Computer Modeling in Engineering & Sciences

Tech Science Press

DOI: 10.32604/cmes.2023.024531

check for updates

ARTICLE

Secure Downlink Transmission Strategies against Active Eavesdropping in NOMA Systems: A Zero-Sum Game Approach

Yanqiu Chen and Xiaopeng Ji*

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

*Corresponding Author: Xiaopeng Ji. Email: jixiaopeng_nj@163.com

Received: 01 June 2022 Accepted: 15 September 2022

ABSTRACT

Non-orthogonal multiple access technology (NOMA), as a potentially promising technology in the 5G/B5G era, suffers from ubiquitous security threats due to the broadcast nature of the wireless medium. In this paper, we focus on artificial-signal-assisted and relay-assisted secure downlink transmission schemes against external eavesdropping in the context of physical layer security, respectively. To characterize the non-cooperative confrontation around the secrecy rate between the legitimate communication party and the eavesdropper, their interactions are modeled as a two-person zero-sum game. The existence of the Nash equilibrium of the proposed game models is proved, and the pure strategy Nash equilibrium and mixed-strategy Nash equilibrium profiles in the two schemes are solved and analyzed, respectively. The numerical simulations are conducted to validate the analytical results, and show that the two schemes improve the secrecy rate and further enhance the physical layer security performance of NOMA systems.

KEYWORDS

Non-orthogonal multiple access technology (NOMA); physical layer security; game theory; nash equilibrium; zero-sum game

1 Introduction

Non-orthogonal multiple access (NOMA) has been envisioned as a potentially promising technology for fifth generation (5G) and beyond 5G (B5G) wireless communication networks for its superior performance over the conventional orthogonal multiple access (OMA) in terms of spectral efficiency, connection density, as well as user fairness [1–4]. However, due to the broadcast nature of wireless communication, the NOMA system is vulnerable to eavesdropping. To secure information transmission against malicious eavesdropping, many countermeasures, such as encryption-based approaches implemented at the higher layers [5] and physical layer security (PLS) [6,7], have been put forward in recent years. PLS, as a promising solution to safeguard confidential transmission from the wireless information-theoretic perspective, exploits the intrinsic randomness of the wireless medium to enhance security, and can provide a secure transmission without keys or sophisticated

encryption/decryption algorithms. In addition, the physical layer security techniques can be easily implemented and have the capability to quickly adapt to different wireless scenarios [8].

Recently, the concept of PLS has been applied to NOMA systems for secure transmission, and has attracted significant attention and increasing interest in both academia and industry [9,10]. The existing work generally falls into two categories: the security-oriented system design, and X-assisted security scheme. Specifically, the security-oriented system design approaches enhance security by optimizing the parameters of the NOMA system, such as beamforming matrix and power allocation coefficients. Whilst, in X-assisted security schemes, X denotes artificial signal, relay, cooperative jamming or something additional. The key idea behind the approaches is to deliberately improve the legitimated communication channel and/or degrade the eavesdropping channel.

Nevertheless, most of the existing studies on secure transmission in NOMA are conducted from the perspective of legitimate communicators, and fail to reflect the confrontation relationship between eavesdroppers and legitimate communicators. In other words, they assume the precondition that the eavesdropper keeps wiretapping regardless of the radio environment. As a matter of fact, eavesdroppers may incur more costs than benefits when faced with harsh eavesdropping channel conditions, and have no intent to eavesdrop in this situation, which makes the precondition more conservative. Therefore, it is of great significance to comprehensively study the interaction strategies between the two sides considering the channel conditions. However, the various and variable channel state information in radio environment complicates the dynamic secure transmission and eavesdropping process, and further affects their optimal strategy selection for both sides, which poses a huge challenge to studying the secure transmission in NOMA system from the interaction perspective.

Fortunately, game theory, as a mathematical theory and tool to study competitive or cooperative behaviors, provides a powerful framework with which the optimal strategies for both/all sides under various solution concepts of equilibrium can be found. In the secure transmission strategy selections of NOMA systems, we study the interaction between the legitimate communicators and the eavesdropper based on game theory. Specifically, both sides will pay the cost and receive the corresponding benefits in the light of the strategy profile comprised of strategies they select, respectively. That is to say, one's gain is influenced not only by his/her strategy, but also by the other's. The advantage of doing so is that the optimal secure transmission strategy can be selected by analyzing the opponent's strategy, and its conservativeness can be reduced to some extent.

Motivated by this, for a NOMA system with external eavesdroppers, we focus on two typical security schemes, artificial-signal-assisted scheme (AS scheme) and relay-station-assisted scheme (RS scheme). Specifically, artificial signals are superimposed in the orthogonal subspace of weak users' transmission directions in AS scheme and relays are employed in weak users' transmission links in RS scheme, to impair the eavesdropping capability. In both schemes, the external active eavesdropper can impose interference signals while eavesdropping to reduce the quality of legitimate communication. In this paper, we first establish the system models, including channel models and signal models, and formulate the information transmission rate for each legitimate communicator and eavesdropper in AS and RS schemes, respectively. Then, the interactions around secure transmission rate, i.e., secrecy rate, are modeled as two-person zero-sum security games. For each security game model, the existence of Nash equilibrium is proved, and the pure strategy Nash equilibrium and mixed-strategy the Nash equilibrium profile are solved and analyzed. Finally, numerical simulations are conducted to validate the theoretical results, and show that AS and RS schemes can improve the secrecy rate and further enhance the physical layer security performance of NOMA systems. By analyzing the Nash equilibrium of the proposed game model, we can shed some light on the decision-making motives, which is of great significance in the design of security schemes.

The main contributions of this paper can be summarized as follows:

- We are the first to investigate artificial-signal-assisted and relay-station-assisted secure downlink transmission schemes for NOMA systems against external active eavesdropping within the framework of game theory, which integrates eavesdropper's strategy in the design of secure transmission scheme, improves secrecy rate and further enhances physical layer security performance accordingly.
- We model the confrontational interaction between them as a two-person zero-sum game with secrecy rate as utilities to characterize the impact mechanism of legitimate communicators and active eavesdropper's strategies on the security performance of the Nash system, prove the existence of the Nash equilibrium, and give the optimal (equilibrium) strategy profile which sheds some light on the design of secure NOMA downlink transmission.
- Through numerical simulations, we demonstrate that legitimate communicators can improve the security performance in terms of secrecy rate by with the help of artificial signals or relay stations, while the active eavesdropper choose to eavesdrop and impose interference signal simultaneously in AS scheme and only eavesdrop in RS scheme.

The rest of the paper is organized as follows. In Section 2, a detailed literature survey of physical layer security issues in NOMA system are discussed. Section 3 describes the system model, including channel model and signal model, in artificial-signal-assisted scheme and relay-assisted scheme, respectively. In Section 4, the interactions between the utility of the legitimate communication party and eavesdropper are modeled as two-person zero-sum game, the utilities are expressed in terms of secrecy rate, the existence of the Nash equilibrium of the proposed game models is proved, and the pure strategy the Nash equilibrium and the mixed-strategy Nash equilibrium profiles are solved and analyzed respectively. In Section 5, the proposed game models are evaluated and verified through numerical simulations. Finally, a conclusion is given in Section 6.

2 Related Works

In the pioneering works on secure communication in NOMA system from the perspective of physical layer security, existing studies in this field can be classified into two categories: the security-oriented system optimization and X-assisted security scheme. In this section, we introduce the security solutions for NOMA communication systems according to the above taxonomy.

2.1 Security-Oriented NOMA System Design

Security-oriented NOMA system design aims to achieve better security performance by optimizing the NOMA communication system in normal operation mode, such as beamforming, power allocation, user pairing, etc. In [11], the authors investigated the physical layer security problem of mm-Wave NOMA network, proposed an analysis framework of security outage probability, develop a minimal angle-difference user pairing scheme and two maximum ratio transmission beamforming schemes to further enhance the secrecy performance. The authors of [12] considered the application of NOMA to a multi-user network with mixed multicasting and unicasting traffic and proposed a design of beamforming and power allocation ensures that the unicasting performance is improved and maintaining the reception reliability of multicasting. In [13], a low-complexity subcarrier assignment scheme was proposed to maximize the achievable secrecy energy efficiency. In [14], the authors investigated the reliable and secure transmission problem of NOMA systems with untrusted near users, and proposed a joint beamforming and power allocation scheme to achieve reliable and secure

transmission. The authors of [15] designed a secure transmission scheme based on beamforming optimization to guard against both internal and external eavesdropping of downlink MISO NOMA networks. In [16], the authors considered the PLS against internal eavesdropping and gave the beamforming design and optimal power allocation problems to guarantee the positive secrecy rate of the system.

2.2 X-Assisted Security Solution

Different from security-oriented NOMA system design, X-assisted security solution enhance security by utilizing external "X", such as artificial signals, relays, etc. We mainly introduce the two mainstream techniques, artificial-signal (AS) and relay-station (RS)-assisted security solutions, respectively.

2.2.1 AS-Assisted Security Solution

The authors of [17] proposed the method of combining weak user information bearing signal and artificial signal in NOMA system to improve the security performance of the system. The security outage performance of artificial noise assisted full duplex downlink NOMA transmission in large-scale networks was investigated in [18]. In [19], the authors proposed a new hierarchical PLS model to ensure the security of the transmitted information. And an auxiliary optimal beamforming scheme was proposed to ensure the layered information security. In [20], a new frequency domain artificial noise assisted transmission strategy was proposed to improve the physical layer security of the information receiver and satisfied the energy acquisition requirements of the energy receiver. The authors investigated the problem for the design of artificial noise assisted beamforming in MISO channels from the perspective of security outage. The optimal structure was found by solving the security rate maximization problem constrained by the security outage in [21].

2.2.2 RS-Assisted Security Solution

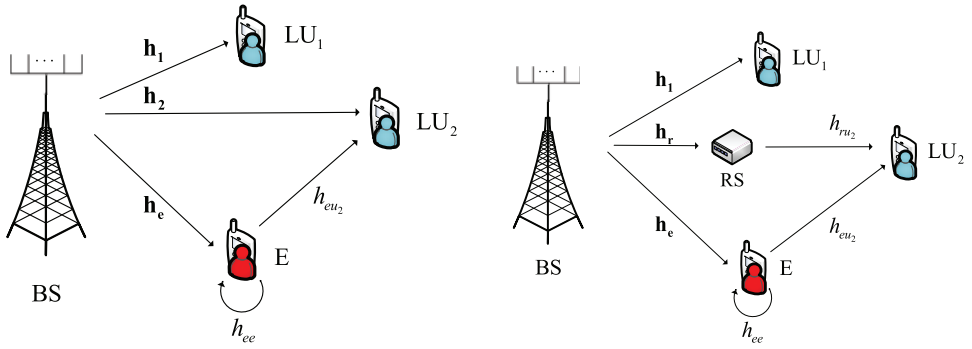
In [22], the security communication problem in multi hop relay systems was considered, the authors proposed to use full duplex relay to enhance the security of the wireless physical layer. The authors of [23] proposed a new two-level secure relay selection scheme in order to protect legitimate communication from eavesdropping. In [24], the authors considered a NOMA network with a half-duplex decode-and-forward relay to improve the physical layer security of two users. Two relay selection schemes termed decode-and-forward and amplify-and-forward protocols based optimal relay selection was proposed in [25]. In [26], the authors proposed a novel cooperative NOMA scheme to guarantee the secure transmission of a specific user via two time slots.

Although scholars have provided many security schemes in the research of NOMA physical layer security, they rarely consider the dynamic confrontational interaction between the two parties. Using the method of game theory, this paper comprehensively considers the confrontation game relationship between the eavesdropper and the legitimate communicator, establishes the interaction behavior of the two sides as a zero-sum game model, and finally realizes the secure transmission of the legitimate communicator.

3 System Model

Consider the standard downlink transmission of a typical NOMA system, consisting of a base station (BS) equipped with N antennas, an external active eavesdropper (E), and two paired legitimate users (LU_1 and LU_2) equipped with a single antenna respectively. In NOMA paired users, the user with better channel condition is called the strong user, and the user with poor channel gain is called the

weak user [1]. Without loss of generality, we assume LU_1 is a strong user and LU_2 is a weak user. In our system model, BS sends signals to legitimate users, and the signals can also be received at E who may decode the message from the received signals. Meanwhile, E may sends jamming signal to the legitimate user to decrease its data rate and therefore the secrecy rate. In addition, we also assume that E is only interested in the information of LU_2, the working mode of LU_1 and LU_2 is half-duplex, and the working mode of E is full-duplex, which can simultaneously eavesdrop and interfere and cause a certain amount of self-interference to oneself. In order to improve the security of the physical layer, two solutions are considered: superimposing artificial signal (AS) in the orthogonal null space in the transmission direction of LU_2 and adding a relay station (RS) on the transmission link of LU_2, as shown in Figs. 1a and 1b, respectively.



(a) System model of AS scheme (b) System model of RS scheme

Figure 1: System model in AS and RS schemes

3.1 Channel Model

Assume that all channels experience independent quasi-static flat Rayleigh fading, where the channel coefficients remain unchanged within one time-frequency block but change independently between different time-frequency blocks, and suffer from additive white Gaussian noise (AWGN) [27,28]. The $1 \times N$ channel gain vectors from the BS to $LU_i (i \in \{1, 2\})$ and E are denoted as $\mathbf{h}_i$ $(i \in \{1, 2\})$ and $\mathbf{h}_e$, respectively. The channel vector from E to LU_2 is denoted as h_{eu_2}, and E's self-interference link gain as h_{ee}. Also, the $1 \times N$ channel gain vector from the BS to RS is denoted by $\mathbf{h}_r$, and the channel gain from RS to LU_2 is denoted by h_{ru_2}. We denote the noise power at LU_1, LU_2, RS and E as σ_1^2, σ_2^2, σ_r^2 and σ_e^2, respectively, with the same variance. We also assume that the quality of the relay channel in the system is better than that of the weak user, and the quality of the eavesdropping channel is worse than that of the weak user. It is reasonable to assume that the base station BS knows the channel state information (CSI) of all channels between BS and $LU_i (i \in \{1, 2\})$ perfectly due to the fact that they are normal transceivers in the NOMA system.

3.2 Signal Model

3.2.1 Signal Model of AS Scheme

In the system model of the AS scheme, the base station transmits superimposed signal to users. To protect the weak user from eavesdropping, the artificial signal is superimposed in the orthogonal null space of the transmission direction. The superimposed signal transmitted from BS to $LU_i (i \in \{1, 2\})$ can be expressed as

$$x = \mathbf{w}_1 \left(\sqrt{\alpha_1 P_s} x_1 + \sqrt{\alpha_2 P_s} x_2 \right) + \sqrt{P_3} \mathbf{w}_2 x_3 \tag{1}$$

where x_1 and x_2 are the information-carrying signals to LU_1 and LU_2, x_3 is the artificial signal, P_s is the power of effective signals in the superimposed signal at the base station BS, P_3 is the transmission power of the artificial signal, α_1 and α_2 are the power sharing coefficients of LU_1 and LU_2 at the BS, with $\alpha_1 + \alpha_2 = 1$ and $\alpha_2 > \alpha_1$ for user fairness, $\mathbf{w}_1 = \frac{\mathbf{h}_2^H}{||\mathbf{h}_2||}$ and $\mathbf{w}_2$ are well designed $N \times 1$ beamforming vectors for effective signals and artificial signal, respectively, and $(\cdot)^H$ denotes the Hermitian (conjugate) transpose operation.

Then, the signals received at LU_1 and LU_2 are given by

$$y_1 = \frac{\mathbf{h}_1 \mathbf{h}_2^H}{||\mathbf{h}_2||} \left(\sqrt{\alpha_1 P_s} x_1 + \sqrt{\alpha_2 P_s} x_2 \right) + \mathbf{h}_1 \mathbf{w}_2 \sqrt{P_3} x_3 + n_1 \tag{2}$$

and

$$y_2 = \frac{\mathbf{h}_2 \mathbf{h}_2^H}{||\mathbf{h}_2||} \left(\sqrt{\alpha_1 P_s} x_1 + \sqrt{\alpha_2 P_s} x_2 \right) + \mathbf{h}_2 \mathbf{w}_2 \sqrt{P_3} x_3 + h_{eu_2} \sqrt{P_e} x_e + n_2, \tag{3}$$

where $\mathbf{h}_i \sim \mathscr{CN}(0, \lambda_i)$, n_1 and n_2 are the additive white Gaussian noise (AWGN) at LU_1 and LU_2, with $n_i \, (i \in \{1, 2\}) \sim \mathscr{CN}\left(0, \sigma^2\right)$, where $\mathscr{CN}(\cdot, \cdot)$ is the complex Gaussian distribution, x_e and P_e represent the interference signal and its power emitted by the eavesdropper E.

Since the artificial signal is allocated into the orthogonal null space of the channel for NOMA users, we have $\mathbf{h}_1 \mathbf{w}_2 = 0$ and $\mathbf{h}_2 \mathbf{w}_2 = 0$ [29]. Then formulas (2) and (3) can be rewritten as

$$y_1 = \frac{\mathbf{h}_1 \mathbf{h}_2^H}{||\mathbf{h}_2||} \left(\sqrt{\alpha_1 P_s} x_1 + \sqrt{\alpha_2 P_s} x_2 \right) + n_1 \tag{4}$$

and

$$y_2 = \frac{\mathbf{h}_2 \mathbf{h}_2^H}{||\mathbf{h}_2||} \left(\sqrt{\alpha_1 P_s} x_1 + \sqrt{\alpha_2 P_s} x_2 \right) + h_{eu_2} \sqrt{P_e} x_e + n_2. \tag{5}$$

According to the power-domain NOMA principle, the strong user decodes his message by employing SIC after decoding the message of the weak user, and the weak user directly decodes his message by treating the signal of the strong user as noise. As a result, the signal-to-interference-to-noise ratio (SINR) at LU_1 in the process of decoding its own information is

$$r_{12} = \frac{\alpha_2 \rho_s \left| h_{su_1} \right|^2}{\alpha_1 \rho_s \left| h_{su_1} \right|^2 + 1} \tag{6}$$

and

$$r_{11} = \alpha_1 \rho_s \left| h_{su_1} \right|^2, \tag{7}$$

where $h_{su_1} = \frac{\mathbf{h}_1 \mathbf{h}_2^H}{||\mathbf{h}_2||}$, and $\rho_s = \frac{P_s}{\sigma^2}$ is the transmit signal to noise ratio (SNR) of BS. Then, the data rate for LU_1 can be shown as

$$R_1 = \log_2 (1 + r_{11}) . \tag{8}$$

Similarly, LU_2 decodes its own information directly, and the SINR can be expressed as

$$r_{22} = \frac{\alpha_2 \rho_s \left|h_{su_2}\right|^2}{\alpha_1 \rho_s \left|h_{su_2}\right|^2 + \rho_e \left|h_{eu_2}\right|^2 + 1}, \tag{9}$$

where $h_{su_2} = \frac{\mathbf{h}_2 \mathbf{h}_2^H}{||\mathbf{h}_2||}$, and $\rho_e = \frac{P_e}{\sigma^2}$ denotes the transmit signal-to-noise ratio (SNR) from the eavesdropper E to the weak user. Then, the data rate for LU_2 can be shown as

$$R_2 = \log_2 (1 + r_{22}) . \tag{10}$$

For the eavesdropper E, the received signal can be expressed as

$$y_e = \frac{\mathbf{h}_e \mathbf{h}_2^H}{||\mathbf{h}_2||} \left(\sqrt{\alpha_1 P_s} x_1 + \sqrt{\alpha_2 P_s} x_2\right) + \mathbf{h}_e \mathbf{w}_2 \sqrt{P_3} x_3 + h_{ee} \sqrt{\eta P_e} x_e + n_e \tag{11}$$

where $\mathbf{h}_e \sim \mathscr{CN}(0, \lambda_e)$, $n_e \sim \mathscr{CN}\left(0, \sigma^2\right)$, and η is the residual self-interference coefficient.

The SINR at the eavesdropper E to decode the message for LU_2 can be expressed as

$$r_e = \frac{\alpha_2 \rho_s \left|h_{se_1}\right|^2}{\alpha_1 \rho_s \left|h_{se_1}\right|^2 + \rho_3 \left|h_{se_2}\right|^2 + \eta \rho_e \left|h_{ee}\right|^2 + 1}, \tag{12}$$

where $h_{se_1} = \frac{\mathbf{h}_e \mathbf{h}_2^H}{||\mathbf{h}_2||}$, $h_{se_2} = \mathbf{h}_e \mathbf{w}_2$, and $\rho_3 = \frac{P_3}{\sigma^2}$. Then, the data rate of E to eavesdrop LU_2 can be given by

$$R_e = \log_2 (1 + r_e) . \tag{13}$$

Similarly, when the eavesdropper E does not emit interference signals, i.e., $\rho_e = 0$, or the BS does not superimpose artificial signals, then we have

$$\begin{cases} r'_{22} = r_{22}|_{\rho e=0} = \dfrac{\alpha_2 \rho_s \left|h_{su_2}\right|^2}{\alpha_1 \rho_s \left|h_{su_2}\right|^2 + 1}, \\ r'_e = r_e|_{\rho e=0} = \dfrac{\alpha_2 \rho_s \left|h_{se_1}\right|^2}{\alpha_1 \rho_s \left|h_{se_1}\right|^2 + \rho_3 \left|h_{se_2}\right|^2 + 1}, \\ r''_e = r_e|_{\rho_3=0} = \dfrac{\alpha_2 \rho_s \left|h_{se_1}\right|^2}{\alpha_1 \rho_s \left|h_{se_1}\right|^2 + \eta \rho_e |h_{ee}|^2 + 1}, \\ r'''_e = r_e|_{\rho e=0, \rho_3=0} = \dfrac{\alpha_2 \rho_s \left|h_{se_1}\right|^2}{\alpha_1 \rho_s \left|h_{se_1}\right|^2 + 1}. \end{cases} \tag{14}$$

3.2.2 Signal Model of RS Scheme

In this scheme, the relay RS works in full duplex mode, and can decode and forward at the same time. In the transmission process, the base station BS first transmits a superimposed signal to the legitimate user LU_1 and RS. After receiving the signal, the legitimate user LU_1 uses SIC technology to decode the signal to obtain its own message, and the relay RS decodes the message for LU_2 and forward it. Since the RS first decodes and then forward the message, it can perfectly eliminate the

influence of self-interference [30]. The eavesdropper E eavesdrops at the base station BS, emits an interference signal at a certain power level to the legitimate user LU_2, and suffers from the influence of self-interference which cannot be perfectly eliminated.

In the system model of the RS scheme, the superimposed signal transmitted to LU_1 and RS at the BS is expressed as

$$x = \mathbf{w}_1 \left(\sqrt{\alpha_1 P_s} x_1 + \sqrt{\alpha_2 P_s} x_2 \right). \tag{15}$$

The signals received at LU_1 and RS are respectively given by

$$y_1 = \frac{\mathbf{h}_1 \mathbf{h}_2^H}{||\mathbf{h}_2||} \left(\sqrt{\alpha_1 P_s} x_1 + \sqrt{\alpha_2 P_s} x_2 \right) + n_1 \tag{16}$$

and

$$y_r = \frac{\mathbf{h}_r \mathbf{h}_2^H}{||\mathbf{h}_2||} \left(\sqrt{\alpha_1 P_s} x_1 + \sqrt{\alpha_2 P_s} x_2 \right) + n_r, \tag{17}$$

where $\mathbf{h}_r \sim \mathscr{CN}(0, \lambda_r)$, $n_r \sim \mathscr{CN}\left(0, \sigma^2\right)$, and the rest variables are similar to that in the AS scheme.

The SINR at RS to decode the message for LU_2 can be expressed as

$$r_{sr} = \frac{\alpha_2 \rho_s |h_{sr}|^2}{\alpha_1 \rho_s |h_{sr}|^2 + 1}, \tag{18}$$

where $h_{sr} = \frac{\mathbf{h}_r \mathbf{h}_2^H}{||\mathbf{h}_2||}$.

The legitimate user LU_2 receives the signal forwarded by the RS, which can be expressed as

$$y_2 = h_{ru_2} \sqrt{P_r} x_2 + h_{eu_2} \sqrt{P_e} w + n_e, \tag{19}$$

where $h_{ru_2} \sim \mathscr{CN}\left(0, \lambda_{ru_2}\right)$, $h_{eu_2} \sim \mathscr{CN}\left(0, \lambda_{eu_2}\right)$, λ_{ru_2} and λ_{eu_2} are the variance of complex Gaussian variables h_{ru_2} and h_{eu_2}, respectively, and P_r is the transmit power of RS to forward the message for LU_2 with $P_r = P_s$.

The SINR at LU_2 to decode his own message can be expressed as

$$r_{r2} = \frac{\rho_r \left| h_{ru_2} \right|^2}{\rho_e \left| h_{eu_2} \right|^2 + 1}. \tag{20}$$

For such a link from the BS to LU_2 with the relay RS, the achievable data rate can be expressed as $\min\left\{\log_2(1 + r_{sr}), \log_2(1 + r_{r2})\right\}$, i.e., with an equivalent SINR as

$$r_2 = \min\{r_{sr}, r_{r2}\}, \tag{21}$$

then the data rate for LU_2 can be expressed as

$$R_2 = \log_2(1 + r_2). \tag{22}$$

For the eavesdropper E, the received signal can be given as

$$y_e = \frac{\mathbf{h}_e \mathbf{h}_2^H}{||\mathbf{h}_2||} \left(\sqrt{\alpha_1 P_s} x_1 + \sqrt{\alpha_2 P_s} x_2 \right) + h_{ee} \sqrt{\eta P_e} w + n_e, \tag{23}$$

and the SINR at the eavesdropper E to decode the message for LU_2 can be expressed as

$$r_e = \frac{\alpha_2 \rho_s |h_{se}|^2}{\alpha_1 \rho_s |h_{se}|^2 + \eta \rho_e |h_{ee}|^2 + 1}, \tag{24}$$

where $h_{se} = \frac{\mathbf{h}_e \mathbf{h}_2{}^H}{||\mathbf{h}_2||}$. Accordingly, the eavesdropping rate can be expressed as $R_e = \log_2(1 + r_e)$.

Similarly, when the eavesdropper E does not emit interference signals, i.e., $\rho_e = 0$, we have

$$\begin{cases} r'_{r2} = r_{r2}|_{\rho_e=0} = \rho_r |h_{ru_2}|^2, \\ r'_e = r_e|_{\rho_e=0} = \dfrac{\alpha_2 \rho_s |h_{se}|^2}{\alpha_1 \rho_s |h_{se}|^2 + 1}. \end{cases} \tag{25}$$

4 Game Model

In this article, we assume that the eavesdropper E only eavesdrops on LU_2. Therefore, the secrecy rate of the system can be expressed as

$$C^{\text{sec}} = [R_2 - R_e]^+ \tag{26}$$

where $[\cdot]^+ = \max\{\cdot, 0\}$.

In the downlink NOMA transmission system with external eavesdropper E, the legitimate user LU_2 exerts to maximize the secrecy rate, which means that he needs to increase his own data rate and/or reduce the eavesdropping rate of E. On the contrary, for the eavesdropper E, he attempts to minimize the secrecy rate by increasing his own eavesdropping rate and/or reducing the data rate of LU_2. This shows that one person or group can gain something only by causing another person or group to lose it, and the sum of the gains and losses is always 'zero'. Therefore, we model the non-cooperative behavior between the legitimate users and the malicious eavesdropper in both AS and RS schemes as a non-cooperative two-person zero-sum game, respectively.

4.1 Game Modeling

4.1.1 Game Modeling for the AS Scheme

In the AS scheme, we regard the base station BS and users $LU_i (i \in \{1, 2\})$ as a legitimate party, who can choose to transmit only the effective signals or the signals superimposed with artificial signal to improve the secrecy rate of the system. The eavesdropper E can choose the strategy of only eavesdropping and not emitting the interference signal, or the strategy of eavesdropping while emitting the interference signal at the same time. We establish the zero-sum game model for secure downlink transmission in strategic form as follows.

Definition 4.1. In the AS scheme, the zero-sum game $G_1 = \left(N_1, (S_i)_{i \in N_1}, (u_i)_{i \in N_1}\right)$ is a triplet, where:

- $N_1 = \{L, E\}$ is a set of players in the game. L represents the legitimate party consisting of the base station BS and the legitimate users $LU_i (i \in \{1, 2\})$, and E represents the external malicious eavesdropper.
- S_i is the set of possible strategies for player $i \in N_1$. For L, its strategy set can be expressed as $S_L = \{A, O\}$, where A represents the strategy of transmitting the effective signals superimposed with artificial signal, and O represents the strategy of transmitting only the effective signals without artificial signal. For E, its strategy set can be expressed as $S_E = \{I, N\}$, where I

means eavesdropping and emitting interference signal at the same time, and N means only eavesdropping and not emitting interference signal.

- u_i is the utility function of the player $i \in N_1$. In this paper, the secrecy rate of the system is taken as the utility function of the game.

According to Definition 4.1, we can further formulate the utility matrix for the zero-sum game, as shown in Table 1. In the utility matrix, there are four strategy profiles in all, and they are (A, I), (A, N), (O, I) and (O, N). Take the profile (A, I) for example, it means the legitimate party L chooses the strategy A and the eavesdropper chooses the strategy I. We will analyze each strategy profile in detail and give their utility functions as follows.

Table 1: Utility matrix of the zero-sum game in the AS scheme

		Eavesdropper	
		I	N
Legitimate party	A	C_{AI}^{sec}	C_{AN}^{sec}
	O	C_{OI}^{sec}	C_{ON}^{sec}

For the profile (A, I), the legitimate party L chooses to superimpose the artificial signal AS in the null space of the weak user LU_2 transmission direction to protect the message for the weak user LU_2. The eavesdropper E chooses to emit an interference signal to the weak user LU_2 while eavesdropping. In such a profile, the utility function of the legitimate party can be expressed as

$$C_{AI}^{\text{sec}} = [\log_2(1 + r_{22}) - \log_2(1 + r_e)]^+ \tag{27}$$

$$= \left[\log_2\left(1 + \frac{\alpha_2\rho_s|h_{su_2}|^2}{\alpha_1\rho_s|h_{su_2}|^2 + \rho_e|h_{eu_2}|^2 + 1}\right) - \log_2\left(1 + \frac{\alpha_2\rho_s|h_{se_1}|^2}{\alpha_1\rho_s|h_{se_1}|^2 + \rho_3|h_{se_2}|^2 + \eta\rho_e|h_{ee}|^2 + 1}\right)\right]^+ \tag{28}$$

For the profile (A, N), the legitimate party L chooses to superimpose the artificial signal AS in the null space of the transmission direction. At this time, the eavesdropper E chooses to eavesdrop only, i.e., $P_e = 0$. Then the utility function is given by

$$C_{AN}^{\text{sec}} = [\log_2(1 + r'_{22}) - \log_2(1 + r'_e)]^+ \tag{29}$$

$$= \left[\log_2\left(1 + \frac{\alpha_2\rho_s|h_{su_2}|^2}{\alpha_1\rho_s|h_{su_2}|^2 + 1}\right) - \log_2\left(1 + \frac{\alpha_2\rho_s|h_{se_1}|^2}{\alpha_1\rho_s|h_{se_1}|^2 + \rho_3|h_{se_2}|^2 + 1}\right)\right]^+ \tag{30}$$

For the profile (O, I), the legitimate party L chooses not to superimpose the artificial signal AS to protect the message for LU_2, i.e., $P_3 = 0$. The eavesdropper E chooses to conduct both eavesdropping and interfering at the same time. The utility function can be expressed as

$$C_{OI}^{\text{sec}} = [\log_2(1 + r_{22}) - \log_2(1 + r''_e)]^+ \tag{31}$$

$$= \left[\log_2\left(1 + \frac{\alpha_2\rho_s|h_{su_2}|^2}{\alpha_1\rho_s|h_{su_2}|^2 + \rho_e|h_{eu_2}|^2 + 1}\right) - \log_2\left(1 + \frac{\alpha_2\rho_s|h_{se_1}|^2}{\alpha_1\rho_s|h_{se_1}|^2 + \eta\rho_e|h_{ee}|^2 + 1}\right)\right]^+ \tag{32}$$

For the profile (O, N), the legitimate party L does not choose the strategy of superimposing the artificial signal AS, and the eavesdropper E only conducts wiretapping. Then, the utility function is given by

$$C_{ON}^{\text{sec}} = [\log_2(1 + r'_{22}) - \log_2(1 + r'''_e)]^+ \tag{33}$$

$$= \left[\log_2\left(1+\frac{\alpha_2\rho_s|h_{su_2}|^2}{\alpha_1\rho_s|h_{su_2}|^2+1}\right)-\log_2\left(1+\frac{\alpha_2\rho_s|h_{se_1}|^2}{\alpha_1\rho_s|h_{se_1}|^2+1}\right)\right]^+ \tag{34}$$

4.1.2 Game Modeling for the RS Scheme

In the system model of the RS scheme, the legitimate party L can choose to use the relay transmission strategy or the direct link transmission strategy. The eavesdropper E can choose from the strategies of eavesdropping strategy with or without emitting interference signal. We can establish the game model for the RS scheme as follows.

Definition 4.2. In the RS scheme, the zero-sum game $G_2 = \left(N_2, (S_j)_{j\in N_2}, (u_j)_{j\in N_2}\right)$ is a triplet, where:

- $N_2 = \{L, E\}$ is a set of players in the game. Same as in the game G_1, L denotes the legitimate communication party, and E the eavesdropper.
- S_j is the set of available strategies for the player $j \in N_2$. For L, its strategy set can be expressed as $S_L = \{R, D\}$, where R represents the strategy of transmission with RS, and D represents the strategy of direct link transmission. For E, its strategy set can be expressed as $S_E = \{I, N\}$, where I means eavesdropping and emitting interference signals, and N means not emitting interference signals but only eavesdropping.
- u_j is the utility function of the player $j \in N_2$.

Similarly, we can formulate the utility matrix as shown in Table 2, and the utility functions can be expressed as follows:

$$C_{RI}^{\text{sec}} = [\log_2(1+\min\{r_{sr}, r_{r2}\}) - \log_2(1+r_e)]^+ \tag{35}$$

$$= \left[\log_2\left(1+\min\left\{\frac{\alpha_2\rho_s|h_{sr}|^2}{\alpha_1\rho_s|h_{sr}|^2+1}, \frac{\rho_r|h_{ru_2}|^2}{\rho_e|h_{eu_2}|^2+1}\right\}\right) - \log_2\left(1+\frac{\alpha_2\rho_s|h_{se}|^2}{\alpha_1\rho_s|h_{se}|^2+\eta\rho_e|h_{ee}|^2+1}\right)\right]^+ \tag{36}$$

$$C_{RN}^{\text{sec}} = \left[\log_2\left(1+\min\left\{r_{sr}, r'_{r2}\right\}\right) - \log_2\left(1+r'_e\right)\right]^+ \tag{37}$$

$$= \left[\log_2\left(1+\min\left\{\frac{\alpha_2\rho_s|h_{sr}|^2}{\alpha_1\rho_s|h_{sr}|^2+1}, \rho_r|h_{ru_2}|^2\right\}\right) - \log_2\left(1+\frac{\alpha_2\rho_s|h_{se}|^2}{\alpha_1\rho_s|h_{se}|^2+1}\right)\right]^+ \tag{38}$$

$$C_{DI}^{\text{sec}} = [\log_2(1+r_{s2}) - \log_2(1+r_e)]^+ \tag{39}$$

$$= \left[\log_2\left(1+\frac{\alpha_2\rho_s|h_{su_2}|^2}{\alpha_1\rho_s|h_{su_2}|^2+\rho_e|h_{eu_2}|^2+1}\right) - \log_2\left(1+\frac{\alpha_2\rho_s|h_{se}|^2}{\alpha_1\rho_s|h_{se}|^2+\eta\rho_e|h_{ee}|^2+1}\right)\right]^+ \tag{40}$$

$$C_{DN}^{\text{sec}} = [\log_2(1+r'_{s2}) - \log_2(1+r'_e)]^+ \tag{41}$$

$$= \left[\log_2\left(1+\frac{\alpha_2\rho_s|h_{su_2}|^2}{\alpha_1\rho_s|h_{su_2}|^2+1}\right) - \log_2\left(1+\frac{\alpha_2\rho_s|h_{se}|^2}{\alpha_1\rho_s|h_{se}|^2+1}\right)\right]^+ \tag{42}$$

where r_{s2} and r'_{s2} are the same with r_{22} and r'_{22} in the AS scheme, respectively.

4.2 Analysis of Game Equilibrium

In this subsection, we will first prove the existence of the Nash equilibrium for the zero-sum game in both AS and RS schemes, and then solve and analyze the pure strategy Nash equilibrium and the mixed strategy Nash equilibrium, respectively.

Table 2: Utility matrix of the zero-sum game in the RS scheme

		Eavesdropper	
		I	N
Legitimate party	R	C_{RI}^{sec}	C_{RN}^{sec}
	D	C_{DI}^{sec}	C_{DN}^{sec}

4.2.1 Existence of NE

We give the results of Nash Equilibrium of the games G_1 and G_2 by the following two theorems.

Theorem 4.1. There is at least one Nash equilibrium in the zero-sum game G_1 of the AS scheme.

Proof. In the zero-sum game G_1, the set of players $N_1 = \{L, E\}$ has two players, which is limited. Additionally, the set of strategies $S_L = \{A, O\}$ and $S_E = \{I, N\}$ are both limited. According to the existence theorem of Nash equilibrium, there is at least one Nash equilibrium in the game G_1.

Theorem 4.2. There is at least one Nash equilibrium in the zero-sum game G_2 of the RS scheme.

The proof is similar to that of Theorem 4.1 and thus omitted for simplicity.

4.2.2 Pure-strategy Nash Equilibrium

In this subsection, we solve the pure-strategy Nash equilibrium of the game G_1 and G_2, respectively. The pure-strategy Nash equilibrium and the corresponding strategies for the games in AS and RS schemes are provided by the following two theorems.

Theorem 4.3. The pure-strategy Nash equilibrium (A,I) exists in the game G_1 provided $C_{AI}^{\text{sec}} < C_{AN}^{\text{sec}}$ and (A,N) exists provided $C_{AI}^{\text{sec}} > C_{AN}^{\text{sec}}$.

Proof. According to the analysis aforementioned and Eqs. (28), (30), (32) and (34), it is easy to find that the utility functions in Table 1 satisfy the following conditions:

$$C_{AN}^{\text{sec}} > C_{ON}^{\text{sec}}, \quad C_{AI}^{\text{sec}} > C_{OI}^{\text{sec}}. \tag{43}$$

Thus, the strategy A is the dominating strategy for the legitimate party in the game G_1, that is, the legitimate party L will choose strategy A, no matter what E chooses. Next, we will prove the conditions for existence for two pure-strategy equilibrium, respectively.

First, if $C_{AI}^{\text{sec}} < C_{AN}^{\text{sec}}$ holds, we have $C_{AN}^{\text{sec}} > C_{AI}^{\text{sec}} > C_{OI}^{\text{sec}}$, and we can observe the following two facts. One is that the utility of L will decrease from C_{AI}^{sec} to C_{OI}^{sec} if L changes its strategy from A to O, i.e., changing the strategy of superimposing artificial signals to not superimposing artificial signals, which violates his goal of maximizing the secrecy rate. Another, if the external eavesdropper E changes its strategy from I to N, i.e., changing the strategy of transmitting interference signals to not transmitting interference signals and only eavesdropping, the utility of E will increase from C_{AI}^{sec} to C_{AN}^{sec}, and yet his goal is to minimize the secrecy rate. In summary, neither the legitimate party L nor the external eavesdropper E could benefit more by unilaterally deviating his strategy from the strategy profile (A, I). Therefore, the pure-strategy Nash equilibrium of the game is (A,I) provided $C_{AI}^{\text{sec}} < C_{AN}^{\text{sec}}$.

Second, if $C_{AI}^{\text{sec}} > C_{AN}^{\text{sec}}$ holds, we have $C_{AI}^{\text{sec}} > C_{AN}^{\text{sec}} > C_{ON}^{\text{sec}}$. Similarly, we can also find that neither the legitimate party L nor the external eavesdropper E could benefit more by unilaterally deviating his

strategy from the strategy profile (A, N), i.e., (A, N) is a pure-strategy Nash equilibrium of G_1 provided $C_{AI}^{\text{sec}} > C_{AN}^{\text{sec}}$.

This completes the proof.

Theorem 4.4. The pure-strategy Nash equilibrium *(R,N)* exists in the game G_2 provided $C_{RI}^{\text{sec}} > C_{RN}^{\text{sec}}$, and *(R,I)* exists provided $C_{RI}^{\text{sec}} < C_{RN}^{\text{sec}}$.

Proof. Since we have assumed $|h_{sr}|^2 > |h_{su_2}|^2$ and $|h_{ru_2}|^2 > |h_{su_2}|^2$, according to the analysis aforementioned and Eqs. (36), (38), (40) and (42), it is easy to find that the utility functions in Table 2 satisfy the following conditions:

$$C_{RN}^{\text{sec}} > C_{DN}^{\text{sec}}, \quad C_{RI}^{\text{sec}} > C_{DI}^{\text{sec}}. \tag{44}$$

Thus, the strategy R is the dominating strategy for the legitimate party in the game G_2, that is, the legitimate party L will choose strategy R, no matter what E chooses. Next, we will prove the conditions for existence for two pure-strategy equilibrium, respectively.

First, if $C_{RI}^{\text{sec}} < C_{RN}^{\text{sec}}$ holds, we have $C_{RN}^{\text{sec}} > C_{RI}^{\text{sec}} > C_{DI}^{\text{sec}}$, and we can observe the following two facts. One is that the utility of L will decrease from C_{RI}^{sec} to C_{DI}^{sec} if L changes its strategy from R to D, i.e., changing the strategy of transmission with RS to without RS, which violates his goal of maximizing the secrecy rate. Another, if the external eavesdropper E changes its strategy from I to N, i.e., changing the strategy of transmitting interference signals to not transmitting interference signals and only eavesdropping, the utility of E will increase from C_{RI}^{sec} to C_{RN}^{sec}, and yet his goal is to minimize the secrecy rate. In summary, neither the legitimate party L nor the external eavesdropper E could benefit more by unilaterally deviating his strategy from the strategy profile (R, I). Therefore, the pure-strategy Nash equilibrium of the game is (R, I) provided $C_{RI}^{\text{sec}} < C_{RN}^{\text{sec}}$.

Second, if $C_{RI}^{\text{sec}} > C_{RN}^{\text{sec}}$ holds, we have $C_{RI}^{\text{sec}} > C_{RN}^{\text{sec}} > C_{DN}^{\text{sec}}$. Similarly, we can also find that neither the legitimate party L nor the external eavesdropper E could benefit more by unilaterally deviating his strategy from the strategy profile (R, N), i.e., (R, N) is a pure-strategy Nash equilibrium of G_1 provided $C_{RI}^{\text{sec}} > C_{RN}^{\text{sec}}$.

This completes the proof.

4.2.3 Algorithms for Pure Strategy Nash Equilibrium Strategy

According to the analysis in the previous section, there are two situations in the pure strategy Nash equilibrium of the game G_1 and G_2. Therefore, we propose two algorithms to determine the pure strategy Nash equilibrium strategy. The algorithms are described as follows.

Algorithm 1: Equilibrium judgment algorithm in the game G_1

1: Initialization: $|h_{su_2}|^2$, $|h_{eu_2}|^2$, $|h_{se_1}|^2$, $|h_{se_2}|^2$, $|h_{ee}|^2$, α_2, α_1, η, ρ_s
2: Input: ρ_e, ρ_3
3: Calculate r_{22},r_e, r'_{22},r'_e according to Eqs. (9), (12), (14), (15),
4: if $(r'_{22} > r'_e$ and $r_{22} < r_e)$ or $(r_{22} > r_e$ and $\frac{1+r22'}{1+r_{22}} \cdot \frac{1+r_e}{1+r'_e} > 1)$
Select the pure-strategy Nash equilibrium *(A,I)*
5: else if $(r'_{22} < r'_e$ and $r_{22} > r_e)$ or $(r'_{22} > r'_e$ and $\frac{1+r_{22}}{1+r'_{22}} \cdot \frac{1+r'_e}{1+r_e} > 1)$
Select the pure-strategy Nash equilibrium *(A,N)*
6: end if

Algorithm 2: Equilibrium judgment algorithm in the game G_2

1: Initialization: $|h_{su_2}|^2$, $|h_{eu_2}|^2$, $|h_{se_1}|^2$, $|h_{se_2}|^2$, $|h_{ee}|^2$,$|h_{sr}|^2$, $|h_{ru_2}|^2$, α_2, α_1, η, ρ_s
2: Input: ρ_e, ρ_r
3: Calculate r_{sr},r_{r2},r_e,r'_{r2},r'_e according to Eqs. (18), (20), (24), (25),
4: if ($\min\{r_{sr}, r_{r2}\} > r_e$ and $\min\left\{r_{sr}, rr'_2\right\} < r'_e$)

or ($\min\{r_{sr}, r_{r2}\} > r_e$ and $\min\{r_{sr}, r'_{r2}\} > r'_e$ and $\frac{1+\min\{r_{sr}, r_{r2}\}}{1+r_e} \cdot \frac{1+r'_e}{1+\min\{r_{sr}, r'_{r2}\}} > 1$)

Select the pure-strategy Nash equilibrium (R,N)

5: else if ($\min\{r_{sr}, r_{r2}\} < r_e$ and $\min\{r_{sr}, r'_{r2}\} > r'_e$)

or ($\min\{r_{sr}, r_{r2}\} > r_e$ and $\min\{r_{sr}, r'_{r2} > r'_e$ and $\frac{1+\min r_{sr}, r'_{r2}}{1+r'_e} \cdot \frac{1+r_e}{1+\min\{r_{sr}, r_{r2}\}} > 1$)

Select the pure-strategy Nash equilibrium (R,I)

6: end if

4.2.4 Mixed-Strategy Nash Equilibrium

Different from the deterministic selection of a strategy in pure-strategy Nash equilibrium, a player may select each pure strategy with a certain probability, which leads to the concept of a mixed strategy. For each player, a mixed strategy consists of a number of possible actions and a probability distribution which corresponds to how frequently each action would be selected by the player. In this subsection, we will discuss the mixed-strategy Nash equilibrium of the game G_1 and G_2, respectively.

The mixed strategy Nash equilibrium in AS and RS schemes are given by the following two theorems.

Theorem 4.5. The utility of the mixed strategy Nash equilibrium (p^*, q^*) of the game G_1 is written as

$$U^*(p^*, q^*) = \frac{C_{AI}^{\text{sec}} C_{ON}^{\text{sec}} - C_{AN}^{\text{sec}} C_{OI}^{\text{sec}}}{C_{AI}^{\text{sec}} + C_{ON}^{\text{sec}} - C_{OI}^{\text{sec}} - C_{AN}^{\text{sec}}},$$

where $p^* = \frac{C_{ON}^{\text{sec}} - C_{OI}^{\text{sec}}}{C_{AI}^{\text{sec}} + C_{ON}^{\text{sec}} - C_{OI}^{\text{sec}} - C_{AN}^{\text{sec}}}$, $q^* = \frac{C_{ON}^{\text{sec}} - C_{AN}^{\text{sec}}}{C_{AI}^{\text{sec}} + C_{ON}^{\text{sec}} - C_{OI}^{\text{sec}} - C_{AN}^{\text{sec}}}$.

Proof. In the AS scheme, we define the probability distribution $P = (p, 1-p)$ for the legitimate party L, where $0 \le p \le 1$ is the probability with which L selects the strategy A, i.e., the selection of superimposing artificial signals. Hence, $1-p$ is the probability with which L selects the strategy O. Similarly, we define the mixed strategy for the eavesdropper E as $Q = (q, 1-q)$, where $0 \le q \le 1$ is the probability with which E selects the strategy I, i.e., the selection of emitting interference signals, and $1-q$ the probability of selecting the strategy N. Hence, the utility of the mixed strategy can be expressed as $U(p,q) = PCQ^T$.

The legitimate party L can find his optimal strategy by solving the following optimization problem: $\max_p \min_q PCQ^T$, where $C = \begin{bmatrix} C_{AI}^{\text{sec}} & C_{AN}^{\text{sec}} \\ C_{OI}^{\text{sec}} & C_{ON}^{\text{sec}} \end{bmatrix}$ is the utility matrix in Table 1, and $(\cdot)^T$ is the transpose operation. The eavesdropper E can obtain his optimal strategy by solving the the problem: $\min_q \max_p PCQ^T$.

Solving the above two optimization problem yields the optimal probability value of each strategy selected by L and E as

$$p^* = \frac{C_{ON}^{sec} - C_{OI}^{sec}}{C_{AI}^{sec} + C_{ON}^{sec} - C_{OI}^{sec} - C_{AN}^{sec}}, q^* = \frac{C_{ON}^{sec} - C_{AN}^{sec}}{C_{AI}^{sec} + C_{ON}^{sec} - C_{OI}^{sec} - C_{AN}^{sec}}.$$

Then substitute p^* and q^* into PCQ^T, the Nash equilibrium utility of the mixed strategy of the game G_1 is written as

$$U^*(p^*, q^*) = \frac{C_{AI}^{sec} C_{ON}^{sec} - C_{AN}^{sec} C_{OI}^{sec}}{C_{AI}^{sec} + C_{ON}^{sec} - C_{OI}^{sec} - C_{AN}^{sec}}.$$

This completes the proof.

Theorem 4.6. The utility of the mixed strategy Nash equilibrium (p^*, q^*) of the game G_2 is written as

$$U^*(p^*, q^*) = \frac{C_{RI}^{sec} C_{DN}^{sec} - C_{RN}^{sec} C_{DI}^{sec}}{C_{RI}^{sec} + C_{DN}^{sec} - C_{DI}^{sec} - C_{RN}^{sec}},$$

where $p^* = \frac{C_{DN}^{sec} - C_{DI}^{sec}}{C_{RI}^{sec} + C_{DN}^{sec} - C_{DI}^{sec} - C_{RN}^{sec}}, q^* = \frac{C_{DN}^{sec} - C_{RN}^{sec}}{C_{RI}^{sec} + C_{DN}^{sec} - C_{DI}^{sec} - C_{RN}^{sec}}.$

The proof is similar to Theorem 4.5, and thus omitted for simplicity.

5 Numerical Simulation and Result Analysis

5.1 Simulation Setting

The main parameter settings in the simulation of AS and RS scheme are as follows. The power allocation coefficients of strong users and weak users in the NOMA system are $\alpha_1 = 0.2$, $\alpha_2 = 0.8$, respectively, the transmission signal-to-noise ratio at each node ranges from 0 to 30 dB, and the residual self-interference coefficient η during the process of eavesdropping transmitting interference power is 0.1.

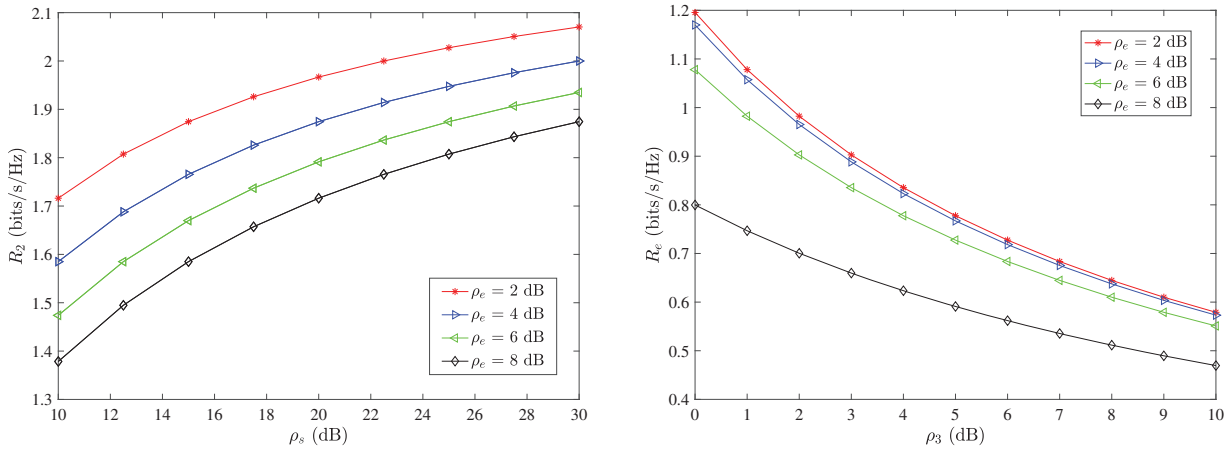
5.2 Result Analysis in the AS Scheme

This subsection mainly analyzes the data rate of the weak user and the eavesdropper, as well as the gains of the pure and mixed strategy in the AS scheme.

5.2.1 Analysis of Data Rate

The curves in Fig. 2a show the data rate R_2 of LU_2 with respect to ρ_s under different ρ_e in the AS scheme. It can be seen from the figure that when ρ_e is constant, R_2 increases as ρ_s increases; when ρ_s is constant, R_2 decreases as ρ_e increases, which implies that, when the power of the interference signal transmitted by E is larger, the information transmission rate of LU_2 can be reduced, so that the security rate of the system is smaller, and its purpose can be achieved. The legitimate party L can appropriately increase the total transmission power to weaken the influence of E interference.

Fig. 2b shows the change of the data rate of E with ρ_3 in the AS scheme. It can be seen from the figure that when ρ_e is constant, R_e decreases as ρ_3 increases; when ρ_3 is constant, R_e decreases as ρ_e increases. It shows that while E is transmitting interference signals, although it can reduce the information transmission rate of LU_2, it will also reduce its own information transmission rate. Therefore, E needs to consider the power value of the transmitted interference signal in the game. The legitimate party can reduce R_e by increasing the power of the artificial signal, thereby increasing the security rate of the system and improving the security of the physical layer.



(a) Data rate of LU_2 (b) Data rate of E

Figure 2: Data rate in the AS scheme

5.2.2 *Analysis of the Pure Strategy Nash Equilibrium and Benefits*

According to the aforementioned analysis, the pure strategy Nash equilibrium depends on the parameter ρ_e and ρ_3. We show the effect of ρ_e and ρ_3 on the pure strategy Nash equilibrium in Fig. 3, and we can find the following results. First, the equilibrium strategy changes from (A, N) to (A, I) as ρ_e increases if $\rho_3 < M$. Second, if $\rho_3 > M$ the equilibrium strategy stays at (A, I) no matter how ρ_e changes. We also have similar results for ρ_e, ρ_3 and some point M' at the axis of ρ_e.

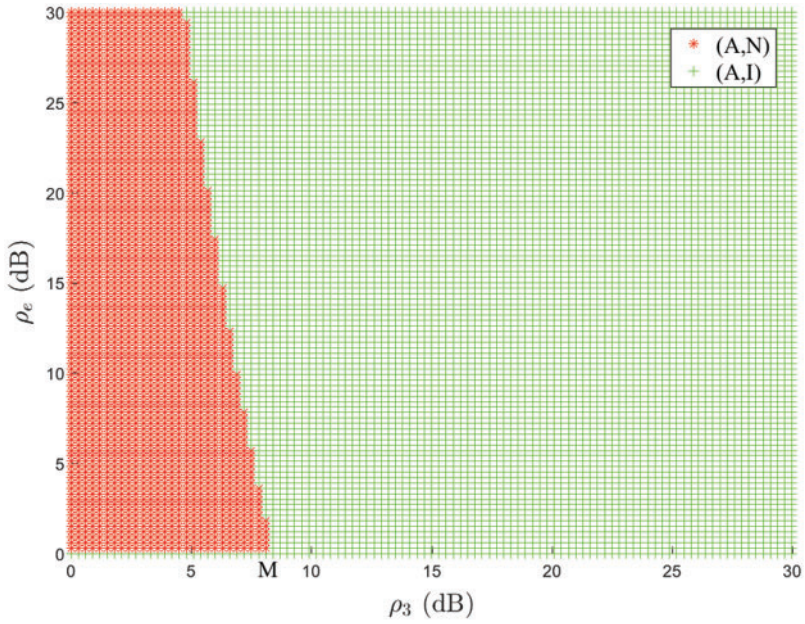
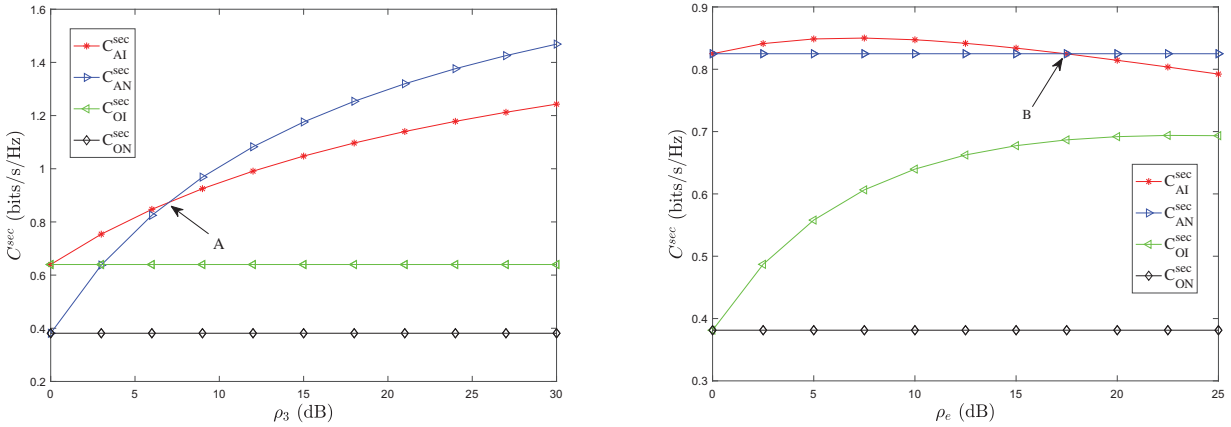


Figure 3: Effect of ρ_e and ρ_3 with $\rho_s = 30$ dB on pure strategy Nash equilibrium in the AS scheme

The curves in Fig. 4 show the benefits (C^{sec}) of pure strategy in the AS scheme with respect to ρ_e and ρ_3, respectively. From Fig. 4a, we can see that the curves of C^{sec}_{AN} and C^{sec}_{AI} intersect at point A. When ρ_3 in the range $(0,\ X(A))$ where $X(A)$ denotes the operation of taking the abscissa value of point A, we have $C^{\text{sec}}_{ON} < C^{\text{sec}}_{AN} < C^{\text{sec}}_{AI}$, thus the pure strategy Nash equilibrium is (A, N) and the corresponding benefit is C^{sec}_{AN}. When $\rho_3 > X(A)$, we have $C^{\text{sec}}_{ON} < C^{\text{sec}}_{AI} < C^{\text{sec}}_{AN}$, thus the pure strategy Nash equilibrium is (A, I) and the corresponding benefit is C^{sec}_{AI}.



(a) C^{sec} against ρ_3 with $\rho_e = 10$ dB, $\rho_s = 30$ dB

(b) C^{sec} against ρ_e with $\rho_3 = 6$ dB, $\rho_s = 30$ dB

Figure 4: The benefits of pure strategy in the AS scheme

Likewise, from Fig. 4b, we can get similar results that the equilibrium strategy and the corresponding benefit is (A, N) and C^{sec}_{AN} when $0 < \rho_e < X(B)$, and the equilibrium strategy and the corresponding benefit is (A, I) and C^{sec}_{AI} when $\rho_e > X(B)$.

5.2.3 Analysis of the Mixed Strategy Benefits

Fig. 5 shows the benefit variation of the mixed strategy in the AS scheme with respect to ρ_s. It can be seen from the figure that the revenue of the mixed strategy under AS scheme increases with the increase of ρ_s. The red curve represents the mixed strategy benefits under the best probability value, and the other three curves represent the mixed strategy benefits when $\pm\varepsilon$, $\pm 2\varepsilon$ and $\pm 3\varepsilon$ are offset on the basis of the best probability value. The figure shows that the benefits of the mixed strategy under the optimal probability is the best, which verifies the previous theoretical analysis results.

Fig. 6 shows the comparison of benefits between the pure strategy Nash equilibrium and the mixed strategy Nash equilibrium in the AS scheme. From the local enlarged subplot, we can clearly find that the benefit curves of potential pure strategy Nash equilibrium profiles (A, I), (A, N) and the mixed strategy Nash equilibrium intersect at point X, Y and Z. With the increase of ρ_s, the equilibrium strategy profile will change from (A, I) to (A, N) when ρ_s goes across the abscissa of Z if the mixed strategy is not considered. Instead, if the mixed strategy is taken into consideration, the equilibrium strategy profile will change from (A, I) to the mixed strategy when ρ_s goes across the abscissa of X.

Additionally, from Fig. 6, we can see that the curve of random-selection method is always below the curves of pure and mixed strategy NE. This is not good for legitimate communicators. Therefore, the legitimate communication party will not select the random-selection strategy to increase the secrecy rate, i.e., the random-selection strategy is unstable in the AS scheme.

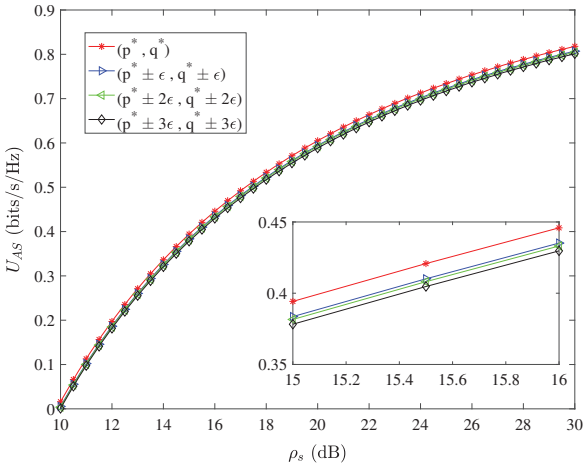


Figure 5: Benefits of mixed strategies in the AS scheme

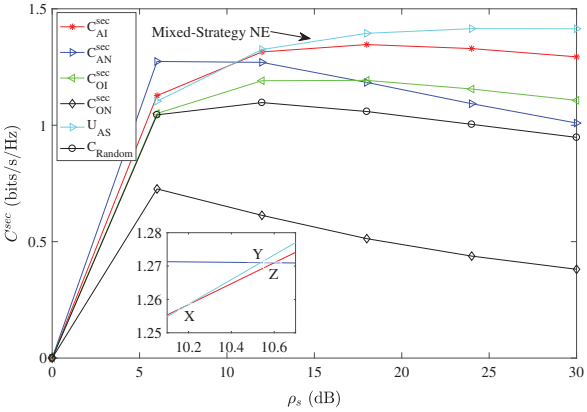


Figure 6: Comparison of the benefits between pure and mixed strategy NE in the AS scheme

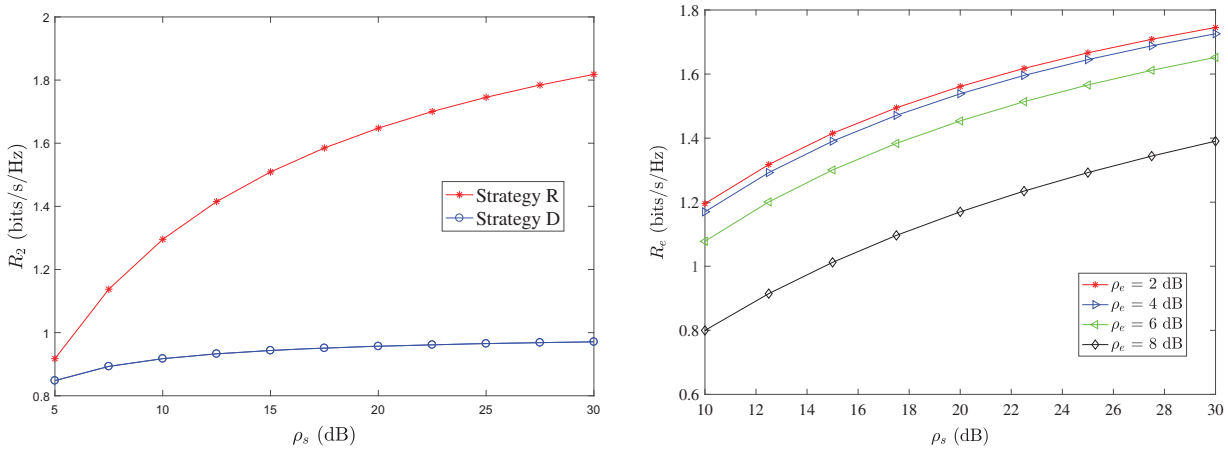
5.3 Result Analysis in the RS Scheme

This subsection mainly analyzes the data rate of the weak user and the eavesdropper, as well as the benefits of the pure and mixed strategy in the RS schemes.

5.3.1 Analysis of Data Rate

Fig. 7a shows the relationship between the information transmission rate of LU_2 and the selection of different strategies in the RS scheme. We can see that when the legitimate party selects strategy 'R' (add relay), the information transmission rate of LU_2 is better than that of strategy 'D' (direct link). It shows that the RS scheme can improve the physical layer security performance of the system.

Fig. 7b shows the relationship between the information transmission rate of E and ρ_s in the RS scheme. When ρ_e is constant, R_e increases with the increase of ρ_s; when ρ_s is constant, R_e decreases with the increase of ρ_e. This shows that if E increases the power of transmitting interference signals, its own transmission rate will be reduced, and the security rate of the system will increase. If the legitimate party blindly increases the total transmission power, the security rate of the system will decrease. Therefore, in order to achieve their respective goals, both parties need to choose an appropriate power value.



(a) Data rate of LU_2 (b) Data rate of E

Figure 7: Data rate in the RS scheme

5.3.2 Analysis of the Pure Strategy Nash Equilibrium and Benefits

According to the analysis, the pure strategy Nash equilibrium depends on the parameter ρ_e and ρ_s. We show the effect of ρ_e and ρ_s on the pure strategy Nash equilibrium in Fig. 8, and we can find the following results. First, if ρ_s keeps constant, the equilibrium strategy changes from (R, N) to (R, I) as ρ_e increases. Second, if ρ_e keeps constant, the equilibrium strategy changes from (R, I) to (R, N) as ρ_s increases.

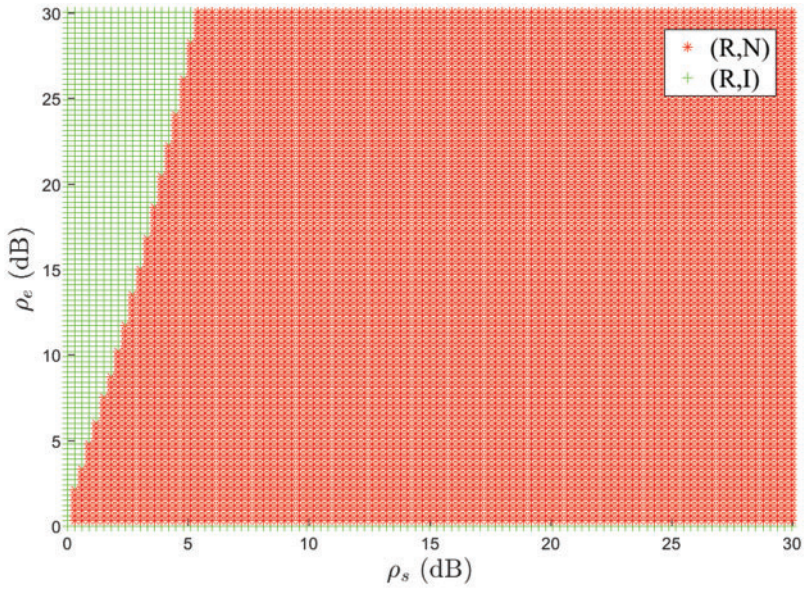
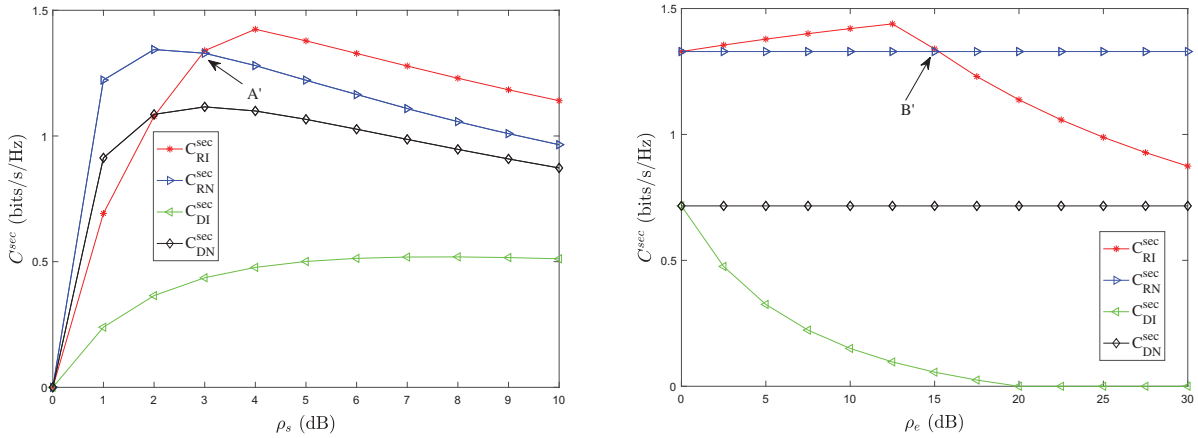


Figure 8: Effect of ρ_e and ρ_s on pure strategy Nash equilibrium in the RS scheme

Fig. 9 shows the pure strategy benefits under different conditions in the zero sum game of RS scheme. Fig. 9a shows the change of pure strategy benefits with ρ_s, and Fig. 9b shows the change of pure strategy benefits with ρ_e. It can be seen from the figure that the benefits of the pure strategy Nash

equilibrium is C_{RN}^{sec}. When the legitimate party changes strategy 'R' to 'D', the benefits will change from C_{RN}^{sec} to C_{DN}^{sec}; When the eavesdropper changes strategy 'N' to 'I', the revenue will increase from C_{RN}^{sec} to C_{RI}^{sec}.



(a) C^{sec} against ρ_s with ρ_e = 15dB (b) C^{sec} against ρ_e with ρ_s = 3dB

Figure 9: The benefits of pure strategy in the RS scheme

5.3.3 Analysis of the Mixed Strategy Benefits

Fig. 10 shows the change of the mixed strategy benefits of the zero sum game of RS scheme with ρ_s. It can be seen from the figure that the mixed strategy benefits under RS scheme decreases with the increases of ρ_s. The red curve represents the mixed strategy benefits under the best probability value, and the other three curves represent the mixed strategy benefits when $\pm\varepsilon$, $\pm 2\varepsilon$ and $\pm 3\varepsilon$ are offset on the basis of the best probability value. The mixed strategy benefits the most under the optimal probability value, that is, the Nash equilibrium value of the mixed strategy.

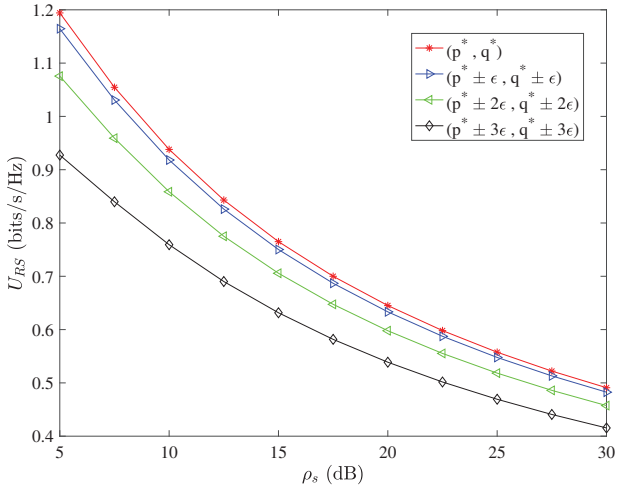


Figure 10: Benefits of mixed strategies in the RS scheme

Fig. 11 shows the comparison of benefits between the pure strategy Nash equilibrium and the mixed strategy Nash equilibrium in the RS scheme. It can be seen that the benefits of the mixed strategy Nash equilibrium are always smaller than that of the pure strategy Nash equilibrium. Therefore, both sides of the game will always choose a pure strategy. That is to say, in the zero-sum game of the RS scheme, both sides will choose the pure strategy NE profile (R, N), that is, the legitimate party L chooses the strategy of adding a relay station, and the eavesdropper E chooses the eavesdropping strategy.

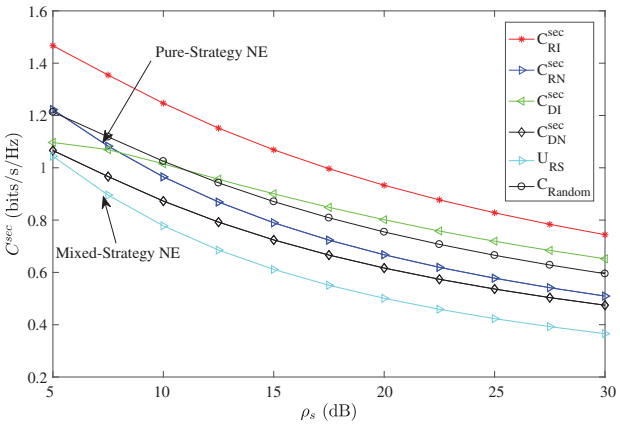


Figure 11: Comparison of the benefits between pure and mixed strategy NE in the RS scheme

Additionally, from Fig. 11, we can observe that the curve of random-selection method is always above the curves of pure and mixed strategy NE. This is not good for the active eavesdropper. Therefore, the active eavesdropper will not select the random-selection strategy to decrease the secrecy rate, i.e., the random-selection strategy is also unstable in the RS scheme.

6 Conclusion

In the scenario of the standard downlink NOMA transmission system, this paper considers two typical physical layer security design schemes based on artificial signals and relay assistance. The non-cooperative behavior between the legitimate communication party and the eavesdropping party under the two schemes is modeled as a two-person zero-sum game. The game is used to characterize the confrontational behavior relationship between the two parties and the process of mutual influence, and prove the existence of the game Nash equilibrium. Through the solution and analysis of the pure strategy and mixed strategy Nash equilibrium of the security game model, the best strategy profile of the two parties in the confrontation environment is given. Numerical simulation results show that both solutions can improve the physical layer security of the NOMA system. The physical layer security game model proposed in this paper can be extended to other scenarios (such as the combination of relay and artificial signals) and can be used to guide the analysis and design of security solutions. However, the cases where there are multiple eavesdroppers and multi-user pairs have not been considered in this paper, and need to be studied in the future.

Acknowledgement: The authors wish to express their appreciation to the reviewers for their helpful suggestions which greatly improved the presentation of this paper.

Funding Statement: This research was supported by the National Natural Science Foundation of China under Grants U1836104, 61801073, 61931004, 62072250, National Key Research and Development Program of China under Grant 2021QY0700, and The Startup Foundation for Introducing Talent of NUIST under Grant 2021r039.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

1. Dai, L., Wang, B., Yuan, Y., Han, S., Chih-Lin, I. et al. (2015). Non-orthogonal multiple access for 5G: Solutions, challenges, opportunities, and future research trends. *IEEE Communications Magazine, 53(9),* 74–81. DOI 10.1109/MCOM.35.
2. Ding, Z. G., Lei, X. F., Karagiannidis, G. K., Schober, R., Yuan, J. H. et al. (2017). A survey on non-orthogonal multiple access for 5G networks: Research challenges and future trends. *IEEE Journal on Selected Areas in Communications, 35(10),* 2181–2195. DOI 10.1109/JSAC.49.
3. Liu, Y., Pan, G. F., Zhang, H. T., Song, M. (2016). On the capacity comparison between mimo-noma and mimo-oma. *IEEE Access, 4,* 2123–2129. DOI 10.1109/ACCESS.2016.2563462.
4. Wu, Y. P., Khisti, A., Xiao, C. S., Caire, G., Wong, K. K. et al. (2018). A survey of physical layer security techniques for 5G wireless networks and challenges ahead. *IEEE Journal on Selected Areas in Communications, 36(4),* 679–695. DOI 10.1109/JSAC.2018.2825560.
5. Yang, N., Wang, L. F., Geraci, G., Elkashlan, M., Yuan, J. H. et al. (2015). Safeguarding 5G wireless communication networks using physical layer security. *IEEE Communications Magazine, 53(4),* 20–27. DOI 10.1109/MCOM.35.
6. Wang, Y., Zhou, X., Zhuang, Z., Sun, L., Qian, Y. et al. (2020). UAV-enabled secure communication with finite blocklength. *IEEE Transactions on Vehicular Technology, 69(12),* 16309–16313. DOI 10.1109/TVT.2020.3042791.
7. Xia, G., Jia, L., Qian, Y., Shu, F., Zhuang, Z. et al. (2019). Power allocation strategies for secure spatial modulation. *IEEE Systems Journal, 13(4),* 3869–3872. DOI 10.1109/JSYST.2019.2918168.
8. Shiu, Y. S., Chang, S. Y., Wu, H. C., Huang, S. C. H., Chen, H. H. (2011). Physical layer security in wireless networks: A tutorial. *IEEE Wireless Communications, 18(2),* 66–74. DOI 10.1109/MWC.2011.5751298.
9. Liu, Y. W., Qin, Z. J., Elkashlan, M., Gao, Y., Hanzo, L. (2017). Enhancing the physical layer security of non-orthogonal multiple access in large-scale networks. *IEEE Transactions on Wireless Communications, 16(3),* 1656–1672. DOI 10.1109/TWC.2017.2650987.
10. Li, A. (2019). Enhancing the physical layer security of cooperative noma system. *2019 IEEE 3rd Information Technology, Networking, Electronic and Automation Control Conference (ITNEC)*, Chengdu, China.
11. Huang, S. C., Xiao, M., Poor, H. V. (2020). On the physical layer security of millimeter wave noma networks. *IEEE Transactions on Vehicular Technology, 69(10),* 11697–11711. DOI 10.1109/TVT.25.
12. Ding, Z. G., Zhao, Z. Y., Peng, M. G., Poor, H. V. (2017). On the spectral efficiency and security enhancements of noma assisted multicast-unicast streaming. *IEEE Transactions on Communications, 65(7),* 3151–3163. DOI 10.1109/TCOMM.2017.2696527.
13. Zhang, H. J., Yang, N., Long, K. P., Pan, M., Karagiannidis, G. K. et al. (2018). Secure communications in noma system: Subcarrier assignment and power allocation. *IEEE Journal on Selected Areas in Communications, 36(7),* 1441–1452. DOI 10.1109/JSAC.2018.2825559.
14. Cao, K. R., Wang, B. H., Ding, H. Y., Li, T. Y., Tian, J. W. et al. (2020). Secure transmission designs for noma systems against internal and external eavesdropping. *IEEE Transactions on Information Forensics and Security, 15,* 2930–2943. DOI 10.1109/TIFS.10206.

15. Cao, Y., Zhao, N., Chen, Y. F., Jin, M. L., Ding, Z. G. et al. (2020). Secure transmission via beamforming optimization for noma networks. *IEEE Wireless Communications, 27(1),* 193–199. DOI 10.1109/MWC.7742.
16. Jia, F., Zhang, C. S., Jiang, C. J., Li, M. D., Ge, J. H. (2021). Guaranteeing positive secrecy rate for noma system against internal eavesdropping. *IEEE Communications Letters, 25(6),* 1805–1809. DOI 10.1109/LCOMM.2021.3062832.
17. Alsaba, Y., Leow, C. Y., Abdul Rahim, S. K. (2018). A zero-sum game approach for non-orthogonal multiple access systems: Legitimate eavesdropper case. *IEEE Access, 6,* 58764–58773. DOI 10.1109/ACCESS.2018.2874215.
18. Gong, C. H., Yue, X. W., Zhang, Z. Y., Wang, X. Y., Dai, X. M. (2021). Enhancing physical layer security with artificial noise in large-scale noma networks. *IEEE Transactions on Vehicular Technology, 70(3),* 2349–2361. DOI 10.1109/TVT.2021.3057661.
19. Zhang, W., Chen, J., Kuo, Y. H., Zhou, Y. C. (2019). Artificial-noise-aided optimal beamforming in layered physical layer security. *IEEE Communications Letters, 23(1),* 72–75. DOI 10.1109/LCOMM.2018.2881182.
20. Zhang, M., Liu, Y., Zhang, R. (2016). Artificial noise aided secrecy information and power transfer in ofdma systems. *IEEE Transactions on Wireless Communications, 15(4),* 3085–3096. DOI 10.1109/TWC.2016.2516528.
21. Wang, B., Mu, P. C., Li, Z. Z. (2017). Artificial-noise-aided beamforming design in the misome wiretap channel under the secrecy outage probability constraint. *IEEE Transactions on Wireless Communications, 16(11),* 7207–7220. DOI 10.1109/TWC.2017.2742954.
22. Lee, J. (2015). Full-duplex relay for enhancing physical layer security in multi-hop relaying systems. *IEEE Communications Letters, 19(4),* 525–528. DOI 10.1109/LCOMM.2015.2401551.
23. Feng, Y. H., Yan, S. H., Liu, C. X., Yang, Z., Yang, N. (2019). Two-stage relay selection for enhancing physical layer security in non-orthogonal multiple access. *IEEE Transactions on Information Forensics and Security, 14(6),* 1670–1683. DOI 10.1109/TIFS.2018.2883273.
24. Chen, B., Li, R., Ning, Q., Lin, K., Han, C. et al. (2022). Security at physical layer in noma relaying networks with cooperative jamming. *IEEE Transactions on Vehicular Technology, 71(4),* 3883–3888. DOI 10.1109/TVT.2022.3144531.
25. Cao, K., Wang, B., Ding, H., Li, T., Gong, F. (2020). Optimal relay selection for secure noma systems under untrusted users. *IEEE Transactions on Vehicular Technology, 69(2),* 1942–1955. DOI 10.1109/TVT.2019.2962860.
26. Chen, B., Chen, Y., Cao, Y., Chen, Y., Zhao, N. et al. (2020). Security enhancement using a novel two-slot cooperative noma scheme. *IEEE Transactions on Vehicular Technology, 69(3),* 3470–3475. DOI 10.1109/TVT.2020.2966996.
27. Zhao, R., Huang, Y. M., Wang, W., Lau, V. N. (2016). Ergodic achievable secrecy rate of multiple-antenna relay systems with cooperative jamming. *IEEE Transactions on Wireless Communications, 15(4),* 2537–2551. DOI 10.1109/TWC.2015.2504526.
28. Lv, L., Zhou, F. H., Chen, J., Al-Dhahir, N. (2019). Secure cooperative communications with an untrusted relay: A noma-inspired jamming and relaying approach. *IEEE Transactions on Information Forensics and Security, 14(12),* 3191–3205. DOI 10.1109/TIFS.10206.
29. Zheng, G. (2015). Joint beamforming optimization and power control for full-duplex mimo two-way relay channel. *IEEE Transactions on Signal Processing, 63(3),* 555–566. DOI 10.1109/TSP.2014.2376885.
30. Kang, Y. Y., Kwak, B., Cho, J. H. (2014). An optimal full-duplex af relay for joint analog and digital domain self-interference cancellation. *IEEE Transactions on Communications, 62(8),* 2758–2772. DOI 10.1109/TCOMM.2014.2342230.