entropy

MDPI

Article

Secure User Pairing and Power Allocation for Downlink Non-Orthogonal Multiple Access against External Eavesdropping

Yuxuan Li, Yanqiu Chen and Xiaopeng Ji *

School of Electronics and Information Engineering, Nanjing University of Information Science and Technology, Nanjing 210044, China

* Correspondence: jixiaopeng@nuist.edu.cn or jixiaopeng_nj@163.com

Abstract: We propose a secure user pairing (UP) and power allocation (PA) strategy for a downlink Non-Orthogonal Multiple Access (NOMA) system when there exists an external eavesdropper. The secure transmission of data through the downlink is constructed to optimize both UP and PA. This optimization aims to maximize the achievable sum secrecy rate (ASSR) while adhering to a limit on the rate for each user. However, this poses a challenge as it involves a mixed integer nonlinear programming (MINLP) problem, which cannot be efficiently solved through direct search methods due to its complexity. To handle this gracefully, we first divide the original problem into two smaller issues, i.e., an optimal PA problem for two paired users and an optimal UP problem. Next, we obtain the closed-form optimal solution for PA between two users and UP in a simplified NOMA system involving four users. Finally, the result is extended to a general 2*K*-user NOMA system. The proposed UP and PA method satisfies the minimum rate constraints with an optimal ASSR as shown theoretically and as validated by numerical simulations. According to the results, the proposed method outperforms random UP and that in a standard OMA system in terms of the ASSR and the average ASSR. It is also interesting to find that increasing the number of user pairs will bring more performance gain in terms of the average ASSR.

Keywords: user pairing; power allocation; NOMA; external eavesdropping; secure communication

Citation: Li, Y.; Chen, Y.; Ji, X. Secure User Pairing and Power Allocation for Downlink Non-Orthogonal Multiple Access against External Eavesdropping. *Entropy* **2024**, *26*, 64. https://doi.org/10.3390/e26010064

Academic Editor: Chintha Tellambura

Received: 21 November 2023
Revised: 6 January 2024
Accepted: 10 January 2024
Published: 11 January 2024

1. Introduction

Over the past decade, NOMA has garnered considerable attention owning to its possibility to enhance spectrum efficiency and capacity by serving a cluster of users over the same resource block [1–5], and has been conceived as a technology with great promise, facilitating fifth-generation (5G) wireless communication [6,7] and serving as a potential foundation for the next generation of multiple access in 6G [8].

While NOMA can yield considerable performance improvements, it faces notable challenges that jeopardize its secure transmission. Specifically, wiretapping is one of a variety of security and confidentiality concerns because of the inherently broadcast nature of the wireless communication and successive interference cancellation (SIC) adopted in NOMA [9]. Therefore, the establishment of secure transmission in NOMA networks has garnered significant interest from academic and industrial spheres alike.

To address these challenging security issues, the concept of physical layer security (PLS) aims to safeguard authentic communication via leveraging the diversity present in physical communication channels through an informational–theoretical lens [10], and various PLS approaches have been proposed to guarantee secure transmission in NOMA networks [11–15]. The work in [11] considered a cognitive radio network employing NOMA with two cells and multiple inputs and outputs, and presented a sequential transmission method employing zero-force beamforming to safeguard communications against potential eavesdropping. The work in [12] proposed a beamforming scheme with the assistance of artificial noise (AN) to maximize the secrecy sum rate (SSR) in an NOMA system.

In [13], the proposed method employed unmanned aerial vehicle (UAV) assistance in NOMA transmission to ensure secure downlink communication by employing artificial jamming, and the exploration of the balance between jamming effectiveness and the total data transmission rate was examined to optimize power distribution, user scheduling, and the UAV's path, aiming to achieve a trade-off that harmonizes security and transmission efficiency. The work in [14] analyzed secure downlink transmission schemes in an NOMA system with artificial-signal assistance and relay assistance and found equilibrium strategies using game theory. Additionally, in recent years, intelligent reflecting surfaces (IRSs) also show potential in enhancing the security of the foundational layer within wireless networks. This was achieved via mitigating the reflected signal at potential eavesdroppers while directing the beam towards authorized receivers through the adjustment of the IRS reflecting elements [15].

Although numerous initial studies have delved into the security aspects of NOMA networks through the lens of beamforming, artificial noise, UAV, IRS, etc., they mainly focus on NOMA systems with two or more users sharing one resource block. However, in future scenarios with massive connections, the decoding complexity and delay of the proposed schemes in the existing literature will increase, and additional hardware resources will be necessary [9,16]. Therefore, NOMA users should be categorized into distinct groups to balance implementation complexity and resource utilization [17]. User pairing to satisfy some system performance indicators, such as achievable sum rates and spectral efficiency, has been investigated in works such as [18–21]. However, as far as we are aware, how to improve secure performance gains via UP has not been investigated thoroughly, and this motivated us to study the secure strategies combined with user pairing. We explore the challenge of UP under the condition of a minimum rate constraint of each authorized user to maximize the ASSR, which results in MINLP. Then, we decompose the MINLP problem into two sub-problems, optimal UP and PA, and obtain an optimal solution for UP and PA in a closed-form globally. Ultimately, through the comparison of the ASSR acquired using the proposed method against those generated by the standard methods, the outcomes from the simulation indicate that the suggested method surpasses both the randomly paired approach with optimal power distribution and the Orthogonal Multiple Access (OMA) configuration in identical channel conditions.

The rest of this paper is structured as follows. In Section 2, a downlink NOMA system with an external eavesdropper is presented, and the joint optimization of an achievable sum secrecy rate is formulated and decomposed into two sub-problems, optimal power allocation and optimal user pairing. We investigate the two sub-problems and obtain the closed-form solutions in Sections 3 and 4, respectively. Numerical simulations are conducted and the outcomes are given in Section 5, followed by the conclusions, which are outlined in Section 6.

2. System Model and Problem Formulation

2.1. System Model

We investigate a downlink NOMA system utilizing one base station (BS), $N = 2K$ legitimate users, and one external eavesdropper (E), as illustrated in Figure 1. We presume that each node is equipped with a single antenna, as in [16,19,20,22], all wireless channels include Rayleigh block fading [16,22,23], and the communication channel gains from the base station to the legitimate user i (denoted by LU_i) and the eavesdropper are denoted by h_i, $(i = 1, 2, \cdots, 2K)$, and h_e. Generally, we make the assumption that the channel gains of $2K$ users adhere to the sequence $|h_1|^2 \leq |h_2|^2 \leq \cdots \leq |h_k|^2 \leq \cdots \leq |h_{2K}|^2$. We also presume that both users and the eavesdropper experience equivalent levels of noise power, denoted as σ^2.

In practice, $2K$ legitimate users are often grouped into K clusters, i.e., each cluster has two users, aiming to minimize the computational complexity and mitigate delays caused by the successive interference cancellation (SIC) being decoded at the receiver [17].

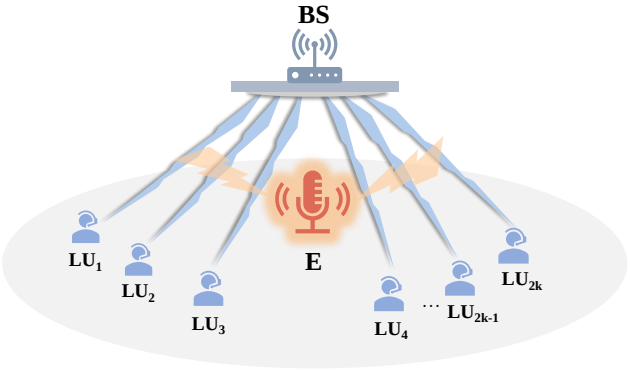

Figure 1. Illustration of the considered system model.

For any pair with two users (users m and n) denoted by (m and n), a constant total transmission power P_s is allocated by the BS. Without a loss of generality, we make the assumption of $|h_m|^2 \geq |h_n|^2$, i.e., the user m is a strong user in NOMA terminology. Then, the superimposed signal transmitted by the BS is

$$s = \sqrt{P_s \alpha_m} s_m + \sqrt{P_s \alpha_n} s_n, \tag{1}$$

where s_i and α_i ($i = m, n$) denote the signal with $\mathbb{E}(|s_i|^2) = 1$ and the PA factor of user i with $\alpha_m + \alpha_n = 1$.

The signals received by users m, n, and the eavesdropper E are

$$\begin{cases} y_m = h_m(\sqrt{P_s \alpha_m} s_m + \sqrt{P_s \alpha_n} s_n) + n_m, \\ y_n = h_n(\sqrt{P_s \alpha_m} s_m + \sqrt{P_s \alpha_n} s_n) + n_n, \\ y_e = h_e(\sqrt{P_s \alpha_m} s_m + \sqrt{P_s \alpha_n} s_n) + n_e, \end{cases} \tag{2}$$

where n_i represents the Gaussian noise that user i and eavesdropper E encounter, which has a mean of zero and an average power of σ^2.

Following the NOMA guideline, the strong user m exploits SIC to remove the interference caused by the weak user n, while the weak user n treats the interference caused by the user m as noise. Thus, the achievable rates of users m and n are provided as follows:

$$R_{nn} = \log_2 \left(1 + \frac{|h_n|^2 \alpha_n \gamma}{|h_n|^2 \alpha_m \gamma + 1} \right), \tag{3}$$

$$R_{mn} = \log_2 \left(1 + \frac{|h_m|^2 \alpha_n \gamma}{|h_m|^2 \alpha_m \gamma + 1} \right), \tag{4}$$

$$R_{mm} = \log_2 \left(1 + |h_m|^2 \alpha_m \gamma \right), \tag{5}$$

where R_{nn} is the achievable rate at which user n decodes its own message; R_{mn} and R_{mm} are the rates at which user m decodes user n's and its own messages, respectively; and $\gamma = P_s/\sigma^2$ represents the average transmitted signal-to-noise ratio (SNR) for the UP at the BS.

Following [12,22], the eavesdropping rates for users m and n by E are

$$R_{em} = \log_2 \left(1 + |h_e|^2 \alpha_m \gamma \right) \tag{6}$$

and

$$R_{en} = \log_2 \left(1 + \frac{|h_e|^2 \alpha_n \gamma}{|h_e|^2 \alpha_m \gamma + 1} \right) = \log_2 \left(\frac{|h_e|^2 \gamma + 1}{|h_e|^2 \alpha_m \gamma + 1} \right). \tag{7}$$

The achievable secrecy rate (ASR) is established as the variance between the achievable rate for the user and that of the eavesdropper. Thus, the ASR for users m and n in the same group, denoted by (m, n), can be expressed as

$$C_m^{(m,n)} = [R_{mm} - R_{em}]^+ = \left[\log_2\left(\frac{1+|h_m|^2\alpha_m\gamma}{1+|h_e|^2\alpha_m\gamma}\right)\right]^+ \tag{8}$$

and

$$\begin{aligned} C_n^{(m,n)} &= [R_{nn} - R_{en}]^+ \\ &= \left[\log_2\frac{\left(|h_n|^2\gamma+1\right)\left(|h_e|^2\alpha_m\gamma+1\right)}{\left(|h_n|^2\alpha_m\gamma+1\right)\left(|h_e|^2\gamma+1\right)}\right]^+, \end{aligned} \tag{9}$$

where $[\cdot]^+ = \max(\cdot, 0)$. The ASSR of the pair (m, n) is

$$\mathrm{ASSR}^{(m,n)} = C_m^{(m,n)} + C_n^{(m,n)}. \tag{10}$$

As a benchmark, following [16], the achievable rate for user i and the eavesdropper in an OMA system with a similar setting can be, respectively, expressed as

$$R_i^{(\mathrm{OMA})} = \frac{1}{2}\log_2(1+|h_i|^2\gamma), \tag{11}$$

$$R_e^{(\mathrm{OMA})} = \log_2(1+|h_e|^2\gamma), \tag{12}$$

where the multiplexing loss in the OMA system attributes to the fraction $\frac{1}{2}$ in Formula (11). The corresponding ASSR can be given by

$$\mathrm{ASSR}_{\mathrm{OMA}}^{(m,n)} = [R_m^{(\mathrm{OMA})} - \frac{1}{2}R_e^{(\mathrm{OMA})}]^+ + [R_n^{(\mathrm{OMA})} - \frac{1}{2}R_e^{(\mathrm{OMA})}]^+. \tag{13}$$

2.2. Problem Formulation

To secure a downlink NOMA system against external eavesdropping, in pursuit of enhancing the ASSR, our focus lies in meticulously designing UP and PA. The co-optimization problem of UP and PA can be formulated as

$$\begin{aligned} \mathbf{P1}\text{: Maximize}_{\alpha_m, u_{m,n}} \quad & \sum_{n=1}^{N-1}\sum_{m=n+1}^{N} u_{m,n}\cdot(C_m^{(m,n)} + C_n^{(m,n)}) \\ \text{Subject to: } \quad & \mathbf{C_1}\text{: } R_m^{(m,n)} \geq u_{m,n}R_m^{(\mathrm{OMA})}, \\ & \mathbf{C_2}\text{: } R_n^{(m,n)} \geq u_{m,n}R_n^{(\mathrm{OMA})}, \\ & \mathbf{C_3}\text{: } 0 \leq \alpha_m \leq 1, \quad 1 \leq m \leq N, \\ & \mathbf{C_4}\text{: } u_{m,n} \in \{0,1\}, \quad 1 \leq m, n \leq N, \\ & \mathbf{C_5}\text{: } u_{m,n} = u_{n,m}, \quad 1 \leq m, n \leq N, \\ & \mathbf{C_6}\text{: } \sum_{m=1}^{N} u_{m,n} = 1, \quad 1 \leq n \leq N, \\ & \mathbf{C_7}\text{: } \sum_{n=1}^{N} u_{m,n} = 1, \quad 1 \leq m \leq N, \end{aligned}$$

where $u_{m,n}$ is a binary variable that indicates that user m pairs with user n if $u_{m,n} = 1$, otherwise $u_{m,n} = 0$; the constraints $\mathbf{C_1}$ and $\mathbf{C_2}$ guarantee the QoS for users m and n, respectively, i.e., the requirement that the achievable rate should not be less than that in the OMA system is considered in this paper; the constraint $\mathbf{C_3}$ insures an achievable power

allocation between users m and n; and the constraints $\mathbf{C_4}\sim\mathbf{C_7}$ imply the pairing relationship among users, such that each user can pair with one and only one of the others.

Problem (P1) constitutes a non-convex and intricately interconnected mixed integer nonlinear programming issue, posing an NP-hard complexity, and it is generally arduous to search for globally optimal solutions directly. Additionally, in real situations, an eavesdropper usually acts passively. Therefore, we presume that the BS lacks access to precise eavesdropper channel details, and we need to investigate the optimization problem based on the quality of the eavesdropping channels, i.e., the worst quality ($|h_e|^2 \leq |h_1|^2$), the medium quality ($|h_1|^2 \leq |h_e|^2 \leq |h_{2K}|^2$), and the best quality ($|h_e|^2 \geq |h_{2K}|^2$).

Obviously, when the eavesdropping channel is superior over all the channels of legitimate users, we have a zero ASSR according to the subsequent theorem.

Theorem 1. *In an NOMA system involving* $2K$ *users (user* $1, 2, \cdots, 2K$*) and an external eavesdropper (E) with* $|h_1|^2 \leq |h_2|^2 \leq \cdots \leq |h_{2K}|^2 \leq |h_e|^2$*, the ASSR is zero.*

When $|h_e|^2 \geq |h_{2K}|^2$, i.e., $|h_e|^2 \geq |h_m|^2$ and $|h_e|^2 \geq |h_n|^2$, hold for any user pair (m, n), it is easy to prove $R_{em} \geq R_{mm}$ and $R_{en} \geq R_{nn}$ according to Formulas (3) and (5)–(7), which, consequently, results in $C_m^{(m,n)} = C_n^{(m,n)} = 0$ for any user pair (m, n) and $ASSR = 0$. The proof is quite simple, and we omit the details here for simplicity. Thus, we only investigate the problem with the worst and the medium eavesdropping channel, i.e., $|h_e|^2 \leq |h_{2K}|^2$, in the following sections, respectively.

We initially partition the primary joint optimization problem encompassing UP and PA (P1) into two subsidiary problems, i.e., the optimal PA between two users in one pair (SP1) and the optimal UP problem (SP2), and we will discuss them in the following two sections, respectively.

3. PA for NOMA Involving Two Paired Users

In sub-problem (SP1), an NOMA system involving two users (users m and n) in one pair and an external eavesdropper (E) is considered. To maximize the ASSR, we formulate the optimization of power allocation as

$$\begin{aligned} \mathbf{SP1}\text{: Maximize}_{\alpha_m} \quad & C_m^{(m,n)} + C_n^{(m,n)} \\ \text{Subject to: } & \mathbf{C_1}\text{: } R_m^{(m,n)} \geq R_m^{(\mathrm{OMA})}, \\ & \mathbf{C_2}\text{: } R_n^{(m,n)} \geq R_n^{(\mathrm{OMA})}, \\ & \mathbf{C_3}\text{: } \alpha_m + \alpha_n = 1, \\ & \mathbf{C_4}\text{: } 0 \leq \alpha_m \leq 1. \end{aligned}$$

The subsequent theorem elucidates the optimal resolution to the aforementioned problem (SP1).

Theorem 2. *In an NOMA system involving two users (users m and n) in one pair and an external eavesdropper (E), the optimal coefficient for power splitting is*

$$\alpha_m^{(m,n)} = \frac{\sqrt{1 + |h_n|^2\gamma} - 1}{|h_n|^2\gamma}. \tag{14}$$

Proof. We prove this in the following two situations according to the quality of the eavesdropping channel, respectively.

(1) : $|h_m|^2 \geq |h_n|^2 \geq |h_e|^2$

Taking the derivative of the achievable sum secrecy rate (ASSR), Formula (10), with regard to α_m, we can obtain

$$\frac{d(\text{ASSR})}{d(\alpha_m)} = \frac{1}{\ln 2} \frac{(|h_m|^2 - |h_n|^2)\gamma}{(|h_m|^2\alpha_m\gamma + 1)(|h_n|^2\alpha_m\gamma + 1)} \geq 0,$$

which implies that the ASSR is a monotonically increasing function of α_m in this situation.

Following similar steps to those in [16], we can obtain the range of α_m from the constraints C_1 and C_2 as

$$\frac{\sqrt{1 + |h_m|^2\gamma} - 1}{|h_m|^2\gamma} \leq \alpha_m \leq \frac{\sqrt{1 + |h_n|^2\gamma} - 1}{|h_n|^2\gamma}.$$

According to the monotonicity of the ASSR with respect to α_m, we can reach the optimal ASSR within the upper limit of the range, i.e.,

$$\alpha_m^{(m,n)} = \frac{\sqrt{1 + |h_n|^2\gamma} - 1}{|h_n|^2\gamma}.$$

(2): $|h_m|^2 \geq |h_e|^2 \geq |h_n|^2$

When $|h_m|^2 \geq |h_e|^2 \geq |h_n|^2$ holds, we can easily infer that $C_n^{(m,n)} = 0$. Thus,

$$\frac{d(\text{ASSR})}{d(\alpha_m)} = \frac{1}{\ln 2} \frac{(|h_m|^2 - |h_e|^2)\gamma}{(|h_m|^2\alpha_m\gamma + 1)(|h_e|^2\alpha_m\gamma + 1)} \geq 0.$$

Similarly, the optimal PA to user m can be inferred as

$$\alpha_m^{(m,n)} = \frac{\sqrt{1 + |h_n|^2\gamma} - 1}{|h_n|^2\gamma}.$$

Combining the above two situations, we can prove Theorem 2. □

It is worthy of note that the optimal PA is solely determined by the channel gain of the weak user, and only allocates necessary power to satisfy the weak user's QoS constraint C_2. Furthermore, we can check the fact that the obtained optimal allocation coefficient $\alpha_m^{(m,n)}$ satisfies the constraint $\mathbf{C_4}$ of SP1.

4. Optimal User Pairing

In sub-problem (SP2), an NOMA system with $N = 2K$ users and an external eavesdropper is considered, and we formulate the optimization of UP as SP2.

$$\begin{aligned}
\mathbf{SP2}\text{: Maximize}_{u_{m,n}} \quad & \sum_{n=1}^{N-1} \sum_{m=n+1}^{N} u_{m,n} \cdot (C_m^{(m,n)} + C_n^{(m,n)}) \\
\text{Subject to: } \quad & \mathbf{C_1}\text{: } u_{mn} \in \{0,1\}, \quad 1 \leq m,n \leq N, \\
& \mathbf{C_2}\text{: } u_{m,n} = u_{n,m}, \quad 1 \leq m,n \leq N, \\
& \mathbf{C_3}\text{: } \sum_{m=1}^{N} u_{m,n} = 1, \quad 1 \leq n \leq N, \\
& \mathbf{C_4}\text{: } \sum_{n=1}^{N} u_{m,n} = 1, \quad 1 \leq m \leq N.
\end{aligned}$$

To investigate the optimal UP problem for an NOMA involving $2K$ users, let us commence from the simplest pairing case with the minimum number of users, i.e., with four users, and then extend the obtained results to the general case.

4.1. UP for NOMA Involving Four Users

4.1.1. Pairing Solutions

In an NOMA system involving four users (users 1, 2, 3, and 4), without a loss of generality, and assuming $|h_1|^2 \leq |h_2|^2 \leq |h_3|^2 \leq |h_4|^2$, there exist three user pairing solutions, referring to *Solution a*, *Solution b*, and *Solution c*, respectively, in the following.

Solution a: User 1 pairs with user 2, and user 3 pairs with user 4, i.e., $u_{1,2} = 1$ and $u_{3,4} = 1$. Thus, the ASSR can be expressed as

$$C_a = C_1^{(1,2)} + C_2^{(1,2)} + C_3^{(3,4)} + C_4^{(3,4)}. \tag{15}$$

Solution b: User 1 pairs with user 3, and user 2 pairs with user 4, i.e., $u_{1,3} = 1$ and $u_{2,4} = 1$. Thus, the ASSR can be expressed as

$$C_b = C_1^{(1,3)} + C_2^{(2,4)} + C_3^{(1,3)} + C_4^{(2,4)}. \tag{16}$$

Solution c: User 1 pairs with user 4, and user 2 pairs with user 3, i.e., $u_{1,4} = 1$ and $u_{2,3} = 1$. Thus, the ASSR can be expressed as

$$C_c = C_1^{(1,4)} + C_2^{(2,3)} + C_3^{(2,3)} + C_4^{(1,4)}. \tag{17}$$

4.1.2. Optimal UP for NOMA with Four Users

After analyzing and comparing the ASSRs of three pairing solutions in detail, we give the optimal UP solution of an NOMA system involving four users and an external eavesdropper according to the theorem below.

Theorem 3. *In an NOMA system involving four users (users* 1, 2, 3, *and* 4*) and an external eavesdropper (E) with* $|h_1|^2 \leq |h_2|^2 \leq |h_3|^2 \leq |h_4|^2$*, we have* $C_a \leq C_b \leq C_c$*, i.e., Solution c is the optimal UP solution.*

Proof. Based on the sequence of channel gains, there are four cases as below, and we will prove $C_a \leq C_b \leq C_c$ case by case.

Case 1: $|h_e|^2 \leq |h_1|^2 \leq |h_2|^2 \leq |h_3|^2 \leq |h_4|^2$

Following Theorem 2, we have

$$\begin{cases} \alpha_2^{(1,2)} & = \alpha_3^{(1,3)} = \alpha_4^{(1,4)} = \frac{\sqrt{1+|h_1|^2\gamma}-1}{|h_1|^2\gamma} \triangleq \beta_1, \\ \alpha_3^{(2,3)} & = \alpha_4^{(2,4)} = \frac{\sqrt{1+|h_2|^2\gamma}-1}{|h_2|^2\gamma} \triangleq \beta_2, \\ \alpha_4^{(3,4)} & = \frac{\sqrt{1+|h_3|^2\gamma}-1}{|h_3|^2\gamma} \triangleq \beta_3. \end{cases} \tag{18}$$

On this basis, following (9), we can obtain

$$\begin{cases} C_1^{(1,2)} = C_1^{(1,3)} = C_1^{(1,4)}, \\ C_2^{(2,3)} = C_2^{(2,4)}. \end{cases} \tag{19}$$

For the function $f(x) = \frac{\sqrt{1+x}-1}{x}$ where $(x > 0)$ monotonously decreases with the increase of x and the presumption $|h_1|^2 \leq |h_2|^2 \leq |h_3|^2$, we have the sequence of β_k $(k = 1, 2, 3)$ as

$$\beta_3 \leq \beta_2 \leq \beta_1 \leq 1. \tag{20}$$

Then, we have

$$\begin{aligned} C_c - C_b &= \left(C_1^{(1,4)} + C_2^{(2,3)} + C_3^{(2,3)} + C_4^{(1,4)}\right) - \left(C_1^{(1,3)} + C_2^{(2,4)} + C_3^{(1,3)} + C_4^{(2,4)}\right) \\ &= \log_2 \frac{\left(1+|h_3|^2\beta_2\gamma\right)\left(1+|h_4|^2\beta_1\gamma\right)}{\left(1+|h_3|^2\beta_1\gamma\right)\left(1+|h_4|^2\beta_2\gamma\right)} \\ &= \log_2 \left(1 + \frac{(\beta_1-\beta_2)\left(|h_4|^2-|h_3|^2\right)\gamma}{\left(1+|h_3|^2\beta_1\gamma\right)\left(1+|h_4|^2\beta_2\gamma\right)}\right) \geq 0, \end{aligned}$$

and

$$\begin{aligned} C_b - C_a &= \left(C_1^{(1,3)} + C_2^{(2,4)} + C_3^{(1,3)} + C_4^{(2,4)}\right) - \left(C_1^{(1,2)} + C_2^{(1,2)} + C_3^{(3,4)} + C_4^{(3,4)}\right) \\ &= \log_2 \frac{\sqrt{1+|h_2|^2\gamma}\left(1+|h_3|^2\beta_1\gamma\right)\left(1+|h_4|^2\beta_2\gamma\right)}{\sqrt{1+|h_3|^2\gamma}\left(1+|h_2|^2\beta_1\gamma\right)\left(1+|h_4|^2\beta_3\gamma\right)} \\ &\geq \log_2 \frac{\sqrt{1+|h_2|^2\gamma}\left(1+|h_3|^2\beta_1\gamma\right)}{\sqrt{1+|h_3|^2\gamma}\left(1+|h_2|^2\beta_1\gamma\right)} \\ &= \frac{1}{2}\left[\log_2 \frac{\left(1+|h_3|^2\beta_1\gamma\right)^2}{1+|h_3|^2\gamma} - \log_2 \frac{\left(1+|h_2|^2\beta_1\gamma\right)^2}{1+|h_2|^2\gamma}\right]. \end{aligned}$$

We define $g(x) = \frac{(1+\beta_1 x)^2}{1+x}$ $(x > 0)$ and it is readily apparent that $g'(x) \geq 0$. Then, we have $C_b - C_a \geq 0$.

Thus, we have $C_a \leq C_b \leq C_c$ in *Case 1*.

Case 2: $|h_1|^2 \leq |h_e|^2 \leq |h_2|^2 \leq |h_3|^2 \leq |h_4|^2$

In this case, the ASSR in three UP solutions can be described as

$$\begin{cases} C_a = C_2^{(1,2)} + C_3^{(3,4)} + C_4^{(3,4)} \\ C_b = C_2^{(2,4)} + C_3^{(1,3)} + C_4^{(2,4)} \\ C_c = C_2^{(2,3)} + C_3^{(2,3)} + C_4^{(1,4)} \end{cases} \tag{21}$$

$$\begin{aligned} C_c - C_b &= C_3^{(2,3)} - C_3^{(1,3)} + C_4^{(1,4)} - C_4^{(2,4)} \\ &= \log_2(1 + \frac{(\beta_1-\beta_2)(|h_4|^2-|h_3|^2)\gamma}{(1+|h_3|^2\beta_1\gamma)(1+|h_4|^2\beta_2\gamma)}) \geq 0, \end{aligned} \tag{22}$$

$$\begin{aligned} C_b - C_a &= C_2^{(2,4)} - C_2^{(1,2)} + C_3^{(1,3)} - C_3^{(3,4)} + C_4^{(2,4)} - C_4^{(3,4)} \\ &= \log_2[\frac{(1+|h_2|^2\gamma)(1+|h_3|^2\beta_1\gamma)}{(1+|h_2|^2\beta_2\gamma)(1+|h_2|^2\beta_1\gamma)} \cdot \frac{(1+|h_3|^2\beta_3\gamma)(1+|h_4|^2\beta_2\gamma)}{(1+|h_3|^2\gamma)(1+|h_4|^2\beta_3\gamma)}] \\ &\underline{\underline{(18)}} \log_2 \frac{\sqrt{1+|h_2|^2\gamma}(1+|h_3|^2\beta_1\gamma)(1+|h_4|^2\beta_2\gamma)}{\sqrt{1+|h_3|^2\gamma}(1+|h_2|^2\beta_1\gamma)(1+|h_4|^2\beta_3\gamma)} \\ &\geq \log_2 \frac{\sqrt{1+|h_2|^2\gamma}(1+|h_3|^2\beta_1\gamma)}{\sqrt{1+|h_3|^2\gamma}(1+|h_2|^2\beta_1\gamma)} \\ &= \frac{1}{2}[\log_2 \frac{(1+|h_3|^2\beta_1\gamma)^2}{1+|h_3|^2\gamma} - \log_2 \frac{(1+|h_2|^2\beta_1\gamma)^2}{1+|h_2|^2\gamma}] \geq 0, \end{aligned} \tag{23}$$

where "(18)" indicates (18) is applied in this step. Thus, we have $C_a \leq C_b \leq C_c$ in *Case 2*.

Case 3: $|h_1|^2 \leq |h_2|^2 \leq |h_e|^2 \leq |h_3|^2 \leq |h_4|^2$

Similar to *Case 2*, we can obtain the ASSR in three UP solutions as

$$\begin{cases} C_a = C_3^{(3,4)} + C_4^{(3,4)} \\ C_b = C_3^{(1,3)} + C_4^{(2,4)} \\ C_c = C_3^{(2,3)} + C_4^{(1,4)} \end{cases} \tag{24}$$

$$\begin{aligned} C_c - C_b &= C_3^{(2,3)} - C_3^{(1,3)} + C_4^{(1,4)} - C_4^{(2,4)} \\ &= \log_2[1 + \frac{(\beta_1 - \beta_2)(|h_4|^2 - |h_3|^2)\gamma}{(1+|h_3|^2\beta_1\gamma)(1+|h_4|^2\beta_2\gamma)}] \geq 0, \\ C_b - C_a &= C_3^{(1,3)} - C_3^{(3,4)} + C_4^{(2,4)} - C_4^{(3,4)} \\ &= \log_2[\frac{(1+|h_3|^2\beta_1\gamma)(1+|h_3|^2\beta_3\gamma)}{(1+|h_3|^2\gamma)(1+|h_4|^2\beta_3\gamma)} \cdot \frac{(1+|h_4|^2\beta_2\gamma)(1+|h_e|^2\gamma)}{(1+|h_e|^2\beta_1\gamma)(1+|h_e|^2\beta_2\gamma)}] \end{aligned} \tag{25}$$

Let $\beta_e = \frac{\sqrt{1+|h_e|^2\gamma}-1}{|h_e|^2\gamma}$. We have

$$1 + |h_e|^2\beta_e\gamma = \sqrt{1+|h_e|^2\gamma}, \tag{26}$$

and it is easy to prove that $\beta_1 \geq \beta_2 \geq \beta_e \geq \beta_3$. Hence, taking (26) into (25), we have

$$C_b - C_a = \underbrace{\log_2 \frac{\sqrt{1+|h_e|^2\gamma}(1+|h_3|^2\beta_1\gamma)}{\sqrt{1+|h_3|^2\gamma}(1+|h_e|^2\beta_1\gamma)}}_{A} + \underbrace{\log_2 \frac{(1+|h_e|^2\beta_e\gamma)(1+|h_4|^2\beta_2\gamma)}{(1+|h_e|^2\beta_2\gamma)(1+|h_4|^2\beta_3\gamma)}}_{B} \geq 0,$$

for the reason that

$$\begin{aligned} A &= \frac{1}{2}[\log_2 \frac{(1+|h_3|^2\beta_1\gamma)^2}{1+|h_3|^2\gamma} - \log_2 \frac{(1+|h_e|^2\beta_1\gamma)^2}{1+|h_e|^2\gamma}] \geq 0, \\ B &\geq \log_2 \frac{(1+|h_e|^2\beta_3\gamma)(1+|h_4|^2\beta_2\gamma)}{(1+|h_e|^2\beta_2\gamma)(1+|h_e|^2\beta_3\gamma)} \\ &= \log_2[1 + \frac{(|h_4|^2 - |h_e|^2)(\beta_2 - \beta_3)\gamma}{(1+|h_e|^2\beta_2\gamma)(1+|h_4|^2\beta_3\gamma)}] \geq 0. \end{aligned}$$

Thus, we have $C_a \leq C_b \leq C_c$ in *Case 3*.

Case 4: $|h_1|^2 \leq |h_2|^2 \leq |h_3|^2 \leq |h_e|^2 \leq |h_4|^2$

Similar to *Cases 2* and *3*, we can obtain the ASSR in three UP solutions as

$$\begin{cases} C_a = C_4^{(3,4)} \\ C_b = C_4^{(2,4)} \\ C_c = C_4^{(1,4)} \end{cases}, \tag{27}$$

$$C_c - C_b = C_4^{(1,4)} - C_4^{(2,4)} = \log_2(1 + \frac{(\beta_1 - \beta_2)(|h_4|^2 - |h_e|^2)\gamma}{(1+|h_e|^2\beta_1\gamma)(1+|h_4|^2\beta_2\gamma)}) \geq 0, \tag{28}$$

$$C_b - C_a = C_4^{(2,4)} - C_4^{(3,4)} = \log_2(1 + \frac{(\beta_2 - \beta_3)(|h_4|^2 - |h_e|^2)\gamma}{(1+|h_e|^2\beta_2\gamma)(1+|h_4|^2\beta_3\gamma)}) \geq 0. \tag{29}$$

We can easily verify that $C_a \leq C_b \leq C_c$ always holds in *Case 4*, and omit the detail here for simplicity.

Combining the above four cases, we can prove Theorem 3. □

4.2. UP for NOMA with 2K Users

We considered an NOMA system with two and four users in Sections 3 and 4.1, and found the optimal PA and UP, respectively. We will give the extended solution to Problem (SP2) using the subsequent theorem.

Theorem 4. *In an NOMA system involving 2K users (user 1, 2, $\cdots$, 2K) and an external eavesdropper (E) with $|h_e|^2 \leq |h_{2K}|^2$, the optimal pairing solution is*

$$u_{m,n} = \begin{cases} 1, & m+n = 2K+1; \\ 0, & \text{others.} \end{cases} \tag{30}$$

In other words, any user k is paired with the user $2K-k+1$, i.e., $u_{k,2K-k+1} = 1$, for all $k \in \mathbb{N}$ $(1 \leq k \leq 2K)$.

Proof. When $K = 1$, there are only two users in the NOMA system, and they have no choice but to pair with each other, which makes (30) hold. Thus, we first consider the case when $K = 2$, which is a case we discussed in Section 4.1. Following Theorem 3, it is readily verifiable that the optimal pairing strategy *Case c* satisfies (30).

Next, we prove (30) in the case when $K > 2$ using mathematical induction in the following four steps.

(1) When $k = 1$, we need to prove $u_{1,2K} = 1$, i.e., user 1 pairs with user $2K$. We prove it by contradiction. We assume user 1 is paired with user i $(2 \leq i \leq 2K-1)$ instead of user $2K$, and user $2K$ is paired with user j $(2 \leq j \leq 2K-1, j \neq i)$ instead of user 1 in the optimal user pairing solution. Following Theorem 3, we have

$$C_1^{(1,2K)} + C_{2K}^{(1,2K)} + C_i^{(i,j)} + C_j^{(i,j)} \geq C_1^{(1,i)} + C_i^{(1,i)} + C_j^{(j,2K)} + C_{2K}^{(j,2K)}.$$

That is to say, we can re-pair users 1, i, j, and $2K$ to increase the ASSR, which contradicts the statement that the original pairing solution is optimal. Thus, user 1 must be paired with user $2K$ to increase the ASSR, i.e., $u_{1,2K} = 1$.

(2) We assume $u_{k,2K-k+1} = 1$ holds when $k = s$, i.e., $u_{1,2K} = u_{2,2K-1} = \cdots = u_{s,2K-s+1} = 1$.

(3) According to the principle of mathematical induction, we need to prove $u_{k,2K-k+1} = 1$ holds when $k = s+1$, i.e., $u_{s+1,2K-s} = 1$ holds, and we also prove it by contradiction. We assume that user $s+1$ is paired with user i $(s+2 \leq i \leq 2K-s-1)$ and user $2K-s$ is paired with user j $(s+2 \leq j \leq 2K-s-1, j \neq i)$. Following Theorem 3, we have

$$C_{s+1}^{(s+1,2K-s)} + C_{2K-s}^{(s+1,2K-s)} + C_i^{(i,j)} + C_j^{(i,j)} \geq_{s+1}^{(s+1,i)} + C_i^{(s+1,i)} + C_j^{(j,2K-s)} + C_{2K-s}^{(j,2K-s)},$$

which contradicts the assumption. Thus, user $s+1$ must pair with user $2K-s$, i.e., $u_{s+1,2K-s} = 1$, to achieve a higher ASSR.

(4) In conclusion, we can conclude that $u_{k,2K-k+1} = 1$ holds for all $k \in \mathbb{N}$ $(1 \leq k \leq 2K)$, and we complete the proof.

□

4.3. Computational Complexity

As mentioned above, the proposed scheme can be implemented in two consecutive steps, the optimal UP and the optimal PA. We analyze the computational complexity of the two parts, respectively.

In the first part, the optimal UP is determined based on Theorem 4, once the order of channel gains is given. Thus, the calculation of channel gain constitutes the primary computational complexity of the first part, such as QuickSort, which runs in $\mathcal{O}(N^2)$ time in the worst case, and in expected $\mathcal{O}(NlogN)$ time [24], where N is the quantity of numbers to be sorted, that is, the number of users in this paper. Although the exhausted searching

method can also find the optimal UP scheme, it runs in $\mathcal{O}(N!)$ time [16], which is much higher than that in the proposed scheme.

In the second part, we calculate the PA coefficient according to (14) for each user pair, and there are $N/2$ user pairs in all. Therefore, the computational complexity of the second part is $\mathcal{O}(N)$.

5. Simulation and Discussion

The security performance regarding the ASSR of downlink NOMA against external eavesdropping scenarios was investigated with numerical simulations. The simulations involve $N = 2K$ users, distributed evenly across a disk with radius $r = 500$ m, and the path-loss coefficient $\alpha = 2$. The height of the BS is assumed to be $H = 50$ m. Two benchmark schemes, termed *random UP with optimal PA* (simply denoted as "random") and the standard *OMA* setup, were utilized to enhance the performance of the proposed scheme. The performance was averaged on 10^3 user distributions and 10^3 channel realizations for each user distribution. Furthermore, 10^3 random user pairings were conducted for each user distribution and channel realization in the random scheme.

Figure 2 shows a performance comparison of the ASSRs between an NOMA with the proposed UP and PA scheme (proposed), and the two benchmark schemes, randomly paired NOMA with optimal PA and standard OMA, with different numbers of user pairs where $P/\sigma^2 = 20$ dB. From Figure 2, it can be inferred that averaged performance of the ASSRs in the NOMA scheme (both optimal pairing and random pairing) outperformed that in the OMA scheme, and the ASSR was a function of the quantity of user pairs. When K was small, the performance difference of the ASSR was not obvious between the NOMA scheme with optimal pairing and that with random pairing. However, with the increase in K, the ASSR of the proposed scheme gradually exceeded that of the rival method owing to the optimality we reached.

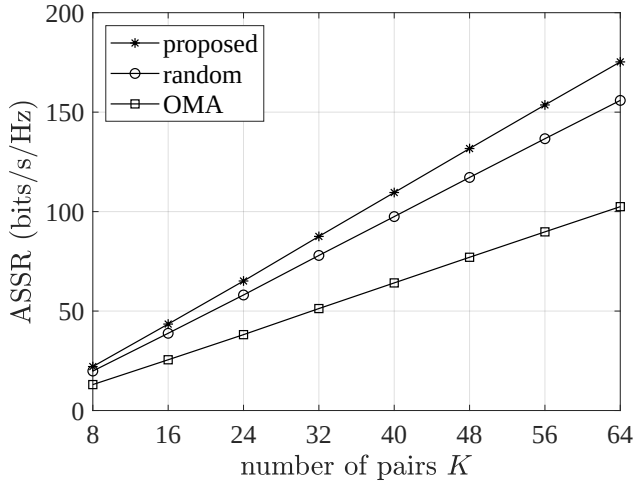

Figure 2. Comparison of ASSRs among NOMA employing optimal pairing, randomly paired NOMA, and OMA using different pair quantities, with parameters set at P/σ^2 = 20 dB and r = 500 m.

In Figure 3, a comparison of the ASSRs among an NOMA employing the proposed optimal UP and PA scheme (proposed), a randomly paired NOMA with an optimal PA, and an OMA are shown in different colors and markers, with varying signal–noise ratios (SNRs) for different numbers of user pairs. It can be observed that with the rise in the SNR, the ASSR proportionally improved. At low SNR values, the difference in the ASSR performance between the NOMA scheme with optimal pairing and that with random pairing was not significant. However, as the SNR escalated, the superiority of our method's ASSR became more evident. Furthermore, as the quantity of user pairs (K) grew, the superiority of the ASSRs over the other two schemes became increasingly apparent.

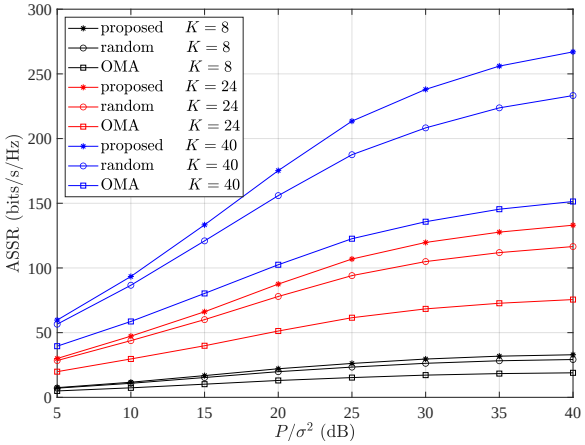

Figure 3. Comparison of ASSRs among NOMA employing optimal pairing, randomly paired NOMA, and OMA with different signal–noise ratio, with parameters set at r = 500 m.

Figure 4 illustrates the average ASSRs (average ASSRs per user, i.e., ASSR/N) employing our proposed Optimal UP and PA scheme. The data points are represented using various colors and markers, indicating different signal–noise ratios (SNRs) for varying numbers of user pairs. From Figure 4, we can see the following three aspects. Initially, as the SNR rose, the average ASSR followed a corresponding increase. Secondly, our method outperformed competitors in terms of the average ASSR. Lastly, enhancing the number of pairs (K) resulted in even greater performance improvements in the average ASSR. Compared to Figure 3, as the quantity of user pairs (K) grew, the improvement in the performance of the average ASSR became more significant than that of the ASSR.

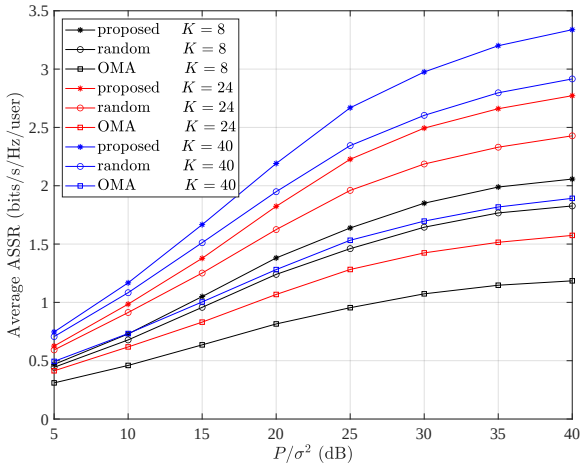

Figure 4. Comparison of average ASSRs among NOMA employing optimal pairing, randomly paired NOMA, and OMA with different signal–noise ratios, with parameters set at r = 500 m.

6. Conclusions

In the manuscript, we explore the optimal UP and PA for secure downlink NOMA against external eavesdropping. To maximize the achievable sum secrecy rate, we formulate a joint optimization problem of UP and PA, which is an MINLP problem which is hard to solve. We break down the original problem into two subordinate problems, i.e., an optimal PA problem for two paired users and an optimal UP problem. Then, the optimal solution for a universal NOMA with 2K users is obtained. We validate the theoretical discoveries with simulation discoveries that demonstrate that the proposed scheme outperforms those obtained by the alternative methods in both achievable sum secrecy rate and average secrecy rate performances.

Author Contributions: Conceptualization, X.J. and Y.C.; methodology, Y.C.; software, Y.L.; validation, Y.L., Y.C. and X.J.; writing—original draft preparation, Y.L.; writing—review and editing, Y.L.; visualization, Y.L.; supervision, X.J.; project administration, X.J.; funding acquisition, X.J. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the National Natural Science Foundation of China, grant numbers 61931004 and 62072250; the National Key Research and Development Program of China, grant number 2021QY0700; the Jiangsu Province Natural Science Foundation, grant number BK20230415; the Natural Science Foundation of the Jiangsu Higher Education Institutions of China, grant number 23KJB120007; and The Startup Foundation for Introducing Talent of NUIST, grant number 2021r039.

Data Availability Statement: Data are contained within the article.

Conflicts of Interest: The authors declare no conflicts of interest. The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript; or in the decision to publish the results.

Abbreviations

The following abbreviations are used in this manuscript:

NOMA	Non-Orthogonal Multiple Access
UP	User Pairing
PA	Power Allocation
ASSR	Achievable Sum Secrecy Rate
MINLP	Mixed Integer Nonlinear Programming
SIC	Successive Interference Cancellation
PLS	Physical Layer Security
MIMO	Multiple Input–Multiple Output
CRN	Cognitive Radio Network
AN	Artificial Noise
SSR	Secrecy Sum Rate
UAV	Unmanned Aerial Vehicle
IRS	Intelligent Reflecting Surface
BS	Base Station
ASR	Achievable Secrecy Rate
CSI	Channel Side Information
SNR	Signal–Noise Ratio

References

1. Ding, Z.; Poor, H.V. On the Application of BAC-NOMA to 6G umMTC. *IEEE Commun. Lett.* **2021**, *25*, 2678–2682. [CrossRef]
2. Vaezi, M.; Schober, R.; Ding, Z.; Poor, H.V. Non-Orthogonal Multiple Access: Common Myths and Critical Questions. *IEEE Wirel. Commun.* **2019**, *26*, 174–180. [CrossRef]
3. Choi, J. Non-Orthogonal Multiple Access in Downlink Coordinated Two-Point Systems. *IEEE Commun. Lett.* **2014**, *18*, 313–316. [CrossRef]
4. Ding, Z.; Yang, Z.; Fan, P.; Poor, H.V. On the Performance of Non-Orthogonal Multiple Access in 5G Systems with Randomly Deployed Users. *IEEE Signal Process. Lett.* **2014**, *21*, 1501–1505. [CrossRef]
5. Wang, P.; Xiao, J.; Ping, L. Comparison of orthogonal and non-orthogonal approaches to future wireless cellular systems. *IEEE Veh. Technol. Mag.* **2006**, *1*, 4–11. [CrossRef]
6. Dai, L.; Wang, B.; Yuan, Y.; Han, S.; Chih-lin, I.; Wang, Z. Non-orthogonal multiple access for 5G: solutions, challenges, opportunities, and future research trends. *IEEE Commun. Mag.* **2015**, *53*, 74–81. [CrossRef]
7. Yu, Y.; Chen, H.; Li, Y.; Ding, Z.; Vucetic, B. On the Performance of Non-Orthogonal Multiple Access in Short-Packet Communications. *IEEE Commun. Lett.* **2018**, *22*, 590–593. [CrossRef]
8. Liu, Y.; Zhang, S.; Mu, X.; Ding, Z.; Schober, R.; Al-Dhahir, N.; Hossain, E.; Shen, X. Evolution of NOMA Toward Next Generation Multiple Access (NGMA) for 6G. *IEEE J. Sel. Areas Commun.* **2022**, *40*, 1037–1071. [CrossRef]
9. Cao, Y.; Zhao, N.; Chen, Y.; Jin, M.; Ding, Z.; Li, Y.; Yu, F.R. Secure Transmission via Beamforming Optimization for NOMA Networks. *IEEE Wirel. Commun.* **2020**, *27*, 193–199. [CrossRef]
10. Poor, H.V.; Schaefer, R.F. Wireless physical layer security. *Proc. Nat. Acad. Sci. USA* **2017**, *114*, 19–26. [CrossRef]
11. Nandan, N.; Majhi, S.; Wu, H.C. Secure Beamforming for MIMO-NOMA-Based Cognitive Radio Network. *IEEE Commun. Lett.* **2018**, *22*, 1708–1711. [CrossRef]

12. Feng, Y.; Yan, S.; Yang, Z.; Yang, N.; Yuan, J. Beamforming Design and Power Allocation for Secure Transmission With NOMA. *IEEE Trans. Wirel. Commun.* **2019**, *18*, 2639–2651. [CrossRef]
13. Li, Y.; Wang, W.; Liu, M.; Zhao, N.; Jiang, X.; Chen, Y.; Wang, X. Joint Trajectory and Power Optimization for Jamming-Aided NOMA-UAV Secure Networks. *IEEE Syst. J.* **2023**, *17*, 732–743. [CrossRef]
14. Chen, Y.; Ji, X. Secure Downlink Transmission Strategies against Active Eavesdropping in NOMA Systems: A Zero-Sum Game Approach. *Comput. Model. Eng. Sci.* **2023**, *136*, 531–553. [CrossRef]
15. Wang, W.; Liu, X.; Tang, J.; Zhao, N.; Chen, Y.; Ding, Z.; Wang, X. Beamforming and Jamming Optimization for IRS-Aided Secure NOMA Networks. *IEEE Trans. Wirel. Commun.* **2022**, *21*, 1557–1569. [CrossRef]
16. Zhu, L.; Zhang, J.; Xiao, Z.; Cao, X.; Wu, D.O. Optimal User Pairing for Downlink Non-Orthogonal Multiple Access (NOMA). *IEEE Wirel. Commun. Lett.* **2019**, *8*, 328–331. [CrossRef]
17. Wei, Z.; Ng, D.W.K.; Yuan, J.; Wang, H.M. Optimal Resource Allocation for Power-Efficient MC-NOMA With Imperfect Channel State Information. *IEEE Trans. Commun.* **2017**, *65*, 3944–3961. [CrossRef]
18. Ding, Z.; Fan, P.; Poor, H.V. Impact of User Pairing on 5G Nonorthogonal Multiple-Access Downlink Transmissions. *IEEE Trans. Veh. Technol.* **2016**, *65*, 6010–6023. [CrossRef]
19. Liang, W.; Ding, Z.; Li, Y.; Song, L. User Pairing for Downlink Non-Orthogonal Multiple Access Networks Using Matching Algorithm. *IEEE Trans. Commun.* **2017**, *65*, 5319–5332. [CrossRef]
20. Köse, A.; Koca, M.; Anarim, E.; Médard, M.; Gökcesu, H. Graph-Theoretical Dynamic User Pairing for Downlink NOMA Systems. *IEEE Commun. Lett.* **2021**, *25*, 3234–3238. [CrossRef]
21. Liu, Z.; Liang, C.; Yuan, Y.; Chan, K.Y.; Guan, X. Resource Allocation Based on User Pairing and Subcarrier Matching for Downlink Non-Orthogonal Multiple Access Networks. *IEEE/CAA J. Autom. Sin.* **2021**, *8*, 679–689. [CrossRef]
22. Zhang, Y.; Wang, H.M.; Yang, Q.; Ding, Z. Secrecy Sum Rate Maximization in Non-orthogonal Multiple Access. *IEEE Commun. Lett.* **2016**, *20*, 930–933. [CrossRef]
23. Tao, L.; Yang, W.; Yan, S.; Wu, D.; Guan, X.; Chen, D. Covert Communication in Downlink NOMA Systems With Random Transmit Power. *IEEE Wirel. Commun. Lett.* **2020**, *9*, 2000–2004. [CrossRef]
24. Cormen, T.H.; Leiserson, C.E.; Rivest, R.L.; Stein, C. *Introduction to Algorithms*, 4th ed.; The MIT Press: Cambridge, MA, USA, 2022; p. 1312.