Robust Secure Design for RIS-aided NOMA Network against Internal Near-End Eavesdropping

CHENGJUN JIANG, CHENSI ZHANG (MEMBER, IEEE), PEILI HAO, ZHE ZHANG AND JIANHUA GE
The State Key Laboratory of Integrated Service Networks, Xidian University, Xi’an 710071, China
Corresponding author: Chensi Zhang (e-mail: cszhang@xidian.edu.cn).
This work was supported in part by the key R & D plan of Shaanxi Province (2019ZDLGY07-02), in part by the National Natural Science Foundation of China (61501347), in part by the “111” project (B08038).

ABSTRACT The reconfigurable intelligent surface (RIS) aided non-orthogonal multiple access (NOMA) network is applied to improve spectral efficiency and energy efficiency of wireless systems. Due to the incorporation of NOMA, RIS-aided NOMA system suffers from physical layer security (PLS) problem when an internal near user (NU) is the eavesdropper. In this case, it is difficult to always guarantee positive secrecy rate. Therefore, a scheme of artificial noise (AN) cooperative jamming and beamforming design is proposed against internal eavesdropper for RIS-aided NOMA in this paper. It is proved theoretically that the positive secrecy rate can be guaranteed if providing sufficient power. In addition, the power allocation of base station is further studied to minimize the total power consumption under the constraints of data rate and secrecy rate, and the closed-form solutions are achieved. Simulation results show that the performance of the proposed scheme is superior to the existing solutions.

INDEX TERMS Reconfigurable intelligent surface (RIS), non-orthogonal multiple access (NOMA), artificial noise (AN), physical layer security (PLS), power allocation.

I. INTRODUCTION

Non-orthogonal multiple access (NOMA) is considered a promising technology because it can improve the spectral efficiency of next-generation networks [1]. NOMA has attracted the attention of many related researchers [2]-[6]. Compared with orthogonal multiple access (OMA) technology, NOMA allocates the same frequency channel to multiple users simultaneously in the same cell, which brings advantages such as higher spectral efficiency and cell-edge throughput [7]. The data traffic requirements of different users can be met by NOMA in the same resource block, such as time-domain, frequency-domain, and code-domain [8]. In addition to spectral efficiency, energy efficiency is also an important indicator that needs to be considered in the design of communication systems. Therefore, reconfigurable intelligent surface\(^1\) (RIS), as a revolutionary new technology expected to be applied to 6G, draws considerable interests from academia [9]. Specifically, RIS consists of large-scale low-cost passive reflective elements, and the reflection angle of each element can be controlled independently. Moreover, using RIS to improve the energy efficiency and coverage of the system is a potential application. RIS changes the attenuation and scattering of the incident electromagnetic wave by adjusting the reflection coefficients so that it can propagate in a desired manner to the intended receiver [10]. Note that 5G networks use high frequencies (e.g., 4.5–6 GHz), this will cause transmission interruptions because the signal can easily be blocked by moving objects and obstacles. However, the blocking problem can be solved by using RIS to control the propagation environment [11]. In addition, the “dead zone” problem in mmWave communications can be solved by RIS [12].

Therefore, inspired by the benefits of NOMA and RIS techniques, the combination of NOMA and RIS is applied to improve the performance of wireless systems [1], [13], [14]. In [15], RIS-assisted NOMA was used to ensure that cell-edge users can get better service by changing the actual channel between the base station and cell edge users with RIS. In order to make full use of the benefits of RIS-aided NOMA system, the authors of [16] considered that power

\(^1\) Other related terms: Intelligent Reflecting Surface (IRS), Software Controlled Metasurface, Intelligent Wall, Passive Intelligent Mirror (PIM), Smart Reflect Array etc.
allocation and phase shift design must be jointly optimized. An energy-efficient algorithm was proposed for RIS-assisted NOMA network in [17], which yield a good tradeoff between the sum-rate maximization and total power consumption minimization. To maximize the data rate of the strong user, the authors of [18] optimized the transmit beamforming and phase shift of RIS for RIS-assisted NOMA. The authors of [19] optimized the beamforming vectors and the RIS phase shift matrix to minimize transmission power.

Due to the broadcasting nature of wireless network, information may be leaked. Mature cryptography is an important tool to ensure communication security. On the other hand, physical layer security (PLS), as an important candidate to supplement the overall security strength, has attracted the attention of many scholars. Particularly, for RIS-aided NOMA, multiple access interference (MAI) is introduced into system due to the utilization of power domain NOMA. To eliminate MAI, SIC is adopted, which the order of decoding is ranked according to power magnitude. Moreover, to guarantee communication quality, more power is allocated to the far user (FU). According to SIC, the signal of FU will be decoded by users first. As a result, if near user (NU) is an untrusted user, it will conveniently eavesdrop the confidential data of FU. In other words, SIC will cause severe internal security problem [20]. Therefore, the NOMA system will suffer more serious transmission security problems than OMA. According to the identity and motivation of the eavesdropper, the security design objectives of RIS-aided NOMA can be divided into four categories:

- Security designs against external eavesdropping.
- Security designs against same location internal passive eavesdropping.
- Security designs against internal NU eavesdropping.

1) Security designs against external eavesdropping: At present, most researches about PLS for NOMA and RIS-aided NOMA are eavesdroppers outside the cell, i.e., external eavesdropping\(^2\). Many related researchers have made outstanding contributions in the above-mentioned fields. In this case, both NU and FU are credible. Therefore, the main goal of security design is to prevent external eavesdroppers from obtaining NU and FU information. Specifically, in [20], an artificial noise (AN)-aided beamforming scheme was proposed against external eavesdropping in NOMA network, and further studied the power allocation. The authors of [21] investigated covert communication in RIS-assisted NOMA system, the RIS-assisted downlink and uplink NOMA schemes were proposed to hide the existence of legitimate user’s covert transmission from an eavesdropper. In [22], the imperfect channel state information of eavesdropper was considered, and a robust beamforming scheme with AN is proposed to ensure the secure RIS-aided NOMA transmission. In [23], the impact of RIS-assisted wireless secure transmission was investigated, RIS was deployed to assist multiple-input multiple-output security systems to improve secure performance, and AN is used to introduce interference to reduce the eavesdropper’s receiving ability. In [24], a power efficient scheme was presented to design the secure transmit power allocation and the reflecting phase shift in RIS-aided multi-antenna transmission, and the transmission power of legitimate user was optimized under the constraint of secrecy rate.

2) Security designs against same location internal passive eavesdropping: In this case, legitimate but curious users may act as internal passive eavesdroppers. Divide users into different secrecy levels, the information of the high-level users is demodulated first at the low-level users if the high-level users are high-power users. Therefore, the low-level users passively eavesdropped on the high-level users. The authors of [25] studied the passive eavesdropping problem of internal users in the RIS-assisted NOMA, and minimized the total transmit power by jointly optimizing the beamforming vectors and the RIS reflecting factors.

3) Security designs against internal FU eavesdropping: In the traditional NOMA principle, FU is allocated more power, it can directly decode considering the information of NU as noise. However, FU can detect the NU’s signal after obtaining its own signal. In this case, base station can use PLS technology based on power distribution, beamforming or any other adaptive algorithm to meet the security requirements of NU, while ensuring the basic data rate requirements of FU [26]. The authors of [27] studied the outage probability and secrecy outage probability in the two-users NOMA system, in which FU is an untrusted/low-security clearance user. In order to achieve secure communication in the NOMA system against internal FU eavesdropping, the authors of [28] proposed two relay selection schemes, namely decode-and-forward and amplify-and-forward protocols based optimal relay selection schemes.

4) Security designs against internal NU eavesdropping: In this case, NU is an internal eavesdropper, trying to decode FU information. According to basic NOMA principle, FU is assigned more power due to its lower channel gain, and NU is the opposite. The NU must first decode the FU signal to apply SIC, which makes the security design in this case more challenging than other cases. Therefore, the system suffers from serious PLS issues when the eavesdropper is NU. Fortunately, there are already literature that pay attention to this thorny issue. In [29], the channel gain of FU was improved by using beamforming technology to directly align the beam at FU, as a result, the PLS of the system was enhanced. As far as we know, few papers had studied PLS of RIS-aided NOMA system for internal NU as active eavesdroppers. In [30], the “dead zone” problem was solved by adopting RIS, and PLS of RIS-aided NOMA with NU eavesdroppers was improved by beamforming, which aims the signal at FU to increase the channel gain of FU.

---

\(^2\) According to whether the eavesdropper is a normal NOMA user, it can be divided into internal eavesdropping and external eavesdropping. The untrusted NOMA user that shares the same resource blocks may eavesdrop information from other users. We call such user as internal eavesdropper.
Motivations and Contributions

We can observe that the security design of the existing NOMA system is less focused on internal NU eavesdropping, and it is difficult to ensure secure communication in this scenario. To the best of our knowledge, except for [30], there are few papers focused on RIS-aided NOMA security design against internal eavesdropping. However, due to the complexity of the wireless channel, the channel gain of FU cannot always be greater than the channel gain of NU, wherefore the positive secrecy rate of this RIS-aided NOMA system cannot always be guaranteed. Therefore, the above analysis is the main motivation of this paper. In this paper, based on the system model of [30], a scheme of AN cooperative jamming and beamforming design is presented against NU for RIS-aided NOMA. The proposed scheme is easy to implement and process. The analytical results evidence that the proposed scheme can guarantee the absolute positive secrecy rate if providing sufficient power. Moreover, the power allocation of base station is further studied to minimize the total power consumption under the constraints of data rate and secrecy rate, and the closed-form solutions are achieved. According to the simulation results, the proposed algorithm has better performance than the solution in [30].

Organization

The remainder of this paper is organized as follows. The system model is described in Section II. In Section III, positive secrecy rate is studied. To further enhance power efficiency, power allocation is studied in Section IV. Simulation of the model is shown in Section V. Finally, conclusions are given in Section VI.

II. SYSTEM MODEL

We consider a RIS-aided downlink NOMA transmission model [30] with an untrusted NU and a trusted FU as shown in Fig. 1. Two users are located in the communication “dead zone”, i.e., there are no direct communication paths between the base station and the users (RIS was adopted to solve the dead zone problem). The model includes one base station with $N_S$ ($N_S > 1$) transmit antennas ($S$), one RIS with $N_R$ reflecting elements ($R$), one NU ($U_1$) and one FU ($U_2$).

Both users are single antenna user, where $U_1$ wants to eavesdrop on the information sent by $S$ to $U_2$, and $U_1$ is closer to RIS than $U_2$.

In traditional NOMA-based communication, $U_1$ will decode its own information by first decoding the information of $U_2$ and then deleting it from the received signal. As a consequence, the information of $U_2$ will be eavesdropped by $U_1$.

To improve PLS of the system, the order of SIC is changed by allocating more power to $U_1$, and the signal is aligned with $U_2$ by beamforming design to improve the channel condition of $U_2$. In addition, AN is sent by the base station with beamforming, and reflected by RIS to jamming NU. The FU is allocated to the channel null space of the AN.

The signals received by $U_1$ and $U_2$, respectively, are shown as

$$ y_1 = h^H_{RU_1} \Phi H_{RS} w_1 \left( \sqrt{(1-\alpha)} P_U x_1 + \sqrt{\alpha P_U} x_2 \right), $$

$$ + h^H_{RU_1} \Phi H_{RS} w_2 \sqrt{P_j} x_j + n_1 $$

$$ y_2 = h^H_{RU_2} \Phi H_{RS} w_1 \left( \sqrt{(1-\alpha)} P_U x_1 + \sqrt{\alpha P_U} x_2 \right), $$

$$ + h^H_{RU_2} \Phi H_{RS} w_2 \sqrt{P_j} x_j + n_2 $$

where $y_1$ and $y_2$ represent the signal received by $U_1$ and $U_2$, respectively. $(\cdot)^H$ denotes the Hermitian transpose operation. We assume that channel state information (CSI) between transport nodes is known. $h_{RU_i} \in \mathbb{C}^{N_R \times 1}$ is $N_R \times 1$ channel complex vector between node $R$ and $U_i$ where $i \in \{U_1, U_2\}$. $\Phi = \text{Diag}(e^{j\varphi_1}, e^{j\varphi_2}, \ldots, e^{j\varphi_{N_R}})$ is the phase shifts applied by the RIS, where $\varphi_n \in (0, 2\pi)$ is phase shift of reflecting element for $n = 1, 2, \ldots, N_R$.

Define $H_{RS} \in \mathbb{C}^{N_R \times N_S}$ as the channel complex matrix between $R$ and $S$. $w_1 \in \mathbb{C}^{N_S \times 1}$ denotes signal beamformer. $w_2 \in \mathbb{C}^{N_S \times 1}$ denotes noise beamformer, which can be obtained by algorithm 2 in [30] by projecting AN into the null space of $U_2$. $P_U$ and $P_j$ indicate the transmit power of data signal and AN, respectively. $\alpha \in (0, 0.5)$ represents power allocation factor of $U_1$ and $U_2$. $n_1 \in \mathbb{C}^{N_0}$ ($N_0$) is the additive white Gaussian noise (AWGN) with zero mean and variance $N_0$ at $U_1$, and $n_2 \in \mathbb{C}^{N_0}$ ($N_0$) is the AWGN at $U_2$. $x_1$ and $x_2$ are the data sent to $U_1$ and $U_2$, respectively. $x_j$ is AN signal. CSI is considered to be estimable in this paper.

Moreover, the FU is allocated to the channel null space of the AN, namely $h^H_{RU_1} \Phi H_{RS} w_2 = 0$. Therefore, the signal received by $U_2$ is rewritten as

$$ y_2 = h^H_{RU_2} \Phi H_{RS} w_1 \left( \sqrt{(1-\alpha)} P_U x_1 + \sqrt{\alpha P_U} x_2 \right) + n_2 $$

Herein, the order of SIC has been adjusted. NU obtains its own information through treating the information of FU and AN as noise. Then, NU tries to decode the information of FU with AN as interference. FU decodes its own information by deleting NU signal from the received signal. $Y_{1,x_j}$ denotes the received signal-to-noise (SNR) ratio of information $x_j$ at
user $U_i$ where $i, j \in \{1, 2\}$. Therefore, the SNR at $U_1$ and $U_2$ can be written as

$$\Upsilon_{1,x_1} = \frac{\|H_{RU_1}^H \Phi H_{RSU_1}\|^2 (1 - \alpha) P_U}{\|H_{RU_1}^H \Phi H_{RSU_1}\|^2 \alpha P_U + \|H_{RU_1}^H \Phi H_{RSU_2}\|^2 P_J + N_0},$$

(4)

$$\Upsilon_{1,x_2} = \frac{\|H_{RU_1}^H \Phi H_{RSU_1}\|^2 \alpha P_U}{\|H_{RU_1}^H \Phi H_{RSU_2}\|^2 P_J + N_0},$$

(5)

$$\Upsilon_{2,x_2} = \frac{\|H_{RU_1}^H \Phi H_{RSU_2}\|^2 \alpha P_U}{N_0}. \quad (6)$$

According to (5) and (6), the secrecy rate $C_S$ can be derived as

$$C_S = \max \{0, \log_2 (1 + \Upsilon_{2,x_2}) - \log_2 (1 + \Upsilon_{1,x_2})\} = \max \left\{0, \log_2 \left(1 + \frac{\|H_{RU_2}^H \Phi H_{RSU_1}\|^2 \alpha P_U}{\|H_{RU_1}^H \Phi H_{RSU_1}\|^2 \alpha P_U + \|H_{RU_1}^H \Phi H_{RSU_2}\|^2 P_J + N_0}\right) \right\}. \quad (7)$$

III. POSITIVE SECRECY RATE

The beamforming technology is adopted to improve the comprehensive channel gain of $U_2$. The locally optimal solution of $\|H_{RU_2}^H \Phi H_{RSU_1}\|$ had been obtained using Algorithm 1 in [30]. When $\|H_{RU_1}^H \Phi H_{RSU_1}\| > \|H_{RU_1}^H \Phi H_{RSU_2}\|$, we can get $C_S > 0$ even if $P_J = 0$. Therefore, a positive secrecy rate can be obtained.

However, when the channel condition of NU is far better than that of FU, the case of $\|H_{RU_1}^H \Phi H_{RSU_1}\| < \|H_{RU_1}^H \Phi H_{RSU_2}\|$ still has a certain possibility to happen, and a positive secrecy rate cannot be guaranteed if $P_J = 0$.

From (7), it is easy to find that the positive secrecy rate can be got after satisfying

$$1 + \frac{\|H_{RU_2}^H \Phi H_{RSU_1}\|^2 \alpha P_U}{\|H_{RU_1}^H \Phi H_{RSU_1}\|^2 \alpha P_U + \|H_{RU_1}^H \Phi H_{RSU_2}\|^2 P_J + N_0} > 1. \quad (8)$$

Formula (8) can be transformed into

$$P_J > \frac{N_0 \|H_{RU_1}^H \Phi H_{RSU_2}\|^2}{\|H_{RU_1}^H \Phi H_{RSU_1}\|^2 \|H_{RU_1}^H \Phi H_{RSU_2}\|^2} \triangleq P_{J,th}. \quad (9)$$

For convenience, we define the right side of (9) as $P_{J,th}$. Therefore, $C_S > 0$ when $P_J > P_{J,th}$ holds. A positive secrecy rate can always be obtained by adjusting $P_J$ even if $\|H_{RU_2}^H \Phi H_{RSU_1}\| < \|H_{RU_1}^H \Phi H_{RSU_1}\|$. It can be observed from Table 1, our scheme is effective to guarantee the positive secrecy rate for RIS-aided NOMA system, and it has higher robustness than [30]. In addition, in order to make full use of the benefits of scheme, power allocation should be further studied.

IV. POWER OPTIMIZATION

According to the previous part, the positive secrecy rate can always be obtained if providing sufficient power, and power allocation will affect the performance of system. Therefore, in this section, we will study the power allocation of base station.

In order to guarantee the communication quality and communication security quality of the system, the data rate of $U_1$, the data rate of $U_2$, and the secrecy rate are needed to be satisfied thresholds $C^{S}_{U_1}$, $C^{D}_{U_2}$ and $C^{S}_{th}$, respectively. Therefore, the power optimization problem can be given as

$$\min_{\alpha, P_U, P_J, \Phi, w_1} \begin{cases} \alpha, P_U, P_J, \Phi, w_1 \quad \text{subject to} \quad \begin{cases} C_S \geq C_{th} \\ \log_2 (\Upsilon_{1,x_1} + 1) \geq C^{D}_{U_1} \\ \log_2 (\Upsilon_{2,x_2} + 1) \geq C^{D}_{U_2} \\ P_U, P_J \geq 0 \end{cases} \end{cases}. \quad (10)$$

Due to the complexity of the objective function, it is difficult to obtain the global optimal solution. We use a sub-optimal algorithm to solve this problem, which can effectively improve the security performance of the system. The problem can be divided into two steps.

The first step: we use the alternating optimization algorithm of [30] to maximize $h_2 = \|H_{RU_2}^H \Phi H_{RSU_1}\|^2$, $\Phi$ and $w_1$ can be determined.

The second step: let $h_1 = \|H_{RU_1}^H \Phi H_{RSU_1}\|^2$, $h_2 = \|H_{RU_2}^H \Phi H_{RSU_2}\|^2$, and substituting (4), (6) and (7) into (10) yields

$$\min_{\alpha, P_U, P_J} \begin{cases} \alpha, P_U, P_J \quad \text{subject to} \quad \begin{cases} 1 + \frac{h_1 P_U + h_2 P_J}{\frac{1}{h_1 (1 - \alpha)} + \frac{1}{h_2 P_J + N_0}} \geq 2 C^{S}_{th} \\ \frac{h_1 (1 - \alpha) P_U}{h_1 (1 - \alpha) P_U + h_2 P_J + N_0} \geq 2 \delta C^{D}_{U_1} - 1 \\ \frac{h_2 P_J}{h_2 P_J + N_0} \geq 2 \delta C^{D}_{U_2} - 1 \end{cases} \end{cases}. \quad (11)$$

To reduce the complexity of the optimization problem, we first study the relaxation states of the constraints. Then, we found that the first and second constraints take the equal sign when the problem is optimal. The method of reduction to absurdity is used to proof.

Relaxed state of the first constraint in (10)

Proof:

Assuming that the optimal value of the objective function is established when the inequality of the first constraint holds, the optimal solution is $\{\alpha^*, P_U^*, P_J^*\}$, and which satisfies

$$\{\alpha^*, P_U^*, P_J^*\} = \arg \min_{\alpha, P_U, P_J} \begin{cases} \alpha, P_U, P_J \quad \text{subject to} \quad \begin{cases} 1 + \frac{h_2 P_J}{\frac{1}{h_1 (1 - \alpha)} + \frac{1}{h_2 P_J + N_0}} \geq 2 C^{S}_{th} \\ \frac{h_1 (1 - \alpha) P_U}{h_1 (1 - \alpha) P_U + h_2 P_J + N_0} \geq 2 \delta C^{D}_{U_1} - 1 \\ \frac{h_2 P_J}{h_2 P_J + N_0} \geq 2 \delta C^{D}_{U_2} - 1 \end{cases} \end{cases}. \quad (12)$$

$P_U^*, P_J^* \geq 0$
There must be $\Delta > 0$ satisfying

$$\frac{1 + \frac{h_2 \alpha P_{i,j}^\circ}{\delta h} + \frac{h_1 (1 - \alpha) P_{i,j}^\circ}{\delta P_{i,j}^\circ}}{1 + \frac{h_2 \alpha P_{i,j}^\circ}{\delta h} + \frac{h_1 (1 - \alpha) P_{i,j}^\circ}{\delta P_{i,j}^\circ}} \geq 2 C_{th}^D,$$

and let $P_{j}^\bullet = P_{j}^\circ - \Delta$. Moreover, we can easily find that the solution $\{\alpha^\circ, P_{U}^\circ, P_{j}^\circ\}$ satisfies

$$\begin{aligned}
\frac{1 + \frac{h_2 \alpha P_{i,j}^\circ}{\delta h} + \frac{h_1 (1 - \alpha) P_{i,j}^\circ}{\delta P_{i,j}^\circ}}{1 + \frac{h_2 \alpha P_{i,j}^\circ}{\delta h} + \frac{h_1 (1 - \alpha) P_{i,j}^\circ}{\delta P_{i,j}^\circ}} & \geq 2 C_{th}^D, \\
\frac{h_1 \alpha P_{i,j}^\circ + h_1 P_{j}^\circ + N_0}{h_2 \alpha P_{i,j}^\circ + N_0} & \geq 2 C_{th}^D - 1.
\end{aligned}$$

Obviously, the objective function is an increasing function to $P_{U}^\circ$, and $P_{U}^\circ + P_{j}^\Delta < P_{U}^\circ + P_{j}^\Delta$, which contradicts the optimality of $\{\alpha^\Delta, P_{U}^\Delta, P_{j}^\Delta\}$. Therefore, when the problem achieves the optimal value, the second constraint takes the equal sign.

Proof end.

Relaxed state of the second constraint in (10)

Proof:

Similarly, assuming that the optimal value of the objective function is established when the inequality of the second constraint holds, the optimal solution is $\{\alpha^\Delta, P_{U}^\Delta, P_{j}^\Delta\}$, and which satisfies

$$\{\alpha^\Delta, P_{U}^\Delta, P_{j}^\Delta\} = \arg\min_{\alpha, P_{U}^\circ, P_{j}} P_{U} + P_{j} \quad \text{s.t.} \quad \frac{1 + \frac{h_2 \alpha P_{i,j}^\circ}{\delta h} + \frac{h_1 (1 - \alpha) P_{i,j}^\circ}{\delta P_{i,j}^\circ}}{1 + \frac{h_2 \alpha P_{i,j}^\circ}{\delta h} + \frac{h_1 (1 - \alpha) P_{i,j}^\circ}{\delta P_{i,j}^\circ}} \geq 2 C_{th}^D - 1.$$ (14)

There must be $\delta > 0$ satisfying

$$\frac{h_1 (1 - \alpha) P_{i,j}^\circ - \delta}{h_1 \alpha P_{i,j}^\circ + h_1 P_{j}^\circ + N_0} \geq 2 C_{th}^D - 1,$$

and let $P_{U}^\circ = P_{U}^\Delta - \delta$. Therefore, we can easily find that $P_{U}^\circ = P_{U}^\Delta - \delta$. Therefore, we can easily find that $\{\alpha^\circ, P_{U}^\circ, P_{j}^\circ\}$ satisfies

$$\begin{aligned}
\frac{1 + \frac{h_2 \alpha P_{i,j}^\circ}{\delta h} + \frac{h_1 (1 - \alpha) P_{i,j}^\circ}{\delta P_{i,j}^\circ}}{1 + \frac{h_2 \alpha P_{i,j}^\circ}{\delta h} + \frac{h_1 (1 - \alpha) P_{i,j}^\circ}{\delta P_{i,j}^\circ}} & = 2 C_{th}^D, \\
\frac{h_1 \alpha P_{i,j}^\circ + h_1 P_{j}^\circ + N_0}{h_2 \alpha P_{i,j}^\circ + N_0} & \geq 2 C_{th}^D - 1.
\end{aligned}$$

Obviously, the objective function is an increasing function to $P_{U}^\circ$, and $P_{U}^\circ + P_{j}^\Delta < P_{U}^\circ + P_{j}^\Delta$, which contradicts the optimality of $\{\alpha^\Delta, P_{U}^\Delta, P_{j}^\Delta\}$. Therefore, when the problem achieves the optimal value, the second constraint takes the equal sign.

Proof end.

According to the first and second constraint states, the problem (11) can be transformed into

$$\min_{\alpha, P_{U}^\circ, P_{j}} P_{U} + P_{j} \quad \text{s.t.} \quad \begin{aligned}
\frac{1 + \frac{h_2 \alpha P_{i,j}^\circ}{\delta h} + \frac{h_1 (1 - \alpha) P_{i,j}^\circ}{\delta P_{i,j}^\circ}}{1 + \frac{h_2 \alpha P_{i,j}^\circ}{\delta h} + \frac{h_1 (1 - \alpha) P_{i,j}^\circ}{\delta P_{i,j}^\circ}} & = 2 C_{th}^D, \\
\frac{h_1 \alpha P_{i,j}^\circ + h_1 P_{j}^\circ + N_0}{h_2 \alpha P_{i,j}^\circ + N_0} & \geq 2 C_{th}^D - 1.
\end{aligned}$$ (16)

According to (16), the objective function can be transformed into a function of $\alpha$, and we define it as

$$\varphi(\alpha) = N_0 \left(\frac{-2 \alpha^D_1 \alpha + (-\alpha + 1) 2 \alpha^s_1 + 2 \alpha^s_1 \alpha + 2 \alpha^s_1 \alpha - 1}{\alpha \left(2 \alpha^D_1 \alpha + 1\right)^{-1} + (-h_1 \alpha (\alpha - 3) 2 \alpha^s_1 + C_{th}^D + 1) + 2 \alpha^s_1 \alpha h_1 + 4 \alpha^s_1 + 2 \alpha^s_1 + C_{th}^D - 1 \alpha - \alpha^2 (h_1 + h_2) 4 \alpha^s_1 - h_1 \alpha (\alpha - 1) + \alpha h_2 - h_1 \right) \times \left(\alpha \left(2 \alpha^D_1 \alpha + 1\right)^{-1}\right).$$ (17)

We temporarily neglect the third constraint, and the optimal value of $\alpha$ called $\alpha_I$ can be obtained by taking a derivative with respect to $\alpha$ from $\varphi(\alpha)$ and making the derivative equal to zero. In addition, substituting $\alpha_I$ into (16), then according to the first and second constraints, the optimal solutions of $P_{U}^\circ$ and $P_{j}^\circ$ are obtained called $P_{U,I}$ and $P_{j,I}$, respectively. Solutions are shown in (18).
Based on the above discussion, a closed-form solution of power optimization can be obtained, which is as follows:

\[
\begin{align*}
P_{U,II} &= N_0 \left(-2C_{U}^P \alpha_I + (\alpha_I - 1) 2C_{th}^S + 1\right) \\
& \quad \times \left(\alpha_I h_2 \left(2C_{U}^P \alpha_I + 1\right)\right)^{-1} \\
\end{align*}
\]

\[
\begin{align*}
P_{J,II} &= \left(-h_1 \alpha_I (\alpha_I - 1)^2 2C_{th}^S + C_{D}^P + 2^3 C_{th}^P \alpha_I h_1 + 4C_{th}^S + C_{U}^P\right) \\
& \quad \times \left(h_1 + 1\right) 2C_{U}^P + h_1 (\alpha_I - 1) 2C_{th}^S - \alpha_I h_2 + h_1 \right) N_0 \\
& \quad \times \left(h_1 \left(2C_{U}^P - 1\right) \alpha_I h_2 \left(2C_{U}^P \alpha_I - 1\right)\right)^{-1}.
\end{align*}
\]

(18)

If \( \{\alpha_I, P_{U,II}, P_{J,II}\} \) do not satisfy the third constraint in (9), the optimal solution can be obtained when the third constraint’s equality holds. In this case, \( 2C_{U}^P > \Psi \left(C_{th}^S, C_{D}^P, C_{U}^P\right) \), which is shown as (19).

\[
\begin{align*}
\Psi \left(C_{th}^S, C_{U}^P\right) &= \left(2C_{th}^S \left(h_1 \left(-2^1+2C_{th}^S+2C_{U}^P h_1\right) \\
& \quad + 32C_{th}^S+2C_{U}^P h_1+h_j \left(h_1 8C_{th}^P - h_1 + h_j\right) 2C_{th}^P + C_{U}^P\right) \\
& \quad + 2^1+C_{th}^S \left(4C_{U}^P h_j - h_1 16C_{th}^P\right) - \left(2^2C_{th}^S - 4C_{th}^P\right) \\
& \quad \times \left(h_1 - 3h_j 8C_{th}^P - 3h_j 2C_{th}^S + 4C_{U}^P + \left(16C_{th}^P + h_j + \left(h_1 - 1\right) 2C_{th}^P + 1\right)\right)^{1/2} \\
& \quad \times \left(-C_{th}^S + 2C_{U}^P\right) + \left(\left(-h_j + h_1\right) 2C_{U}^P + h_1 (\alpha_I - 1) 2C_{th}^S - \alpha_I h_2 + h_1\right) \\
& \quad \times \left(h_1 \left(2C_{U}^P - 1\right) \alpha_I h_2 \left(2C_{U}^P \alpha_I - 1\right)\right)^{-1}.
\end{align*}
\]

(19)

Then, the minimum value of \( \alpha, P_U \) and \( P_J \) can be given by combining the three constraint equations, and called \( \alpha_{II} \), \( P_{U,II} \) and \( P_{J,II} \), respectively. Solutions are shown in (20).

\[
\begin{align*}
\alpha_{II} &= \left(2C_{U}^P - 2C_{th}^S\right) \left(2C_{U}^P v_1 2C_{U}^P - 2C_{th}^S\right) \\
P_{U,II} &= N_0 \left(-2C_{U}^P \alpha_{II} + (\alpha_{II} - 1) 2C_{th}^S + 1\right) \\
& \quad \times \left(\alpha_{II} h_2 \left(2C_{U}^P \alpha_{II} + 1\right)\right)^{-1} \\
P_{J,II} &= \left(-h_1 \alpha_{II} (\alpha_{II} - 1)^2 2C_{th}^S + C_{D}^P - 2^1+C_{th}^P \alpha_{II} h_1 + 4C_{th}^S + C_{U}^P\right) \\
& \quad \times \left(h_1 + 1\right) 2C_{U}^P + (\alpha_{II} - 1) 2C_{th}^S - \alpha_{II} h_2 + h_1 \right) N_0 \\
& \quad \times \left(h_1 \left(2C_{U}^P - 1\right) \alpha_{II} h_2 \left(2C_{U}^P \alpha_{II} - 1\right)\right)^{-1}.
\end{align*}
\]

(20)

V. SIMULATION RESULTS

In this part, the simulation results are presented to verify the performance of our algorithm. Set \( N_0 = 0dBm \). Let \( C_{U1} = C_{U2} = 1bps/Hz \). To conform to actual communications, all of channels are set as Rician fading channels with a Rician factor \( K_{ad} = 10 \) as in [30]. We illustrate the simulation model as Fig. 2, and suppose the position of \( S \) is \((0, 0)\), the position of \( R \) is \((1, 0.5)\), the position of \( U_1 \) is \((2, 0)\), and the position of \( U_2 \) is \((3, 0)\), i.e., \( d_{R} = 0.5, d_{R_{u_1}} = 1, d_{U_1} = 2 \) and \( d_{U_2} = 3 \). The relationship between the secrecy rate and the total power is shown in Fig. 3.

We used a simulation model similar to [30]. The curve of the algorithm in [30] is also presented with \( N_S = 16 \) and
Fig. 2. Simulation model.

Fig. 3. Total power consumption under different security rates.

Fig. 4. Total power consumption against $d_{U_1}$ with $d_{U_2} = 3$.

Fig. 5. Secrecy Outage Probability against $d_{U_1}$ with $d_{U_2} = 3$.

$N_R = 16$. From Fig. 3, we can find that the proposed method costs less power under the same condition, highlighting the effectiveness of our design. We can also observe that different $N_S$ and $N_R$ have different curves, and as the number of both increase, the total power of the system increases. Moreover, the curve of $N_S = 8$ while $N_R = 16$ is obviously better than the curve of $N_S = 16$ while $N_R = 8$, we can get that the number of RIS has a greater impact on system performance gain than the number of antennas of $S$.

In addition, there is a relationship between the total power consumption and the position of node. The data rate requirements of user will affect the total power of the entire system. In order to make a comparison, we simulate the total power under the different data rates as shown in Fig. 4. Let $U_1$ move freely on the right side of $R$ until it approaches $U_2$.

From Fig. 4 we can see that when $U_1$ approaches $U_2$, the total power consumption of the system increases. Moreover, when $d_{U_1} > 2$, the total power of the system is close to stable. The total power consumption of $C_{U_1} = C_{U_2} = 1$ is the largest in the three cases, and the total power consumption of $C_{U_1} = 0.5$ is more than the total power consumption of $C_{U_2} = 0.5$. From this we can conclude that the increase of $C_{U_2}$ consumes more power than the increase of $C_{U_1}$ under the same circumstances. Therefore, the path loss has a greater impact on $FU$, and it is necessary to align the signal with $U_2$ by beamforming design. When the NU is far enough from the base station, the probability of $h_2 > h_1$ is very high, so the security of the system is easily guaranteed and the total power also tends to stabilize.

The secrecy outage probability against $d_{U_1}$ with $d_{U_2} = 3$ under the different total power constraint $P_T$ are shown in Fig. 5. We can see that the secrecy rate of our proposed algorithm is better than that of [30], and obviously algorithm of [30] needs more power to guarantee positive secrecy rate. Moreover, when $U_1$ is close to RIS, the secrecy of the system cannot be guaranteed even if enough power is given in [30]. There is little difference between the two algorithms when giving algorithm of [30] enough power, but proposed algorithm is still excellent in energy efficiency. Moreover,
as the channel of $U_1$ becomes worse due to the distance increases, the security is greatly increased when the power is limited. Therefore, we can infer that even if $U_1$ becomes a "FU", the algorithm in this paper is still applicable to improve system security.

VI. CONCLUSION

In this paper, we have studied the PLS design of the RIS-aided NOMA system based on AN and beamforming to against the internal eavesdropping. It is proved theoretically that a positive secrecy rate can always be obtained if providing sufficient power. Moreover, a power allocation optimization problem has been established to improve the system power efficiency, and the closed-form solutions are achieved. Simulation results show that the performance of the proposed scheme is superior to the solution in [30]. The algorithm can still improve the security of the system when the positions of two users are exchanged. In addition, the scenario of NU and FU eavesdropping on each other is not considered in this article, which will be a direction of our work in the future.

REFERENCES

[1] T. Hou, Y. Liu, Z. Song, X. Sun, Y. Chen and L. Hanzo, “Reconfigurable Intelligent Surface Aided NOMA Networks,” IEEE J. Sel. Areas Commun., vol. 38, no. 11, pp. 2575–2588, Nov. 2020.

[2] A. A. Khansa, Y. Yin, G. Gui and H. Sari, “Power-Domain NOMA or NOMA-2000?,” in Proc. 2019 25th Asia-Pacific Conf. on Communications (APCC), Ho Chi Minh City, Vietnam, 2019, pp. 336–341.

[3] J. Zeng et al., “Investigation on Evolving Single-Carrier NOMA Into Multi-Carrier NOMA in 5G,” IEEE Access, vol. 6, pp. 48268–48288, 2018.

[4] C. Zhang, F. Jia, Z. Jiang, J. Ge and F. Gong, “Physical Layer Security Designs for 5G NOMA Systems With A Stronger Near-End Internal Eavesdropper,” IEEE Trans. Veh. Technol., vol. 69, no. 11, pp. 13005–13017, Nov. 2020.

[5] Liu, Tianqi, Han, et al., “Dynamic power allocation scheme with clustering based on physical layer security,” IET Commun., 2018, 12, 2546–2551.

[6] Lv G, X Li, Xue P, et al., “Outage analysis and optimisation of NOMA-based amplify-and-forward relay systems,” IET Commun., 2021, 15, 410–420.

[7] J. Cao, B. Wang, H. Ding, T. Li, and F. Gong, “Optimal relay selection for secure NOMA systems under limited power,” in Proc. IEEE Global Commun. Conf. (GLOBECOM), Dec. 2018, pp. 1–6.

[8] Y. Liu, Z. Qin, M. Elkashtan, Z. Ding, A. Nallanathan, and L. Hanzo, “Nonorthogonal multiple access for 5G and beyond,” in Proc. of the IEEE, vol. 105, no. 12, pp. 2347–2381, 2017.

[9] Z. Ding and H. Vincent Poor, “A Simple Design of IRS-NOMA Transmission,” IEEE Commun. Lett., vol. 24, no. 5, pp. 1119–1123, May 2020.

[10] H. Wang, C. Liu, Z. Shi, Y. Fu and R. Song, “On Power Minimization for IRS-Aided Downlink NOMA Systems,” IEEE Wireless Commun. Lett., vol. 9, no. 11, pp. 1808–1811, Nov. 2020.

[11] Z. Ding and H. Vincent Poor, “A Simple Design of IRS-NOMA Transmission,” IEEE Commun. Lett., vol. 24, no. 5, pp. 1119–1123, May 2020.

[12] Z. Zhang, L. Lv, Q. Wu, H. Deng and J. Chen, “Covert Communication in Intelligent Reflecting Surface-Assisted NOMA Systems: Design, Analysis, and Optimization,” IEEE Trans. Wireless Commun., 2021.

[13] B. M. ElHalawany and K. Wu, “Physical-layer security of NOMA systems: A comprehensive survey,” IEEE Commun. Surveys Tuts., pp. 1–1, 2018.

[14] B. M. ElHalawany and K. Wu, “Physical-layer security of NOMA systems: A comprehensive survey,” IEEE Commun. Surveys Tuts., pp. 1–1, 2018.

[15] Z. Ding and H. Vincent Poor, “A Simple Design of IRS-NOMA Transmission,” IEEE Commun. Lett., vol. 24, no. 5, pp. 1119–1123, May 2020.

[16] H. Wang, C. Liu, Z. Shi, Y. Fu and R. Song, “On Power Minimization for IRS-Aided Downlink NOMA Systems,” IEEE Wireless Commun. Lett., vol. 9, no. 11, pp. 1808–1811, Nov. 2020.

[17] Z. Zhang and H. Ding, “Energy-Efficient Design of IRS-NOMA Networks,” IEEE Trans. Veh. Technol., vol. 69, no. 11, pp. 14088–14092, Nov. 2020.

[18] S. Jiao, F. Fang, X. Zhou and H. Zhang, “Joint Beamforming and Phase Shift Design in Downlink UAV Networks with IRS-Assisted NOMA,” J. Commun. Inf. Networks, vol. 5, no. 2, pp. 138–149, June 2020.

[19] X. Tao, Y. Chen, X. Yang, and L. Guo, “Optimal Relay Selection for Secure Transmission in IRS-NOMA Systems,” IEEE Trans. Veh. Technol., vol. 69, no. 7, pp. 6468–6479, Nov. 2020.

[20] Z. Ding and H. Vincent Poor, “A Simple Design of IRS-NOMA Transmission,” IEEE Commun. Lett., vol. 24, no. 5, pp. 1119–1123, May 2020.

[21] Z. Ding and H. Vincent Poor, “A Simple Design of IRS-NOMA Transmission,” IEEE Commun. Lett., vol. 24, no. 5, pp. 1119–1123, May 2020.

[22] Z. Ding and H. Vincent Poor, “A Simple Design of IRS-NOMA Transmission,” IEEE Commun. Lett., vol. 24, no. 5, pp. 1119–1123, May 2020.

[23] Z. Ding and H. Vincent Poor, “A Simple Design of IRS-NOMA Transmission,” IEEE Commun. Lett., vol. 24, no. 5, pp. 1119–1123, May 2020.

[24] Z. Ding and H. Vincent Poor, “A Simple Design of IRS-NOMA Transmission,” IEEE Commun. Lett., vol. 24, no. 5, pp. 1119–1123, May 2020.

[25] Z. Ding and H. Vincent Poor, “A Simple Design of IRS-NOMA Transmission,” IEEE Commun. Lett., vol. 24, no. 5, pp. 1119–1123, May 2020.
CHENSI ZHANG (Member, IEEE) received the B.S. and Ph.D. degrees in telecommunications engineering from Xidian University, Xi’an, China, in 2010 and 2015, respectively.

He currently is an Associate Professor with the State Key Laboratory of Integrated Services Networks, School of Telecommunications Engineering, Xidian University. His research interests include deep learning, wireless sensing, cooperative communications, green communications, the key technology of 6G communication-sensing-computing integration, nonorthogonal multiple access (NOMA), reconfigurable intelligent surface and physical layer security. He is a member of IEEE.

PEILI HAO received the B.E. degree in communication engineering from North University of China, Taiyuan, China, in 2019.

She is currently pursuing the master’s degree with the School of Telecommunications Engineering, Xidian University, Xi’an, China. Her research interests include physical layer security and signal processing for massive MIMO systems.

ZHE ZHANG received the B.S. in Mathematics from Xidian University, Xi’an, China, in 2019.

He currently pursue the master’s degree in School of Telecommunications Engineering, Xidian University. He is very interested in system design and the performance analysis of wireless communication systems. His research interests include 5G wireless networks, nonorthogonal multiple access (NOMA), reconfigurable intelligent surface and cooperative communications.

JIANHUA GE received the Ph.D. degree from the School of Telecommunications Engineering, Xidian University, Xi’an, China, in 1990.

He is currently a Professor and the Deputy Director of the State Key Laboratory of Integrated Services Networks, School of Telecommunications Engineering, Xidian University. He has worked on digital television (DTV) standardization as a DTV technical expert. His research interests include digital communications, digital video broadcasting, performance enhancement techniques for 4G/5G cellular communication systems.

***