Journal of Trends and Challenges in Artificial Intelligence

Vol. 03, No. 03 (2026) 141-150, DOI: 10.61552/JAI.2026.03.003 - http://jai.aspur.rs

APPLICATION PHYSICAL LAYER SECURITY TECHNIQUES FOR ENHANCEMENT OF COOPERATIVE NOMA

Jouana H. Hassan[1]
Ibrahim Khalil Silleh

Received 02.07.2025.
Revised 22.08.2025.
Accepted 24.09.2025.

Keywords:

Artificial Noise, Cooperative Jamming, Physical Layer Security, Non-Orthogonal Multiple Access, Raley.

Original research

A B S T R A C T

Over the past decades, wireless communications have proliferated, and the growing demand for wireless applications and the number of connected users have led to the advancing commercialization of 5G technology and the predicted development of 6G technologies. Physical layer security is one of the technologies that keep pace with the advancement of generations. This progress offers significant advantages to users and requires strong security. Data transmission in wireless communications suffers from serious threats. To protect users from eavesdropping attacks, two PLS techniques are applied: Artificial Noise (AN) and Cooperative Jamming (CJ). These techniques aim to degrade the reception quality of potential eavesdroppers without affecting users. Several metrics are applied to maintain information confidentiality, including SR, SC, SOP, and SEE for SNR. This practical analysis was conducted in MATLAB (Monte Carlo) on the application of AN and CJ techniques on the AF relay. The results showed that the artificial noise technique achieves better results in providing high security to users. The main characteristic of artificial noise is its ability to generate a specific interference signal based on channel characteristics. Future work indicates the application of other PLS techniques on the relay.

1. INTRODUCTION

Wireless communications have become an integral part of our daily lives and have a significant societal impact. Applications related to medical data, e-banking, and e-commerce, in particular, require privacy and confidentiality regarding information transmitted over wireless media. The emergence of 5G networks as a successor to 4G is a concerning trend. The increase in wireless devices necessitates low-cost, low-latency networks, which 4G and prior generation networks excel at (Nguyen et al., 2019).

One of the most exciting 5G criteria, non-orthogonal multiple access (NOMA), is evolving with the times. The capacity of NOMA to accommodate several users on a single Frequency, time slot, or code guarantees spectral efficiency. In addition, NOMA has the potential to improve user equality (Lee et al., 2018). Nevertheless, cooperative communication may enhance throughput and coverage in single-antenna systems (Ahmed & Gharavi, 2018). In a collaborative system, relays or adjacent nodes assist the source in sending altered signals to a destination. A relay's manipulation of the source signal relies on the relaying protocol used.

The most common relaying protocols are amplify-and-forward AF and decode-and-forward DF). The AF relay amplifies and sends the received signal to the destination (Van Nguyen et al., 2018). Eavesdropping and signal interception are common risks to wireless

[1] Corresponding author: Jouana H. Hassan
Email: jh230046en@st.tu.edu.iq

communications, making NOMA networks insecure (Atallah et al., 2015). The wiretap channel, pioneered by Wyner, enabled secure communication without secret keys. When an eavesdropper uses a degraded channel, the source and destination may exchange secure messages at a non-zero rate. However, the eavesdropper can learn nothing about the messages from its observations (which Wyner demonstrated) (Jameel et al., 2018).

Physical Layer Security (PLS) is a technology that accompanies the advancement of 6G. It is essential to maintain the confidentiality of information during its transmission to NOMA networks and to combat eavesdropping attacks. Physical layer security (PLS) improves information security by utilizing wireless channel characteristics like fading, noise, and interference to prevent eavesdroppers from gaining access to legitimate information (Hamamreh et al., 2018). The research aims to provide confidentiality for information during its transmission from the base station to the users, improve the signal quality through relay-type amplification and Forward AF, and maintain the confidentiality of information while preventing eavesdropping attacks. As NOMA downlink and uplink have unique security features (Tabassum et al., 2017), PLS has been studied independently. In Zhang et al. (2016), the authors examined the downlink secrecy sum rate maximization in an SISO NOMA system.

There was no further NOMA effort to address this problem. Presentation of closed-form formulas for an optimum power allocation strategy maximizing secrecy sum rate, with numerical data demonstrating performance improvement over OMA. A single eavesdropper scenario was considered (He et al,. 2017) for NOMA downlink. Design characteristics examined were transmit power, decoding order, and transmission rate. The secrecy measure used was the outage probability. Two PLS techniques are applied to maintain the confidentiality of information from eavesdroppers, artificial noise, and cooperative jamming through physical measures, including SOP, SC, SR, and SEE for SNR.

This helps protect NOMA network users from eavesdropping attacks by applying artificial noise to the relay and cooperative jamming, as well as to prevent information from reaching the eavesdropper or reaching him in a confused Form that he cannot understand. This paper is organized as follows: Section 2 discusses the proposed system model, and Section 3 discusses Physical Layer Security Applications. Section 4 presents Performance Metrics for Secrecy. Section 5 presents Results and Discussion. Section 6 presents Future Research Direction, and Section 7 presents Conclusion.

2. LITERATURE REVIEW

Consider a cooperative wireless network consisting of one source, two users, and one relay, with an eavesdropper listening to the relay, as shown in Figure 1. All nodes are equipped with a single antenna. The link between the base station and the users is called the home channel, and the link between the base station and the eavesdropper is called the eavesdropping channel. This model is typical of most secure multi-user communications systems. To evaluate the use of several confidentiality metrics, such as Secrecy outage probability (SOP), Secrecy capacity (SC), Secrecy rate (SR), and Secrecy energy efficiency (SEE), in different channel environments using MATLAB 2018. It should be noted that all user nodes are equally located from the base station, and the power allocation is fixed for users.

To study the impact of layer physical security techniques on the cooperative NOMA system, the following methods were chosen: artificial noise (AN) and cooperative jamming (CJ). The NOMA approach was applied to both PLS amplify and Forward AF routing techniques. First, artificial noise is added to the AF relay, where the AF nodes, upon receiving the signal, amplify the signal and send it to the users without the eavesdropper knowing, as the high noise is sent, and the eavesdropper cannot understand the signal. Similarly, cooperative jamming is applied in the same way, where high jamming is sent to the eavesdropper. These topologies are explained in Table 1.

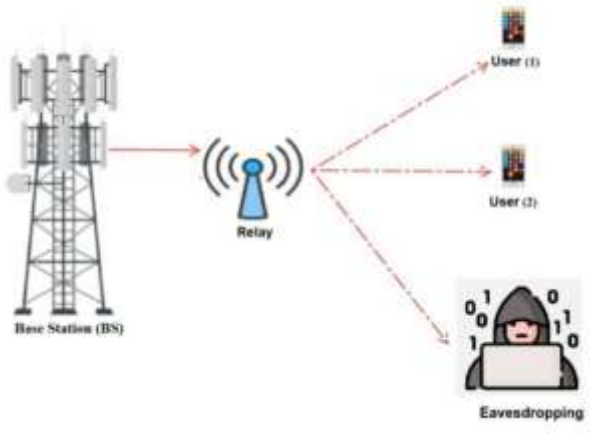

Figure 1. A cooperative wireless network consisting of one source, two users, and one relay in the presence of an eavesdropper.

Table 1. Model Configuration

Particle	Details
Cooperative schemes	AF
Number of nodes	(2),(3)
Power allocation	Fixed
Cannel model	Rayleigh channel
Power allocation for user1	0.48
Power allocation for user2	0.47
Power allocation for eavesdropping	0.05
SNR	(0-30)dB

2.1 Physical Layer Security Technologies

The literature presents several approaches to improving transmission rate and validating terminal identities, making it easier to implement Physical Layer security.

These approaches can be divided into several categories, including PHY-authentication technologies, secure multi-antenna technologies, secure relay technologies, and wiretap code designs (Liu et al., 2016). Our work will be limited to secure relay techniques.

2.1.1 Secure Relay Techniques

When transmitters in multi-hop wireless networks have limited power to carry messages, relay systems are crucial. Relay cooperation methods (Illi et al., 2023), including decode and forward (DF), amplify and forward (AF), noise and forward (NF), and compress and forward (CF), can increase wireless networks' secrecy capabilities. We take into consideration the AF relaying protocol, which uses a scaled version of the signal it receives to send it to its destination without requiring any decoding. Specifically, the signal is broadcast by the source node first. The best relay node will then be chosen to send a scaled-down version of the signal it has received (Zou et al., 2016). Observe that the source signal is sent twice from the source and relayed throughout the AF relaying procedure. The total transmit power at the source and relay must be kept to P in order to allow for a fair comparison with direct transmission. For simplicity, the transmit power at the source and relay is provided by P/2 using the equal-power allocation (Li et al., 2019). Consequently, given that the source node uses power P/2 to send its signal, the received signal at the relay can be provided by

$$\text{ri}=\sqrt{\frac{p}{2}}\, hsi\, s + ni$$

Where his represents a fading coefficient of the channel from the source relay

$n_i \sim CN(0, \sigma^2)$represents AWGN at the relay(Zou et al. 2016).

2-2 Effect of the Eavesdropper on the NOMA Relay

Only information from the relay is audible to the eavesdropper in this situation. The received signal that is sent from the relay to the eavesdropper E in the second phase of communication is more precisely provided by

$$\boldsymbol{y_{RE}^{NoMA} = h_{RE}\left(\sqrt{p_r}a1x_1 + \sqrt{p_r}a_2x_2\right) + W_E}$$

hRE denotes the channel between the relay and the eavesdropper. E stands for additive white Gaussian noise with zero mean and variance (NE), hRE∼CN (0, λRE), i=1,2, ωE Pr is the relay's transmit power. It is noteworthy that using SIC as a means of achieving the SNR at

$$\boldsymbol{y_{RE\text{i}}^{NOMA} = \frac{a^2 P_r |h_{RE}|^2}{N_E} = a_i^2 \rho E |h_{RE}|^2}$$

Where ρE=Pr /NE, i= {1,2} and αi2 is the power allocation fraction, the BS sends the overlaid signal (x=α1x1+α2x2) to the relay. This study defines xi (i = 1, 2) as the unit power signal received by users D1 and D2, and αi as the power allocation fractions. To meet NOMA criteria, assume α1 ≥ α2 and set the power allocation restriction to α1+α2 =1 (Van Nguyen & Do, 2020).

3. PHYSICAL LAYER SECURITY APPLICATIONS

Physical layer security applications can be classified into several techniques, including artificial noise, multi-antenna diversity, and cooperative jamming (Sánchez et al., 2021). We will discuss in detail each of artificial noise and cooperative jamming and their application to NOMA users to maintain the confidentiality of information from eavesdroppers.

3.1 Artificial Noise (AN)

Using a portion of the transmitter node's power, this technique adds synthetic noise to the eavesdropper's channel (da Silva et al., 2023). The AN and the information-bearing signal are introduced into the channel matrix of the authorized user's range space and null space, respectively. In this way, the AN has minimal adverse effects on the authorized recipient and only degrades the eavesdropper (Lv et al., 2024).

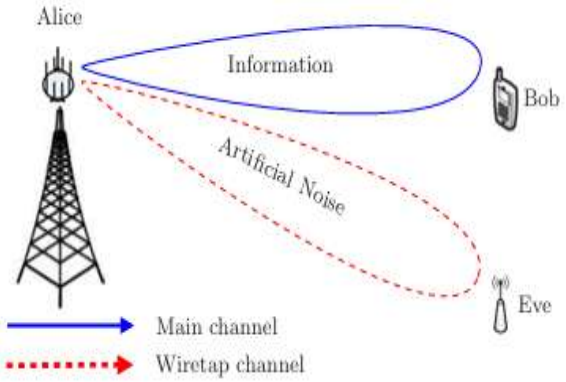

Figure 2. Depicts an AN network model for a wiretap channel with two nodes and an eavesdropper.

An efficient way to give the valid transmission connection a channel quality advantage is by AN injection. The majority of AN-based PLS systems, however, depend on the installation of several antennas at the transmitter (Zhang et al. 2015a; Zhang et al. 2015b; Zhang et al. 2015c; Wang et al., 2018), which goes against the IoT devices' need for low cost and compact size. Cooperative AN injection emerges as a viable remedy for this problem, guaranteeing the secure transmission (Sun & Du, 2018). In Figure 2, the basic system model of the AN network for PLS is depicted.
This technique aims to impair Eve's channel by adding artificial noise (AN). According to (Cumanan et al, 2016), an authorized node in the network, such as Alice or Bob, adds well-designed fake jamming signals to the broadcast signal, harming Eve's channel (Sánchez et al., 2021).

3.2 Cooperative Jamming(CJ)

Cooperative jamming has garnered considerable interest and is a promising technique. Initially, a multiple-access wiretap channel was suggested in which several authorized users wished to securely communicate with an intended recipient while an eavesdropper was present (Atallah et al., 2015). Cooperative jamming involves the relay transmitting an independent signal while the source transmits. The objective is to disrupt the eavesdropper's signal. In particular, the source sends the message signal $\sqrt{p_s}s$, where Ps is the transmit power, while the relay sends a weighted version of a common jamming signal z, wz, where w is the antenna weight vector (Chen et al,. 2016). Thus, the transmit power budget for the jamming signal transmission is:

$$p_j = p - p_S$$

Received signal at destination equals

$$y_d = \sqrt{P_s}h_{sD}s + w^{\dagger}h_{RD^z} + n_d$$

Where nd is white, complicated Gaussian noise at the destination and Hermitian transposition.The received signal at the eavesdropper equals

$$y_e = \sqrt{p_S}h_{SE}s + w^{\dagger}h_{RE}z + n_e$$

Where a white complex Gaussian eavesdropping noise is present (Chen et al,. 2016).

3.2.1 Types of Artificial Jamming Signals

To create interference at the eavesdropper's side, cooperative jamming uses fake signals that can be split into four groups (Long et al., 2014):

1- The most head-dative noise at the receiver is Gaussian noise (Liu et al., 2016; Zhang et al. 2015b).
2- jamming signals that legal receivers already know about, which merely affect the performance of the eavesdropper. Because the genuine receiver is unaffected by the jamming signals, this sort of transmission is superior to the prior one (Long et al., 2014; Atallah et al., 2015).
3- The genuine receiver may decode and cancel the jamming signals using random codewords from a public codebook that are known to all nodes, including the eavesdroppers. However, decoding the codewords necessitates a complex self-interference cancellation receiver (Yener & Ulukus, 2015).
4- This type of signal is challenging to apply due to the change of the multiple transmission pairs. Examples of sound signals for the other legitimate nodes include the uplink and downlink of neighboring cells, signals of multiple simultaneous source-destination pairs, or signals of the invited cognitive radio users (Atallah et al., 2015).

3.2.2 Cooperative jamming using the Power Allocation technique

Given that the jamming strategy and jamming power level have a significant impact on the system's performance in cooperative jamming (Hamamreh et al., 2018), three power allocation strategies are derived in (Hamamreh et al., 2018) to minimize the outage probability of the secrecy rate. In addition, three types of jamming power allocation schemes are proposed based on the available channel state information (CSI) at the destination to minimize the outage probability. In order to divide the received signal for information decoding and energy harvesting, the valid receiver uses a power splitting method, which the authors of (Zhang et al., 2015c) offer as an alternative scenario. An alternative approach to power allocation is examined in Long et al. (2013), where the source nodes should use their power to emit jamming signals rather than using additional nodes to jam the eavesdropper.

4. PERFORMANCE METRICS FOR SECRECY

A number of measures have been proposed to examine the security level of PLS NOMA systems. Although (Khoshafa et al., 2024) provided several PLS metrics, our work will only focus on SR, SC, SEE, and SOPs for SNR.

4.1 Secrecy Rate(SR)

Calculating the difference between the main channel's and the wiretap channel's attainable rates while using a Gaussian codebook yields the SR of the Gaussian noise wiretap channel (Wang & Zheng, 2016). Mathematically, the SR and RS can be represented as

$$R_S = [R_D - R_E, 0]^+$$

Where RD is the achievable rate of the legitimate link,RE is the achievable rate of the eavesdropping link, and $[x, 0]^+ = max(0, x)$

4.2 Secrecy Capacity(SC)

The most significant possible rate Rs that guarantees absolute secrecy, or the fastest rate at which secure data may be sent over a wireless channel while preserving confidentiality, is known as the SC, or Cs (Lv et al., 2024). SC shows how secure communication is possible even when eavesdroppers are present. Regarding this, Cs can be acquired by

$$C_s = [C_D - C_E, 0]^+$$

Here, CD and CE represent the legitimate and eavesdropping link capacity, respectively. CD must be bigger than CE, emphasizing the importance of the main channel quality over the wiretap channel, regardless of the eavesdropper's computational capability.

4.3 Secrecy Outage Probability(SOP)

This measure is the likelihood that the SC will go below the predetermined secure transmission rate, Rs > 0. In light of this definition, the SOP is described as follows (Pakravan et al., 2023).

$$p_{sop} = p_r(C_s \leq R_s)$$

4.4 Secrecy Energy Efficiency(SEE)

When considering wireless secure communication systems under energy constraints, one of the most important metrics for assessing their effectiveness is the ratio of the available secure channel (ASC), which stands for the safe and dependable transmission of private communications, to the total power consumption. SEE is a statistic that evaluates a communication system's energy efficiency while taking security into account to guarantee transmission security (Ghadi et al., 2024).

4.5 Signal to Noise Ratio (SNR)

The strength of the received signal divided by the power of the unwanted signals in a given frequency range is known as the signal-to-noise ratio. It measures how much noise skews the information that is transmitted. If this ratio is acceptable, the signal may be filtered to remove noise (Saeed & Sileh, 2023).

$$SNR = 10\,log_{10}\frac{signal\ power}{noise\ power}\mathrm{d}B$$

The inverse relationship between bit error rate (BER) and signal-to-noise ratio (SNR) means that any increase in BER results in a decrease in SNR. With an increase in BER, system throughput decreases. Decibels (dB) are used to indicate A high signal-to-noise proportion.

4.6 Bit Error Rate(BER)

The most widely used performance metric for communication systems is bit error rate (BER). In a communication system, data is transmitted in bits. The exchange process involves a few mistakes. The average rate of these transmission defects is known as the bit error rate (BER) (Ahmed et al., 2018).

$$BER = \frac{number\ of\ error\ bits}{Total\ number\ of\ transmitted\ bits}$$

5. RESULTS AND DISCUSSION

The results represent the performance of a system, for example, NOMA for downlink communications between a single base station and two or three equally and unequally located user stations, under the PLS algorithm to protect signals from eavesdroppers within the network. The performance improvement of the NOMA network system over PLS is examined using MATLAB 2018 (Monte Carlo) by optimizing the information confidentiality coefficients. The procedure is implemented using two methods: artificial noise and cooperative Jamming. Each method includes four different measures of confidential information transfer, such as (SR), (SC), (SOP), and (SEE), under the AF cooperation protocols.

Figure 3 illustrates the impact of artificial noise on the SR of legitimate users and eavesdroppers in a NOMA downlink system via AF relaying. The SR of users improves as the capability to decode the transmitted information enhances, whereas the SR of the eavesdropper decreases.

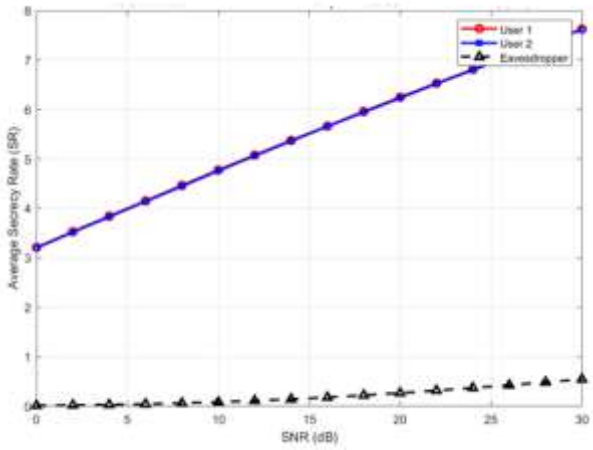

Figure 3. Secrecy Rate (SR) Performance with Artificial Noise.

The joint injection of artificial noise introduces the controlled interference to the joint received signal of the eavesdropper, which cannot be decoded as useful information. At the same time, the AF relay ensures that the intended users are able to receive the desired message with minimal distortion. This effect further highlights the dual role of artificial noise: it not only plays a security layer against eavesdropping, but also maintains user performance. The results are in agreement with the effectiveness of artificial noise for increasing network security, particularly under scenarios where multiple users have distinct channel conditions, showing that the legitimate communication is still secure when confronted with adversarial eavesdropping attacks.

Figure (4) illustrates how artificial noise influences the secrecy capacity (SC) of a NOMA system. The user's SC value rises with added noise to around 6.9, while the SR value reaches 7.6. This means that valid users enjoy better channel conditions irrespective of interference, while the capacity of the eavesdropper is reduced due to distortion of the signal.

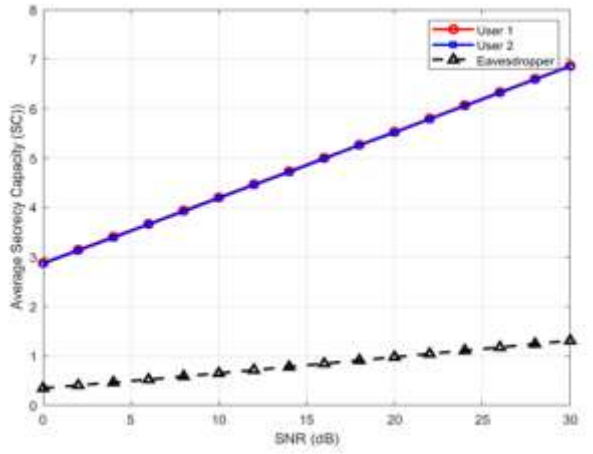

Figure 4. Secrecy Capacity (SC) with Artificial Noise

The SC measure captures the highest rate of data that can be reliably transmitted securely and demonstrates that artificial noise widens the gap between user and eavesdropper channels. Through degrading the channel of the eavesdropper while leaving the original users untouched, the system achieves secure communication. These results illustrate the importance of artificial noise in physical layer security systems and demonstrate that properly optimized interference can enhance confidentiality without degrading the quality and reliability of the communication for the intended receivers.

Figure 5 illustrates the SOP of eavesdroppers and legitimate users for artificial noise. The SOP of legitimate users slows down with growing SNR, achieving minimum points at 30 dB, indicating that the probability of failure to keep the information secret diminishes under high channel conditions.

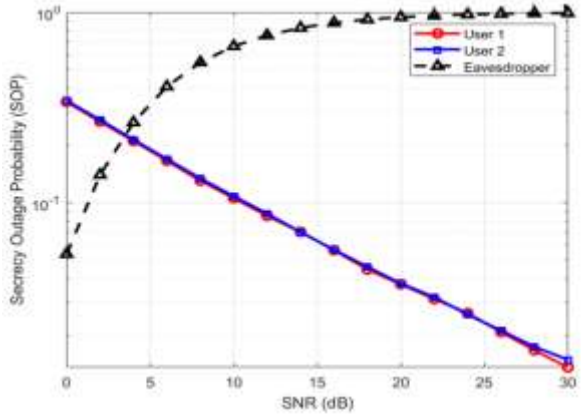

Figure 5. Secrecy Outage Probability (SOP) with Artificial Noise

For the eavesdropper, there is an ever-increasing SOP, eventually leading to full outage, which shows the worsening difficulty in intercepting the signal. This move confirms that the system possesses a reliable and secure communication link for users and makes attempts at interception increasingly unlikely. Mathematically, the result is consistent with the RS ≥ CS criterion, confirming that the secrecy rate is larger than the eavesdropper capacity. Overall, this figure indicates the efficiency of artificial noise in reducing security breaches, with evidence that NOMA systems can guarantee secure protection against eavesdroppers while ensuring efficient communication for legitimate users.

Figure 6 shows SEE for eavesdropper and user when using artificial noise. SEE of user increases gradually with SNR to a value of 86, while that of an eavesdropper is nearly zero at 30 dB. The result indicates that the system optimizes energy utilization for secure communication, allowing users to get quality signals without power loss. Artificial noise causes the eavesdropper to obtain a grossly degraded signal, thereby rendering energy utilization for interception futile. The results indicate that physical layer security methods can improve energy efficiency by focusing resources on legitimate users simultaneously while canceling out potential eavesdroppers. SEE thus is an end-to-end measure of the performance of a system, combining secrecy and energy expenditure. The results verify the role of artificial noise in rendering sustainable, energy-efficient, and secure NOMA communication networks easier to deploy in actual energy-constrained environments.

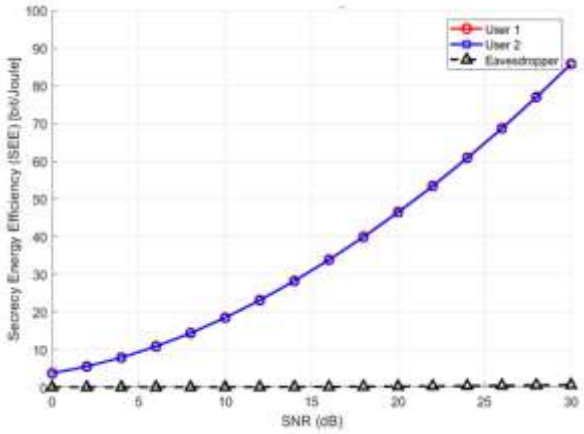

Figure 6. Secrecy Energy Efficiency (SEE) with Artificial Noise

Figure 7 illustrates SR with cooperative jamming in NOMA system with AF relays. Cooperative jamming constitutes intentional interference from trusted nodes to deceive eavesdroppers without compromising the legitimate users' signals. With an increase in SR, users are successful in decoding the messages, whereas SR of the eavesdropper reduces due to the large amount of interference. This approach is particularly effective when multiple users are located at different distances from the base station because it jams the eavesdropper's channel in a selective fashion without affecting users. The results demonstrate that cooperative jamming provides an extra layer of physical layer security on top of artificial noise. With the implementation of cooperative nodes, the system achieves a compromise between the promotion of user confidentiality and the retention of high data rates, proving its effectiveness as a reliable method for preventing information leakage in dynamic multi-user communication.

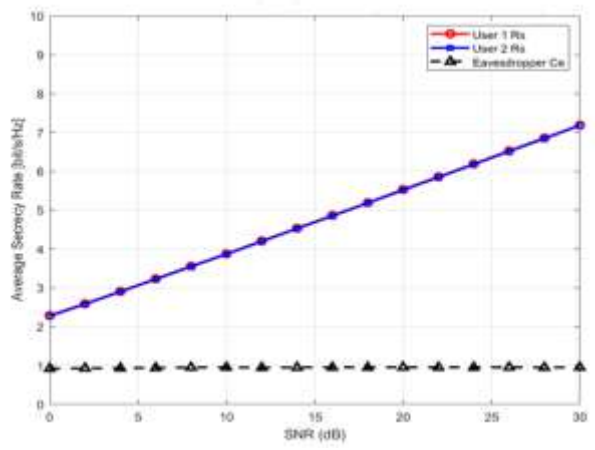

Figure 7. Secrecy Rate (SR) with Cooperative Jamming

The plot in Figure 8 shows how cooperative jamming influences SC for users and eavesdroppers. SC of users is augmented with jamming amplitude, reflecting better secure transmission rates, whereas SC of the eavesdropper decreases due to signal distortion.

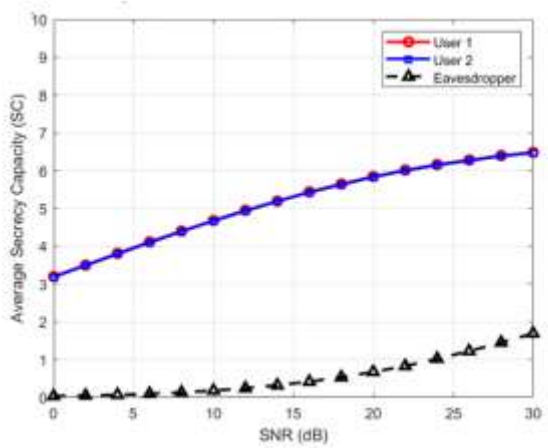

Figure 8. Secrecy Capacity (SC) with Cooperative Jamming

Cooperative jamming effectively brings about interference at the right positions, degrading the eavesdropper's decoding ability without interfering with legitimate communication. The results indicate that SC can be optimized for users while maintaining the risk of interception to a minimum, demonstrating the application of cooperative interference to enhance confidentiality. These outcomes confirm the strategic advantage of cooperative security features in NOMA networks, wherein users cooperate to maximize the secrecy gap. With the provision of a strong SC for users and a weak SC for eavesdroppers, the system is capable of preserving secure and reliable communication even under situations of time-varying network conditions and multi-user interference.

Figure 9 illustrates SOP of users and eavesdroppers in cooperative jamming. As SNR increases, users' SOP decreases linearly, tending towards minimum values at 30 dB, whereas eavesdroppers' SOP tends toward complete outage.

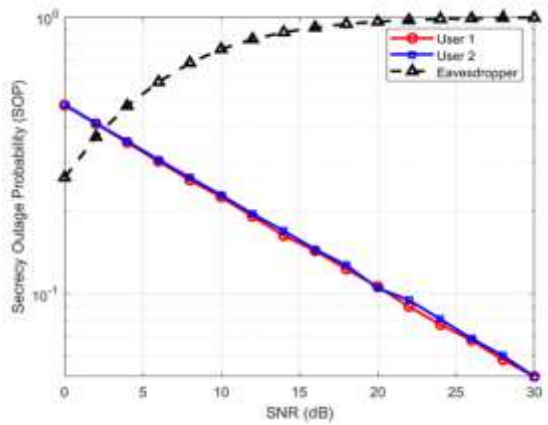

Figure 9. Secrecy Outage Probability (SOP) with Cooperative Jamming

This indicates that cooperative jamming effectively guards legitimate transmissions such that users' secrecy failure probability is minimal. The increasing SOP of eavesdroppers illustrates that the ability of eavesdroppers to intercept or demodulate messages is reduced as the system adds intended interference. The figure highlights the guard role of cooperative jamming in multi-user networks, which depicts interference from trusted nodes can be strategically used to reinforce security. The results confirm that the NOMA system can deliver secure communication reliably and eliminate potential threats, and cooperative jamming is a key component of advanced physical layer security techniques.

SEE for users and eavesdroppers with cooperative jamming is illustrated in Figure 10. The SEE of users rises gradually with SNR and reaches its maximum at 75, whereas the efficiency of the eavesdropper remains near zero. This means that cooperative jamming allows energy to be used effectively towards secure communication while attempts at interception are expensive and inefficient.

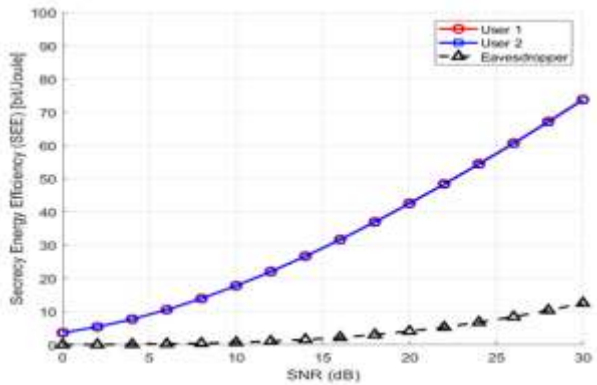

Figure 10 . Secrecy Energy Efficiency (SEE) with Cooperative Jamming

By introducing interference in a strategic manner, the system improves user performance without increasing energy consumption. The results show that SEE is an effective metric for evaluating the dual benefit of energy efficiency and secrecy in NOMA systems. Typically, cooperative jamming enhances secure throughput and energy efficiency, justifying it for use in real networks under energy constraints and proving its relevance to maintaining user secrecy against eavesdropping attacks.

Physical Layer Security (PLS) and Non-Orthogonal Multiple Access (NOMA) provide new developments, keeping up with generational advancements in various fields.

1- An AF encoding and routing protocol will be implemented to select the optimal sequence, and future work refers to the implementation of a decoding and routing protocol (DF) and a hybrid relay protocol (HRP).
2- The practical study and analysis are conducted by placing the listening device close to the relay and applying PLS techniques. Future studies propose

placing the listening device close to the base station (BS) and applying PLS techniques there.

3- Implementing two PLS techniques. Future work indicates implementing other techniques on NOMA users to provide security.

6. CONCLUSIONS

This research aims to improve user security and protect them from eavesdropping attempts by investigating the physical layer security of the NOMA collaborative network. Artificial noise and cooperative jamming are the two PLS techniques introduced. When applying PLS to a NOMA system, the AF relay first transmits a large amount of noise to deceive an eavesdropper, then jams the signal to prevent information theft during transmission. The most significant results of these two methods are presented after applying four confidentiality guarantees. The confidentiality ratio (SR) of artificial noise was found to be 7.8 for artificial noise and 7.1 for cooperative jamming. The confidentiality capacity (SC) was 6.5 for cooperative jamming, while the SC was 7 for artificial noise. The secrecy outage probability (SOP) result was similar in the case of artificial noise and cooperative jamming. The confidentiality energy efficiency (SEE) of artificial noise was 86%, while the SEE for cooperative jamming was 74%. This demonstrates that users feel safer when using artificial noise than when using cooperative jamming.

References

Ahmed, E., & Gharavi, H. (2018). Cooperative vehicular networking: A survey. *IEEE Transactions on Intelligent Transportation Systems*, *19*(3), 996–1014.

Ahmed, T., Yasmin, R., Homyara, H., & Hasan, M. A. F. M. (2018). Generalized power allocation (GPA) scheme for non-orthogonal multiple access (NOMA) based wireless communication system. *International Journal of Computer Science, Engineering and Information Technology, 8*(06), 1–9.

Atallah, M., Kaddoum, G., & Kong, L. (2015). A survey on cooperative jamming applied to physical layer security. In *2015 IEEE International Conference on Ubiquitous Wireless Broadband (ICUWB)* (pp. 1–5). IEEE

Chen, X., Ng, D. W. K., Gerstacker, W. H., & Chen, H.-H. (2016). A survey on multiple-antenna techniques for physical layer security. *IEEE Communications Surveys & Tutorials*, *19*(2), 1027–1053.

Cumanan, K., Xing, H., Xu, P., Zheng, G., Dai, X., Nallanathan, A., ... & Karagiannidis, G. K. (2016). Physical layer security jamming: Theoretical limits and practical designs in wireless networks. *IEEE Access*, *5*, 3603-3611.

da Silva, L. B., Fernández, E. M. G., & Camponogara, Â. (2023). Physical Layer Security Techniques Applied to Vehicle-to-Everything Networks. *arXiv preprint arXiv:2301.05123*.

Ghadi, F. R., Kaveh, M., Wong, K.-K., & Martín, D. (2024). Physical layer security performance of cooperative dual-RIS-aided V2V NOMA communications. *IEEE Systems Journal*.

Hamamreh, J. M., Furqan, H. M., & Arslan, H. (2018). Classifications and applications of physical layer security techniques for confidentiality: A comprehensive survey. *IEEE Communications Surveys & Tutorials, 21*(2), 1773–1828.

He, B., Liu, A., Yang, N., & Lau, V. K. N. (2017). On the design of secure non-orthogonal multiple access systems. *IEEE Journal on Selected Areas in Communications, 35*(10), 2196–2206.

Illi, E., Qaraqe, M., Althunibat, S., Alhasanat, A., Alsafasfeh, M., De Ree, M., ... & Al-Kuwari, S. (2023). Physical layer security for authentication, confidentiality, and malicious node detection: A paradigm shift in securing IoT networks. *IEEE Communications Surveys & Tutorials*, *26*(1), 347-388.

Jameel, F., Wyne, S., Kaddoum, G., & Duong, T. Q. (2018). A comprehensive survey on cooperative relaying and jamming strategies for physical layer security. *IEEE Communications Surveys & Tutorials, 21*(3), 2734–2771.

Khoshafa, M. H., Maraqa, O., Moualeu, J. M., Aboagye, S., Ngatched, T. M., Ahmed, M. H., ... & Di Renzo, M. (2024). RIS-assisted physical layer security in emerging RF and optical wireless communication systems: A comprehensive survey. *IEEE Communications Surveys & Tutorials*.

Lee, S., Duong, T. Q., da Costa, D. B., Ha, D. B., & Nguyen, S. Q. (2018). Underlay cognitive radio networks with cooperative non-orthogonal multiple access. *IET Communications*, *12*(3), 359-366.

Li, B., Fei, Z., Zhou, C., & Zhang, Y. (2019). Physical-layer security in space informationetworks: A survey. *IEEE Internet of Things Journal*, *7*(1), 33–52.

Liu, Y., Chen, H.-H., & Wang, L. (2016). Physical layer security for next generation wireless networks: Theories, technologies, and challenges. *IEEE Communications Surveys & Tutorials*, *19*(1), 347–376.

Long, H., Xiang, W., Wang, J., Zhang, Y., & Wang, W. (2014). Cooperative jamming and power allocation with untrusty two-way relay nodes. *Iet Communications*, *8*(13), 2290-2297.

Long, H., Xiang, W., Wang, J., Zhang, Y., & Wang, W. (2013, April). Cooperative jamming and power allocation in three-phase two-way relaying wiretap systems. In *2013 IEEE Wireless Communications and Networking Conference (WCNC)* (pp. 4175-4179). IEEE.

Lv, L., Xu, D., Hu, R. Q., Ye, Y., Yang, L., Lei, X., ... & Nallanathan, A. (2024). Safeguarding next-generation multiple access using physical layer security techniques: A tutorial. *Proceedings of the IEEE*.

Nguyen, V.-L., Ha, D.-B., Tran, D.-D., & Lee, Y. (2019). Enhancing physical layer security for cooperative non-orthogonal multiple access networks with artificial noise. *EAI Endorsed Transactions on Industrial Networks and Intelligent Systems, 6*(20), e4.

Pakravan, S., Chouinard, J. Y., Li, X., Zeng, M., Hao, W., Pham, Q. V., & Dobre, O. A. (2023). Physical layer security for NOMA systems: Requirements, issues, and recommendations. *IEEE Internet of Things Journal*, *10*(24), 21721-21737.

Saeed, S. H., & Sileh, I. K. (2023). Performance analysis of cooperative NOMA for different power allocation strategies. *Tikrit Journal of Engineering Sciences, 30*(4), 102–117.

Sánchez, J. D. V., Urquiza-Aguiar, L., Paredes, M. C. P., & Osorio, D. P. M. (2021). Survey on physical layer security for 5G wireless networks. *Annals of Telecommunications, 76*(3), 155–174.

Sun, L., & Du, Q. (2018). A review of physical layer security techniques for Internet of Things: Challenges and solutions. *Entropy, 20*(10), 730.

Tabassum, H., Ali, M. S., Hossain, E., Hossain, M. J., & Kim, D. I. (2017, June). Uplink vs. downlink NOMA in cellular networks: Challenges and research directions. In *2017 IEEE 85th vehicular technology conference (VTC Spring)* (pp. 1-7). IEEE.

Van Nguyen, B., Jung, H., & Kim, K. (2018). Physical layer security schemes for full-duplex cooperative systems: State of the art and beyond. *IEEE Communications Magazine, 56*(11), 131–137.

Van Nguyen, M.-S., & Do, D.-T. (2020). Evaluating secrecy performance of cooperative NOMA networks under existence of relay link and direct link. *International Journal of Communication Systems, 33*(6), e4284.

Wang, G., Meng, C., Heng, W., & Chen, X. (2018). Secrecy energy efficiency optimization in AN-aided distributed antenna systems with energy harvesting. *IEEE Access, 6*, 32830–32838.

Wang, H.-M., & Zheng, T.-X. (2016). *Physical layer security in random cellular networks*. Springer.

Yener, A., & Ulukus, S. (2015). Wireless physical-layer security: Lessons learned from information theory. *Proceedings of the IEEE, 103*(10), 1814–1825.

Zhang, H., Wang, T., Song, L., & Han, Z. (2015a). Interference improves PHY security for cognitive radio networks. *IEEE Transactions on Information Forensics and Security, 11*(3), 609–620.

Zhang, Q., Huang, X., Li, Q., & Qin, J. (2015b). Cooperative jamming aided robust secure transmission for wireless information and power transfer in MISO channels. *IEEE Transactions on Communications, 63*(3), 906–915.

Zhang, X., McKay, M. R., Zhou, X., & Heath, R. W. (2015c). Artificial-noise-aided secure multi-antenna transmission with limited feedback. *IEEE Transactions on Wireless Communications, 14*(5), 2742–2754.

Zhang, Y., Wang, H.-M., Yang, Q., & Ding, Z. (2016). Secrecy sum rate maximization in non-orthogonal multiple access. *IEEE Communications Letters, 20*(5), 930–933.

Zou, Y., Zhu, J., Wang, X., & Hanzo, L. (2016). A survey on wireless security: Technical challenges, recent advances, and future trends. *Proceedings of the IEEE, 104*(9), 1727–1765.

Jouana H. Hassan
Tikrit University,
Iraq.
jh230046en@st.tu.edu.iq
ORCID: 0009-0002-6620-5124

Ibrahim Khalil Silleh
Tikrit University,
Iraq
ibrahimkhalil.sileh@usq.edu.au
ORCID: 0000-0002-6484-0055