Security Optimization of Cooperative NOMA Networks with Friendly Jamming

Jianglong Li, Xianfu Lei, *Member, IEEE*, Panagiotis D. Diamantoulakis, *Senior Member, IEEE*, Lisheng Fan, *Member, IEEE*, and George K. Karagiannidis, *Fellow, IEEE*

***Abstract*—We investigate physical layer security of a downlink cooperative non-orthogonal multiple access system with an untrusted relay. A friendly jammer (FJ) is employed in order to improve the secrecy sum rate. Aiming at maximizing the secrecy sum rate by optimizing the power allocation at both the source and the FJ, an optimization problem is formulated and solved iteratively by using alternating optimization method. Specifically, the problem is decoupled into two sub-problems, each of which is optimally solved. Moreover, the secrecy sum rate of the proposed system with imperfect channel state information is studied. Finally, simulation results validate the effectiveness of the proposed FJ based schemes.**

***Index Terms*—Cooperative non-orthogonal multiple access, untrusted relay, friendly jammer, power allocation.**

I. Introduction

Non-orthogonal multiple access (NOMA) is a competitive candidate for the beyond fifth generation (B5G) mobile communication systems, since compared to orthogonal multiple access (OMA) it can enhance spectral efficiency and provide massive connectivity [1]. Applying the cooperative transmission in NOMA systems is able to improve the network reliability and extend the wireless coverage. Particularly, two types of cooperative NOMA (C-NOMA) schemes are usually operated. In the first type, the stronger user, which also acts as a relay, assists the communication of the weaker user, while in the second type, a dedicated relay assists the NOMA users which do not have direct communication links with the source. C-NOMA has been combined with many other wireless technologies, e.g., multiple-input multiple-output, cognitive radio networks, physical layer network coding and unmanned aerial vehicles networks, etc. The major challenges and future research trends of C-NOMA systems have been highlighted in [2].

 This work was supported by the National Key Research and Development Program of China under Grant 2019YFB1803400, the National Natural Science Foundation of China under Grant 61971360, the Fundamental Research Funds for the Central Universities under Grant XJ2021KJZK007, and the open research fund of National Mobile Communications Research Laboratory, Southeast University (No. 2021D05). (Corresponding author: Xianfu Lei.)

J. Li and X. Lei are with the School of Information Science and Technology, Southwest Jiaotong University, Chengdu 610000, China, and also with the National Mobile Communications Research Laboratory, Southeast University, Nanjing 210096, China (e-mail: JLLi@my.swjtu.edu.cn; xflei@swjtu.edu.cn). P. D. Diamantoulakis and G. K. Karagiannidis are with Department of Electrical and Computer Engineering, Aristotle University of Thessaloniki, 54124 Thessaloniki, Greece (e-mail: padiaman@auth.gr; geokarag@auth.gr). L. Fan is with Guangzhou University, Guangzhou, China (e-mail: lsfan@gzhu.edu.cn).

The physical layer security (PLS) of wireless communication systems has attracted significant research interests in recent years, e.g., [3], [4]. Usually, two scenarios for PLS are investigated in C-NOMA networks. In the first scenario, a passive eavesdropper degrades the confidential communication, while the utilized relay is untrsuted in the other scenario. Both the above scenarios were investigated in [5], where beamforming schemes and cooperative jamming schemes were proposed to mitigate the impacts of the passive eavesdropper and the untrusted relay, respectively. A system model consisting of four half-duplex and single-antenna nodes, i.e., a source, a trusted relay and two NOMA users in the presence of an eavesdropper was investigated in [6]–[8], assuming that the direct links are blocked. More specifically, the analytical expressions of secrecy outage probability and secrecy capacity were derived for both amplify-and-forward (AF) and decode-and-forward (DF) techniques [6]. A secure transmission protocol consisting of two phases was proposed in [7], where the source transmits a NOMA signal to the relay and the stronger user during the first phase, while in the second phase, the relay forwards the decoded signal to the weaker user and the source retransmits the signal for the stronger user as interference to prevent the eavesdropping. In [8], the authors proposed a new C-NOMA scheme in which the source is actively to jam the eavesdropper when the relay is forwarding information to the users. The scenario of utilizing an untrusted relay to serve the NOMA users was investigated in [9]–[11]. In more detail, a scheduling scheme was proposed to select one of the near users, in order to jam the untrusted relay [9]. Considering a similar system model, exact and asymptotic expressions for the effective secrecy throughput were derived for Nakagami-m fading channels in [10]. In [11], cooperative jamming schemes were proposed to achieve the positive ergodic secrecy sum rate lower bound for both downlink and uplink C-NOMA systems with an untrusted relay. Moreover, the PLS of C-NOMA systems applying some other technologies have been widely investigated, e.g., multiple-relay selection [12]–[14], multiple antenna transmissions [15]–[17], full-duplex relaying [18]–[20], artificial noise [21] and mobile edge computing [22], etc.

Friendly jamming has been proposed in [23] as an efficient solution to improve the PLS of cooperative networks with an untrusted relay. The key idea behind friendly jamming is to introduce a friendly jammer (FJ) node into the system for the sake of interfering the eavesdropping node. A number of papers have studied the FJ utilization in various wireless networks, especially the uplink NOMA systems [24]. In [5],

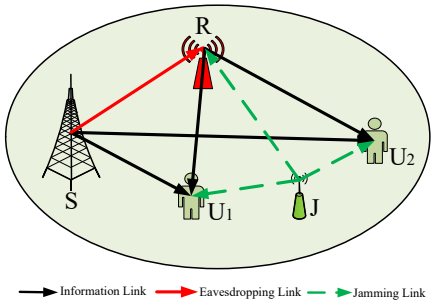

Fig. 1. Downlink C-NOMA system with an untrusted relay and a friendly jammer.

the achievable secrecy rate region was derived for a C-NOMA system that consists of a source, an untrusted AF relay and two users, in the presence of the direct links from the source to the users. However, it has been identified that the achievable secrecy rate may be equal to zero. In order to improve the secrecy rate of the above system, we use a FJ to jam the untrusted relay. To this end, considering the power allocation at the source and the FJ, an optimization problem that aims at maximizing the secrecy sum rate of two users is formulated and solved iteratively by using alternating optimization (AO) method. Specifically, the problem is decoupled into two sub-problems, each of which is optimally solved. Moreover, the secrecy sum rate of the proposed system with imperfect CSI is studied.

II. System and Signal Model

A. System Model

We consider a downlink C-NOMA system consisting of four single-antenna nodes, namely a source (S), an AF relay (R), one cell-center user (U_1) and one cell-edge user (U_2), as shown in Fig. 1. It is assumed that there is a direct link between S and each user. The node S can transmit information to the users through the direct links and the relaying links. Moreover, it is assumed that R is trusted at service level and performs the expected functionalities of the AF protocol, but R is untrusted in the sense that it should not decode the messages sent towards the users. Thus, the confidential information delivery in downlink C-NOMA should be secured against R. To this end, an external jammer node (J), e.g., a user served by S but in an idle state when S is serving U_1 and U_2, is scheduled to broadcast a jamming signal against the potential eavesdropping node[1]. The jamming signal is received at both the R and the users, due to the broadcast nature of radio communications. Furthermore, it is assumed that all the channels are subject to independent Rayleigh fading and $h_{s1}, h_{s2}, h_{sr}, h_{r1}$, h_{r2}, h_{jr}, h_{j1} and h_{j2} are the channel power gains of S-U_1, S-U_2, S-R, R-U_1, R-U_2, J-R, J-U_1 and J-U_2 links, respectively. In addition, it is assumed that $h_{n_1n_2}{=}g_{n_1n_2}/d_{n_1n_2}^{\frac{\gamma}{2}}(n_1n_2{\in}\{sr,s1,s2,r1,r2,jr,j1,j2\})$, where $d_{n_1n_2}$ is the distance between the nodes n_1 and n_2, γ is the path loss exponent, and $g_{n_1n_2} \in \mathcal{CN}(0,1)$ is Rayleigh fading channel gain between node n_1 and n_2. It is worthwhile to notice that the distances from J to U_1 and U_2 are shorter than that from J to R, so the channel gains from J to U_1 and U_2 are generally better than that from J to R. Let P denote the maximum transmit power at S and R and P_j denote the transmit power level at J. Moreover, the existence of additive white Gaussian noise (AWGN) with zero mean and unit variance is considered at both the R and the users. Since S typically requires the channel state information (CSI) of all links and can afford the complexity of performing the proposed power allocation scheme, it is assumed that the CSI of all the involved links is available at S [10], [11], which also performs the optimization. The procedure for S to acquire the CSI of all links consists of two phases. In the first phase, the relay and the users estimate the CSI of the source-relay and source/relay-users links, respectively. In the second phase, the relay and the users estimate the CSI of the jammer-relay and jammer-users links, respectively. S acquires the CSI of the links through the dedicated feedback channel. Then, it performs the proposed optimization algorithm, and informs the jammer about the power allocation scheme.

[1]In the considered scenario, the relay R is untrusted in the sense that it would be curious enough to decode its received NOMA signal. In order to prevent the users information leakage at R, another authenticated cellular user is scheduled as a friendly jammer to interfere the untrusted relay.

B. Signal Model

The signal transmission from S to U_1 and U_2 consists of two hops. In the first hop, S transmits the superposed signal

$$x_s = \sqrt{\alpha}x_{s1} + \sqrt{(1-\alpha)}x_{s2}, \tag{1}$$

to U_1, U_2 and R, where x_{s1} and x_{s2} are the messages of U_1 and U_2, respectively, and $\alpha \leq 0.5$ denotes the power allocation coefficient of NOMA scheme. At the same time, FJ broadcasts a jamming signal x_j. Thus, the received signal at R is expressed as

$$y_R = \sqrt{Ph_{sr}}x_s + \sqrt{P_jh_{jr}}x_j + z_R, \tag{2}$$

where z_R is the AWGN at R. It's worth noting that the jamming signal is generally unknown for the untrusted R [23], thus R can directly treat x_j as noise when decoding the users' messages. According to [11], successive interference cancellation (SIC) with fixed decoding order is used at R for improving its eavesdropping capability. In more detail, R firstly decodes the cell-edge user's message x_{s2} by treating x_{s1} and x_j as interferences. Then, x_{s2} is subtracted from y_r and R decodes the cell-center user's message x_{s1} by treating x_j as interference. Thus, the signal-to-interference-plus-noise ratios (SINRs) for R to decode x_{s1} and x_{s2} are expressed as

$$\mathrm{SINR}_{R\to\mathrm{U}_1} = \frac{\alpha Ph_{sr}}{1+P_jh_{jr}}, \tag{3}$$

$$\mathrm{SINR}_{R\to\mathrm{U}_2} = \frac{(1-\alpha)Ph_{sr}}{1+\alpha Ph_{sr}+P_jh_{jr}}, \tag{4}$$

respectively. Moreover, the received signals at U_1 and U_2 in the first hop are

$$y_{\mathrm{U}_1}^1 = \sqrt{Ph_{s1}}x_s + \sqrt{P_jh_{j1}}x_j + z_{\mathrm{U}_1}, \tag{5}$$

$$y_{\mathrm{U}_2}^1 = \sqrt{Ph_{s2}}x_s + \sqrt{P_jh_{j2}}x_j + z_{\mathrm{U}_2}, \tag{6}$$

respectively, where z_{U_1} and z_{U_2} denote the AWGN at U_1 and U_2, respectively. In the second hop, R amplifies the received signal y_r via multiplying a coefficient G, then immediately transmits the amplified signal to the users. The signals received at U_1 and U_2 are expressed as

$$y_{\mathrm{U}_1}^2 = \sqrt{Ph_{r1}}Gy_R + z_{\mathrm{U}_1}, \tag{7}$$

$$y_{\mathrm{U}_2}^2 = \sqrt{Ph_{r2}}Gy_R + z_{\mathrm{U}_2}, \tag{8}$$

respectively. Note that a variable-gain AF R is adopted so that $G = \sqrt{\frac{P}{Ph_{sr}+P_j h_{jr}+1}}$. Furthermore, it is assumed that the users use maximum ratio combination (MRC) to detect the desired messages by combining the signals received in both two hops [25]. The jamming signal is firstly detected in order to improve the data rate at users [11]. According to [25], MRC is applied to y_k^1 and $y_k^2 (k = \mathrm{U}_1, \mathrm{U}_2)$ so the SINRs for U_1 and U_2 to decode x_j are expressed as

$$\mathrm{SINR}_{\mathrm{J}\to\mathrm{U}_1} = \frac{G^2 P P_j h_{jr} h_{r1} + P_j h_{j1}}{Ph_{s1} + G^2 P^2 h_{sr} h_{r1} + G^2 P h_{r1} + 1}, \tag{9}$$

$$\mathrm{SINR}_{\mathrm{J}\to\mathrm{U}_2} = \frac{G^2 P P_j h_{jr} h_{r2} + P_j h_{j2}}{Ph_{s2} + G^2 P^2 h_{sr} h_{r2} + G^2 P h_{r2} + 1}, \tag{10}$$

respectively. After correctly decoding x_j, it is removed from the received signals, i.e., y_k^1 and y_k^2. Next, U_1 utilizes MRC to decode x_{s2}, the corresponding SINR is expressed as

$$\mathrm{SINR}_{\mathrm{U}_1\to\mathrm{U}_2} = \frac{(1-\alpha)[Ph_{s1} + G^2 P^2 h_{sr} h_{r1}]}{\alpha[Ph_{s1} + G^2 P^2 h_{sr} h_{r1}] + 1}. \tag{11}$$

After U_1 successfully decodes x_{s2} and subtracts it from its received signal, x_{s1} is decoded and the following SINR is obtained

$$\mathrm{SINR}_{\mathrm{U}_1} = \alpha[Ph_{s1} + G^2 P^2 h_{sr} h_{r1}]. \tag{12}$$

Similarly, U_2 also applies MRC to decode x_{s2}, and the SINR at U_2 can be expressed as

$$\mathrm{SINR}_{\mathrm{U}_2} = \frac{(1-\alpha)[Ph_{s2} + G^2 P^2 h_{sr} h_{r2}]}{\alpha[Ph_{s2} + G^2 P^2 h_{sr} h_{r2}] + 1}. \tag{13}$$

III. Secrecy sum rate optimization

A. Problem Formulation

In this work, our goal is to maximize the secrecy sum rate of two users. The secrecy rate of U_1 is defined as

$$S_{\mathrm{U}_1} = \frac{1}{2}[\log_2(1+\mathrm{SINR}_{\mathrm{U}_1}) - \log_2(1+\mathrm{SINR}_{R\to\mathrm{U}_1})]^+, \tag{14}$$

where $[x]^+$ denotes $\max\{0, x\}$. As it has already been mentioned, U_1 needs to firstly decode the message of U_2. Hence, the secrecy rate of U_2 is expressed as

$$S_{\mathrm{U}_2} = \frac{1}{2}\left[\log_2(1 + \min\{\mathrm{SINR}_{\mathrm{U}_1\to\mathrm{U}_2}, \mathrm{SINR}_{\mathrm{U}_2}\}) - \log_2(1 + \mathrm{SINR}_{R\to\mathrm{U}_2})\right]^+. \tag{15}$$

According to [26], if the distance from the source to the cell-edge user is far greater than that from the source to the cell-center user, the SIC at the cell-center user could be almost always successful. This will also hold for the proposed system model, since we assume that the distances from S and R to U_2 are far greater than the distances from S and R to U_1. Thus, one has $\mathrm{SINR}_{\mathrm{U}_1\to\mathrm{U}_2} \geq \mathrm{SINR}_{\mathrm{U}_2}$ and S_{U_2} can be reexpressed as

$$S_{\mathrm{U}_2} = \frac{1}{2}[\log_2(1+\mathrm{SINR}_{\mathrm{U}_2}) - \log_2(1+\mathrm{SINR}_{R\to\mathrm{U}_2})]^+. \tag{16}$$

Based on the above analysis, the secrecy sum rate of the two users can be given as

$$S_{\text{sum}} = S_{\mathrm{U}_1} + S_{\mathrm{U}_2}. \tag{17}$$

It should be noted that S_{sum} is achievable under the condition that the jamming signal cannot be decoded by R prior to decoding the users' messages and the users can successfully decode the jamming signal before decoding their own messages. This condition will be satisfied in the optimization procedure, by using a required SINR threshold ϵ_j for the FJ, which guarantees that two unwanted events are avoided. The first one is that R successfully decodes and subtracts x_j before decoding x_{s1} and x_{s2}. The other one is that R successfully decodes x_{s2}, x_j and x_{s1} in a consecutive manner. It is observed from (2) that the SINRs for decoding x_j at R in these two cases are expressed as $\mathrm{SINR}_{\mathrm{R}\to\mathrm{J}}^{\text{case 1}} = \frac{P_j h_{jr}}{1+Ph_{sr}}$ and $\mathrm{SINR}_{\mathrm{R}\to\mathrm{J}}^{\text{case 2}} = \frac{P_j h_{jr}}{1+\alpha Ph_{sr}}$, respectively. Then, the following constraint is constructed:

$$\mathrm{C}_1 : \mathrm{SINR}_{\mathrm{R}\to\mathrm{J}}^{\text{case 2}} \leq \epsilon_j. \tag{18}$$

Note that $\mathrm{SINR}_{\mathrm{R}\to\mathrm{J}}^{\text{case 1}} < \mathrm{SINR}_{\mathrm{R}\to\mathrm{J}}^{\text{case 2}}$, thus C_1 is utilized to avoid both the two aforementioned events. In addition, to ensure that the users can completely decode and subtract the jamming signal, the following constraints are also needed:

$$\mathrm{C}_2 : \mathrm{SINR}_{\mathrm{J}\to\mathrm{U}_1} \geq \epsilon_j, \tag{19}$$

$$\mathrm{C}_3 : \mathrm{SINR}_{\mathrm{J}\to\mathrm{U}_2} \geq \epsilon_j. \tag{20}$$

Furthermore, in order to improve the rate of NOMA transmission, the power that is allocated to U_1 and U_2 is also subject to optimization. It should be noticed that the power allocation coefficient needs to satisfy the following constraint:

$$\mathrm{C}_4 : 0 \leq \alpha \leq 0.5. \tag{21}$$

Since the power allocation for the users at S is subject to optimization, a quality of service (QoS) mechanism is required, otherwise the performance of cell-edge user might be severely degraded. Motivated by this, it is assumed that each user has a minimum QoS demand, corresponding to the minimum required SINRs at U_1 and U_2, which are denoted by ϵ_1 and ϵ_2, respectively. Then, one has the following constraints:

$$\mathrm{C}_5 : \mathrm{SINR}_{\mathrm{U}_1} \geq \epsilon_1, \tag{22}$$

$$\mathrm{C}_6 : \mathrm{SINR}_{\mathrm{U}_2} \geq \epsilon_2, \tag{23}$$

To this end, an optimization problem with the aim to maximize S_{sum}, is formulated as

$$\begin{aligned} \max_{\alpha, P_j} \quad & S_{\text{sum}} \\ \text{s.t.} \quad & \mathrm{C}_1, \mathrm{C}_2, \mathrm{C}_3, \mathrm{C}_4, \mathrm{C}_5, \mathrm{C}_6. \end{aligned} \tag{24}$$

It can be observed that (54) is a non-linear and non-convex problem, since the objective function and the constraints are non-linear and non-convex. In order to solve (54), we will decouple it into two sub-problems which will be solved in the following subsections.

B. Transmit Power Optimization at J

For a given $\alpha \in [0, 0.5]$, problem (54) can be reexpressed as

$$\begin{aligned} \max_{P_j} \quad & S_{\text{sum}} \\ \text{s.t.} \quad & \mathrm{C}_1, \mathrm{C}_2, \mathrm{C}_3, \mathrm{C}_5, \mathrm{C}_6. \end{aligned} \tag{25}$$

Moreover, it can be observed that the constraints C_1, C_2, C_3, C_5 and C_6 can be rewritten as

$$\mathrm{C}_1: P_j \le \frac{\epsilon_j(1+\alpha P h_{sr})}{h_{jr}},$$

$$\mathrm{C}_2: \begin{cases} P_j \ge \frac{\sqrt{\eta_1^2+4h_{jr}h_{j1}\epsilon_j\eta_2}-\eta_1}{2h_{jr}h_{j1}}, & \text{if } \sqrt{\eta_1^2+h_{jr}h_{j1}\epsilon_j\eta_2} \ge 0, \\ P_j \le \frac{-\sqrt{\eta_1^2+4h_{jr}h_{j1}\epsilon_j\eta_2}-\eta_1}{2h_{jr}h_{j1}}, & \text{if } \sqrt{\eta_1^2+h_{jr}h_{j1}\epsilon_j\eta_2} < 0, \end{cases}$$

$$\mathrm{C}_3: \begin{cases} P_j \ge \frac{\sqrt{\eta_3^2+4h_{j2}h_{jr}\epsilon_j\eta_4}-\eta_3}{2h_{j2}h_{jr}}, & \text{if } \sqrt{\eta_3^2+h_{j2}h_{jr}\epsilon_j\eta_4} \ge 0, \\ P_j \le \frac{-\sqrt{\eta_3^2+4h_{j2}h_{jr}\epsilon_j\eta_4}-\eta_3}{2h_{j2}h_{jr}}, & \text{if } \sqrt{\eta_3^2+h_{j2}h_{jr}\epsilon_j\eta_4} < 0, \end{cases}$$

$$\mathrm{C}_5: \begin{cases} P_j \le \frac{\epsilon_1(Ph_{sr}+1)-\alpha\eta_5}{\alpha P h_{s1}h_{jr}-\epsilon_1 h_{jr}}, & \text{if } \epsilon_1 \ge \alpha P h_{s1}, \\ P_j \ge \frac{\epsilon_1(Ph_{sr}+1)-\alpha\eta_5}{\alpha P h_{s1}h_{jr}-\epsilon_1 h_{jr}}, & \text{if } \epsilon_1 < \alpha P h_{s1}, \end{cases}$$

$$\mathrm{C}_6: \begin{cases} P_j \le \frac{(1-\alpha-\epsilon_2\alpha)\eta_6-\epsilon_2(Ph_{sr}+1)}{(\alpha+\epsilon_2\alpha-1)Ph_{s2}h_{jr}+\epsilon_2 h_{jr}}, & \text{if } \epsilon_2 \ge \frac{(1-\alpha)Ph_{s2}}{1+\alpha Ph_{s2}}; \\ P_j \ge \frac{(1-\alpha-\epsilon_2\alpha)\eta_6-\epsilon_2(Ph_{sr}+1)}{(\alpha+\epsilon_2\alpha-1)Ph_{s2}h_{jr}+\epsilon_2 h_{jr}}, & \text{if } \epsilon_2 < \frac{(1-\alpha)Ph_{s2}}{1+\alpha Ph_{s2}}, \end{cases} \tag{26}$$

where

$$\begin{aligned} \eta_1 &= P^2 h_{jr}h_{r1} + P(h_{sr}h_{j1} - \epsilon_j h_{s1}h_{jr}) + h_{j1} - \epsilon_j h_{jr}, \\ \eta_2 &= P^3 h_{sr}h_{r1} + P^2(h_{s1}h_{sr} + h_{r1}) + P(h_{s1} + h_{sr}) + 1, \\ \eta_3 &= P^2 h_{jr}h_{r2} + P(h_{sr}h_{j2} - \epsilon_j h_{s2}h_{jr}) + h_{j2} - \epsilon_j h_{jr}, \\ \eta_4 &= P^3 h_{sr}h_{r2} + P^2(h_{s2}h_{sr} + h_{r2}) + P(h_{s2} + h_{sr}) + 1, \\ \eta_5 &= P^3 h_{sr}h_{r1} + P^2 h_{s1}h_{sr} + P h_{s1}, \\ \eta_6 &= P^3 h_{sr}h_{r2} + P^2 h_{s2}h_{sr} + P h_{s2}. \end{aligned} \tag{27}$$

Based on the above, it can be seen that all the constraints of problem (25) is equivalent to the following constraint:

$$\mathrm{C}_7: \Phi_1 \le P_j \le \Phi_2, \tag{28}$$

where

$$\Phi_1 = \max\{\nabla_1, \nabla_2, \nabla_3, \nabla_4, \nabla_5, \nabla_6, \nabla_7, \nabla_8\}, \tag{29}$$

$$\Phi_2 = \min\{\theta, \nabla_1', \nabla_2', \nabla_3', \nabla_4', \nabla_5', \nabla_6', \nabla_7', \nabla_8'\}. \tag{30}$$

Note that $\theta = \frac{\epsilon_j(1+\alpha P h_{sr})}{h_{jr}}$ and ∇_i, $\nabla_i'(i = 1, 2, \ldots, 8)$ are shown in the Table I. The term 'null' implies no value in the adopted symbol. Then, the optimization problem in (25) can be rewritten as

$$\begin{aligned} \underset{P_j}{\textbf{max}} \quad & S_{\text{sum}} \\ \textbf{s.t.} \quad & \mathrm{C}_7. \end{aligned} \tag{31}$$

To solve (31), we first take the derivative of S_{sum} with respect to P_j. Let $Y = \frac{\partial S_{\text{sum}}}{\partial P_j}$, we have

$$Y = \frac{UNT + VMT + VNW}{2VNT}, \tag{32}$$

where U, V, M, N, W and T are respectively given by

$$\begin{aligned} U =& \alpha P^2 h_{sr}^2 h_{jr} + \left[\alpha P h_{sr}h_{jr} - \alpha P^5 h_{sr}^3 h_{jr}h_{r1}(1+\alpha P h_{s1}) \right. \\ & \left. - \alpha P^7 h_{sr}^3 h_{jr}h_{r1}^2\right](1+P_j h_{jr}) - \left[(1+\alpha)(1+\alpha P h_{s1})P^4 h_{sr}^2 \right. \\ & \left. \times h_{jr}h_{r1} + P^6 h_{sr}^2 h_{jr}h_{r1}^2\right](1+P_j h_{jr})^2 - (1+\alpha P h_{s1})P^3 h_{sr} \\ & \times h_{jr}h_{r1}(1+P_j h_{jr})^3, \end{aligned} \tag{33}$$

TABLE I

Conditions	∇_i	∇_i'
$\sqrt{\eta_1^2+4h_{jr}h_{j1}\epsilon_j\eta_2} \ge 0$	$\nabla_1 = \frac{\sqrt{\eta_1^2+4h_{jr}h_{j1}\epsilon_j\eta_2}-\eta_1}{2h_{jr}h_{j1}}$	∇_1'=null
$\sqrt{\eta_1^2+4h_{jr}h_{j1}\epsilon_j\eta_2} < 0$	∇_2=null	$\nabla_2' = \frac{-\sqrt{\eta_1^2+4h_{jr}h_{j1}\epsilon_j\eta_2}-\eta_1}{2h_{jr}h_{j1}}$
$\sqrt{\eta_3^2+4h_{j2}h_{jr}\epsilon_j\eta_4} \ge 0$	$\nabla_3 = \frac{\sqrt{\eta_3^2+4h_{j2}h_{jr}\epsilon_j\eta_4}-\eta_3}{2h_{j2}h_{jr}}$	∇_3'=null
$\sqrt{\eta_3^2+4h_{j2}h_{jr}\epsilon_j\eta_4} < 0$	∇_4=null	$\nabla_4' = \frac{-\sqrt{\eta_3^2+4h_{j2}h_{jr}\epsilon_j\eta_4}-\eta_3}{2h_{j2}h_{jr}}$
$\alpha P h_{s1} \ge \epsilon_1$	$\nabla_5 = \frac{\epsilon_1(Ph_{sr}+1)-\alpha\eta_5}{\alpha P h_{s1}h_{jr}-\epsilon_1 h_{jr}}$	∇_5' = null
$\alpha P h_{s1} < \epsilon_1$	∇_6 = null	$\nabla_6' = \frac{\epsilon_1(Ph_{sr}+1)-\alpha\eta_5}{\alpha P h_{s1}h_{jr}-\epsilon_1 h_{jr}}$
$(1+\alpha)Ph_{s2}+1 > \frac{Ph_{s2}}{\epsilon_2}$	∇_7=null	$\nabla_7' = \frac{(1-\alpha-\epsilon_2\alpha)\eta_6-\epsilon_2(Ph_{sr}+1)}{(\alpha+\epsilon_2\alpha-1)Ph_{s2}h_{jr}+\epsilon_2 h_{jr}}$
$(1+\alpha)Ph_{s2}+1 < \frac{Ph_{s2}}{\epsilon_2}$	$\nabla_8 = \frac{(1-\alpha-\epsilon_2\alpha)\eta_6-\epsilon_2(Ph_{sr}+1)}{(\alpha+\epsilon_2\alpha-1)Ph_{s2}h_{jr}+\epsilon_2 h_{jr}}$	∇_8'=null

$$\begin{aligned} V =& \ln 2\left[\alpha P^2 h_{sr}^2(1+P_j h_{jr}) + (1+\alpha)P h_{sr}(1+P_j h_{jr})^2 \right. \\ & \left. + (1+P_j h_{jr})^3\right], \end{aligned} \tag{34}$$

$$\begin{aligned} M =& (\alpha-1)\left[(1+\alpha P h_{s2})P^4 h_{sr}^2 h_{jr}h_{r2} + \alpha P^6 h_{sr}^2 h_{r2}^2 h_{jr} \right. \\ & \left. + (1+\alpha P h_{s2})P^3 h_{sr}h_{jr}h_{r2}(1+P_j h_{jr})\right], \end{aligned} \tag{35}$$

$$\begin{aligned} N =& \ln 2\left[\alpha^2 P^9 h_{sr}^2 h_{r2}^2 + P^6 h_{sr}h_{r2}\left[\alpha(1+Ph_{s2}) + 2\alpha \right.\right. \\ & \left. \times (1+\alpha P h_{s2})\right](1+Ph_{sr}+P_j h_{jr}) + P^3 h_{sr}h_{r2}[2\alpha(1+Ph_{s2}) \\ & \times (1+\alpha P h_{s2}) + (1+\alpha P h_{s2})^2(1+Ph_{sr}+P_j h_{jr})^2 + (1+Ph_{s2}) \\ & \left. \times (1+\alpha P h_{s2})^2(1+Ph_{sr}+P_j h_{jr})^3\right], \end{aligned} \tag{36}$$

$$W = (1-\alpha)Ph_{sr}h_{jr}, \tag{37}$$

$$T = \ln 2(1+Ph_{sr}+P_j h_{jr})(1+\alpha P h_{sr}+P_j h_{jr}). \tag{38}$$

It can be observed that Y is a continuous function of P_j since its denominator is large than zero. Let $Y^* = UNT + VMT - VNW$, then the roots of Y equal to those of Y^*. Therefore, (31) can be optimally solved by utilizing the following process. Firstly, all the roots of Y^* are calculated. Then, only the roots that can satisfy C_7 are further considered as potential solutions of (31). Finally, the aforementioned roots and the boundaries of C_7 are substituted into S_{sum}, where the value that maximizes S_{sum} will be the optimal solution of problem (31).

C. Optimal Power Allocation at S

For the given P_j obtained by the above, it can be seen that constraints C_2 and C_3 are ineffective for problem (54). Thus we can reformulate (54) as

$$\begin{aligned} \underset{\alpha}{\textbf{max}} \quad & S_{\text{sum}} \\ \textbf{s.t.} \quad & \mathrm{C}_1, \mathrm{C}_4, \mathrm{C}_5, \mathrm{C}_6. \end{aligned} \tag{39}$$

Furthermore, the constraints C_1, C_5 and C_6 can be reexpressed as

$$\begin{aligned} &\mathrm{C}_1: \alpha \ge \frac{P_j h_{jr} - \epsilon_j}{P h_{sr}\epsilon_j}, \\ &\mathrm{C}_5: \alpha \ge \frac{\epsilon_1}{P h_{s1} + G^2 P^2 h_{sr}h_{r1}}, \\ &\mathrm{C}_6: \alpha \le \frac{G^2 P^2 h_{sr}h_{r2} + P h_{s2} - \epsilon_2}{(1+\epsilon_2)(P h_{s2} + G^2 P^2 h_{sr}h_{r2})}, \end{aligned} \tag{40}$$

respectively. Combining (40) and C_4, it can be observed that all the constraints of problem (39) can be equivalently replaced by the following constraint:

$$\mathrm{C}_8: \max\{0, \Gamma_1, \Gamma_2\} \le \alpha \le \min\{0.5, \Gamma_3\}, \tag{41}$$

where

$$\begin{aligned}\Gamma_1 &= \tfrac{P_j h_{jr}-\epsilon_j}{P h_{sr}\epsilon_j},\\ \Gamma_2 &= \tfrac{\epsilon_1}{P h_{s1}+G^2P^2h_{sr}h_{r1}},\\ \Gamma_3 &= \tfrac{G^2P^2h_{sr}h_{r2}+Ph_{s2}-\epsilon_2}{(1+\epsilon_2)(Ph_{s2}+G^2P^2h_{sr}h_{r2})},\end{aligned} \tag{42}$$

Thus, problem (39) can be rewritten as

$$\begin{aligned}\max_{\alpha}\quad & S_{\text{sum}}\\ \text{s.t.}\quad & \mathrm{C}_8.\end{aligned} \tag{43}$$

To solve (43), we first take the derivative of S_{sum} with respect to α. Let $Z=\frac{\partial S_{\text{sum}}}{\partial \alpha}$, we have

$$Z=\frac{L}{B}, \tag{44}$$

where L and B are given by

$$L=Ph_{s1}+G^2P^2h_{sr}h_{r1}-Ph_{s2}-G^2P^2h_{sr}h_{r2}, \tag{45}$$

$$\begin{aligned}B=&\ln 2(1+\alpha Ph_{sr}+P_jh_{jr})(1+\alpha Ph_{s1}+\alpha G^2P^2h_{sr}h_{r1})\\ &\times(1+\alpha Ph_{s2}-\alpha G^2P^2h_{sr}h_{r2}).\end{aligned} \tag{46}$$

It is observed that S_{sum} is a monotone increasing function of α since Z is larger than zero. As a result, problem (43) can be solved by substituting 0.5 and Γ_3 into S_{sum}, where the value that maximizes the S_{sum} is just the optimal solution of (43).

D. Alternating Optimization

To approach the optimal solution of problem (54), the AO method is used. Specifically, the adaptive power optimization at FJ and the power allocation at S are alternately optimized, by solving problems (25) and (39) respectively, while keeping the other one fixed. It should be noticed that the convergence of the AO method is guaranteed, since each of the two subproblems is optimally solved. According to the optimization process, the closed-form solutions of the subproblems (30) and (43) can be obtained, thus the number of iterations for AO method is the dominating factor that affects the complexity. Assuming that the iteration numbers of AO method is I, then the computational complexity of the proposed scheme is $\mathcal{O}(I)$.

IV. Secrecy sum rate optimization with imperfect CSI

In this section, the proposed system model with imperfect CSI is investigated. Let's assume the estimate for the channel coefficient $h_{n_1n_2}(n_1n_2\in\{sr,s1,s2,r1,r2,jr,j1,j2\})$ is $\bar{h}_{n_1n_2}$. In this work, we focus on the minimum mean square error (MMSE) channel estimation error model [27]. Thus, it holds that

$$h_{n_1n_2}=\bar{h}_{n_1n_2}+\xi, \tag{47}$$

where ξ is the channel estimation error, which follows a complex Gaussian distribution with mean 0 and variance σ_ξ^2. According to the same two-hop C-NOMA transmission protocol as in the perfect CSI case, the received signals at R in the first hop, U_1 and U_2 in the first and second hops, which are denoted by $\bar{y}_R$, $\bar{y}^1_{\mathrm{U}_1}$, $\bar{y}^1_{\mathrm{U}_2}$, $\bar{y}^2_{\mathrm{U}_1}$ and $\bar{y}^2_{\mathrm{U}_2}$, respectively, are given by

$$\bar{y}_R=\sqrt{P}\bar{h}_{sr}x_s+\sqrt{P_j}\bar{h}_{jr}x_j+\xi(\sqrt{P}x_s+\sqrt{P_j}x_j)+z_R, \tag{48}$$

$$\bar{y}^1_{\mathrm{U}_1}=\sqrt{P}\bar{h}_{s1}x_s+\sqrt{P_j}\bar{h}_{j1}x_j+\xi(\sqrt{P}x_s+\sqrt{P_j}x_j)+z_{\mathrm{U}_1}, \tag{49}$$

$$\bar{y}^1_{\mathrm{U}_2}=\sqrt{P}\bar{h}_{s2}x_s+\sqrt{P_j}\bar{h}_{j2}x_j+\xi(\sqrt{P}x_s+\sqrt{P_j}x_j)+z_{\mathrm{U}_2}, \tag{50}$$

$$\bar{y}^2_{\mathrm{U}_1}=\sqrt{P}\bar{h}_{r1}G\bar{y}_R+\xi\sqrt{P}G\bar{y}_R+z_{\mathrm{U}_1}, \tag{51}$$

$$\bar{y}^2_{\mathrm{U}_2}=\sqrt{P}\bar{h}_{r2}G\bar{y}_R+\xi\sqrt{P}G\bar{y}_R+z_{\mathrm{U}_2}. \tag{52}$$

TABLE II

$\overline{\text{SINR}}$	Expressions
$\overline{\text{SINR}}_{R\to\mathrm{U}_1}$	$\frac{\alpha P\bar{h}^2_{sr}}{1+P_j\bar{h}^2_{jr}+P\sigma^2_\xi+P_j\sigma^2_\xi}$
$\overline{\text{SINR}}_{R\to\mathrm{U}_2}$	$\frac{(1-\alpha)P\bar{h}^2_{sr}}{1+\alpha P\bar{h}^2_{sr}+P_j\bar{h}^2_{jr}+P\sigma^2_\xi+P_j\sigma^2_\xi}$
$\overline{\text{SINR}}_{\mathrm{U}_1\to\mathrm{J}}$	$\frac{G^2PP_j\bar{h}^2_{jr}\bar{h}^2_{r1}+P_j\bar{h}^2_{j1}}{P\bar{h}^2_{s1}+G^2P^2\bar{h}^2_{sr}\bar{h}^2_{r1}+G^2P\bar{h}^2_{r1}+(G^2P^2\bar{h}^2_{r1}+G^2PP_j\bar{h}^2_{r1}+P+P_j)\sigma^2_\xi+1}$
$\overline{\text{SINR}}_{\mathrm{U}_2\to\mathrm{J}}$	$\frac{G^2PP_j\bar{h}^2_{jr}\bar{h}^2_{r2}+P_j\bar{h}^2_{j2}}{P\bar{h}^2_{s2}+G^2P^2\bar{h}^2_{sr}\bar{h}^2_{r2}+G^2P\bar{h}^2_{r2}+(G^2P^2\bar{h}^2_{r2}+G^2PP_j\bar{h}^2_{r2}+P+P_j)\sigma^2_\xi+1}$
$\overline{\text{SINR}}_{\mathrm{U}_1\to\mathrm{U}_2}$	$\frac{(1-\alpha)[P\bar{h}^2_{s1}+G^2P^2\bar{h}^2_{sr}\bar{h}^2_{r1}]}{\alpha P\bar{h}^2_{s1}+\alpha G^2P^2\bar{h}^2_{sr}\bar{h}^2_{r1}+(G^2P\bar{h}^2_{r1}+G^2P^2\bar{h}^2_{r1}+G^2PP_j\bar{h}^2_{r1})\sigma^2_\xi+1}$
$\overline{\text{SINR}}_{\mathrm{U}_1}$	$\frac{\alpha[P\bar{h}^2_{s1}+G^2P^2\bar{h}^2_{sr}\bar{h}^2_{r1}]}{G^2P\bar{h}^2_{r1}+G^2P^2\bar{h}^2_{r1}\sigma^2_\xi+G^2PP_j\bar{h}^2_{r1}\sigma^2_\xi+1}$
$\overline{\text{SINR}}_{\mathrm{U}_2}$	$\frac{(1-\alpha)[P\bar{h}^2_{s2}+G^2P^2\bar{h}^2_{sr}\bar{h}^2_{r2}]}{\alpha P\bar{h}^2_{s2}+\alpha G^2P^2\bar{h}^2_{sr}\bar{h}^2_{r21}+G^2P\bar{h}^2_{r2}+(G^2P^2\bar{h}^2_{r2}+G^2PP_j\bar{h}^2_{r2})\sigma^2_\xi+1}$

Furthermore, the same SIC process as in the perfect CSI case is utilized, and the SINRs for R to decode x_{s1} and x_{s2}, for U_1 and U_2 to decode x_j, for U_1 to decode x_{s2} and x_{s1} and for U_2 to decode x_{s2}, which are denoted by $\overline{\text{SINR}}_{R\to\mathrm{U}_1}$, $\overline{\text{SINR}}_{R\to\mathrm{U}_2}$, $\overline{\text{SINR}}_{\mathrm{U}_1\to\mathrm{J}}$, $\overline{\text{SINR}}_{\mathrm{U}_2\to\mathrm{J}}$, $\overline{\text{SINR}}_{\mathrm{U}_1\to\mathrm{U}_2}$, $\overline{\text{SINR}}_{\mathrm{U}_1}$ and $\overline{\text{SINR}}_{\mathrm{U}_2}$, respectively, are shown in Table II. As a result, the secrecy sum rate under the imperfect CSI assumption is given by

$$\begin{aligned}\bar{S}_{\text{sum}}=&\frac{1}{2}\left[\log_2(1+\overline{\text{SINR}}_{\mathrm{U}_1})-\log_2(1+\overline{\text{SINR}}_{R\to\mathrm{U}_1})\right]^+\\ &+\frac{1}{2}\left[\log_2(1+\overline{\text{SINR}}_{\mathrm{U}_2})-\log_2(1+\overline{\text{SINR}}_{R\to\mathrm{U}_2})\right]^+.\end{aligned} \tag{53}$$

Similarly to the perfect CSI case, the SINRs for R to decode x_j for different events are expressed as $\overline{\text{SINR}}^{\text{case 1}}_{\mathrm{R}\to\mathrm{J}}=\frac{P_j\bar{h}^2_{jr}}{1+P\bar{h}^2_{sr}+P\sigma^2_\xi+P_j\sigma^2_\xi+1}$ and $\overline{\text{SINR}}^{\text{case 2}}_{\mathrm{R}\to\mathrm{J}}=\frac{P_j\bar{h}^2_{jr}}{1+\alpha P\bar{h}^2_{sr}+P\sigma^2_\xi+P_j\sigma^2_\xi}$. Then, based on the same problem formulation process as in the perfect CSI case, the optimization problem with the aim to maximize the secrecy sum rate is formulated as

$$\begin{aligned}\max_{\alpha,P_j}\quad & \bar{S}_{\text{sum}}\\ \text{s.t.}\quad & \bar{\mathrm{C}}_1,\bar{\mathrm{C}}_2,\bar{\mathrm{C}}_3,\bar{\mathrm{C}}_4,\bar{\mathrm{C}}_5,\bar{\mathrm{C}}_6,\end{aligned} \tag{54}$$

where $\bar{\mathrm{C}}_1$, $\bar{\mathrm{C}}_2$, $\bar{\mathrm{C}}_3$, $\bar{\mathrm{C}}_5$ and $\bar{\mathrm{C}}_6$ are expressed as $\overline{\text{SINR}}^{\text{case 2}}_{\mathrm{R}\to\mathrm{J}}\le\epsilon_j$, $\overline{\text{SINR}}_{\mathrm{U}_1\to\mathrm{J}}\ge\epsilon_j$, $\overline{\text{SINR}}_{\mathrm{U}_2\to\mathrm{J}}\ge\epsilon_j$, $\overline{\text{SINR}}_{\mathrm{U}_1}\ge\epsilon_1$ and $\overline{\text{SINR}}_{\mathrm{U}_2}\ge\epsilon_2$, respectively, and $\bar{\mathrm{C}}_4$ is the same as C_4. The optimization problem (54) can be solved by using the same AO method as in the perfect CSI case.

V. Simulation Results and Discussion

To illustrate the advantages of the proposed scheme (C^{FJ}-NOMA), we will compare it with the traditional C-NOMA scheme which does not utilize FJ technology. The parameters used in the simulations are set as follows. The disk radius is D=50m with the path loss exponent, γ=2, 3, 4, and the distances between the nodes are set as d_{sr}=5m, d_{s1}=10m, d_{s2}=50m, d_{r1}=10m, d_{r2}=40m, d_{jr}=40m, d_{j1}=20m and d_{j2}=10m.

Fig. 2 illustrates the secrecy sum rate achieved by C^{FJ}-NOMA and C-NOMA for different path loss exponents, with ϵ_j=1 dB, ϵ_1=2 dB and ϵ_2=-5 dB. It is clearly observed that the proposed scheme outperforms the baseline schemes, indicating that the PLS performance of the investigated C-NOMA system with an untrusted relay can be significantly improved by introducing the FJ. Fig. 3 illustrates the effect of ϵ_j and

This article has been accepted for publication in IEEE Transactions on Vehicular Technology. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TVT.2022.3200253

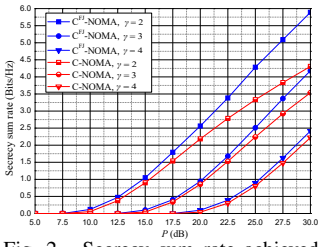

Fig. 2. Secrecy sum rate achieved by the C^{FJ}-NOMA and C-NOMA schemes vs. P.

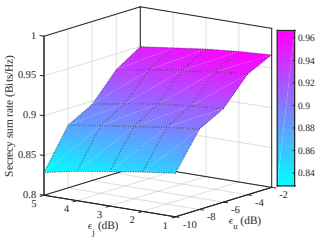

Fig. 3. The effect of ϵ_j and ϵ_u on the secrecy sum rate.

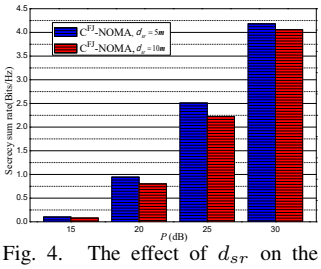

Fig. 4. The effect of d_{sr} on the secrecy sum rate.

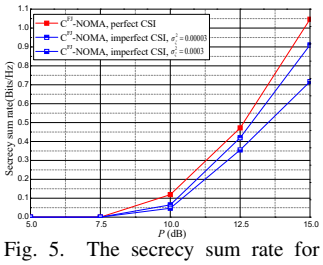

Fig. 5. The secrecy sum rate for imperfect CSI vs. perfect CSI .

$\epsilon_u = \min\{\epsilon_1, \epsilon_2\}$ on the secrecy sum rate for $\gamma = 3$ and $P = 20$ dB. It is observed that the secrecy sum rate increases and decreases in proportion to ϵ_u and ϵ_j, respectively. The reason for this is two-fold: i) as ϵ_u increases, P_j needs to be increased to guarantee that the QoS of the users are satisfied, and a larger P_j is able to decrease the eavesdropping rate, ii) as ϵ_j increases, only a smaller P_j is required to ensure that the users can completely decode the jamming signal, and a smaller P_j is able to increase the eavesdropping rate. In Fig. 4, it is observed that a larger distance between S and R decreases the secrecy sum rate. In Fig.5, the secrecy sum rate achieved by the proposed scheme with imperfect CSI is presented and compared with that for the perfect CSI case. For γ=2 and $\sigma_\xi^2 = 0.00003, 0.0003$, the results clearly show that the secrecy sum rate is degraded by the imperfect CSI.

VI. CONCLUSIONS

The PLS of a downlink C-NOMA system with an untrusted relay has been investigated. The FJ has been utilized to improve secrecy sum rate. Aiming at maximizing the secrecy sum rate by optimizing the power allocation at S and FJ, the corresponding optimization problem has been formulated and solved iteratively by using AO algorithm. Moreover, the secrecy sum rate of the proposed system with imperfect CSI has also been studied. Finally, simulation results have shown the superiority of the proposed FJ based schemes.

REFERENCES

[1] Z. Ding, X. Lei, G. K. Karagiannidis, R. Schober, J. Yuan, and V. K. 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] D. Wan, M. Wen, F. Ji, H. Yu, and F. Chen, "Non-orthogonal multiple access for cooperative communications: Challenges, opportunities, and trends," *IEEE Wireless Commun.*, vol. 25, no. 2, pp. 109–117, Apr. 2018.

[3] Z. Yin, M. Jia, N. Cheng, W. Wang, F. Lyu, Q. Guo, and X. Shen, "UAV-assisted physical layer security in multi-beam satellite-enabled vehicle communications," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 3, pp. 2739–2751, Mar. 2022.

[4] Z. Yin, N. Cheng, T. H. Luan, Y. Hui, and W. Wang, "Green interference based symbiotic security in integrated satellite-terrestrial communications," *IEEE Trans. Wireless Commun.*, pp. 1–1, 2022.

[5] A. Arafa, W. Shin, M. Vaezi, and H. V. Poor, "Secure relaying in non-orthogonal multiple access: Trusted and untrusted scenarios," *IEEE Trans. Inf. Forensics Security.*, vol. 15, pp. 210–222, Apr. 2020.

[6] J. Chen, L. Yang, and M. -S. Alouini, "Physical layer security for cooperative NOMA systems," *IEEE Trans. Veh. Technol.*, vol. 67, no. 5, pp. 4645–4649, May 2018.

[7] B. Chen *et al.*, "Security enhancement using a novel two-slot cooperative NOMA scheme," *IEEE Trans. Veh. Technol.*, vol. 69, no. 3, pp. 3470–3475, Mar. 2020.

[8] C. Yuan, X. Tao, N. Li, W. Ni, R. P. Liu, and P. Zhang, "Analysis on secrecy capacity of cooperative non-orthogonal multiple access with proactive jamming," *IEEE Trans. Veh. Technol.*, vol. 68, no. 3, pp. 2682–2696, Mar. 2019.

[9] B. He, L. Lv, L. Yang, and J. Chen, "Enhancing secrecy for NOMA untrusted relay networks with user scheduling and jamming," *IEEE Commun. Lett.*, vol. 24, no. 12, pp. 2682–2686, Dec. 2020.

[10] Z. Xiang, W. Yang, G. Pan, Y. Cai, and X. Sun, "Secure transmission in non-orthogonal multiple access networks with an untrusted relay," *IEEE Wireless Commun. Lett.*, vol. 8, no. 3, pp. 905–908, Jun. 2019.

[11] L. Lv, H. Jiang, Z. Ding, L. Yang, and J. Chen, "Secrecy-enhancing design for cooperative downlink and uplink NOMA with an untrusted relay," *IEEE Trans. Commun.*, vol. 68, no. 3, pp. 1698–1715, Mar. 2020.

[12] K. Cao, B. Wang, H. Ding, T. Li, and F. Gong, "Optimal relay selection for secure NOMA systems under untrusted users," *IEEE Trans. Veh. Technol.*, vol. 69, no. 2, pp. 1942–1955, Feb. 2020.

[13] H. Lei *et al.*, "Secrecy outage analysis for cooperative NOMA systems with relay selection schemes," *IEEE Trans. Commun.*, vol. 67, no. 9, pp. 6282–6298, Sep. 2019.

[14] Y. Feng, S. Yan, C. Liu, Z. Yang, and N. Yang, "Two-stage relay selection for enhancing physical layer security in non-orthogonal multiple access," *IEEE Trans. Inf. Forensics Security.*, vol. 14, no. 6, pp. 1670–1683, Jun. 2019.

[15] 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.

[16] Y. Cao *et al.*, "Secrecy analysis for cooperative noma networks with multi-antenna full-duplex relay," *IEEE Trans. Commun.*, vol. 67, no. 8, pp. 5574–5587, Aug. 2019.

[17] 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. Forensics Security.*, vol. 14, no. 12, pp. 3191–3205, Dec. 2019.

[18] Y. Cao *et al.*, "Power optimization for enhancing secrecy of cooperative user relaying NOMA networks," *IEEE Trans. Veh. Technol.*, vol. 69, no. 7, pp. 8008–8012, Jul. 2020.

[19] B. Zheng *et al.*, "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.

[20] B. Chen *et al.*, "Secure primary transmission assisted by a secondary full-duplex NOMA relay," *IEEE Trans. Veh. Technol.*, vol. 68, no. 7, pp. 7214–7219, Jul. 2019.

[21] R. Ruby *et al.*, "Enhancing secrecy performance of cooperative NOMA-based IoT networks via multiantenna-aided artificial noise," *IEEE Internet of Things Journal*, vol. 9, no. 7, pp. 5108–5127, Apr. 2022.

[22] B. Li, W. Wu, W. Zhao, and H. Zhang, "Security enhancement with a hybrid cooperative NOMA scheme for MEC system," *IEEE Trans. Veh. Technol.*, vol. 70, no. 3, pp. 2635–2648, March 2021.

[23] X. He, and A. Yener, "Two-hop secure communication using an untrusted relay: A case for cooperative jamming," in *Proc. IEEE Global Commun. Conf., New Orleans, USA*, Nov. 2008, pp. 1–5.

[24] K. Cao, B. Wang, H. Ding, L. Lv, J. Tian, and F. Gong, "On the security enhancement of uplink NOMA systems with jammer selection," *IEEE Trans. Commun.*, vol. 68, no. 9, pp. 5747–5763, Sep. 2020.

[25] H. Liu *et al.*, "Decode-and-forward relaying for cooperative NOMA systems with direct links," *IEEE Trans. Wireless Commun.*, vol. 17, no. 12, pp. 8077–8093, Dec. 2018.

[26] Z. Chen, Z. Ding, P. Xu, and X. Dai, "Optimal precoding for a QoS optimization problem in two-user MISO-NOMA downlink," *IEEE Commun. Lett.*, vol. 20, no. 6, pp. 1263–1266, Jun. 2016.

[27] Z. Yang, Z. Ding, P. Fan, and G. K. Karagiannidis, "On the performance of non-orthogonal multiple access systems with partial channel information," *IEEE Trans. Commun.*, vol. 64, no. 2, pp. 654–667, Feb. 2016.