Hindawi
Mobile Information Systems
Volume 2022, Article ID 6303210, 11 pages
https://doi.org/10.1155/2022/6303210

Research Article

Physical Layer Security Technology Based on Nonorthogonal Multiple Access Communication

Qingmei Wei,[1] **Buhong Wang**,[2] **and Kunrui Cao**[3]

[1]*Department of Basic Science, Air Force Engineering University, Xi'an 710043, China*
[2]*School of Information and Navigation, Air Force Engineering University, Xi'an 710077, China*
[3]*School of Information and Communications, National University of Defense Technology, Wuhan 430030, China*

Correspondence should be addressed to Qingmei Wei; 161002106@stu.cuz.edu.cn

Received 25 April 2022; Revised 26 May 2022; Accepted 2 June 2022; Published 29 June 2022

Academic Editor: Muhammad Muzammal

NOMA (nonorthogonal multiple access) technology is an effective technical means to improve spectral efficiency and system capacity. At present, due to the proliferation of access devices and other reasons, the network security communication is facing very serious challenges. This research combines TAS (antenna selection) technology and AN (artificial noise) technology, applies them to NOMA system, and proposes a physical layer optimized security transmission scheme in which AN signals are superimposed at the base station. In this scheme, a part of the total power is divided into the AN signal, and the AN signal and the useful information are superimposed and encoded for transmission. The exact solution of SOP and the asymptotic solution under high signal-to-noise ratio are obtained by mathematical derivation. Moreover, the influence of the power allocation coefficient and target rate of legitimate users on the security performance of the physical layer is explored. The study found that when the solution proposed in this study is adopted, when the fixed SOP size is 10^{-2}, taking the ideal SOP curve as the benchmark, it can be observed that the RHI only occurs when the user node is eavesdropped, and performance improvement of about 2 dB can be obtained. This is because only the system eavesdropping user performance is degraded at this time, so the security performance is improved. In addition, under the same SOP performance, the user is closer to the legal node and can obtain a better channel to resist fading and eavesdropping. The scheme proposed in this study effectively improves the security performance of the NOMA scenario and provides some theoretical guidance for the design process of the secure communication system.

1. Introduction

According to the research results of physical layer security of untrusted relays, even when there are untrusted relays, reliable and secure relay network can be realized through the corresponding security scheme design. However, the existing research work also has some limitations; in particular, the system security design in multiuser and new wireless communication modes still has room for improvement. Due to the broadcast nature of wireless communication, the sensitivity of information also increases, which makes the physical layer security problem under NOMA technology more and more prominent.

Compared with wired communication, the transmission of wireless communication has the characteristics of broadcasting and openness, which makes the transmission between users vulnerable to illegal eavesdropping and malicious interference from third parties, and the system security of wireless communication transmission faces very serious challenges. It can improve the efficiency of spectrum access while improving the security of system transmission. The 5th Generation Mobile Communication Technology (5G for short) is a new generation of broadband mobile communication technology with high speed, low latency, and large connection, and it is the network infrastructure that realizes the interconnection of human, machine, and things. It is of very important theoretical research significance and practical value to study how to realize secure cooperative communication in 5G wireless network based on NOMA technology and provide differentiated security service experience for different users.

This study starts with the most basic NOMA downlink transmission system physical layer security and introduces the basic models and theories. This paper studies the security performance of the NOMA-based downlink wireless security transmission system and the NOMA transmission system based on cooperative interference. The transmission outage probability (COP) and the security outage probability (SOP) of each user in NOMA system are deduced, and the influence of each parameter on the system performance is analyzed. It is proved that there is a trade-off between reliability and security in the system, and the equivalent secrecy throughput (EST) and the effects of various parameters on it are deduced. In the research process, when 7 dB, 4 dB, and 0 dB are taken in turn, the average SOP is also reduced, and the safety performance is improved. The interruption probability is actually another expression of the link capacity. When the link capacity cannot meet the required user rate, an interruption event will occur. This event is probabilistically distributed and depends on the average signal-to-noise ratio of the link and its channel fading distribution model.

2. Related Work

Physical layer security research is of great significance for the advancement of future networks and the design of security systems. Hoang TM considered a cooperative wireless network [1]. Qi X investigated physical layer security in downlink MIMO [2]. Obeed M studied physical layer security [3]. Qian W believed that due to the rapid development and evolution of UAVs, mobile relays have recently attracted a great deal of interest in wireless communication [4]. Wu Y believed that methods to protect data confidentiality have recently received great research interest [5]. The physical layer security technology research they proposed is not very comprehensive. To solve this problem, people will introduce nonorthogonal multiple access communication and collect related research on nonorthogonal multiple access communication.

Nonorthogonal multiple access communication has a wide range of applications in the field of communication security. believed that M2M (Machine-to-Machine/Man) is a networked application and service centered on the intelligent interaction of machine terminals, which enables unimpeded, anytime, and anywhere communication [6]. Cai et al. studied the problem of power allocation and the analysis of spectral efficiency for systems with minimum rate constraints and rate maximization criteria [7]. Yan et al. study uses a full-duplex base station to design an algorithm for resource allocation in a multi-carrier nonorthogonal multiple access system that serves [8]. Marshoud et al. believes that the mobile Internet equipment is a new Internet terminal [9]. Ali et al. believed that NOMA based on power domain multiplexing is easy to implement in technical principle [10]. Nonorthogonal multiple access technology mainly uses code domain, spread spectrum domain, spatial domain, or a combination of different domains to distinguish different users. This study will further explore the nonorthogonal multiple access technology in the following sections.

3. Method

In a multiuser untrusted relay network, there are potential security risks in the multiuser transmission, but it also brings potential multiuser diversity to the system. This research will make full use of the link degree of freedom in the multiuser pair scenario and design the user pair selection scheme security performance of the multiuser system.

As a transmission method with high spectral efficiency, NOMA communication will bring higher system benefits to the next-generation communication technology. Compared with the orthogonal transmission scenario, the NOMA untrusted relay scenario has its own particularity: (1) Although the relay is only introduced to serve the remote users, the relay can not only eavesdrop on the information of the near-end users, but also affect the information security of the remote users due to the transmission method of the NOMA superimposed signal. (2) The scheme based on destination node cooperative interference can achieve good security performance, but the interference caused by the interference signal to other users in non-orthogonal transmission needs to be considered.

3.1. Physical Layer Security Model of the Downlink Transmission System Based on NOMA. The existing research has made more in-depth research safety performance of NOMA transmission system, especially in the downlink system, when sending node is limited by factors such as processing complexity, power consumption, and overhead. However, when using a more realistic fixed rate transmission, the research from the perspective of system reliability and security is still insufficient. What kind of beamforming and AN can better take into account the security and reliability of the transmission system is still an issue to be deeply considered and studied. In addition, in the downlink NOMA transmission system in which the eavesdropper obeys the Poisson space distribution—Poisson distribution is a discrete probability distribution commonly seen in statistics and probability—the relationship between its security and reliability also needs further analysis and research.

The physical layer security model of the downlink transmission system is shown in Figure 1. Considering the classic three-node NOMA transmission scenario, there is an external passive eavesdropper (Eve) in the system, and it is assumed here that all transceivers use coefficients from the transmitter to the legitimate user receiver and the passive Eve, denoted as h_k, $k \in \{1, 2\}$, and h_e, respectively. Moreover, it obeys Rayleigh block fading with mean value 0 and variance γk; that is, the channel changes independently between different transport blocks and remains unchanged within the same transport block [11].

It is assumed that the source node can obtain the CSI of legitimate users. Since the Eve does not send any information and tries to hide their existence, the source node only knows the statistical CSI (channel state information). Here,

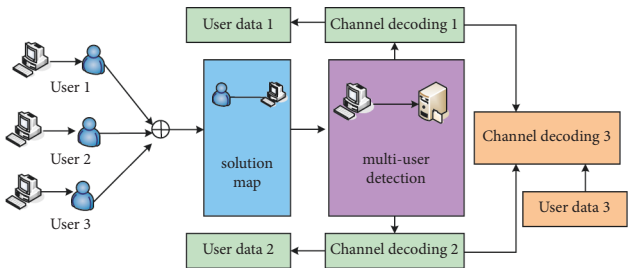

Figure 1: Downlink transmission system physical layer security model.

the legitimate channel gains satisfy the increasing ordering; that is [12],

$$0 < |h_1|^2 < |h_2|^2. \tag{1}$$

The node is denoted as P. The superimposed signal can be expressed as follows:

$$D_J = \sqrt{a_1}s_1 + \sqrt{a_2}s_2. \tag{2}$$

In addition,

$$a_1 + a_2 = 1. \tag{3}$$

It should be emphasized here that, in NOMA transmission, information of weak users (users with poor channel quality) is more susceptible to interference than those with better channel quality. However, both of them are internal legitimate users of the system, and strong users will not deliberately disclose the information of weak users.

The source node sends the superimposed signals of the two users; then, the received signal Y_K of the legitimate user and the received signal Y_e of the Eve can be expressed as follows [13]:

$$\begin{aligned} Y_K &= \sqrt{P}\left(\sqrt{a}\, s_1 + \sqrt{a}\, s_2\right)h_k + n_k, \\ Y_e &= \sqrt{P}\left(\sqrt{a}\, s_1 + \sqrt{a}\, s_2\right)h_e + n_e. \end{aligned} \tag{4}$$

Therefore, the signal-to-noise ratio of the decoded signal "S_2" for the user 1 decoded signal "S_1" can be written as

$$\begin{aligned} \gamma_1 &= \frac{ap|h_1|^2}{ap|h_2|^2 + \varepsilon} = \frac{apg}{apg + 1}, \\ \gamma_{2\longrightarrow 1} &= \phi\frac{ap|h_2|^2}{ap|h_1|^2 + \varepsilon} = \frac{apg}{ap_2 g + 1}. \end{aligned} \tag{5}$$

The existing literature on physical layer security defines the security capacity as follows [14]:

$$C_S = [C_b - C_e]^+. \tag{6}$$

Among them,

$$[X]^+ = \max\{0, X\}. \tag{7}$$

However, since eavesdroppers are passive eavesdroppers and try to hide themselves as much as possible, they may not be part of legitimate transmission users. Therefore, the CSI of the eavesdropping channel cannot be easily obtained, so the capacity of the eavesdropping channel cannot be obtained. Therefore, instead of using the typical information-theoretic-related secrecy capacity, we consider a new metric that can characterize both reliability and secrecy constraints, namely, equivalent secrecy throughput (EST). To ensure security, two different types of constraints are considered: reliability constraints and confidentiality constraints. Confidential information needs to be encoded and transmitted to legitimate users. If the selected codeword rate Rg is less than the channel capacity Cg of the legal channel, that is, $Rp \le Cp$, the information satisfying the legal user can be transmitted reliably [15].

Since the channel changes randomly, the transmission (COP) legal channel capacity is less than the channel transmission codeword rate under the ergodic channel. Similarly, if the channel capacity C is greater than the redundancy rate, the security of the transmitted information cannot be guaranteed, and this probability is defined as the Secrecy outage probability (SOP). EST describes the average confidentiality rate at which information of legitimate users will not be leaked to eavesdroppers, which is defined as follows:

$$\varphi(R_b, R_e) = (R_b, R_e)\left[1 - P_{cop}R_b\right]\left[1 - R_e\right]. \tag{8}$$

Among them, $R_s = R_b - R_e$. $[1 - P_{cop}R_b][1 - R_e]$ represents the probability that the information can be transmitted to legitimate users confidentially.

The worst eavesdropping scenario is considered, can distinguish different user information well, and can eliminate the signal interference between different users through SIC technology. SINR of the eavesdropping signal S_K, $k \in \{1, 2\}$, at the Eve receiver can be expressed as follows:

$$\gamma_s = \frac{A_K P|H_K|^2}{\eta}. \tag{9}$$

3.2. Physical Layer Security Model of the NOMA Downlink Wireless Transmission System under Eavesdropper Poisson Distribution. The NOMA downlink wireless security transmission system is shown in Figure 2. Here, the users are randomly paired. The coverage area is divided into two mutually disjoint concentric circle areas, D1 and D2. The radius of the inner circle D1 is R, the user group n is located in this area, and the user m is located in the annular area D2, whose inner and outer radii are R and $R2$, respectively. The paired two users were randomly selected from the D1 and D2 areas, respectively. This processing can bring two advantages. On the one hand, paired users can produce obvious channel gain differences. On the other hand, the overhead required for user channel gain sorting is reduced, and better flexibility and adaptability can be obtained.

Furthermore, it is assumed that they have strong signal detection ability, which can eavesdrop and distinguish the signals of each user. The Eves obeys a homogeneous Poisson process ε with a density of g. It is assumed here that Eve cannot be too close to BS; otherwise, it will be detected and

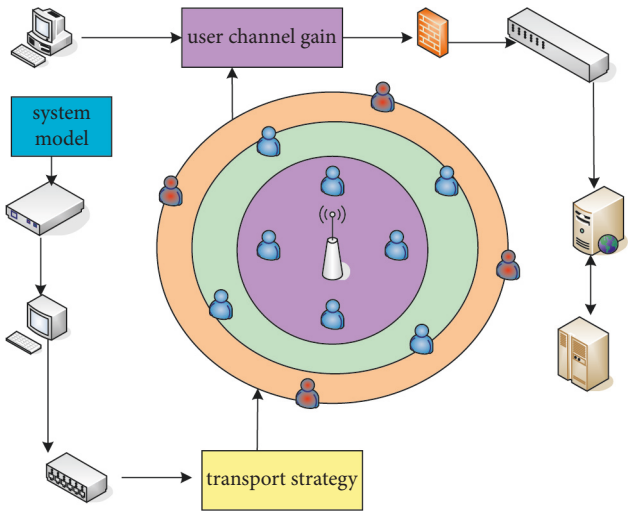

Figure 2: NOMA downlink wireless security transmission system.

cleared; that is, there is a protection area with BS as the center and radius p, and no Eve exists in this area.

Considering the worst case, since the eavesdropper's CSI is unknown, the instantaneous SNR worst eavesdropper can be expressed as follows:

$$\gamma_{e\longrightarrow n} = \max\left\{\frac{a_n p_s |h|^2}{\delta d}\right\} = \max\left\{\frac{a_n \rho e}{d}\right\}. \tag{10}$$

When the eavesdropper adopts the SIC (strong interference channel) operation similar to that of the legitimate user, the user m at the worst eavesdropper can be expressed as follows:

$$\gamma_{e\longrightarrow n} = \max\left\{\frac{a_m p_s |h_e|^2}{a_n p_s |h_e|^2 + de^2}\right\} = \max\left\{\frac{a_m \rho e}{a_n p_s g + d}\right\}. \tag{11}$$

When considering the worst case, the instantaneous SNR formula for detecting user m information at Eve is similar.

3.3. Physical Layer Security Performance Inspection. Assuming that the source node transmits legal user information at a fixed rate, due to the randomness caused, the transmission of legal user information will be interrupted to some extent. When the legal channel is lower than the fixed codeword transmission rate R_B, the transmission interruption (connection outage, CO) event will occur. The security of the transmitted information cannot be guaranteed. At this time, Eve can intercept the confidential information; that is, a security outage (SO) event occurs. The COP and SOP of each legal user of the system are calculated below.

The expression for COP is as follows:

$$P_{CO} = \Pr\left\{\gamma_1 = \frac{A\beta g}{A\beta g + 1}\right\} = 1 - \exp\left(-\frac{\chi}{A\beta g + 1}\right). \tag{12}$$

At this time, the COP of user 2 can be expressed as follows:

$$\begin{aligned} P_{CO}^2 &= \Pr\{\gamma_{2\longrightarrow 1} < \tau_1\} + \Pr(\gamma_{2\longrightarrow 1} > \tau_1, \gamma_1 < \tau_2), \\ &= 1 - \Pr(\gamma_{2\longrightarrow 1} > \tau_1, \gamma_2 < \tau_2). \end{aligned} \tag{13}$$

Considering the eavesdropping scenario in the worst case, according to the definition of SOP, the SOP expression of user k can be obtained as follows:

$$P_{SO}^k = \Pr\left(g_e < \tau_e^k\right) = \mathrm{EXP}\left(-\frac{\tau^k}{a\varphi\lambda}\right). \tag{14}$$

Similarly, if the eavesdropper adopts a detection method similar to that of a legitimate user, the user's SOP expression is as follows:

$$\begin{aligned} P_{SO}^1 &= e^{-\chi/(a_1 - a_2)\lambda}, \\ P_{SO}^1 &= e^{-\gamma^2/a_2\beta\lambda}. \end{aligned} \tag{15}$$

From the definition of EST and the COP and SOP of each user, the EST expression of each user can be obtained as follows:

$$\begin{aligned} \varphi(R_b, R_e) &= \left(R_b^1, R_e^1\right) e^{-\gamma^2/a_2\beta\lambda}\left[1 - \exp\left(-\frac{\chi}{a_1\chi\lambda}\right)\right], \\ (R_b, R_e) &= \left(R_b^2, R_e^1\right)\gamma\left[1 - \exp\left(-\frac{\chi}{a_2\chi\lambda}\right)\right]. \end{aligned} \tag{16}$$

NOMA allows multiple users to share time and frequency resources in the same spatial layer through power domain or code domain multiplexing. Multiple access interference is actively introduced at the transmitting end, and the multiuser signal is recovered by the (successive interference cancelation, SIC) demodulation technology. According to the analysis of multiuser channel capacity, the total capacity obtained by using SIC is greater than that of orthogonal multiple access. The comparison of the channel capacity of two different users is shown in Figure 3.

4. Experimental Simulation and Result Analysis

When the M-LaE-SNR (Maximized SNR for Legitimate and Eavesdropping link) relay selection scheme is adopted, the relationship between the SOP and SNR of a pair of NOMA users in the RHI-D-E-MR-NOMA system is shown in Figure 4. SOP decreases significantly, and the security performance obtained by user D2, is better than that of remote user D1. This shows that in the large SNR situation, the performance of weak users should be of main concern.

Then, the achievable performance of the optimization algorithm DC-VPA-based-JSBPA is verified by computer simulation, and the analysis is carried out. The system parameter settings are shown in Table 1.

We compare the spectral efficiency of uplink NOMA and OMA systems—OMA (open mobile alliance) is an organization established by the merger of the WAP Forum and the Open Mobile Architecture standardization organizations—in the case of 2 users, 3 users, and 4 users in each cluster. The relevant parameter settings of the multiuser NOMA system are shown in Table 2.

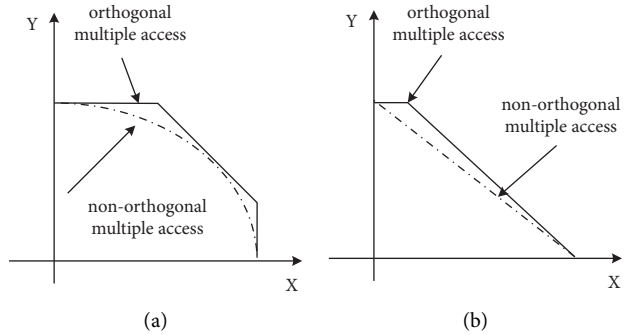

Figure 3: Comparison of channel capacity for two different users. (a) User channel 1. (b) User channel 2.

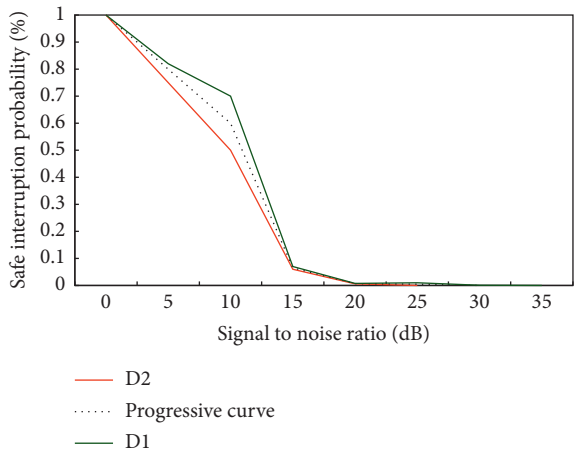

Figure 4: SOP versus SNR for a pair of NOMA users in the RHI-D-E-MR-NOMA system.

Table 1: System parameter settings.

Parameter settings	Numerical value
TTI length	1 ms
Time window length	1 s
Maximum number of iterations	20
Tolerance value	e^{-10}

There are more than ten kinds of NOMA schemes at present, which are divided into four categories: NOMA based on scrambling, NOMA based on interleaving, NOMA based on spread spectrum, and NOMA based on coding. The difference between these schemes is mainly due to the way of distinguishing multiple users, such as using different scrambling sequences, different interleaving sequences, different nonsparse spreading matrices, and different sparse spreading matrices to distinguish different users. Using a corresponding multiuser receiver at the receiving end can distinguish different user information from the superimposed multiuser information according to the difference of the scrambling code sequence, the interleaving sequence, or the spreading matrix. The specific classification is shown in Table 3.

The presence of RHI can lead to a significant reduction in system performance because RHI is modeled as an additional noise. Under the M-LaE-SNR scheme, when the SOP

Table 2: Related parameter settings of the multiuser NOMA system.

System parameters	Parameter value
Number of cell users	12
Number of base station antennas	1
Number of user antennas	1
System effective bandwidth	20 MHz

Table 3: NOMA scheme classification.

Serial number	Type	Sender features
1	Scrambling class	Different low-correlation scrambling sequences
2	Interweaving	Different interleaving sequences
3	Spread spectrum	Design of different spreading sequences
4	Coding class	Design of different low-density signature matrices

is 10^{-3}, the SNR requirement of the receiver under nonideal hardware is about 3 dB higher than that under ideal conditions (ideal SNR is shown in Figure 5(a)). Figure 5(b) is the comparison of RR and MRC (MRC (MRAChain) will establish the most powerful infrastructure in the digital asset industry, provide users with the best quality, safe, convenient, and efficient services, and promote the application of blockchain technology in all walks of life, and lead changes).

When RHI only occurs at the source node and relay node, the impact on SOP is small (Ideal, Source RHI only, Relay RHI only as shown in Figure 6(a)). In addition, we can also see from the simulation results that when using the M-LaE-SNR scheme, we fixed the size of the SOP to be 10^{-2}. Taking the ideal SOP curve as the benchmark, it can be observed that the RHI only occurs when the user node is eavesdropped, and the performance can be improved by about 2 dB. This is because only the performance of the system eavesdropping user is degraded at this time, so the security performance is improved (Destination RHI, Eve RHI only, and Joint RHI are shown in Figure 6(b)).

When the proposed M-LaE-SNR scheme is adopted, the effects of different values of the eavesdropping link SNR on the average SOP are shown in Figure 7. Observing Figure 7, we can clearly see that when 7 dB, 4 dB, and 0 dB are taken in

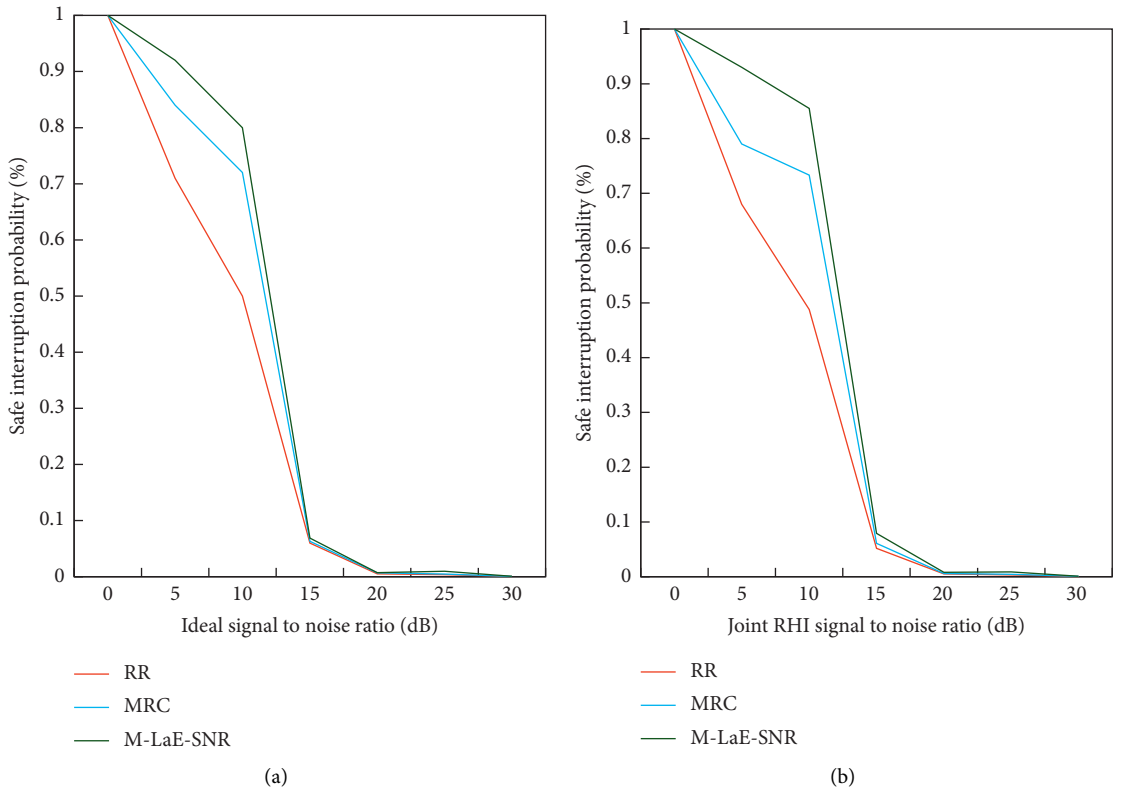

Figure 5: Effects of different RS schemes on the safety performance of NOMA systems. (a) Ideal signal-to-noise ratio. (b) Joint RHI signal-to-noise ratio.

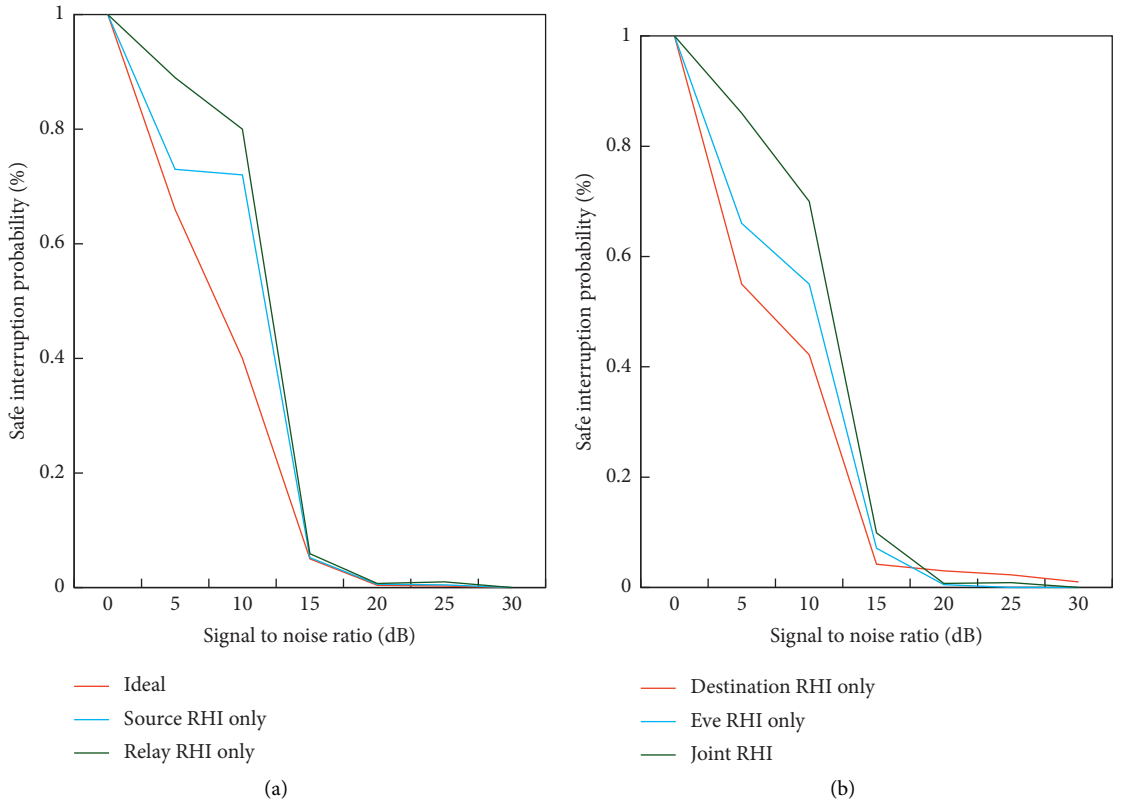

Figure 6: The effect of RHI on different nodes in the system. (a) Ideal, Source RHI only, and Relay RHI only. (b) Destination RHI, Eve RHI only, and Joint RHI.

turn, the average SOP is also reduced. This is because when the value of the eavesdropping link decreases, the eavesdropper's eavesdropping ability is deteriorated and a more secure transmission is achieved.

The simulation parameters of the channel model are shown in Table 4. These are code rate, physical resource block, modulation coding, and channel model.

Since the MUSA scheme also uses short spreading sequences, it is considered to be one of the most potential NOMA candidate schemes at present. Therefore, this part mainly compares and analyzes the cross-correlation of the MUSA spreading sequence and the cross-correlation of the MWBE spreading sequence, as shown in Table 5. All in all, through the analysis of mutual characteristics, it can be seen that the cross-correlation characteristics of MWSMA spread spectrum sequences are better than those of MUSA and can meet the high overload requirements of NOMA systems.

It can be seen from Figure 8 that the effective safe throughput first rises rapidly and then decreases, which verifies that the effective safe throughput has a maximum value with respect to the safe rate. Another verification is that the optimal security rate to obtain the maximum value is related to the number of interferers n; the smaller the n is, the larger the optimal security rate is, and vice versa. Comparing the two subgraphs, we find that for the same number of interferers, the effective safe throughput increases with the SNR (SNR of −3 dB is shown in Figure 8(a)). In addition, the effective safe throughput without interference has a greater advantage than other cases, and this advantage also increases; that is, the effective safe throughput without interference accounts for an increasing proportion of the total effective safe throughput. This point also illustrates that it is reasonable to directly evaluate its interference-free effective safe throughput when comparing SIC scheduling strategies before (SNR of 3 dB is shown in Figure 8(b)).

There is a certain trade-off relationship between the COP and SOP between legitimate users; that is, when the COP increases, the SOP decreases, and when the COP decreases, the SOP increases. When the reliability is enhanced, the confidentiality is relatively weakened; when the confidentiality is improved, the reliability is lost. Under the same COP performance, user 2's SOP performance is always better than user 1's SOP performance; under the same SOP performance, user 2's COP performance is always better than user 1's COP performance. This is because user 2 is closer to the location of the legitimate node and can get a better channel to resist fading and eavesdropping. The reliability and security performance of users are improved with the increase of d3 (the COP-SOP of the system changes with the distance between Eve and the source node as shown in Figure 9(a)).

With the increase of transmit power, each user and the total EST first increase, then decrease, and tend to zero gradually. This is because at low SNR, the COP of the system is relatively high, almost all data transmissions are in an interrupted state, and the reliability is poor. Reliability is the main limiting factor for the system. The reliability of the system is enhanced. At the same time, the Eve can obtain greater signal power, the SOP increases,

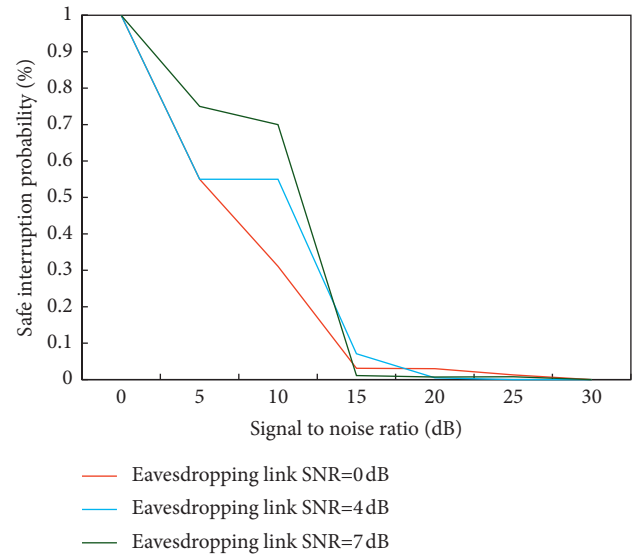

Figure 7: The effect of different values of the eavesdropping link SNR on the average SOP.

Table 4: Simulation parameters of the channel model.

Parameter	Type
Code rate	1/2
Physical resource block	6PRBs
Modulation coding	QPSK
Channel model	TDL-A-30 ns

Table 5: Cross-correlation of MUSA spreading sequences and cross-correlation of MWBE spreading sequences.

N	K	Welch bound
5	6	0.3612
5	8	0.3780
5	10	0.4082
5	12	0.4264

and the confidentiality decreases. At this time, the confidentiality becomes the main factor restricting the continuous increase of the system EST. As the SNR tends to infinity, Eve can always eavesdrop on the information sent, so the EST tends to zero. At the same time, it can be seen that the SNR required for the maximum EST value of user 2 is smaller than the SNR required for the maximum EST value of user 1, because the distance is closer and the reliability is easier to satisfy. The main limitation of the EST performance is the SOP, so a better SOP can be achieved by lowering the transmit power, thereby increasing the EST. Therefore, under the condition of satisfying the system SOP and COP at the same time, it is very important to choose the transmit power reasonably. Therefore, a better transmission scheme needs to be designed to achieve stronger confidentiality and higher EST. This can be achieved by sending a specific AN and increasing degrees of freedom (the EST as a function of SNR is shown in Figure 9(b)).

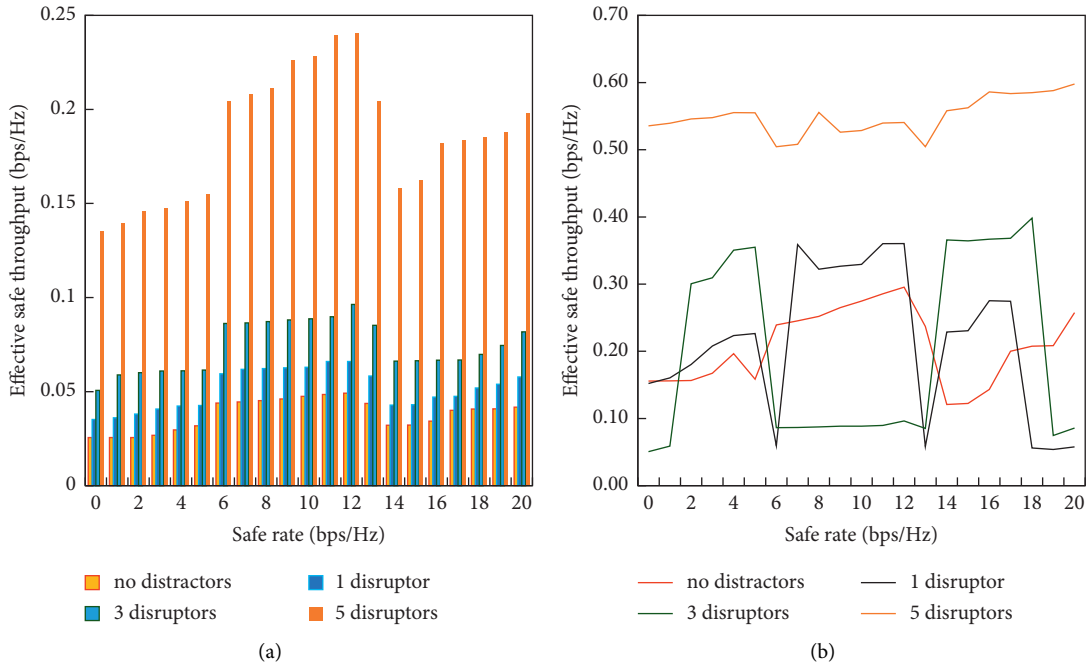

Figure 8: Safe throughput at different signal-to-noise ratios. (a) The signal-to-noise ratio is −3 dB. (b) The signal-to-noise ratio is 3 dB.

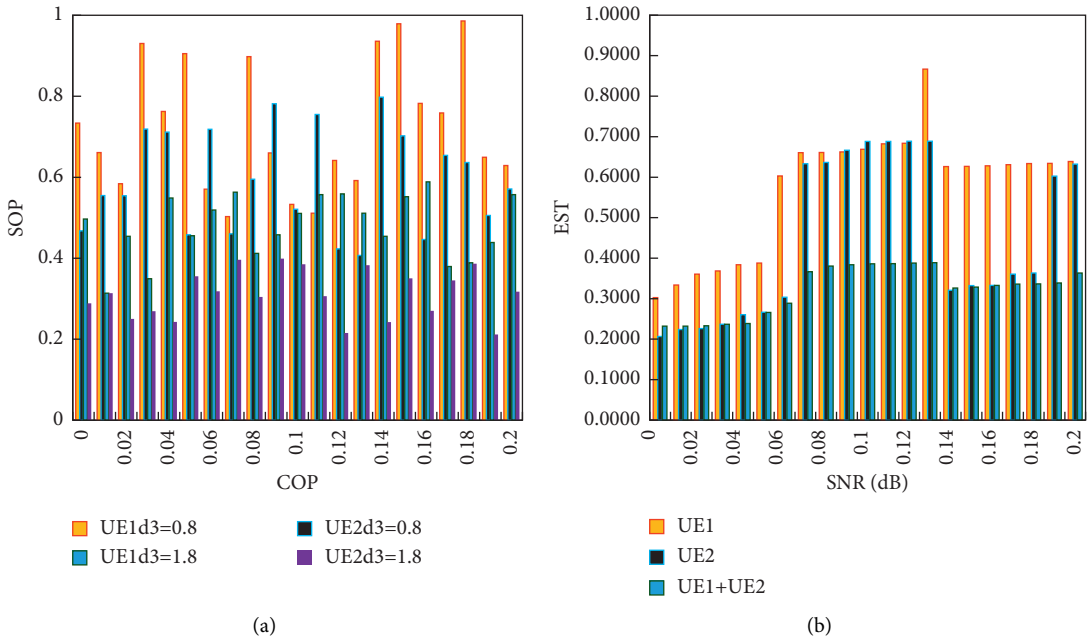

Figure 9: Variation of SOP and EST. (a) COP-SOP varies with the distance between the Eve and the source node. (b) Equivalent secrecy throughput (EST) varies with SNR.

It can be seen from Figure 10 that the deduced theoretical results are in almost perfect simulation results. At the same time, the results of the asymptotic expression in the high SNR region are also consistent, and the simulation curve is formula curve. Thus, the formula is verified, and the diversity gain is 1. The SOP of each user tends to a constant 1 as the transmit power P increases. Since a part of the power is used to transmit artificial interference, the value of COP is slightly increased; that is, a certain reliability is lost. The value of SOP is greatly reduced, which improves the confidentiality performance of each user. Therefore, by sending artificial jamming signals of a certain power, a small loss of reliability can be exchanged for a large increase in confidentiality. The transmission interruption probability and the security interruption probability change are shown in Figure 10.

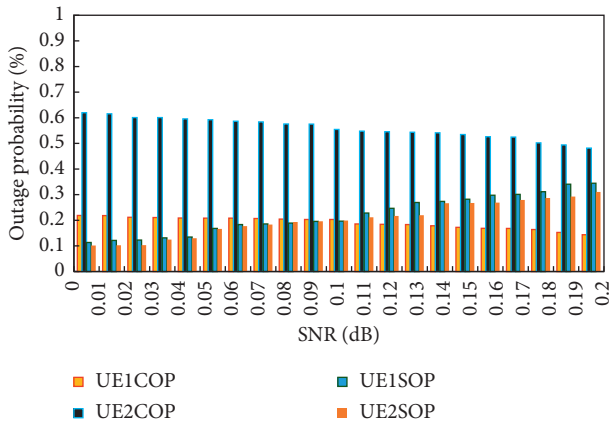

Figure 10: Transmission outage probability and privacy outage probability changes.

5. Discussion

Mobile communication technology has experienced great development in just a few decades and has even become a booster to stimulate national economic growth and improve national living standards and social development. The growth of mobile communication technology has changed people's communication habits and methods. With the gradual completion of the 4G network, the standardization of the fifth-generation mobile communication technology is also in progress. Since the EU launched the 5G research project group in 2012, the discussions on key technologies in 5G in academia and industry have gradually been carried out on a global scale. In the grand blueprint of the new generation of mobile communication, the goals of ultrahigh spectral efficiency, peak rate and transmission speed, large system capacity, and network coverage will be realized one by one. The International Telecommunication Union Committee on Wireless Communications summarizes these needs into three categories: the number of connections to multiple devices, the ultrahigh data traffic, and the ultralow access latency. The 5G network not only satisfies these needs by establishing communication connections between people, but also integrates the connection between people and things and things and things into the mobile Internet. Tens of thousands of user devices will be connected to the network, realizing the true intelligent interconnection of all things.

The gradual improvement of mobile communications has catalyzed the birth of new technologies from generation to generation. To meet the needs of realizing interconnected society, the core point of access technology is to effectively increase the data rate and minimize the network delay. One of the very important means is to choose the appropriate multiple access method. Therefore, the multiple access technology has also gained wider attention. The so-called multiple access technology, that is, proposed to make better use of communication channels, let different users share the same wireless communication channel for data transmission; divide the channel according to time, frequency, etc.; and divide it into countless resource blocks (resource element, RE). In this way, users can use different one or several resource blocks during transmission, as if each user is assigned a different address during transmission. Therefore, multiple users who transmit on the same channel are assigned multiple different addresses, that is, multiple access technology.

At present, NOMA based on spread spectrum is one of the key directions of academic research. Traditional CDMA uses very long PN sequences for spreading, the correlation between sequences is easily reduced to a very low level, and it is easy to provide soft capacity for the system; that is, the number of users accessing the system at the same time is greater than the length of the PN sequence. At this point, we say that the system is in an overloaded state. In the future, when mobile communication spectrum resources are tight with massive connections, it is necessary to further improve the overload of the system. At the same time, it is necessary to reduce the transmission delay of the system. However, with the increase of the number of users and in the case of high overload, the long PN sequence causes the detection complexity of the receiver to be particularly high. In addition, long spreading sequences make a user's data occupy more time-frequency resources, which will lead to higher transmission delay and power consumption. Therefore, it is almost impossible for long spreading sequences higher user overload and lower delay in 5G communication systems at the same time. Because the length of the spreading sequence is short, it can support a high overload rate, that is, the spectral efficiency, and the delay of the system at the same time.

Since NOMA technology can realize multiuser multiplexing in the same resource in different dimensions, it is more suitable for facing the transmission requirements of massive users in the next-generation wireless communication system. Since it was proposed, it has received extensive attention in the industry. At present, there are many types of NOMA technologies, and the application scenarios are gradually expanding. Through in-depth research and analysis of NOMA technology in different aspects, this paper tries to propose an effective optimization scheme, such as sum rate, bit error rate, and user fairness.

The characteristics of 5G mobile communication networks determine that the security transmission challenges it faces are far greater than those of previous generations of mobile communication networks. For a long time, the security of wireless communication has been of concern, and the security of communication is the key factor to ensure that the mobile communication network can provide users with continuous and stable services. In order to avoid stagnation caused by the threat of security problems in the future research of wireless communication technology, the security performance analysis and security strategy research of 5G network should be put on the agenda, in order to provide certain data reference and theoretical guidance for the actual 5G network design. Different from the traditional high-level encryption security technology, PLS technology starts from Shannon's information theory and uses the physical channels the security performance systems. Therefore, this paper combines the NOMA system and PLS

technology to carry out research on NOMA technology R&D safety, and at the same time help the communication system to achieve secure transmission in the future network.

At present, most are biased towards the direction of jamming attack. This paper is of selfish and malicious behavior of multi-untrusted nodes, which has been rarely studied before. A four-node model (source node, relay node, destination node, eavesdropping node) is considered in this paper. The cooperative communication between nodes adopts the AF standard. For most AF systems, each relay node is cooperative with full power output. However, different from the traditional AF mode, if the relay node is an untrusted node in the system, the situation will be completely different.

The 5G digital scheme with its potential advantages in integration of existing communication technologies, has become a revolutionary technology choice in the post-5G era. In the future, facing the era of the Internet of Things, the introduction of technologies such as heterogeneous networks and cooperative communication will make the wireless communication environment more complex. In addition to the transmission of user privacy data related to traditional networks, 5G will involve personal data in different industries and privacy data of industry users. These data often have high sensitivity; once leaked, they will bring great loss of life and property. It starts from the characteristics of wireless signal propagation and combines the uniqueness of the wireless channel and the endogenous security properties of immeasurability, which provides a new idea for the secure transmission of wireless communication. Compared with encryption technology, physical layer security does not depend on computational complexity. Wireless communication security is transformed into exploring various advanced technologies at the physical layer to increase the system capacity; that is, the enhancement of security capabilities is transformed into the improvement of communication capabilities and the effective use of communication resources.

Whether it is private information or state secrets, secure network transmission is required. Whether it is wired communication or wireless communication, more and more researchers pay attention to security issues. However, the channels make it easy for eavesdropping to occur, and any node within the wireless communication range may receive or even decode the transmitted signal. In traditional wireless communication networks, security issues are mainly carried out at the physical layer.

With the requirements of massive connections, ultralow latency, and high reliability in next-generation communication systems, especially in the case of increasingly tight spectrum resources, how to make reliability and spectrum utilization of the communication realize the benign development of the future is the key problem that needs to be solved urgently. Here, the multiple access technology is the key technology of each generation of communication systems. However, it is difficult to meet these requirements with the current orthogonal multiple access. NOMA can not only increase the number of service users by means of multiuser stacking, but also improve the spectrum utilization of the system by overloading. It can also effectively reduce the delay of the system through the scheduling-free method. Therefore, among the many new technologies for 5G, the new NOMA scheme is considered as a key and promising candidate technology. The following is a detailed principle analysis of the mainstream solutions currently discussed in the industry, focusing on the principle of the transmitter and the corresponding receiver algorithm. Finally, based on the in-depth research and analysis of each technical scheme, the corresponding NOMA classification scheme is proposed, and the performance analysis is given by the method of link-level simulation test.

6. Conclusions

NOMA technology has high spectrum utilization and is considered as one of the innovative technologies in 5G and beyond. Different from traditional orthogonal technologies such as TDMA, FDMA, and CDMA, NOMA technology allows multiple users to utilize the same resources (such as time, frequency, and code) at the same time. NOMA technology is an effective technical means. In the future, due to the proliferation of access devices, secure communication will face severe challenges. This study describes the working principle and technical characteristics of NOMA technology. The theoretical basis of physical layer security is summarized, and the research direction of physical layer security is introduced. The relay technology is introduced from the perspective of transmission mode and signal processing protocol. Diversity combining technology, antenna selection technology, and full-duplex technology are briefly described in turn. This paper studies the physical layer security of NOMA system. Although some progress has been made, it is limited by the research time and the length of this paper, and the actual communication systems are not all ideal. In addition, multi-antenna technology will be widely used in future communication networks, so multi-antenna scenarios should also be considered in the future.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare no conflicts of interest.

References

[1] T. M. Hoang, T. Q. Duong, N.-S. Vo, and C. Kundu, "Physical layer security in cooperative energy harvesting networks with a friendly jammer," *IEEE Wireless Communications Letters*, vol. 6, no. 2, pp. 174–177, 2017.

[2] X. Qi, K. Huang, and Z. Zhong, "Physical layer security of multi-hop aided downlink MIMO heterogeneous cellular networks," *China Communications*, vol. 13, pp. 120–130, 2017.

[3] M. Obeed and W. Mesbah, "Efficient algorithms for physical layer security in one-way relay systems," *Wireless Networks*, vol. 25, no. 3, pp. 1327–1339, 2018.

[4] Q. Wang, Z. Chen, W. Mei, and J. Fang, "Improving physical layer security using UAV-enabled mobile relaying," *IEEE Wireless Communications Letters*, vol. 6, no. 3, pp. 310–313, 2017.

[5] Y. Wu, A. Khisti, C. Xiao, and G. K.-K. X. Caire, "A survey of physical layer security techniques for 5G wireless networks and challenges ahead," *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 4, pp. 679–695, 2018.

[6] M. Shirvanimoghaddam, M. Dohler, and S. J. Johnson, "Massive non-orthogonal multiple access for cellular IoT: potentials and limitations," *IEEE Communications Magazine*, vol. 55, no. 9, pp. 55–61, 2017.

[7] W. Cai, C. Chen, L. Bai, and Y. Jin, "Power allocation scheme and spectral efficiency analysis for downlink non-orthogonal multiple access systems," *IET Signal Processing*, vol. 11, no. 5, pp. 537–543, 2017.

[8] S. Yan, D. Ng, and Z. Ding, "Optimal Joint power and subcarrier allocation for full-duplex multicarrier non-orthogonal multiple access systems[J]," *IEEE Transactions on Communications*, vol. 65, no. 3, pp. 1077–1091, 2017.

[9] H. Marshoud, S. Muhaidat, P. C. Sofotasios, and S. M. A. Hussain, "Optical non-orthogonal multiple access for visible light communication," *IEEE Wireless Communications*, vol. 25, no. 2, pp. 82–88, 2018.

[10] M. S. Ali, H. Tabassum, and E. Hossain, "Dynamic user clustering and power allocation for uplink and downlink non-orthogonal multiple access (NOMA) systems[J]," *IEEE Access*, vol. 4, no. 99, pp. 6325–6343, 2017.

[11] B. He, A. Liu, N. Yang, and V. K. N. Lau, "On the design of secure non-orthogonal multiple access systems," *IEEE Journal on Selected Areas in Communications*, vol. 35, no. 10, pp. 2196–2206, 2017.

[12] Y. Zheng, Z. Ding, and P. Fan, "The impact of power allocation on cooperative non-orthogonal multiple access networks with SWIPT[J]," *IEEE Transactions on Wireless Communications*, vol. 16, no. 7, pp. 4332–4343, 2017.

[13] J. Zhao, Y. Liu, K. K. Chai, and A. Y. Nallanathan, "Spectrum allocation and power control for non-orthogonal multiple access in HetNets," *IEEE Transactions on Wireless Communications*, vol. 16, no. 9, pp. 5825–5837, 2017.

[14] F. Alavi, K. Cumanan, and Z. G. Ding, "Robust beamforming techniques for non-orthogonal multiple access systems with bounded channel uncertainties," *IEEE Communications Letters*, vol. 21, no. 9, pp. 2033–2036, 2017.

[15] C. Xu, Y. Hu, C. Liang, and J. Ma, "Massive MIMO, non-orthogonal multiple access and interleave division multiple access," *IEEE Access*, vol. 5, no. 99, pp. 14728–14748, 2017.