1 + \sqrt{P_2} h_{BE} x_2 + n_e, \tag{9}$$

where n_e is the AWGN with zero mean and variance σ^2 at the eavesdropper. The received SINR at the eavesdropper to decode x_2 in the first time slot can be denoted as

$$\mathrm{SINR}_{E2}^{[1]} = \frac{P_2 |h_{BE}|^2}{P_1 |h_{BE}|^2 + \sigma^2}. \tag{10}$$

B. Second Time Slot

In the second time slot, the relay transmits x_2 to U2, while the BS transmits x_1 to disrupt the eavesdropping. Thus, the eavesdropper receives x_2 from the relay and the interference of x_1 from the BS as

$$y_E^{[2]} = \sqrt{P_B} h_{BE} x_1 + \sqrt{P_R} h_{RE} x_2 + n_e. \tag{11}$$

The received SINR at the eavesdropper to decode x_2 in the second time slot can be obtained as

$$\mathrm{SINR}_{E2}^{[2]} = \frac{P_R |h_{RE}|^2}{P_B |h_{BE}|^2 + \sigma^2}. \tag{12}$$

Using (10) and (12), we can obtain the overall eavesdropping rate of the two slots towards x_2 by using the maximal-ratio combining (MRC) as[3]

$$R_E = \frac{1}{2} \log_2 \left(1 + \mathrm{SINR}_{E2}^{[1]} + \mathrm{SINR}_{E2}^{[2]} \right). \tag{13}$$

On the other hand, if U2 can successfully decode x_1 in the first time slot, the interference of x_1 in the second time slot can be perfectly eliminated at U2, and the received SINR at U2 for x_2 can be denoted as

$$\mathrm{SINR}_{221} = \frac{P_R |h_{R2}|^2}{\sigma^2}. \tag{14}$$

[2] If U2 is closer to the BS than U1, the security of U2 can be easily satisfied via NOMA due to its lower transmit power.

[3] The full CSI is not used to perform the proposed scheme, and it is only used in the performance analysis.

Based on (5) and (14), the transmission rate of U2 can be expressed as

$$R_{21} = \frac{1}{2}\log_2\left(1+\min[\mathrm{SINR}_{R2}, \mathrm{SINR}_{221}]\right). \tag{15}$$

Thus, the secrecy rate of x_2 can be obtained as

$$R_{s1} = [R_{21} - R_E]^+, \tag{16}$$

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

If U2 fails to decode x_1 in the first time slot, the received SINR at U2 for x_2 can be denoted as

$$\mathrm{SINR}_{222} = \frac{P_R|h_{R2}|^2}{P_B|h_{B2}|^2 + \sigma^2}, \tag{17}$$

and the transmission rate of U2 can be expressed as

$$R_{22} = \frac{1}{2}\log_2\left(1+\min[\mathrm{SINR}_{R2}, \mathrm{SINR}_{222}]\right). \tag{18}$$

Thus, the secrecy rate of x_2 can be obtained as

$$R_{s2} = [R_{22} - R_E]^+. \tag{19}$$

IV. Performance Analysis

In this section, we will analyze the OP for U1 and the SOP for U2.

A. Outage Probability for U1

According to (2) and (4), the transmission rate of U1 can be denoted as

$$R_1 = \frac{1}{2}\log_2\left(1+\min[\mathrm{SINR}_{R1}, \mathrm{SINR}_{11}]\right). \tag{20}$$

Then, the OP of U1 can be expressed as

$$\mathrm{Pr}_1 = \Pr(R_1 < r_1), \tag{21}$$

where r_1 is the rate threshold of x_1. To simplify the expression, we define $S = |h_{BR}|^2, K = |h_{B1}|^2$ and $a = \frac{\gamma_1\sigma^2}{P_1 - \gamma_1 P_2}$, where S and K follow the exponential distribution with parameters $\lambda_s = 1/(\beta d_{BR}^{-\alpha})$ and $\lambda_k = 1/(\beta d_{B1}^{-\alpha})$, respectively. Hence, the cumulative density function (CDF) of S and K can be calculated as $F_S(s) = 1 - e^{-\lambda_s s}$ and $F_K(k) = 1 - e^{-\lambda_k k}$, respectively. The probability density function (PDF) of S and K can be calculated as $f_S(s) = \lambda_s e^{-\lambda_s s}$ and $f_K(k) = \lambda_k e^{-\lambda_k k}$, respectively. Define $\gamma_1 = 2^{2r_1} - 1$ as the SINR threshold of x_1. The OP for U1 can be obtained in Proposition 1.

Proposition 1: When $P_1 - \gamma_1 P_2 \leq 0$, $\mathrm{Pr}_1 = 1$. Otherwise, the OP for U1 can be expressed as

$$\mathrm{Pr}_1 = 1 - e^{-(\lambda_s+\lambda_k)a}. \tag{22}$$

Proof: (21) is equivalent to

$$\mathrm{Pr}_1 = \Pr(\min[\mathrm{SINR}_{R1}, \mathrm{SINR}_{11}] < \gamma_1). \tag{23}$$

When $P_1 - \gamma_1 P_2 \leq 0$, we can obtain $(P_1 - \gamma_1 P_2)S < \gamma_1\sigma^2$ and $(P_1 - \gamma_1 P_2)K < \gamma_1\sigma^2$, that is $\mathrm{SINR}_{R1} < \gamma_1$ and $\mathrm{SINR}_{11} < \gamma_1$. Thus, $\mathrm{Pr}_1 = \Pr(\min[\mathrm{SINR}_{R1}, \mathrm{SINR}_{11}] < \gamma_1) = 1$.

When $P_1 - \gamma_1 P_2 > 0$, (23) can be simplified as $\mathrm{Pr}_1 = \Pr(S \leq a, S \leq K) + \Pr(K \leq a, K \leq S)$.

Due to the independence between S and K, $\Pr(S \leq a, S \leq K) = \int_0^a f_S(s)ds \int_s^{+\infty} f_K(k)dk = \int_0^a f_S(s)(1 - F_K(s)) = \int_0^a \lambda_s e^{-(\lambda_s+\lambda_k)s}ds = \frac{\lambda_s}{\lambda_s+\lambda_k}(1 - e^{-(\lambda_s+\lambda_k)a})$.

Similarly, we can get $\Pr(K \leq a, K \leq S) = \frac{\lambda_k}{\lambda_s+\lambda_k}(1 - e^{-(\lambda_s+\lambda_k)a})$. Thus, we have $\mathrm{Pr}_1 = \Pr(S \leq a, S \leq K) + \Pr(K \leq a, K \leq S) = 1 - e^{-(\lambda_s+\lambda_k)a}$. ■

B. Secrecy Outage Probability for U2

The SOP of U2 can be expressed as

$$\begin{aligned} \mathrm{Pr}_2 = &\underbrace{\Pr\left(\mathrm{SINR}_{R1} < \gamma_1\right)}_{I_1} \\ &+ \underbrace{\Pr\left(\mathrm{SINR}_{R1} > \gamma_1, R_{s1} < r_2\right)\Pr\left(\mathrm{SINR}_{21} > \gamma_1\right)}_{I_2} \\ &+ \underbrace{\Pr\left(\mathrm{SINR}_{R1} > \gamma_1, \mathrm{SINR}_{21} < \gamma_1, R_{s2} < r_2\right)}_{I_3}, \end{aligned} \tag{24}$$

where r_2 is the rate threshold of x_2.

To simplify the expression, we define $V = \mathrm{SINR}_{221}, L = |h_{R2}|^2, J = |h_{B2}|^2, T_1 = \mathrm{SINR}_{E2}^{[1]}, T_2 = \mathrm{SINR}_{E2}^{[2]}, T = T_1 + T_2$, and $b = \frac{P_1}{(P_1 - \gamma_1 P_2)2^{2r_2}} - 1$, where V, L and J follow the exponential distribution with parameters $\lambda_v = \sigma^2/(\beta d_{R2}^{-\alpha} P_R)$, $\lambda_l = 1/(\beta d_{R2}^{-\alpha})$ and $\lambda_j = 1/(\beta d_{B2}^{-\alpha})$, respectively. d_{R2} is the distance from the relay to U2. Thus, the CDF of V, L and J can be calculated as $F_V(v) = 1 - e^{-\lambda_v v}$, $F_L(l) = 1 - e^{-\lambda_l l}$ and $F_J(j) = 1 - e^{-\lambda_j j}$, respectively. The PDF of V, L and J can be calculated as $f_V(v) = \lambda_v e^{-\lambda_v v}$, $f_L(l) = \lambda_l e^{-\lambda_l l}$ and $f_J(j) = \lambda_j e^{-\lambda_j j}$, respectively. The PDF of T_1 and T_2 can be calculated as

$$f_{T_1}(t_1) = \begin{cases} \dfrac{P_2\sigma^2\lambda_1}{(P_2 - P_1 t_1)^2} e^{\frac{-t_1\sigma^2\lambda_1}{P_2 - P_1 t_1}}, & t_1 < P_2/P_1, \\ 0, & t_1 \geq P_2/P_1, \end{cases} \tag{25}$$

$$f_{T_2}(t_2) = (\lambda_1+\lambda_2)e^{-\lambda_2 t_2\sigma^2}\left(\frac{\sigma^2}{\lambda_2 t_2+\lambda_1} + \frac{1}{(\lambda_2 t_2+\lambda_1)^2}\right), \tag{26}$$

where $\lambda_1 = 1/(\beta d_{BE}^{-\alpha})$ and $\lambda_2 = 1/(\beta d_{RE}^{-\alpha})$ are parameters of the exponential distribution of $|h_{BE}|^2$ and $|h_{RE}|^2$, respectively. d_{BE} and d_{RE} are the distance from the BS to the eavesdropper and the distance from the relay to the eavesdropper, respectively. Due to $T_1 \geq 0$, $T_2 \geq 0$ and $T_1 + T_2 = T$, we can obtain that $0 \leq T_1 \leq T$. Thus, according to the independence between T_1 and T_2, we can obtain the PDF of T as

$$f_T(t) = \int_0^t f_{T_1}(t_1) f_{T_2}(t - t_1)dt_1. \tag{27}$$

The accurate solution to (27) is difficult to calculate. Using the Chebyshev-Guass quadrature, we can get an approximate of PDF for T as

$$\begin{aligned} f_T(t) &= \int_0^t f_{T_1}(t_1) f_{T_2}(t - t_1)dt_1 \\ &\approx \frac{\pi t}{2L}\sum_{l=1}^{L}\sqrt{1 - x_l^2}\, f_{T_1}\left(\frac{t}{2}x_l + \frac{t}{2}\right) f_{T_2}\left(\frac{t}{2} - \frac{t}{2}x_l\right), \end{aligned} \tag{28}$$

where L is the number of Gauss-Chebyshev nodes, and $x_l = \cos(\frac{2l-1}{2L})$.

When $P_1 - \gamma_1 P_2 \leq 0$, Pr_2 can be given as Proposition 2.

Proposition 2: When $P_1 - \gamma_1 P_2 \leq 0$, $\mathrm{Pr}_2 = 1$.

Proof: When $P_1 - \gamma_1 P_2 \leq 0$, we can obtain that $(P_1 - \gamma_1 P_2)S < \gamma_1 \sigma^2$, i.e., $\mathrm{SINR}_{R1} < \gamma_1$. Thus, we can obtain $I_1 = 1$, $I_2 = I_3 = 0$ and $\mathrm{Pr}_2 = 1$. ■

When $P_1 - \gamma_1 P_2 > 0$, I_1, I_2 and I_3 are discussed as follows.

(1) Calculation of I_1

I_1 can be calculated as

$$I_1 = F_S(a) = 1 - e^{-\lambda_s a}. \tag{29}$$

(2) Calculation of I_2

$\Pr\left(\mathrm{SINR}_{R1} > \gamma_1, R_{s1} < r_2\right)$ can be expressed as

$$\begin{aligned} &\Pr\left(\mathrm{SINR}_{R1} > \gamma_1, R_{s1} < r_2\right) \\ &= \underbrace{\Pr\left(T > b, a < S < g_1(T), V > \frac{P_2 S}{\sigma^2}\right)}_{I_{21}} \\ &+ \underbrace{\Pr\left(V < \frac{P_2 a}{\sigma^2}, T > g_2(V)\right) Pr(S > a)}_{I_{22}} \\ &+ \underbrace{\Pr\left(V > \frac{P_2 a}{\sigma^2}, T > g_2(V), S > \frac{V\sigma^2}{P_2}\right)}_{I_{23}}, \end{aligned} \tag{30}$$

where $g_1(T) = \left(2^{2r_2}(1+T) - 1\right)\sigma^2 / P_2$ and $g_2(V) = \frac{V+1}{2^{2r_2}} - 1$.

I_{21} can be calculated as

$$\begin{aligned} I_{21} &= \int_b^\infty f_T(t)dt \int_a^{g_1(t)} f_S(s)ds \int_{\frac{P_2 s}{\sigma^2}}^\infty f_V(v)dv \\ &= \int_b^\infty h_1(t)dt, \end{aligned} \tag{31}$$

where $h_1(t) = \frac{f_T(t)\lambda_s}{a_2}\left(e^{a_2 g_1(t)} - e^{a_2 a}\right)$ and $a_2 = -(\lambda_s + \lambda_v P_2/\sigma^2)$. Due to the fact that (31) is convergent, we can approximate (31) as

$$I_{21} \approx \int_b^D h_1(t)dt, \tag{32}$$

where D denotes a sufficiently large positive number. Then, we can use Gauss-Chebyshev quadrature to yield its approximation as

$$I_{21} \approx \frac{\pi(D-b)}{2L}\sum_{l=1}^{L}\sqrt{1-x_l^2}\, h_1\left(\frac{D-b}{2}x_l + \frac{D+b}{2}\right). \tag{33}$$

Similarly, we can obtain the approximate solutions to I_{22} and I_{23} as

$$\begin{aligned} I_{22} &\approx \int_0^{\frac{P_2 a}{\sigma^2}} h_2(v)dv\,(1 - F_S(a)) \\ &\approx \frac{\pi P_2 a}{2L\sigma^2}\sum_{l=1}^{L}\sqrt{1-x_l^2}\, h_2\left(\frac{P_2 a}{2\sigma^2}x_l + \frac{P_2 a}{2\sigma^2}\right)(1 - F_S(a)), \end{aligned} \tag{34}$$

where

$$\begin{aligned} h_2(v) = &f_V(v)\frac{\pi(D - g_2(v))}{2L}\sum_{l=1}^{L}\sqrt{1-x_l^2} \\ &f_T\left(\frac{D - g_2(v)}{2}x_l + \frac{D + g_2(v)}{2}\right). \end{aligned} \tag{35}$$

$$\begin{aligned} I_{23} &\approx \int_{\frac{P_2 a}{\sigma^2}}^\infty h_3(v)dv \\ &\approx \frac{\pi(D - \frac{P_2 a}{\sigma^2})}{2L}\sum_{l=1}^{L}\sqrt{1-x_l^2}\, h_3\left(\frac{D - \frac{P_2 a}{\sigma^2}}{2}x_l + \frac{D + \frac{P_2 a}{\sigma^2}}{2}\right), \end{aligned} \tag{36}$$

where

$$\begin{aligned} h_3(v) = &f_V(v)\left(1 - F_S\left(\frac{v\sigma^2}{P_2}\right)\right)\frac{\pi(D - g_2(v))}{2L} \\ &\sum_{l=1}^{L}\sqrt{1-x_l^2}\, f_T\left(\frac{D - g_2(v)}{2}x_l + \frac{D + g_2(v)}{2}\right). \end{aligned} \tag{37}$$

From (7), we can easily get

$$\Pr\left(\mathrm{SINR}_{21} > \gamma_1\right) = 1 - F_J(a). \tag{38}$$

From (33), (34), (36) and (38), I_2 can be expressed as

$$I_2 = (I_{21} + I_{22} + I_{23})(1 - F_J(a)). \tag{39}$$

(3) Calculation of I_3

I_3 can be calculated as

$$\begin{aligned} I_3 = &\underbrace{\Pr\left(a < S < g_1(T), J < a, L > g_3(S, J)\right)}_{I_{31}} \\ &+ \underbrace{\Pr\left(a < S < g_1(T), J < a, L < g_3(S, J)\right)}_{I_{32}} \\ &+ \underbrace{\Pr\left(T > b, S > g_1(T), J < a, L < g_4(T, J)\right)}_{I_{33}} \\ &+ \underbrace{\Pr\left(T < b, S > a, J < a, L < g_4(T, J)\right)}_{I_{34}}, \end{aligned} \tag{40}$$

where $g_3(S, J) = \frac{P_2 S(P_B J + \sigma^2)}{P_R \sigma^2}$ and $g_4(T, J) = \frac{g_1(T) P_2 (P_B J + \sigma^2)}{P_R \sigma^2}$. The approximate solutions to I_{31}, I_{32}, I_{33} and I_{34} can be expressed as follows.

$$\begin{aligned} I_{31} &\approx \int_b^\infty h_4(t)dt \\ &\approx \frac{\pi(D-b)}{2L}\sum_{l=1}^{L}\sqrt{1-x_l^2}\, h_4\left(\frac{D-b}{2}x_l + \frac{D+b}{2}\right), \end{aligned} \tag{41}$$

where

$$\begin{aligned} h_4(t) = &f_T(t)\frac{\pi(g_1(t) - a)}{2L}\sum_{l=1}^{L}\sqrt{1-x_l^2} \\ &g_5\left(\frac{g_1(t) - a}{2}x_l + \frac{g_1(t) + a}{2}\right) \end{aligned} \tag{42}$$

and

$$g_5(s) = f_S(s)\lambda_j e^{\frac{-\lambda_l P_2 s}{P_R}} \frac{1 - e^{-(\lambda_j + \frac{\lambda^l P_2 P_B S}{P_R \sigma^2})a}}{\lambda_j + \frac{\lambda^l P_2 P_B S}{P_R \sigma^2}}. \tag{43}$$

$$\begin{aligned} I_{32} &\approx \int_b^\infty h_5(t)dt \\ &\approx \frac{\pi(D-b)}{2L}\sum_{l=1}^{L}\sqrt{1-x_l^2}\, h_5\left(\frac{D-b}{2}x_l + \frac{D+b}{2}\right), \end{aligned} \tag{44}$$

where

$$h_5(t) = f_T(t)\frac{\pi(g_1(t)-a)}{2L}\sum_{l=1}^{L}\sqrt{1-x_l^2}\, g_6\left(\frac{g_1(t)-a}{2}x_l + \frac{g_1(t)+a}{2}\right) \tag{45}$$

and

$$g_6(s) = F_J(a)f_S(s) - g_5(s). \tag{46}$$

$$\begin{aligned} I_{33} &\approx \int_b^{\infty} h_6(t)dt \\ &\approx \frac{\pi(D-b)}{2L}\sum_{l=1}^{L}\sqrt{1-x_l^2}\, h_6\left(\frac{D-b}{2}x_l + \frac{D+b}{2}\right), \end{aligned} \tag{47}$$

where

$$h_6(t) = f_T(t)(1-F_S(g_1(t)))g_7(t) \tag{48}$$

and

$$g_7(t) = F_J(a) - \lambda_j e^{\frac{-\lambda_l g_1(t)P_2}{P_R}}\frac{1-e^{-(\lambda_j+\frac{\lambda_l g_1(t)P_2P_B}{P_R\sigma^2})a}}{\lambda_j+\frac{\lambda_l g_1(t)P_2P_B}{P_R\sigma^2}}. \tag{49}$$

$$\begin{aligned} I_{34} &\approx \int_0^{b} h_7(t)dt(1-F_S(a)) \\ &\approx \frac{\pi b}{2L}\sum_{l=1}^{L}\sqrt{1-x_l^2}\, h_7\left(\frac{b}{2}x_l + \frac{b}{2}\right), \end{aligned} \tag{50}$$

where

$$h_7(t) = f_T(t)g_7(t). \tag{51}$$

Therefore, when $P_1 - \gamma_1 P_2 > 0$, according to (29), (39) and (40), we can obtain Pr_2 as

$$\begin{aligned} \mathrm{Pr}_2 = 1 - e^{-\lambda_s a} &+ (I_{21}+I_{22}+I_{23})(1-F_J(a)) \\ &+ I_{31}+I_{32}+I_{33}+I_{34}. \end{aligned} \tag{52}$$

V. Numerical Results and Discussion

In the simulation, we set $P_B = P_R = P$. The distance from the BS to the relay, the eavesdropper, U1 and U2 is d_{br}=30 m, d_{be}=40 m, d_{b1}=60 m and d_{b2}=70 m, respectively. The distance from the relay to the eavesdropper and U2 is d_{re}=40 m, d_{r2}=60 m, respectively. The noise power is $\sigma^2 = -110$ dBm. $\alpha = 3$ and $\beta = 10^{-4}$. The rate threshold of x_1 and x_2 is set to $r_1 = r_2 = 0.5$ bit/s/Hz, and thus, the SINR threshold of x_1 can be calculated as $\gamma_1 = 2^{2r_1} - 1 = 1$.

First, the OP of U1 and SOP of U2 in the proposed scheme and the conventional NOMA scheme are compared in Fig. 2 for different values of P when the power allocation coefficient for x_1 is α_1=0.8. In addition, in the conventional NOMA scheme, α_1 denotes the power allocation coefficient for x_2. From the results, we can see that the SOP of U2 in the conventional NOMA scheme is close to 1 due to the high transmit power allocated to x_2, which gives great threat to the security of U2. On the contrary, in the proposed scheme, the SOP of U2 is low, and the security of U2 can be guaranteed. This is because in the first time slot, the transmit power allocated to x_2 is low, and in the second time slot, the BS transmits x_1 to disrupt the eavesdropping towards x_2. Furthermore, the OP of U1 in the proposed scheme is lower than that of the conventional NOMA scheme, because in the proposed scheme, U1 is allocated with a higher transmit power in the first time slot, while in the conventional NOMA scheme, U1 is a weak user allocated with a lower transmit power. Besides, we can also see that the SOP of U2 and the OP of U1 decrease with P in the proposed scheme. This is because both of the transmit power of x_2 and x_1 increases, which results in the increasing of the transmission rate of x_1 and x_2 with the eavesdropping rate towards x_2 almost unchanged. In addition, the theoretical OP of U1 and SOP of U2 are consistent with the simulation results.

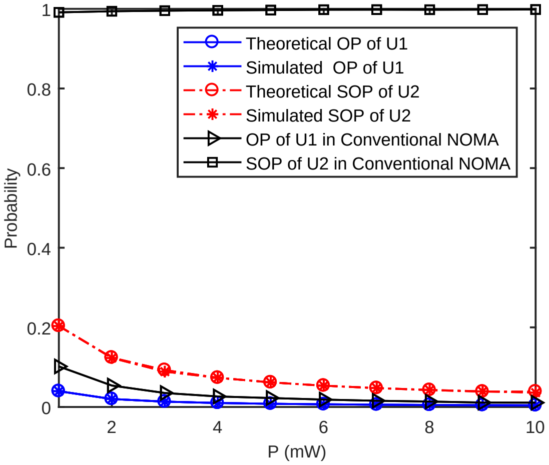

Fig. 2. Comparison of OP for U1 and SOP for U2 for different values of P when α_1=0.8 in different schemes.

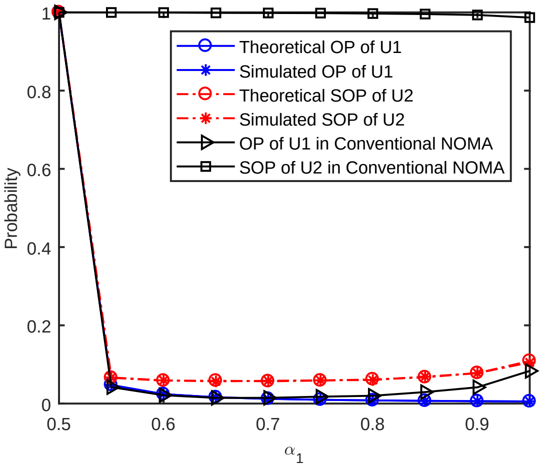

Fig. 3. Comparison of OP for U1 and SOP for U2 for different values of α_1 when P=5 mW.

Then, the OP of U1 and SOP of U2 in the proposed scheme and the conventional NOMA scheme are compared in Fig. 3 for different values of α_1 when P=5 mW. From the results, we can observe that the security of U2 can be significantly improved with different values of α_1 via the proposed scheme compared to the conventional NOMA scheme, and the OP of U1 in the proposed scheme is lower than that of the conventional NOMA scheme. Besides, we can also see that the SOP of U2 decreases first and then increases with α_1. This is because when α_1 is small, x_1 cannot be decoded correctly to recover x_2 at the relay; when α_1 is large, the transmit power allocated to x_2 is so small that its rate requirement cannot be satisfied. Moreover, the OP of U1 decreases with α_1, due to the fact that higher transmit power allocated to x_1 will increase its transmission rate. In addition, the theoretical and simulation results are consistent with each other.

VI. Conclusions and Future Work

In this paper, we have proposed a two-slot cooperative NOMA scheme with two users and a potential eavesdropper. First, superimposed signals are sent to U1 and the relay by BS. U2 decodes the high-power signal of U1 and caches it locally. Then, the relay transmits the signal to U2, while the BS transmits the signal of U1 to disrupt the eavesdropping. Due to the fact that U2 has obtained the signal for U1, the interference can be eliminated. To further analyze the performance of U1 and U2, the OP of U1 and the SOP of U2 are derived. Simulation results are presented to verify the derivation of OP and SOP, and show the effectiveness of the proposed scheme. In our future work, artificial jamming will be introduced to further improve the security when both users require secure transmission or the eavesdropper can detect multi-user data.

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] L. Dai, B. Wang, Y. Yuan, S. Han, C. I, and Z. Wang, “Non-orthogonal multiple access for 5G: solutions, challenges, opportunities, and future research trends,” *IEEE Commun. Mag.*, vol. 53, no. 9, pp. 74–81, Sept. 2015.

[3] G. Liu, Z. Wang, J. Hu, Z. Ding, and P. Fan, “Cooperative NOMA broadcasting/multicasting for low-latency and high-reliability 5G cellular V2X communications,” *IEEE Internet Things J.*, vol. 6, no. 5, pp. 7828–7838, Oct. 2019.

[4] 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.

[5] 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.

[6] H. Liu, Z. Ding, K. J. Kim, K. S. Kwak, and H. V. Poor, “Decode-and-forward relaying for cooperative NOMA systems with direct links,” *IEEE Trans. Wireless Commun.*, vol. 17, no. 12, pp. 8077–8093, Dec. 2018.

[7] R. Jiao, L. Dai, J. Zhang, R. MacKenzie, and M. Hao, “On the performance of NOMA-based cooperative relaying systems over Rician fading channels,” *IEEE Trans. Veh. Technol.*, vol. 66, no. 12, pp. 11409–11413, Dec. 2017.

[8] 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.*, Online, DOI: 10.1109/MWC.001.1900159.

[9] Y. Feng, S. Yan, Z. Yang, N. Yang, and J. Yuan, “Beamforming design and power allocation for secure transmission with NOMA,” *IEEE Trans. Wireless Commun.*, vol. 18, no. 5, pp. 2639–2651, May 2019.

[10] L. Lv, F. Zhou, J. Chen, and N. Al-Dhahir, “Secure cooperative communications with an untrusted relay: A NOMA-inspired jamming and relaying approach,” *IEEE Trans. Inf. Forens. Security*, vol. 14, no. 12, pp. 3191–3205, Dec. 2019.

[11] 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.

[12] H. Lei, J. Zhang, K. Park, P. Xu, Z. Zhang, G. Pan, and M. Alouini, “Secrecy outage of max-min TAS scheme in MIMO-NOMA systems,” *IEEE Trans. Veh. Technol.*, vol. 67, no. 8, pp. 6981–6990, Aug. 2018.

[13] 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.

[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] B. Li, Z. Fei, Z. Chu, F. Zhou, K. Wong, and P. Xiao, “Robust chance-constrained secure transmission for cognitive satellite-terrestrial networks,” *IEEE Trans. Veh. Technol.*, vol. 67, no. 5, pp. 4208–4219, May 2018.