Al-Rafidain Journal of Engineering Sciences

Journal homepage https://rjes.iq/index.php/rjes

ISSN 3005-3153 (Online)

Physical Layer Security Enhancement for Cooperative NOAM Systems

Jouana hamed hassan [1], Ibrahim Khalil Sileh [2]

[1]Tikrit University, College of Engineering, Electrical Engineering Department, Tikrit, Iraq

ARTICLE INFO

Article history:
Received 6 March 2026
Revised 6 March 2026
Accepted 24 April 2026
Available online 29 April 2026

Keywords:
Non-Orthogonal-Multiple-Access (NOMA),
Physical Layer Security (PLS),
Artificial Noise (AN),
Cooperative Jamming (CJ),
Spectral Efficiency (SE),
Energy Efficiency (EE).

ABSTRACT

NOMA (Non-Orthogonal Multiple Access) has been recognized as new multiple access technology for wireless communication networks of the fifth generation and beyond, owing to its ability to improve spectral efficiency, support massive connectivity, and provide user fairness. However, it has been observed that the superposition-based transmission principle of NOMA is highly susceptible to eavesdropping attacks, especially in an open wireless network where all wireless communications are inherently broadcast in nature. Hence, ensuring secure wireless communications for NOMA systems has now become an important area of research. This research aims to improve the secrecy level of wireless communications for NOMA systems by employing Physical Layer Security (PLS) techniques. Specifically, two prominent PLS techniques, Artificial Noise (AN) and Cooperative Jamming (CJ), have been employed to provide security against passive eavesdropping attacks. The cooperative NOMA system architecture is considered, and the secrecy enhancement is analyzed for two possible scenarios when the eavesdropper is close to the relay node and when the eavesdropper is close to the base station. The secrecy performance of the proposed system is analyzed through various parameters, namely, Secrecy Outage Probability (SOP), Secrecy Capacity (SC), Secrecy Rate (SR), and Secrecy Energy Efficiency (SEE) in terms of the Signal to Noise Ratio (SNR). The numerical results for the secrecy metrics are obtained through MATLAB-based simulations, whereas the system-level model is developed using the Simulink platform to verify the suggested system's functionality in the presence of AN and CJ for the legitimate NOMA users and the eavesdropper. The results show that the secrecy performance is significantly enhanced with the introduction of AN and CJ, and the system shows robust performance in terms of energy efficiency. This paper provides significant insights into the design of the NOMA system from the secrecy perspective and validates the potential of PLS techniques for the design of the future wireless system.

1. Introduction

The tremendous growth of wireless communication services, fueled by the development of new applications such as massive Internet of Things (IoT), ultra-reliable low-latency communications (URLLC), and high data rate multimedia services, has put tremendous demands on the forthcoming communication systems. Smart cities, transportation, autos, manufacturing, agriculture, healthcare, and wearable technology are just a few of the industries that have embraced the Internet of Things (IoT). The necessity for vast connectivity poses serious hurdles to the 5G mobile network's limited communication capacity as the number of linked communication devices increases rapidly [1], [2]. Orthogonal time and frequency resources are used by conventional Orthogonal Multiple Access

Corresponding author E-mail address: jh230046en@st.tu.edu.iq
https://doi.org/10.61268/wc5t7g44

(OMA) techniques, such as Time Division Multiple Access (TDMA) and Frequency Division Multiple Access (FDMA), to provide non-interfering communication. While OMA has been successful in the past for wireless communication, it has low spectral efficiency and limited scalability for large numbers of users. Non-Orthogonal Multiple Access (NOMA) is one potential multiple access technique for 5G and other wireless communication networks. Through power domain multiplexing, NOMA increases the system's spectrum efficiency by enabling numerous users to share time-frequency resources [3]. In order to obtain the desired signal, power-domain NOMA relies on successive interference cancellation at the receiver end and superposition coding at the transmitter end. By supplying varying power levels according to the channel conditions of the users, it maintains interference at a level that is easily controlled, allowing simultaneous transmission between the users [4]. Apart from NOMA, cooperative communication has been widely recognized as an effective means to increase coverage and spectral efficiency for wireless communication systems [5], [6]. By allowing user cooperation to forward information to other users, it improves the reliability of the system. The combination of cooperative communication and NOMA was first introduced in [7], where cooperative NOMA was introduced to improve the capacity and reliability of wireless communication systems. Since then, extensive research has been conducted on cooperative NOMA systems to improve spectrum efficiency under scarce spectrum resources [8]–[16]. Nevertheless, despite its major advantages, it is important to note that the broadcast nature of NOMA systems creates major security issues. Unlike OMA systems, which offer some level of security through orthogonal resource allocation, NOMA systems employ superposition coding, which might enable an unauthorized receiver/eavesdropper to receive and potentially decode multiple users' information if the channel conditions are sufficiently good. Therefore, it is imperative to note that NOMA systems are susceptible to eavesdropping attacks, which creates major security concerns regarding information security and user privacy in future wireless networks. Apart from the need for high data rates, security risks another major limitation for IoT application deployment. The open electromagnetic environment poses a risk of information leaking, although NOMA uses user multiplexing, which takes place simultaneously over the same resource block. This further increases the security risks associated with wireless communications. In contrast to other security measures, which involve complex encryption and key exchange, physical layer security has been considered an attractive approach to wireless security by leveraging the characteristics of wireless channels to provide security, and it does not involve extensive communication resources to share keys between authorized parties, which is important for defending against eavesdropping attacks, especially in IoT networks [17]. With the security issues in cooperative NOMA systems in mind, this study is motivated by the requirement to apply physical layer security solutions in order to enhance wireless communications security. In this regard, the study proposes an approach that aims to improve the secrecy of information transmission in cooperative NOMA systems by considering utilization of physical layer security methods that ensure the confidentiality of the transmitted information is protected against the possible eavesdropping of the transmitted signals. In this study, the feasibility of the application of artificial noise and cooperative jamming techniques in protecting the transmitted signals against eavesdropping is investigated. Moreover, the effect of these PLS-based techniques on secure information delivery is examined in different scenarios in which the potential eavesdroppers are placed close to the BS or the R node. In addition, the secrecy performance of the proposed cooperative NOMA system is evaluated using some critical secrecy metrics, such as secrecy outage probability (SOP), secrecy capacity (SC), secrecy rate (SR), and secure energy efficiency (SEE), in different signal-to-noise ratio (SNR) environments.

2. Research Gaps

In cooperative non-orthogonal multiple access (Co-NOMA) systems, information-bearing signals can be transmitted either through dedicated relay nodes [18–20] or by exploiting strong user relays with favorable channel conditions. In this context, different relaying protocols have been investigated to enhance system performance. To further enhance security, an adaptive cooperative jamming scheme for both uplink and downlink transmissions in the presence of untrusted relays was proposed in [19]. User-assisted Co-NOMA is an appealing solution for multi-user NOMA systems because it offers substantial advantages over relay-assisted Co-NOMA by lowering the infrastructure expenses related to specialized relays while also taking use of spatial diversity. Additionally, methods for adaptive cooperation have been included to increase productivity. In [21, 22], an 'on/off' method of relaying was proposed, in which the conditions are such that the cooperative relay connection needs to be 'on' or 'off'. In other words, in [22], the intra-cell users are allowed to forward signals from cell-edge users after successive interference cancellation (SIC) when the SINR exceeds a specific level, but in [21], the requirements are determined by the cell-edge users' quality of service (QoS) needs. To solve the problems of interest, A dynamic DF-based Co-NOMA strategy that takes into account the pairing techniques for the geographically random users was presented by the authors of [23]. This approach resolves issues related to the full-duplex system, such as self-interference and the use of the additional time slots. Furthermore, a space-time block code-assisted Co-NOMA scheme was proposed in [24] to reduce the number of operations involved in the subsequent interference cancellation. The performance was evaluated considering the constraints of insufficient channel state information and poor time synchronization. The security issues have become a major concern due to the open nature of the wireless transmission medium, especially in the IoT-based wireless communication system. In order to address the aforementioned problems, the RS method has been extensively researched for efficient enhancement of the PLS of the multi-relay wiretap Co-NOMA system. For the smooth integration of orthogonal multiple access and NOMA approaches, the priority-based buffer-assisted RS method was presented in [25], and significant throughput benefits were achieved in both the high and low SNR zones. Furthermore, [26] provided the ideal single RS approach, the two-step single RS method, and the optimal dual RS method. Additionally, [26] examined the RS techniques' secrecy outage performance. The best RS schemes utilizing the DF/AF relaying techniques in the Co-NOMA system were suggested in [27] to increase the system's security and dependability in the presence of untrusted users. In addition, the cognitive collaboration approach for the Co-NOMA cognitive wireless network was proposed in [28]. Moreover, the cooperative relaying scheme for the Co-NOMA system using the partial NOMA approach was proposed in [29]. The following four cooperative solutions were put out to further enhance the PLS by taking into account the eavesdropper's location (Eve), imperfect successive interference cancellation, channel conditions, power allocation, and decoding principles. One of the most common PLS approaches in Co-NOMA systems is the deliberate degradation of the channel for the eavesdropper (Eve) through the use of artificial noise (AN) or jamming signals. The following two types of two-way RS strategies—optimal and suboptimal RS—are simultaneously studied in [30] to further enhance the overall performance of the Co-NOMA system in the presence of AN. In the context of the Co-NOMA system in IoT networks using the multi-antenna technology, the artificial noise was proposed in [31]. This type of artificial noise is transmitted by the base station and the strong IoT users in order to further improve the security of the Co-NOMA system. In addition, full-duplex (FD) systems allow the transmission and reception of signals on the same frequency band, which could potentially triple the data rate compared with the traditional half-duplex (HD) systems. This ability not only increases the spectral efficiency but also improves the PLS performance. In this direction, a novel communication system based on the integration

of NOMA, beamforming, SWIPT, and FD was proposed in [32] to achieve a high sum rate for downlink communication systems. The influence of SI cancellation on the system security was also investigated when three different SI scenarios were considered in FD mode. Furthermore, a novel system based on the cooperative NOMA system was proposed in [33], where the source node directly transmits information to a near user using a multi-antenna system, while multiple FD relays aid the system in the transmission of information to the distant user in the presence of passive eavesdroppers. For the purpose of addressing the wiretapping attack, a novel 2-stage FD-based AN scheme was proposed, in which the AN was utilized not only as an interference signal but also as a secret key in order to protect the remote user's privacy. Finally, the secrecy outage probability of large-scale NOMA systems using FD relays and AN was evaluated in [90] for the purpose of assessing the performance of the use of the combination of FD relays and AN for the purpose of enhancing the performance of PLS. As illustrated in the above discussion related to the existing literature associated with cooperative NOMA systems and PLS, the gaps in the existing literature are as follows. Firstly, the existing literature does not address the comparative evaluation of the use of the two techniques, namely, artificial noise and cooperative jamming. Secondly, the existing literature does not address the use of the proximity of the eavesdroppers to the base station and the relay. Thirdly, the existing literature does not address the evaluation of the secrecy energy efficiency. Fourthly, the existing literature does not address the use of system-level modeling tools, namely, Simulink, for the evaluation of the physical layer security techniques.

3. System Model

In this section, the system model that is used in this paper for the analysis of the secrecy performance of cooperative non-orthogonal multiple access systems with the help of physical layer security techniques is explained. In the system model that is used for the analysis, the scenario that is considered for the analysis of the cooperative non-orthogonal multiple access system with the help of physical layer security techniques is the scenario where the base station is communicating with the users with the help of the relay node, considering the presence of an eavesdropper.

- **Base Station (BS):** The base station functions as the main transmitter in the system. It uses the NOMA principle to superimpose the signals of various users with varying power levels based on their channel conditions. Moreover, the BS may also incorporate physical layer security, which uses the concept of artificial noise to impair the quality of the wiretap channel.
- **Relay Node:** The relay plays an important role in providing coverage extension as well as improving the reliability of the transmission, especially for the distant user. It receives the composite signal sent from the BS, then forwards the signal to the intended users using an appropriate relaying protocol, such as the decode-and-forward (DF) or the amplify-and-forward (AF) protocol. In addition, the relay can also assist in the enhancement of the security of the system through the generation of cooperative jamming (CJ) signals.
- **Near User (User N) and Far User (User F):** The user, denoted by N, is referred to as the near user with good channel conditions, whereas User F is referred to serve as the distant user with low channel conditions. In accordance with NOMA, User N uses successive interference cancellation to recover the superimposed signal, whereas User F is allocated higher power to meet its quality of service (QoS) demands.
- **Eavesdropper (Eve):** The eavesdropper is an unauthorized entity seeking to intercept the information being transmitted. Its inclusion in the system model enables assessing the efficacy of PLS techniques, such as artificial noise and cooperative jamming, in mitigating secrecy outage for secure communication.

- **Wireless Channels:** All the links in the system are assumed to be wireless fading channels, subject to noise and interference. The legitimate channel is defined as the BS, relay, and legitimate users, while the wiretap channel is defined as the relay (or BS) and the eavesdropper.

In summary, Figure 1 shows the overall network topology of the proposed cooperative NOMA system, considering the interaction between the base station, relay, legitimate user, and eavesdropper from the physical layer security perspective.

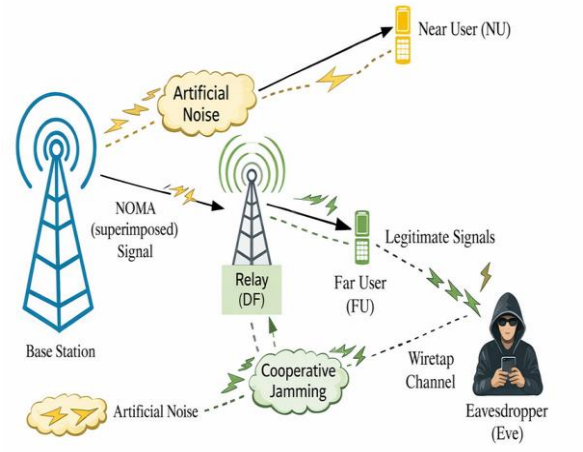

Figure 1. Cooperative NOMA System Model with PLS

3.1 Power-Domain Multiplexing in NOMA

In contrast to the concept of orthogonal multiple access (OMA), the concept of non-orthogonal multiple access (NOMA) allows multiple users to simultaneously share the same time-frequency resources by multiplexing the signals in the power domain. The theory behind the concept of NOMA is based on the use of superposition coding in the transmitter and successive interference cancellation in the receiver. Accordingly, the transmitted signal in the form of a superposition can be represented as follows:

$$x = \sum_{k=1}^{K} \sqrt{a_k P} s_k \quad (1)$$

Where s_k denotes the information signal of the k-th user, P represents the total transmit power, and a_k the power allocation coefficient assigned to the k-th user. These coefficients satisfy the following constraint.

$$\sum_{k=1}^{K} a_k = 1, a_1 \leq a_2 \leq \cdots \leq a_K \quad (2)$$

Users experiencing weaker channel conditions are allocated higher transmission power to ensure reliable decoding.

3.2 Successive Interference Cancellation

Successive interference cancellation (SIC) allows strong users to cancel weaker users' information before decoding their information. Even though SIC improves the spectral efficiency and capacity of the system, it also poses security risks. For instance, an eavesdropper with good channel conditions may use SIC to intercept confidential information. Therefore, other security measures must be put in place to ensure the security of the information sent through the NOMA system.

3.3 Cooperative Relay Model

Relaying techniques are commonly employed to enhance network coverage and improve transmission reliability. In this work, a decode-and-forward (DF) relay protocol is considered. The received signal at the relay can be expressed as:

$$y_R = h_{BR} x + n_R \quad (3)$$

Where h_{BR} symbolizes the coefficient of the channel between the base station and the relay, and n_R denotes additive white Gaussian noise (AWGN). The relay forwards the decoded signal to the intended users only when successful decoding is achieved.

3.4 Eavesdropper Model

The eavesdropper is assumed to be a passive malicious node attempting to intercept confidential transmissions. Two practical eavesdropping scenarios are considered:

- Scenario 1: Eavesdropper located near the relay, attempting to intercept the forwarded signals.
- Scenario 2: Eavesdropper located near the base station, attempting to intercept the superimposed NOMA signal.

These scenarios represent realistic worst-case security conditions commonly considered in secrecy performance analysis.

3.5 Artificial Noise Injection

Artificial noise (AN) is employed as a physical layer security technique to degrade the eavesdropper's channel without significantly affecting legitimate users. The transmitted signal with artificial noise can be expressed as**:**

$$x_{AN} = \sqrt{\alpha P}x_s + \sqrt{(1-\alpha)P}z \quad (4)$$

Where x_s is the information signal, z represents artificial noise, and α represents the ratio of power allocation between the injected noise and the usable signal.

3.6 Cooperative Jamming

Cooperative jamming (CJ) is another security mechanism in which trusted nodes transmit intentional interference signals to degrade the eavesdropper's reception capability.

$$x_{CJ} = \sqrt{\beta P}x_s + \sqrt{(1-\beta)P}x_J \quad (5)$$

Where x_J represents the jamming signal and β is the power allocation factor.

3.7 Secrecy Performance Metrics

To evaluate the effectiveness of the proposed security techniques, several secrecy performance metrics are adopted.

1. Secrecy Outage Probability (SOP)
$$SOP = \Pr(C_s < R_s) \quad (6)$$
2. Secrecy Rate (SR)
$$SR = E[C_s] \quad (7)$$
3. Secure Energy Efficiency (SEE)

$$SEE = \frac{SR}{P_{\text{total}}} \quad (8)$$

These metrics enable comprehensive evaluation of the secrecy performance of the proposed cooperative NOMA system under different signal-to-noise ratio conditions.

4. Results

The performance study and simulation results of the suggested cooperative NOMA system enhanced with physical layer security techniques. The results are obtained using MATLAB-based numerical simulations and are further validated through Simulink system-level models to ensure the reliability of the evaluated performance metrics. Two eavesdropping scenarios are considered in this research to examine the efficacy of the suggested security mechanisms under different threat conditions. In the first scenario, the eavesdropper is located near the relay node, attempting to intercept the forwarded signals during the relaying phase. In the second scenario, the eavesdropper is positioned close to the base station, where it attempts to intercept the superimposed NOMA transmission directly from the transmitter. The overall communication architecture considered in the simulations is illustrated in Figure 2, which depicts the cooperative NOMA system including the base station, relay node, legitimate users, and the eavesdropper under the physical layer security framework.

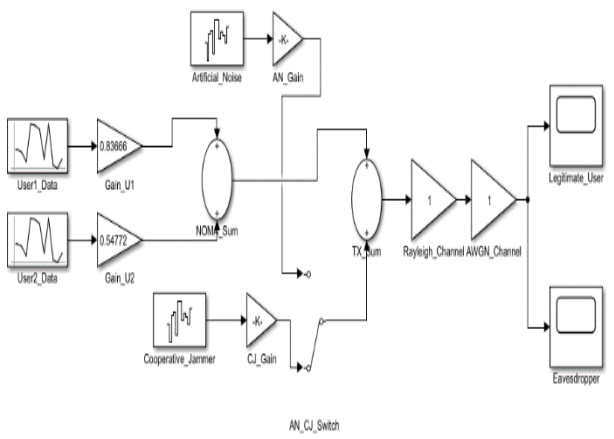

Figure2. Simulink signal-level model of cooperative NOMA with AN and CJ

The parameters considered in the simulation setup include realistic parameters for the wireless communication system, such as power, bandwidth, channel, etc. These parameters have been chosen based on the 5G and beyond wireless communication systems. Table1 shows the key simulation parameters used in the study.

Table1. Simulation Parameters

Parameter	Value
Total transmit power $\boldsymbol{P}$	30 dBm
Noise variance $\boldsymbol{\sigma^2}$	1
Power allocation coefficients $\boldsymbol{a_1, a_2}$	0.3, 0.7
AN/CJ power allocation $\boldsymbol{\alpha, \beta}$	0.7
Number of Monte Carlo trials	10^5
Channel model	Rayleigh fading

Based on the parameters used in the simulation, as presented in Table1, the performance of the proposed cooperative NOMA system is evaluated under different eavesdropping scenarios. The secrecy capacity performance of the artificial noise (AN) and cooperative jamming (CJ) schemes with different levels of SNR is shown in Figure 3.

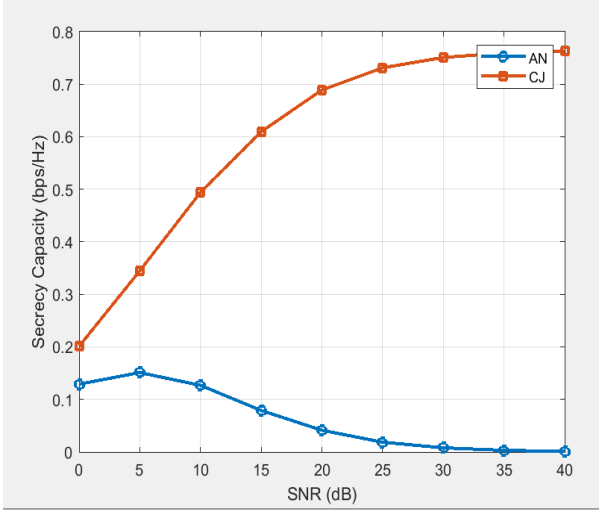

Figure 3. Secrecy capacity performance of artificial noise (AN) and cooperative jamming (CJ) schemes versus SNR.

Based on the secrecy capacity results, the secrecy outage probability performance of the artificial noise (AN) scheme and the cooperative jamming (CJ) scheme at different SNR levels is shown in Figure 4.

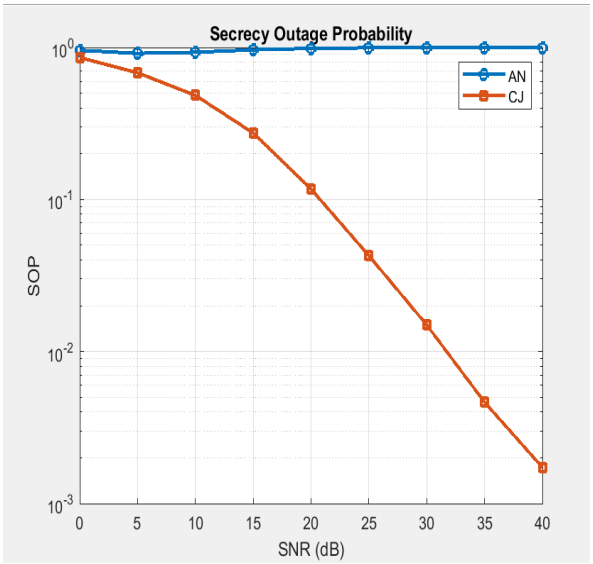

Figure 4. Secrecy outage probability (SOP) performance of artificial noise (AN) and cooperative jamming (CJ) schemes versus SNR.

In addition to secrecy capacity and probability of a secret outage, the secure energy efficiency performance of artificial noise (AN) and cooperative jamming (CJ) schemes with different SNR levels is shown in Figure 5.

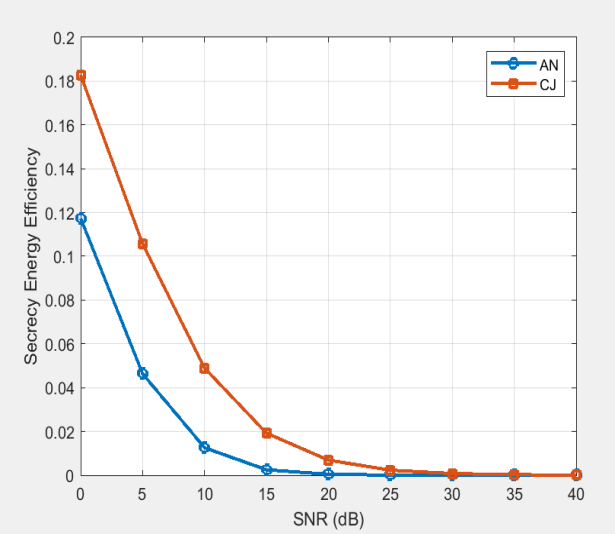

Figure 5. Secure energy efficiency performance of artificial noise (AN) and cooperative jamming (CJ) schemes versus SNR.

The performance of cooperative jamming (CJ) and artificial noise (AN) techniques under various eavesdropper locations is summarized in Table2.

Table2. Comparison of Secrecy Performance Metrics under Different Eavesdropper Locations

Metric	Eavesdropper Near Relay	Eavesdropper Near BS
Secrecy Capacity	CJ > AN	AN > CJ
SOP	CJ < AN	AN < CJ
Secrecy Rate	CJ > AN	AN > CJ
Secure Energy Efficiency (SEE)	CJ > AN	AN > CJ

According to results, cooperative jamming works better when the eavesdropper is close to the relay, whereas artificial noise improves secrecy performance when the eavesdropper is close to the base station.

5. Conclusion

In conclusion, the study showed that the use of physical layer security techniques such as artificial noise and cooperative jamming is beneficial in terms of improving The confidentiality of cooperative NOMA systems. The findings obtained in this study showed that the performance of the proposed techniques is affected by the location of the eavesdropper, where the cooperative jamming technique is more effective when the eavesdropper is near the relay, while the artificial noise technique is more effective when the eavesdropper is near the base station. The use of analytical modeling, MATLAB simulation, and Simulink system-level validation is beneficial in terms of analyzing secure, energy-efficient, and spectrally efficient systems for wireless communication.

References

[1] Chettri, L.; Bera, R. A Comprehensive Survey on Internet of Things (IoT) Toward 5G Wireless Systems. *IEEE Internet Things J.* **2020**, *7*, 16–32.

[2] Yu, B.; Chen, X.; Cai, Y. Age of Information for the Cellular Internet of Things: Challenges, Key Techniques, and Future Trends. *IEEE Commun. Mag.* **2022**, *60*, 20–26.

[3] Liu, Y.; Zhang, S.; Mu, X.; Ding, Z.; Schober, R.; Dhahir, N.; Hossain, E.; Shen, X. Evolution of NOMA Toward Next Generation Multiple Access (NGMA) for 6G. *IEEE J. Sel. Areas Commun.* **2022**, *40*, 1037–1071.

[4] Ding, Z.; Lei, X.; Karagiannidis, G.K.; Schober, R.; Yuan, J.; Bhargava, V.K. A Survey on Non-Orthogonal Multiple Access for 5G Networks: Research Challenges and Future Trends. *IEEE J. Sel. Areas Commun.* **2017**, *35*, 2181–2195.

[5] Chen, S.; Zhao, J. The requirements, challenges, and technologies for 5G of terrestrial mobile telecommunication. *IEEE Commun. Mag.* **2014**, *52*, 36–43.

[6] Sami, M.; Noordin, N.K.; Khabazian, M.; Hashim, F.; Subramaniam, S. A Survey and Taxonomy on Medium Access Control Strategies for Cooperative Communication in Wireless Networks: Research Issues and Challenges. *IEEE Commun. Surv. Tutor.* **2016**, *18*, 2493–2521.

[7] Ding, Z.; Peng, M.; Poor, H.V. Cooperative Non-Orthogonal Multiple Access in 5G Systems. *IEEE Commun. Lett.* **2015**, *19*, 1462–1465.

[8] Lv, L.; Jiang, H.; Ding, Z.; Yang, L.; Chen, J. Secrecy-Enhancing Design for Cooperative Downlink and Uplink NOMA With an Untrusted Relay. *IEEE Trans. Commun.* **2020**, *68*, 1698–1715.

[9]Jiang, D.; Gao, Y.; Sha, N.; Wang, X.; Li, N. Physical Layer Security of Cooperative NOMA Systems with an Untrusted User. In Proceedings of the 2022 IEEE 22nd International Conference on Communication Technology (ICCT), Nanjing, China, 11–14 November 2022; pp. 1287–1292.

[10] Yue, X.; Liu, Y.; Kang, S.; Nallanathan, A.; Ding, Z. Exploiting Full/Half-Duplex User Relaying in NOMA Systems. *IEEE Trans. Commun.* **2018**, *66*, 560–575.

[11] Do, T.N.; da Costa, D.B.; Duong, T.Q.; An, B. Improving the Performance of Cell-Edge Users in NOMA Systems Using Cooperative Relaying. *IEEE Trans. Commun.* **2018**, *66*, 1883–1901.

[12] Kara, F.; Kaya, H. Threshold-Based Selective Cooperative-NOMA. *IEEE Commun. Lett.* **2019**, *23*, 1263–1266.

[13] Zhou, Y.; Wong, V.W.S.; Schober, R. Dynamic Decode-and-Forward Based Cooperative NOMA With Spatially Random Users. *IEEE Trans. Wirel. Commun.* **2018**, *17*, 3340–3356.

[14] Akhtar, M.W.; Hassan, S.A.; Saleem, S.; Jung, H. STBC-Aided Cooperative NOMA With Timing Offsets, Imperfect Successive Interference Cancellation, and Imperfect Channel State Information. *IEEE Trans. Veh. Technol.* **2020**, *69*, 11712–11727.

[15] Alkhawatrah, M.; Gong, Y.; Chen, G.; Lambotharan, S.; Chambers, J.A. Buffer-Aided Relay Selection for Cooperative NOMA in the Internet of Things. *IEEE Internet Things J.* **2019**, *6*, 5722–5731.

[16] Lei, H.; Yang, Z.; Park, K.-H.; Ansari, I.S.; Guo, Y.; Pan, G.; Alouini, M.-S. Secrecy Outage Analysis for Cooperative NOMA Systems With Relay Selection Schemes. *IEEE Trans. Commun.* **2019**, *67*, 6282–6298.

[17] Wu, Y.; Khisti, A.; Xiao, C.; Caire, G.; Wong, K.-K.; Gao, X. A Survey of Physical Layer Security Techniques for 5G Wireless Networks and Challenges Ahead. *IEEE J. Sel. Areas Commun.* **2018**, *36*, 679–695.

[18] Ding, Z.; Peng, M.; Poor, H.V. Cooperative Non-Orthogonal Multiple Access in 5G Systems. *IEEE Commun. Lett.* **2015**, *19*, 1462–1465.

[19] Lv, L.; Jiang, H.; Ding, Z.; Yang, L.; Chen, J. Secrecy-Enhancing Design for Cooperative Downlink and Uplink NOMA With an Untrusted Relay. *IEEE Trans. Commun.* **2020**, *68*, 1698–1715.

[20] Jiang, D.; Gao, Y.; Sha, N.; Wang, X.; Li, N. Physical Layer Security of Cooperative NOMA Systems with an Untrusted User. In Proceedings of the 2022 IEEE 22nd International Conference on Communication Technology (ICCT), Nanjing, China, 11–14 November 2022; pp. 1287–1292.

[21] Do, T.N.; da Costa, D.B.; Duong, T.Q.; An, B. Improving the Performance of Cell-Edge Users in NOMA Systems Using Cooperative Relaying. *IEEE Trans. Commun.* **2018**, *66*, 1883–1901.

[22] Kara, F.; Kaya, H. Threshold-Based Selective Cooperative-NOMA. *IEEE Commun. Lett.* **2019**, *23*, 1263–1266.

[23] Zhou, Y.; Wong, V.W.S.; Schober, R. Dynamic Decode-and-Forward Based Cooperative NOMA With Spatially Random Users. *IEEE Trans. Wirel. Commun.* **2018**, *17*, 3340–3356.

[24] Akhtar, M.W.; Hassan, S.A.; Saleem, S.; Jung, H. STBC-Aided Cooperative NOMA With Timing Offsets, Imperfect Successive Interference Cancellation, and Imperfect Channel State Information. *IEEE Trans. Veh. Technol.* **2020**, *69*, 11712–11727.

[25] Alkhawatrah, M.; Gong, Y.; Chen, G.; Lambotharan, S.; Chambers, J.A. Buffer-Aided Relay Selection for Cooperative NOMA in the Internet of Things. *IEEE Internet Things J.* **2019**, *6*, 5722–5731.

[26] Lei, H.; Yang, Z.; Park, K.-H.; Ansari, I.S.; Guo, Y.; Pan, G.; Alouini, M.-S. Secrecy Outage Analysis for Cooperative NOMA Systems With Relay Selection Schemes. *IEEE Trans. Commun.* **2019**, *67*, 6282–6298.

[27] Cao, K.; Wang, B.; Ding, H.; Li, T.; Gong, F. Optimal Relay Selection for Secure NOMA Systems Under Untrusted Users. *IEEE Trans. Veh. Technol.* **2020**, *69*, 1942–1955.

[28] Li, M.; Yuan, H.; Maple, C.; Cheng, W.; Epiphaniou, G. Physical Layer Security Analysis of Cognitive NOMA Internet of Things Networks. *IEEE Syst. J.* **2023**, *17*, 1045–1055.

[29] Zhuo, B.; Duan, W.; Gu, J.; Gu, X.; Zhang, G.; Ji, Y.; Choi, J.; Wen, M. Partial-NOMA Based Physical Layer Security: Forwarding Design and Secrecy Analysis. *IEEE Trans. Intell. Transp. Syst.* **2022** , 1–14.

[30] Huang, M.; Gong, F.; Zhang, N.; Li, G.; Qian, F. Reliability and Security Performance Analysis of Hybrid Satellite-Terrestrial Multi-Relay Systems With Artificial Noise. *IEEE Access* **2021**, *9*, 34708–34721.

[31] Alsaba, Y.; Leow, C.Y.; Rahim, S.K.A. Full-Duplex Cooperative Non-Orthogonal Multiple Access With Beamforming and Energy Harvesting. *IEEE Access* **2018**, *6*, 19726–19738.

[32] Cao, Z.; Ji, X.; Wang, J.; Wang, W.; Cumanan, K.; Ding, Z.; Dobre, O.A. Artificial Noise Aided Secure Communications for Cooperative NOMA Networks. *IEEE Trans. Cogn. Commun. Netw.* **2022**, *8*, 946–963.

[33] Gong, C.; Yue, X.; Zhang, Z.; Wang, X.; Dai, X. Enhancing Physical Layer Security With Artificial Noise in Large-Scale NOMA Networks. *IEEE Trans. Veh. Technol.* **2021**, *70*, 2349–2361.