IJERMT

International Journal of Engineering Research & Management Technology

ISSN: 2348-4039

March-2020 Volume 7, Issue-2

Email: editor@ijermt.org www.ijermt.org

ASSESSMENT OF SECRECY CAPACITY DURING PRESENCE OF EAVESDROPPER OF NON-ORTHOGONAL MULTIPLE ACCESS NETWORK UTILIZING JAMMING SCHEMES

Jitender Pratap chitra
Himalayan University Arunachal Pradesh

Dr. Satish Kumar
Himalayan University Arunachal Pradesh

ABSTRACT

Introduction - Non-orthogonal multiple access (NOMA), which has shown the potential to significantly improve spectral efficiency, is envisaged as a promising technique for the 5G wireless networks. In contrast to the conventional orthogonal multiple access (OMA), NOMA exploits the power domain to serve multiple users simultaneously

Aim of the study –The main aim of this study is to assess the Secrecy Performance Assessment Through Power Allocation of Df Relaying-Based on Cooperative Noma Network Utilizing Control Jamming, Without Jamming and Jamming Schemes.

Experimental Setup - The system model consists of a source that broadcasts the multiplexed signal to two NOMA users via a DF relay, and information security against the eavesdropper nodes is provided by a helpful jammer. The performance metric is secrecy rate and ergodic secrecy capacity is approximated analytically. In addition, a differential evolution algorithm-based power allocation scheme is proposed to find the optimal power allocation factors for relay, jammer, and NOMA users by employing different jamming schemes.

Data analysis - Simulation results demonstrate the superiority of CJ over the J and WJ schemes. Finally, the proposed power allocation outperforms the fixed power allocation under all conditions considered in this work.

Conclusion –It can be observed that CJ attains a better secrecy performance. Moreover, the DF relaying protocol with PPAoutperforms that of FPA under both C and NC eavesdropping conditions

Keywords - Jamming, DF, NOMA, secrecy rate, power, allocation etc.

1. INTRODUCTION

1.1 Overview

The higher spectral efficiency of non-orthogonal multiple access (NOMA) has led to its inclusion as a promising technology for the next generation of wireless networks, including 5G and even beyond. Using NOMA technology, multiple users can share the same resources with varying power levels while still receiving their own signals at the source in the power domain. In NOMA, super position coding is used at the source to combine the signals, and the multiplexed signal is sent to numerous users at the same time in different locations. On top of that, users' personal information can be extracted using successive interference cancellation (SIC). When combined with other existing technologies (like cooperative communications, physical layer security, and SWIPT), NOMA has great integration potential. In cooperative NOMA, the relay node used basic amplify-forward and decode-forward protocols to transmit information. It has been shown that a cooperative NOMA system with fixed power allocation (FPA) aids in data transfer between users. Outage probability analysis of the cooperative NOMA system explored in full-duplex and half-duplex modes suggested a new relay selection scheme for a cooperative NOMA network to improve outage probability performance. The need for next-generation wireless networks to transmit data at high speeds while maintaining security has lately piqued the interest of researchers.

NOMA has recently gotten a lot of attention from researchers and business leaders alike. 3GPP's long-term transformation proposal has been proposed to use power-domain NOMA as a radio access technology. NOMA's downlink performance with randomly deployed users in a cellular downlink scenario. NOMA outperformed its traditional orthogonal multiple access (OMA) counterparts in terms of ergodic sum rate performance. NOMA design challenges, chances, and future research trends are highlighted to give researchers a glimpse into what they might be working on in the future. Invoking the protected zone and creating noise at the BS can increase the security performance of NOMA networks.

1.2 Non-orthogonal multiple access (NOMA)

5th-generation (5G) networks face numerous challenges as mobile internet and the Internet of Things develop, including increased high data rate and low latency. For 5G cellular networks, nonorthogonal multiple access has been deemed one of the most promising multiple access candidates. As a result of the increased intracell interference, NOMA enables the simultaneous service of multiple users while utilising the same frequency/time resources. Multiple users' messages are superimposed using superposition coding at the base station. The intended message is extracted on the receiver side using the successive interference cancellation (SIC) technique. Because wireless radio propagation is broadcast in nature, eavesdroppers can easily overhear traffic on wireless networks.

Multiple access non-orthogonal (NOMA) has shown the potential to significantly improve spectral efficiency, and is expected to be a promising technique in 5G wireless networks. NOMA utilises the power domain instead of the traditional orthogonal multiple access (OMA) to serve multiple users at the same time. For noticeable properties such as attaining spatial degrees of freedom and diversity gains, cooperative communication techniques based on multi-antenna techniques have become appealing methods for improving the performance of wireless systems.

Cooperative NOMA systems provide new possibilities and security challenges because wireless channels are open. Physical layer security techniques have recently attracted considerable attention and have been applied in cooperative NOMA systems as promising answers against eavesdropping and guaranteeing secure transmission.

1.3 Secrecy Capacity

Secure communication over noisy channels is limited by the secrecy capacity, which is the inverse of the usual point-to-point channel capacity when communications are also subject to reliability constraints and an information-theoretic secrecy requirement. Metrics for measuring performance. At the heart of any communications system is the concept of secrecy capacity, which measures how much data can be reliably transmitted over the channel to the receiver while preserving the listener completely unaware of what is being transmitted.

2. REVIEW OF LITERATURE

V. Narasimha Nayak and Kiran Kumar Gurrala (2021) - As a result, this research assessed the security of a typical wireless cooperative NOMA dual hop decode and forward relay network, as well as the effect of both collaborative and noncollaborative eavesdropping methods. A source broadcasts the multiplexed signal to two NOMA users via a DF relay, and a helpful jammer protects the information from snooper nodes. Ergodic secrecy capacity can be approximated rationally using the secrecy rate performance metric. The optimal power allocation factors for relay, jammer, and NOMA users using various jamming schemes are found by using a differential evolution algorithm-based power allocation scheme, as well. As an added bonus, NOMA users validate the secrecy rate analysis by using various jamming schemes like conventional relaying with no jamming (WJ) or jamming (J) and control jamming (CJ). The CJ scheme outperforms the J and WJ alternatives in simulations. Last but not least, under all the conditions examined in this study, the proposed power allocation surpasses the fixed power allocation.

Yang Chen, et al (2020) - Here, we look at cooperative secure transmission in NOMA networks where a source (Alice) seeks to send confidential messages to one legitimate user with high security requirements (LU1) while also serving another legitimate user (LU2) simultaneously. A cooperative jammer (Charlie) is used to misguide multiple non-colluding eavesdroppers in order to improve transmission security (Eves). We propose an adaptive power allocation strategy for maximising the secrecy rate while taking into account the LU1 secrecy outage restriction and the LU2 QoS requirement. To demonstrate that our scheme outperforms the traditional NOMA secure transmission scheme numerical solutions are provided.

Van Phu Tuan and Ic-Pyo Hong (2020) - An energy-harvesting (EH) relay helps secure NOMA communication between a source and two users when there is an eavesdropper present. This paper investigates how to make NOMA communication secure when there is an eavesdropper present. The relay uses a power-splitting (PS) policy to extract some of the received signal strength before harvesting energy with a non-linear EH (NLEH) circuit. Jamming signals are sent by a helpful jammer for the purpose of securing communication The jammer is used to generate more power. This SaT scheme allows the EH relay to store energy and transmit information at the same time. Three metrics, including the probability of a secrecy outage (SOP), the average achievable secrecy rate (AASR), and the average stored energy (ASE), have closed-form expressions for performance evaluation. It's possible to investigate the impact of various system parameters, such as the NOMA power-allocation factors, target secrecy rates, jammer placement details and relay power levels, by using these findings.

Chao Yu, et al (2019) - When one relay is being used to deliver information and other relays act as jammers, it's known as a jammer-aided cooperative non-orthogonal multiple access (NOMA). This letter examines two basic relay selection (RS) strategies, namely random RS and max-min RS. Both RS schemes have analytical and asymptotical expressions for secrecy outage probability (SOP). In the moderate to high SNR range, the NOMA framework with jammer has a lower SOP than the one without jammer, according to simulated data. The secrecy outage performance can be further improved in low SNR regions by using the max-min RS strategic plan, while it remains unchanged in high SNR regions.

Lu Lv, et al (2019) - When a base station (BS) serves a near user (NU) as well as a far user (FU) using the NOMA principle, and transmission between the BS and FU is aided by an untrusted relay, we investigate secure communications with an untrusted relay. To improve transmission security, we propose an adaptive jamming scheme in which FU is questioned to emit a jamming signal adaptively to confuse an untrusted relay. Because only NU can correctly decode the jamming signal, transmission rates for jamming are set to ensure maximum secrecy sum rates. We look at the scheme's security and derive the ergodic secrecy sum rate and its scaling law from that. The proposed adaptive jamming scheme's effectiveness is validated using simulated results.

3. OBJECTIVES OF THE STUDY

1. To study the concept of NOMA and Secrecy Capacity.
2. To propose a power allocation outperforms one that is fixed under the NOMA scheme
3. To evaluate the secrecy capacity in the presence of jamming
4. To determine the NOMA-based DF relay network's Secrecy Rate using the CJ scheme.

4. EXPERIMENTAL SETUP

4.1 System Model

For this system, the source (S) node in the network broadcasts the multiplexed signal to both NOMA users (D_1 and D_2) in cooperation with the DF relay (R) node, even though there are multiple listeners. Figure 1 depicts the introduction of a jammer (J) node, which sends an interference signal to the listeners (E) on purpose. To simplify things, we assume that all of the channel links are completely independent, have Rayleigh flat fading, and operate in half-duplex. There are no direct connections between the sources and the eavesdroppers in this network. Phases 1 and 2 are involved in the transmission of information (broadcast phase and cooperation phase). To transmit $x_s = (a_1x_1 + a_2x_2)$ to the relay, the source uses the super position principle during broadcast phase. Power allocation factors a_1 and a_2 are used to represent the far and near users, respectively. At this point, we'll assume that the data being transmitted from source to relay has been protected against interception.

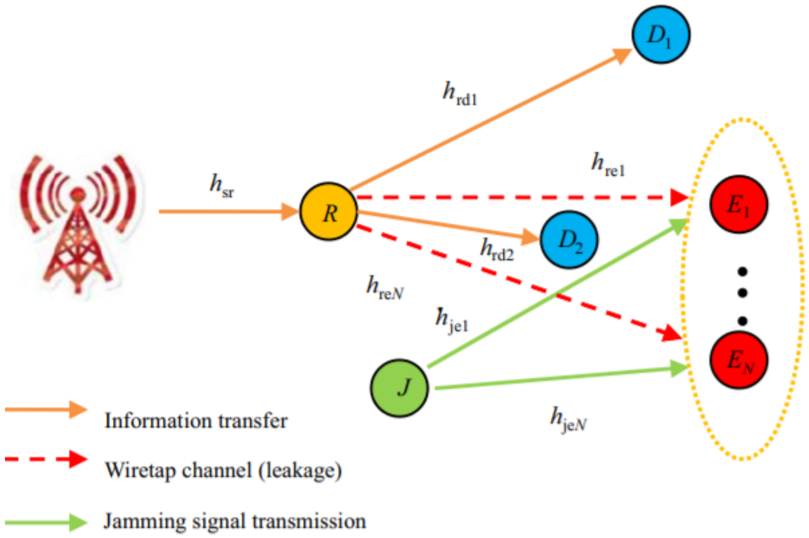

Figure 1:NOMA cooperative network with dual hops and PLS

The received signal at the relay is provided by during the first time slot which is given below:

$$y_{sr} = h_{sr}\left(\sqrt{P_s a_1 x_1} + \sqrt{P_s a_2 x_2}\right) + n_{sr}(\mathbf{1})$$

where $P_s$reflects the power source's output. It receives a signal from the source and sends it to its designated destinations in a phase of cooperative operation. Depending on where you are, the signal you receive can be expressed as:

$$\mathbf{y_{rd_i}} = \sqrt{\mathbf{P_r}}\mathbf{h_{rd_i}}\hat{\mathbf{y}}_{\mathbf{sr}} + \mathbf{n_{rd_i}} \qquad \mathbf{i = 1, 2,} \qquad (\mathbf{2})$$

Where$\hat{\mathbf{y}}_{\mathbf{sr}}$symbolises the signal's decoded version as it was received from the transmitter. When more than one eavesdropper is listening in on a transmission, the relay-to-destination jammer has sent the interference signal to all of them simultaneously. The eavesdroppers' received signal could be expressed as

$$y_{e_n} = y_{re_n} + y_{je_n} \; n = 1, \ldots\ldots, N, \qquad (3)$$

Where

$$y_{je_n} = \sqrt{P_j} h_{je_n} x + n_{je_n} n = 1, \ldots., N; \qquad (4)$$

$$y_{re_n} = \sqrt{P_r} h_{re_n} (\hat{\mathbf{y}}_{\mathbf{sr}}) + n_{re_n} \; n = 1, \ldots., N. \qquad (5)$$

The NOMA users receive a signal from the jammer that is given to them by:

$$\mathbf{y_{jd_i}} = \sqrt{\mathbf{P_j}} h_{jd_i} x + n_{jd_i} \; i = 1{,}2. \qquad (6)$$

where x is the jammer's interference signal. P_r and $P_j$are used to show the difference in power between the relay and jammer nodes. The channel's popularity is rising$h_{sr}, h_{rd_i}, h_{re_n}, h_{je_n}$CN $(0, \Omega_1)$zero-mean complexes between all of the nodes Random variables with Gaussian distributions, and $n_{sr}, n_{rd_i}, n_{re_n}, n_{je_n} \sim$ CN $\left(0, \sigma_A^2\right)$portray white Gaussian complex additive noise with noise variance N_0 at all nodes.

Here, the performance of two jamming strategies is compared to that of conventional and WJ schemes, in order to see if the latter offers better confidentiality. There is no jamming process used in the WJ scheme because the relay and destinations (NOMA users) can decode the received signal properly. There is no way to tell where a jammer is interfering with a signal in the J scheme. Finally, in a cooperative NOMA network, a special new jamming scheme is introduced in which information about the interference signals produced by jammer is known to NOMA users, but the eavesdroppers are unaware of it.

4.2 DF relay network with a NOMA-based secrecy rate evaluation using the CJ scheme

With control jamming on a DF-operated relay network, the secrecy rate can be calculated as follows: 1. To ensure that all users are treated equally, and in accordance with the fundamental principle of NOMA, more power is given to the far user (D_1) when channel conditions are poor, and less power is given to the near user (D_2) when channel conditions are good. The user at a distance (D_1) decodes its own signal x_1 by treating the signal at a close (D_2) as interfering. When the near user decodes its own signal x_2 using perfect SIC, the far user's signal is removed from the combined NOMA signal. The signal-to-noise ratio (SNR) calculations are made based on the received signals at the relay and the corresponding destinations. As shown in (1), the received signal-to-noise ratios (SNRs) at the relay are provided by:

$$\gamma_{sr} = \frac{P_s a_1 |h_{sr}|^2}{P_s a_2 |h_{sr}|^2 + N_0} \quad \text{w.r.t.} D_1; \qquad (7)$$

$$\gamma_{sr} = \frac{P_s a_2 |h_{sr}|^2}{N_0} \quad \text{w.r.t.} D_2; \qquad (8)$$

This is what the destination signal looks like when it's in the cooperation phase:

$$y_{rd_i} = \sqrt{P_r} h_{rdi} (\hat{\mathbf{y}}_{\mathbf{sr}}) + n_{rd_i} i = 1{,}2 \qquad (9)$$

With (9), the SINR received by the distant user (D_1) can be expressed as follows:

$$\gamma_{D1} = \frac{P_r a_1 |h_{rd_1}|^2}{P_r a_2 |h_{rd_1}|^2 + N_0} \qquad (10)$$

Also, the received SNR (D_2) at the close user is provided by:

$$\gamma_{D2} = \frac{P_r a_2 |h_{rd_2}|^2}{N_0} \qquad (11)$$

It is possible for eavesdroppers to detect both information signals when the system is in cooperation phase. In both collaborative and non-collaborative eavesdropping scenarios, the received SNRs at the eavesdroppers could be acquired utilising(3).

- **Collaborative case:**

$$\mathbf{w.r.t.x_1}: \gamma_{\mathbf{E1}}^{\mathbf{C}} = \sum_{\mathbf{n=1}}^{\mathbf{N}} \frac{P_r a_1 |h_{re_n}|^2}{P_j |h_{je_n}|^2 + 2N_0} \qquad (\mathbf{12})$$

$$\mathbf{w.r.t.x_2}: \gamma_{\mathbf{E2}}^{\mathbf{C}} = \sum_{\mathbf{n=1}}^{\mathbf{N}} \frac{P_r a_2 |h_{re_n}|^2}{P_j |h_{je_n}|^2 + 2N_0} \qquad (\mathbf{13})$$

- **Non-collaborative case:**

$$\mathbf{w.r.t.x_1}: \gamma_{\mathbf{E1}}^{\mathbf{NC}} = \underset{\mathbf{e_n} \varepsilon\, S_{eaves}}{\mathbf{max}} \frac{P_r a_1 |h_{re_n}|^2}{P_j |h_{je_n}|^2 + 2N_0} \quad n = 1, \ldots\ldots, N; \qquad (14)$$

$$\mathbf{w.r.t.x_2}: \gamma_{\mathbf{E2}}^{\mathbf{NC}} = \underset{\mathbf{e_n} \varepsilon\, S_{eaves}}{\mathbf{max}} \frac{P_r a_2 |h_{re_n}|^2}{P_j |h_{je_n}|^2 + 2N_0} \quad n = 1, \ldots\ldots, N; \qquad (15)$$

Here, S_{eaves}denotes the total number of eavesdroppers who aren't working together. The impact of the eavesdropper with the highest SNR is taken into account in the non-collaborative eavesdropping case. A final calculation uses control jamming at D_1 and $D_2$to increase the secrecy rate for collaborative and non-collaborative conditions:

$$C_{Di}^{cj} = 0.5 * \log_2 \left[\frac{1 + \min(\gamma_{sr}, \gamma_{Di})}{1 + (\gamma_{Ei}^{C})} \right] \quad i = 1,2; \qquad (16)$$

$$C_{Di}^{cj} = 0.5 * \log_2 \left[\frac{1 + \min(\gamma_{sr}, \gamma_{Di})}{1 + (\gamma_{Ei}^{NC})} \right] \quad i = 1,2; \qquad (17)$$

5. DATA ANALYSIS AND RESULTS

5.1 Simulation Parameters

Table 1:Simulation Parameters

Parameter	Specifications
Total number of bits	10^4
Modulation	QPSK
Channel	Rayleigh flat fading
Path Loss Exponent (m)	3
Number of relays (R)	1
Number of jammers (J)	1
Number of eavesdroppers (N)	4
Noise variance (No)	1
DE parameters	For the objective function, the DE step size is set to F=0.8, the crossover probability is set to CR=0.5, and the total population size is 50*D, D = N (the number of parameters of the objective function), Iterations = 200
Relay network topology	Linear topology

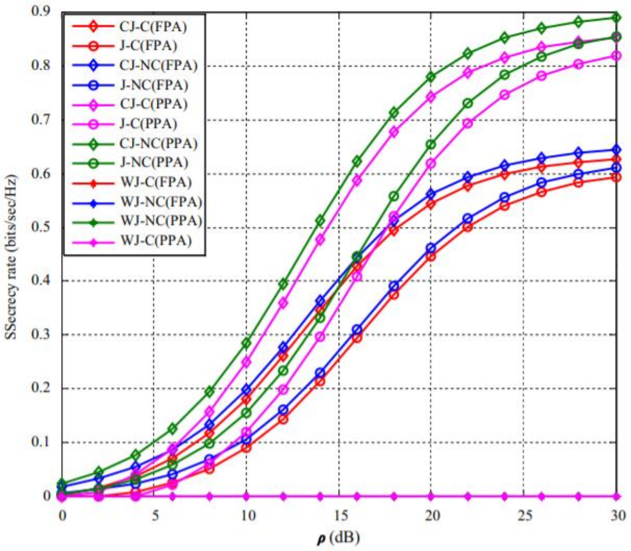

Figure 2:Ratio of confidentiality to signal noise ratio at D_1 with FPA and PPA under eavesdropping conditions in C and NC

Figure 2 depicts the secrecy rate analysis for the CJ and other jamming schemes for the far user (D_1) using PPA and FPA. These eavesdropping scenarios consider both collaborative (C) and non-collaborative (NC) listening techniques. When there are multiple eavesdroppers, the secrecy rate is lower for the C situation than for the NC situation because the relay-to-destination information transmission is affected by all eavesdroppers, and the relay and eavesdroppers are intimately linked. The CJ scheme outperforms all other jamming schemes because the destination is aware of the interference generated by the jammer in all cases. Furthermore, in both the C and NC eavesdropping conditions, PPA has a higher secrecy rate than the FPA scheme. The secrecy rate with PPA and FPA under the CJ condition is 0.78 bits/s/Hz for the NC eavesdropping condition at ρ= 20 dB and 0.56

bits/s/Hz. The observed secrecy rate is low because D_1 is a weak user with worse channel conditions, but it is increased in the high SNR region when PPA allocates proportionate signal power.

Table 2:Optimal best transmission powers in Watts when the relay is close to eavesdroppers (ρ = 15 dB)

Power allocation method	Relay power (P_r)	Jammer power (P_j)	Near user power	Far user power
FPA	0.4706	0.4706	0.1883	0.2823
DEPA (PPA)	0.6146	0.3268	0.1315	0.3391

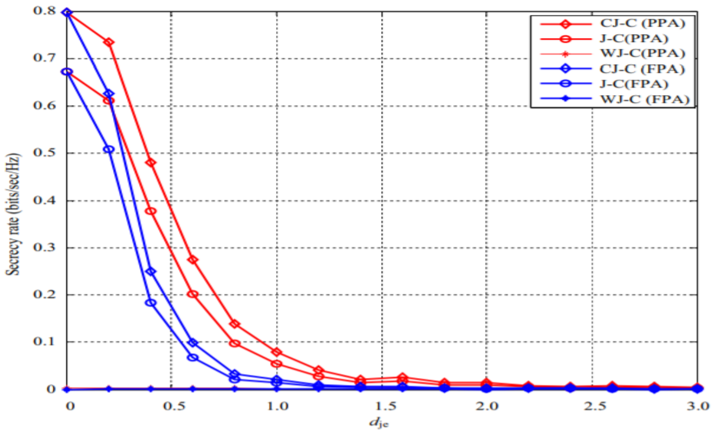

Figure 3:Measurement effects on secrecy rates in the C eavesdropping condition of PPA and FPA in relation to jammer-to-eavesdropper distance at D_1

It is shown in Figure 3 for collaborative eavesdropping with PPA and FPA at a distance from user D_1 how the location of the jammer affects the performance metric secrecy rate. When dealing with strong relay-to-eavesdropper links, control jamming is an effective way to minimise interference and maximise the secrecy rate. Increasing the distance between a jammer and an eavesdropper lowers the security because jamming has become ineffective when the eavesdroppers are far away from the jammers. PPA as well outdoes FPA in this instance.

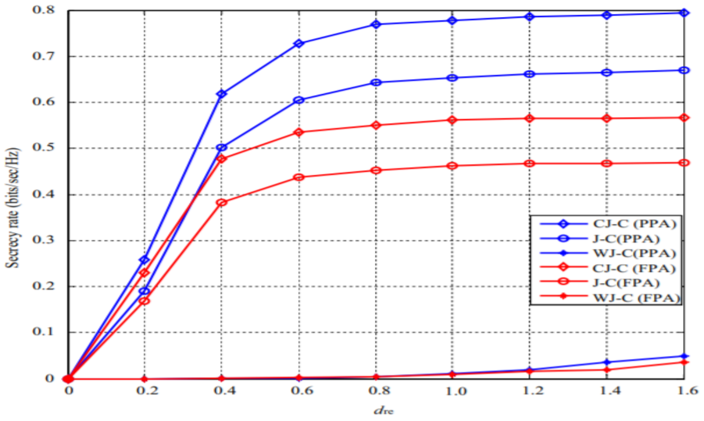

Figure 4:Relay-to-eavesdropper Vs Secrecy rate's distance during collaborative eavesdroppers at D_1

Distance from the relay to the eavesdropper has an effect on the secrecy rate, as shown in Figure 4. As the distance between the relay and the eavesdropper rises, the link between the relay and the eavesdropper weakens, resulting in improved secrecy effectiveness. When it comes to increasing the security, the CJ scheme, which has the ability to decode the jammer signal at a distance (D_1), is an excellent option. PPA has the highest secrecy rate, while FPA does not.

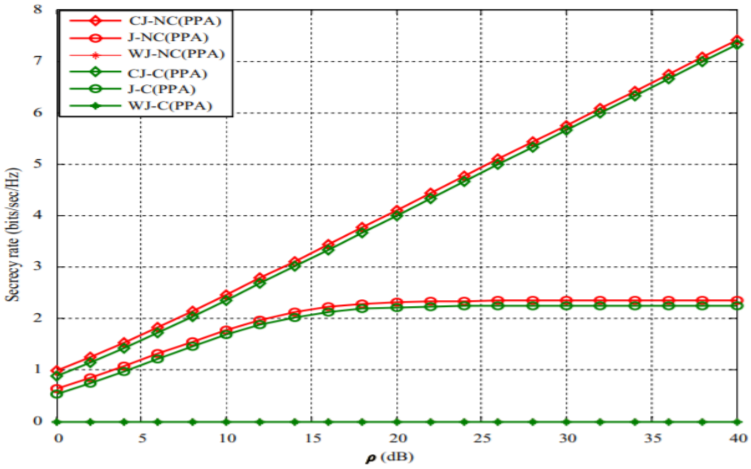

Figure 5:SNR versus Secrecy Rate at D_2 for C and NC

With CJ and other jamming schemes under C and NC eavesdropping conditions, the secrecy rate versus transmit SNR for the near user (D_2) is shown in Figure 5. Because of the strong connection between the jammer and the nearby user, the secrecy rate is higher in this case (D_2). There's no doubt that D_2's proximity to SIC makes it more secretive than the far user (D_1). Because the relay is located so close to the eavesdroppers, the WJ scheme is ineffective. Here, we can see that the NC eavesdropping scenario outperforms the C eavesdropping scenario. In terms of secrecy rate, the CJ scheme outperforms the J and WJ schemes.

5.2 Secrecy capacity when an eavesdropper uses jamming

Figure 6 shows secrecy capacity when E is present. Figure 6's total secrecy capacity is higher and nearly identical to the outcome. Figure 6 shows that the jamming signals sent by users UE1 and UE2 significantly reduced E's decoding capacity.

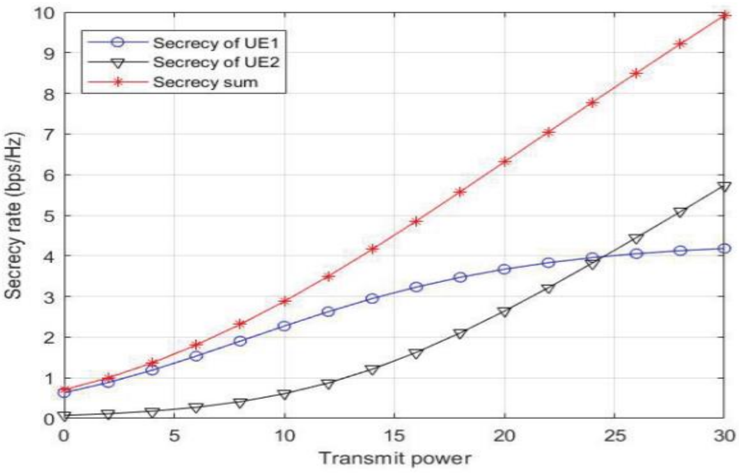

Figure 6: Transmit power vs Secrecy capacityduring E with jamming

This section uses Monte Carlo simulations to look at the secrecy performance of a DF relaying-based cooperative NOMA network with collaborative and non-collaborative eavesdroppers under various J and WJ schemes. The simulation parameters are listed in Table 1. Table 2 shows the optimal DE-based power allocation algorithm 1 (relay, jammer power allocation factor) and 2 (NOMA users' power allocation factor) values. The MATLAB platform was used for the simulation, and a total of 10^4 separate simulations were performed for each result. The study used an SNR range of 0 to 30 dB.

6. CONCLUSION

Multiple eavesdroppers in collaborative and non-collaborative cases were investigated in this work for the secrecy performance monitoring of the NOMA enabled DF relay network and a novel power allocation scheme was postulated for the further advancement in secrecy rate. To find the optimal power allocation factors for relay, jammer, and NOMA users using various jamming schemes, a DE algorithm-based power allocation was proposed. Additionally, the proposed CJ scheme was compared to the J and WJ schemes for the wireless network under consideration by moving the relay and jammer away from the eavesdroppers to see which one performed better. The simulation results demonstrate that CJ has better secrecy than the other candidates. Furthermore, under both C and NC eavesdropping conditions, the DF relaying protocol with PPA outperforms the FPA.

6.1 Future Work

In light of popular jamming and artificial noise methods, the interference signal is an artificial interference for the eavesdropper to confuse the eavesdropper and degrade its decoding performance. It is capable of decoding the signal at the beginning, while legitimate users are only able to do so at the end. As a result, different approaches should be considered while considering all possible outcomes. For future research, we can improve the jammer selection, the exclusion zone radius, and the NOMA power allocation in order to achieve confidentiality transmission.

REFERENCES

1. V. Narasimha Nayak and Kiran Kumar Gurrala (2021). Power allocation-Assisted secrecy analysis for NOMA enabled cooperative network under multiple eavesdroppers. Volume43, Issue4. August 2021. Pages 758-768
2. Yang Chen, et al (2020). Cooperative Secure Transmission in MISO-NOMA Networks. Electronics 2020, 9, 352; doi:10.3390/electronics9020352
3. Tuan VP, Hong IP (2020). Secure Communication in Cooperative SWIPT NOMA Systems with Non-Linear Energy Harvesting and Friendly Jamming. Sensors (Basel). 14;20(4):1047. doi: 10.3390/s20041047. PMID: 32075184; PMCID: PMC7070649.
4. C. Yu, H. Ko, X. Peng, W. Xie and P. Zhu, "Jammer-Aided Secure Communications for Cooperative NOMA Systems," in IEEE Communications Letters, vol. 23, no. 11, pp. 1935-1939, Nov. 2019, doi: 10.1109/LCOMM.2019.2934410.
5. L. Lv, H. Jiang, Z. Ding, L. Yang and J. Chen, "Exploiting Adaptive Jamming in Secure Cooperative NOMA with an Untrusted Relay," ICC 2019 - 2019 IEEE International Conference on Communications (ICC), 2019, pp. 1-6, doi: 10.1109/ICC.2019.8761928.

6. O. Abbasi and A. Ebrahimi, "Secrecy analysis of a noma system with full duplex and half duplex relay," in 2017 Iran Workshop on Communication and Information Theory (IWCIT), 2017, pp. 1–6.
7. C. Yu et al., Secrecy outage performance analysis for cooperative NOMA over Nakagami-m Channel, IEEE Access 7 (2019), 79866–79876.
8. J. Chen, L. Yang, and M.-S. Alouini, Physical layer security for cooperative NOMA systems, IEEE Trans. Veh. Technol. 67 (2018), 4645–4649.
9. H. Lei et al., Secrecy outage analysis for cooperative NOMA systems with relay selection schemes, IEEE Trans. Commun. 67 (2018), 6282–6298.
10. M. K. Shukla, H. H. Nguyen, and O. J. Pandey, Secrecy performance analysis of two-way relay non-orthogonal multiple access systems, IEEE Access 8 (2020), 39502–39512.