Cooperative Relay Transmission under Physical Layer Security for Non-Orthogonal Networks

Mohammed A. Salem[1], Azlan B. Abd.Aziz[1], and Mohamad Y. Alias[2]
[1]Faculty of Engineering and technology, Multimedia university, Malacca 75450, Malaysia
[2] Faculty of Engineering and technology, Multimedia university, Selangor and 63100, Malaysia
Email: mohammedmmu94@gmail.com; azlan.abdaziz@mmu.edu.my; yusoff@mmu.edu.my

Abstract—In this paper, the secrecy performance for a downlink cooperative non-orthogonal multiple access (NOMA) communication system is studied under two cases. In the first case, the presence of an untrusted user is studied. While, the presence of an eavesdropper node is considered in the second case. The base station transmits superimposed information signals to the half-duplex two-way relay node. The relay amplifies-and-forwards the received signal towards the users. This paper studies the effectiveness of two factors on the secrecy performance in terms of secrecy capacity. these factors are the power allocated for each user, and the distance between the untrusted user and the cooperative relay node with respect to the strong user. Moreover, this paper proposes the shared jamming signal strategy in order to enhance the physical layer security of the cooperative NOMA in the presence of an eavesdropper node. Furthermore, simulations of the secrecy capacity are presented and compared with a conventional scheme based on null-steering jamming scheme. Based on the result the proposed technique outperforms the conventional technique in terms the of secrecy capacity.

Index Terms—Physical Layer Security (PLS), cooperative relay transmission, Non-orthogonal Multiple Access (NOMA), secrecy capacity

I. Introduction

The growth of wireless communication field causes an open nature of the wireless networks. This nature is an aspect of the eavesdropping attacks. In order to overcome this issue, the implementation of security in wireless networks becomes an essential factor.

A. Motivation and Related Literature

The concept of Physical Layer Security (PLS) has been proposed to complement the traditional security solutions such as the cryptographic techniques [1], by exploiting the physical layer properties of the wireless communication network. The baseline of Shannon's cipher system [2] and the developments of Aaron Wyner's Wiretap channel [3], introduce the interests of using the physical wireless characterization to enhance the security of data transmission [4].

Cooperative communication is a promising technique for wireless networks on terms of throughput and energy efficiency [5].

Manuscript received December 8, 2019; revised July 2, 2020.
Corresponding author email: mohammedmmu94@gmail.com.
doi:10.12720/jcm.15.8.633-638

Authors of [6], explains the use of jamming signals generated from the destination node to attack an un-trusted relay that is assumed to be the eavesdropper node. The secrecy performance of this strategy is analyzed in terms of SOP metric. Authors of [7], illustrates the benefits and uses of the untrusted relay node in cooperative networks. Moreover, several strategies have been considered in the literature in order to improve the PLS, such as, cooperative jamming [8], [9], cognitive radio [10], and energy harvesting [11]. However, these strategies are not related with the cooperative NOMA system.

For the fifth generation (5G) wireless networks, NOMA is an essential enabling technology to meet the heterogeneous demands on high throughput, improved fairness, massive connectivity, high reliability and low latency [12]. The main idea of NOMA is to support multi-users in a single resource block, such as spreading code, subcarrier or time slot. In [13], the authors consider the use of a relay node with two protocols (amplify-and-forward and decode-and-forward) in a cooperative NOMA system. The authors of [14] investigated the optimal designs of a NOMA system in terms of the transmission rates, power allocation for each user, and the decoding factor. In [15], NOMA system is considered in large scale communication system. In this strategy the PLS is approached by using artificial noise generated from each user node. The authors of [16] proposed a downlink cooperative NOMA for MIMO network based on signal to leakage ratio (SLR). The proposed scheme aims to minimize the transmission power by exploiting the solution of the maximal signal to leakage ratio (maximal-SLR).

To the best of the authors' knowledge, no related research has considered the PLS performance of cooperative NOMA systems at which a strong user ($User_1$) is paired with a weak untrusted user ($User_2$) as shown in Fig. 1. In this paper, we study the secrecy performance of a cooperative NOMA system with an untrusted weak user.

B. Main Contributions

The main contributions of this paper are summarized as follows.

- Study the secrecy performance of a cooperative NOMA system in the presence of a weak untrusted user.

- Investigate the effect of the distance between the untrusted weak user and the cooperative relay with respect to the strong user.
- Investigate the effect of varying the power allocation coefficients of both users.
- Propose the shared jamming signal strategy and compare it with the null-steering jamming scheme proposed in [17].

C. Paper Organization

The rest of this paper is organized as follows. Section II demonstrates the system model. Section III illustrates the secrecy performance of the system model. Section IV shows the results and discussions of the paper. Finally, Section V presents the conclusion of this paper.

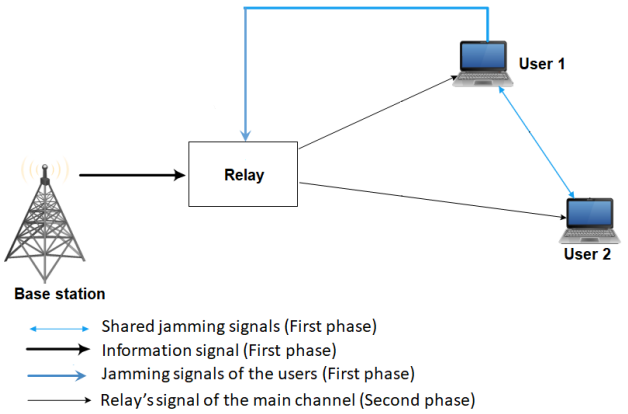

Fig. 1. System model.

II. System Model

We consider a secure cooperative NOMA system, where a base-station (B_S) communicates with a strong user ($User_1$) and a weak user ($User_2$), as shown in Fig. 1. The cooperative relay node ($Relay$) is employed to enhance the secrecy performance of the communication scenario. In this system model, we assume that the strong user is the legitimate node, while $user_2$ is assumed to be an untrusted user. Also, we assumed that each node of the system model is equipped with a single antenna.

A. Relay Node and Channel Assumptions

In this paper, we consider a cooperative NOMA with a single half-duplex two-way relay node having an amplify-and-forward protocol. The relay is used as transmission node between the base station and the users so that the direct channel between base station and users is not existing. Thus, the base station and the users communicate with the help of the relay node in two-time slots as illustrated in Fig. 1.

In this model, the communication links between the nodes are assumed to be slow fading Rayleigh channel. However, the coefficient of a channel link between two nodes is expressed by h_{ab}, where a is the node where the transmission starts, and b is the node where the transmission ends. Moreover, the channel state information (CSI) is assumed to be perfectly available at the base station. Furthermore, through this paper, the noise is assumed to be a complex additive white Gaussian noise (AWGN) with zero mean and unit variance.

B. Signal Transmission Model (Untrusted Weak User)

In the first time slot, the base station transmits the superimposed information signals to the relay node. The received signal at the relay node is written as,

$$X_{BS,R} = \sqrt{P_{BS} a_{u_1}} h_{BS,R} x_1 + \sqrt{P_{BS} a_{u_2}} h_{BS,R} x_2 + n_{BS,R} \quad (1)$$

where, P_{BS} is the power of the base station, a_{u_1} and a_{u_2} are the power allocation coefficient for $user_2$ and $user_2$ respectively, x_1 and x_2 are the information to $user_2$ and $user_2$ respectively, $h_{BS,R}$ is the channel gain between the relay and the base-station and $n_{BS,R}$ is the AWGN noise from the base station to the relay.

At the same time slot, $user_1$ and $user_2$ generate jamming signals and share these signals. The jamming signals are given as,

$$\begin{aligned} J_{u_1} &= \sqrt{P_{u_1}} h_{u_1,u_2} j_1 + n_{u_1,u_2} \\ J_{u_2} &= \sqrt{P_{u_2}} h_{u_2,u_1} j_2 + n_{u_2,u_1} \end{aligned} \quad (2)$$

where, P_{u_1} and P_{u_2} are the powers of the users respectively, j_1 and j_2 are the artificial jamming signals from $user_1$ and $user_2$ respectively, h_{u_1,u_2} and h_{u_2,u_1} are the channel gain between the users, and n_{u_1,u_2} and n_{u_2,u_1} are the AWGN noise between the users.

The shared jamming signal is transmitted by the strong user to the relay node. The received jamming signal at the relay is given as,

$$J_{u_1,R} = (J_{u_1} + J_{u_2}) h_{u_1,R} j_1 + n_{u_1,R} \quad (3)$$

This shared jamming signal is generated to ensure that there are no illegal nodes eavesdropping the superimposed information signals sent from the base station.

In the second time slot, the combination of the received signals at the relay (the superimposed information signals and the shared jamming signal) is amplified and forwarded to the users. The amplification factor (A_F) is expressed as [1],

$$A_F = \sqrt{\frac{P_R}{P_{BS} |h_{BS,R}| + P_{u_1} |h_{u_1,R}| + \sigma}} \quad (4)$$

The forwarded signal to the strong user ($user_1$) after filtering the shared jamming signal is expressed as,

$$Y_{R,u_1}^{A_F} = A_F h_{R,u_1} X_{BS,R} + n_{R,u_1} \quad (5)$$

The forwarded signal to the untrusted weak user ($user_2$) after filtering the shared jamming signal is expressed as,

$$Y_{R,u_2}^{A_F} = A_F h_{R,u_2} X_{BS,R} + n_{R,u_2} \quad (6)$$

C. Signal Transmission Model (Eavesdropper)

In this section, we assume that an illegal node is eavesdropping the main channels ($User_1$ and $User_2$). Hence, in the second time slot, the eavesdropper node wiretaps the main channels to receive the transmitted signal. The signal received by the eavesdropper is expressed as,

$$Y_{R,E}^{A_F} = A_F h_{R,E}\left(X_{BS,R} + J_{u_1,R}\right) + n_{R,E} \tag{7}$$

D. Secrecy Performance (Secrecy Capacity)

For the untrusted weak user case, the secrecy capacity is the deference between the legitimate user capacity ($user_1$) and the untrusted user capacity ($user_2$). However, in the presence of an eavesdropper node, the secrecy capacity is the difference between the capacities of the legitimate users and the eavesdropper node.

E. Secrecy Capacity

The capacity of the strong user ($user_1$) is given as,

$$\varsigma_{u_1} = \frac{1}{2}\log_2\left(1+\xi_{u_1}\right) \tag{8}$$

where, ξ_{u_1} is the signal to noise ratio (SNR) at the strong user ($user_1$) (the strong user is able to decode the weak user's information signal and suppressed it by using the successive interference cancellation (SIC) strategy). The signal to noise ratio at the strong user ($user_1$) is given as,

$$\xi_{u_1} = \frac{{A_F}^2 P_{BS} a_{u_1} \left|h_{R,u_1}\right|^2 \left|h_{BS,R}\right|^2}{\left({A_F}^2 \left|h_{R,u_1}\right|^2 + 1\right)\sigma^2} \tag{9}$$

The capacity of the weak user ($user_2$) is given as,

$$\varsigma_{u_2} = \frac{1}{2}\log_2\left(1+\xi_{u_2}\right) \tag{10}$$

where, ξ_{u_2} is the signal to interference plus noise ratio ($SINR$) at the weak user ($user_2$) (the weak user is not able to decode the strong user's information signal, so the strong user's information signal is considered as an interference to the weak user). The signal to interference plus noise ratio at the weak user ($user_2$) is given as,

$$\xi_{u_2} = \frac{{A_F}^2 P_{BS} a_{u_2} \left|h_{R,u_2}\right|^2 \left|h_{BS,R}\right|^2}{{A_F}^2 P_{BS} a_{u_2} \left|h_{R,u_2}\right|^2 \left|h_{BS,R}\right|^2 + \left({A_F}^2 \left|h_{R,u_2}\right|^2 + 1\right)\sigma^2} \tag{11}$$

The secrecy capacity of the eavesdropper node is given as,

$$\varsigma_E = \frac{1}{2}\log_2\left(1+\xi_E\right) \tag{12}$$

where, ξ_E is the signal to jamming plus noise ratio ($SJNR$) at the eavesdropper node (we assume that the eavesdropper node can distinguish the superimposed mixture signal by using the parallel interference cancellation (PIC) strategy). The signal to jamming plus noise ratio at the eavesdropper is given as,

$$\xi_E = \frac{{A_F}^2 P_{BS} a_m \left|h_{R,E}\right|^2 \left|h_{BS,R}\right|^2}{{A_F}^2 \left|h_{R,E}\right|^2 J_{u_1,R} + \left({A_F}^2 \left|h_{R,E}\right|^2 + 1\right)\sigma^2} \tag{13}$$

where, $a_m \in a_1, a_2$. The secrecy capacity of the cooperative NOMA system for the untrusted weak user case is expressed as,

$$\left[\varsigma_{u_1}^{u_2}\right]^+ = \max\left\{\left[\log_2\left(\frac{1+\xi_{u_1}}{1+\xi_{u_2}}\right)\right], 0\right\} \tag{14}$$

For the presence of the eavesdropper node the secrecy capacity of the cooperative NOMA system is expressed as,

$$\left[\varsigma_{u_m}^{E}\right]^+ = \max\left\{\left[\log_2\left(\frac{1+\xi_{u_m}}{1+\xi_E}\right)\right], 0\right\} \tag{15}$$

where, $u_m \in u_1, u_2$.

III. Numerical Results

In this section, the numerical results are obtained to evaluate the secrecy performance of the proposed cooperative NOMA technique in Section II. The simulation set up parameters of the proposed technique are summarized in Table I.

TABLE I: SIMULATION SET UP PARAMETERS

Parameters	Details
base station location	(0,0)
Relay node location	(100,0)
Strong user location	(200,0)
Weak user locations	([200 300 400 1000],10)
Eavesdropper location	(1000,20)
Power allocation for the strong user	0.2
Power allocation for the weak user	0.8
Path loss model	128 + 37 log(distance) dB
Transmission power	46 dBm
Noise density	-169 dBm
channel model	Rayleigh channel

Table I illustrates that the distance between the strong user and the half-duplex two-way relay is assumed to be equidistance to the distance between the source and the relay. However, the weak untrusted user is positioned at different locations to observe the effect of the distance factor on the secrecy performance. Moreover, the eavesdropper node is placed at a fixed position to observe the effect of the shared jamming signal on secrecy performance.

Fig. 2 demonstrates the secrecy performance metric of the NOMA system shown in Fig. 1, in terms of the secrecy capacity. Based on Fig. 2, the weak user is assumed to be away from the relay by a sequenced distance. As shown in Fig. 2, the secrecy capacity of the

NOMA system is evaluated increasing signal to noise ratio (SNR).

Based on Fig. 2, we observe that the secrecy performance of the strong user ($user_1$) is better than the secrecy performance of the weak untrusted user ($user_2$). This result is achieved due to the strong decoding abilities (SIC strategy) at $user_2$ that enables the user to decode the information signal of $user_2$ directly. However, the weak untrusted user treats the information signal of the strong user as interference signal.

Fig. 2 shows the effect of the distance between the weak untrusted user and the relay nodes on the secrecy performance in terms of the secrecy capacity. More specifically, the further the untrusted weak user, the lower SNR required to increase the secrecy capacity of the NOMA system.

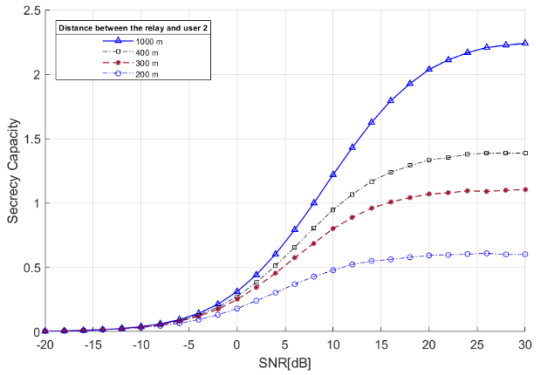

Fig. 2. Secrecy capacity versus SNR with different untrusted user locations, $a_{\{u_1=0.2\}}$, and $a_{\{u_1=0.8\}}$.

Fig. 2 shows the effect of the distance between the weak untrusted user and the relay nodes on the secrecy performance in terms of the secrecy capacity. More specifically, the further the untrusted weak user, the lower SNR required to increase the secrecy capacity of the NOMA system.

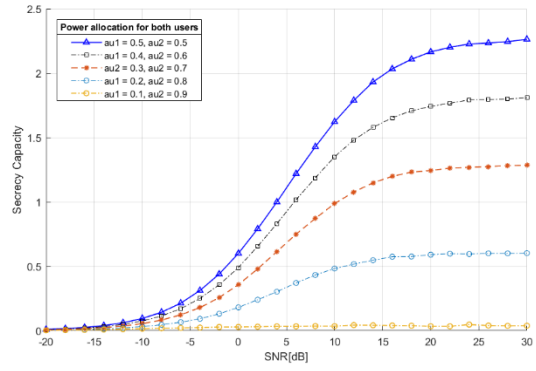

Fig. 3. Secrecy capacity versus SNR with different power allocation coefficient for both users.

Fig. 3 depicts the secrecy performance metric of the NOMA system shown in Fig. 1, in terms of the secrecy capacity with respect to the power allocation coefficients of both users.

Fig. 3 illustrates the effect of varying the power coefficient allocated for each user on the secrecy performance of the cooperative NOMA system. Precisely, the highest secrecy capacity is achieved by increasing the power allocation of the strong user and decreasing the power allocation of the weak untrusted user. In contrast, the secrecy capacity decreased as the power allocation of the weak untrusted user increased.

Equations 8 and 10 explain this observation, where the power allocation coefficient of the strong user (a_{u_1}) is directly proportional to the signal to noise ratio at the strong user nodes (ξ_{u_1}). However, the power allocation coefficient of the weak untrusted user (a_{u_2}) is inversely proportional to the signal to interference plus noise ratio at the weak user nodes (ξ_{u_2}). Due to the effect of the power allocation coefficient, we observe that the capacity of the weak user increases significantly and compensates the interference power produced by the strong user's information signal. This leads to a decrease the secrecy capacity of the cooperative NOMA system.

In this paper, we evaluate the proposed shared jamming signal strategy in the presence of an eavesdropper node by comparing it with the null-steering jamming proposed in [17]. Fig. 4 illustrates the secrecy capacity for both approaches.

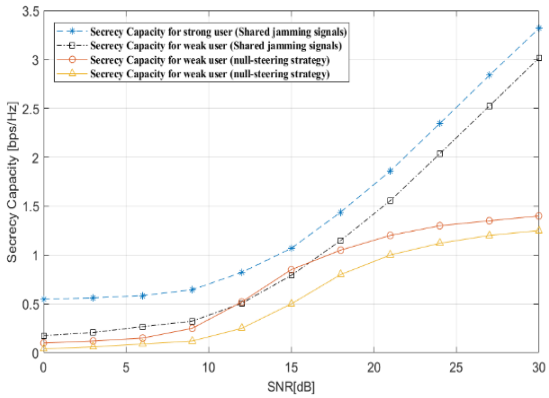

Fig. 4. Secrecy capacity versus SNR comparison.

Fig. 4 shows that the comparison between null-steering jamming and shared jamming signal strategies yield that the proposed shared jamming signal strategy provides a better performance in secrecy than the null-steering jamming scheme, since in the proposed scheme a half-duplex two-way relay node is used in order to amplify the transmitted signal and only the eavesdropper node in both approaches is susceptible to the jamming signal.

Based on the results, we observe that the secrecy capacity of the strong user is better than the secrecy performance of the weak user. The reason behind this is the successive interference cancellation technique used by the strong user. This technique enables the strong user to decode the information signal aimed to be sent to the weak user node. Thus, the strong user is not affected by the signal interference. However, the weak user is affected by the strong user signal as the interference signal. Thus, the secrecy capacity performance is

decreased at the weak user. We observe that at low SNR, the difference between the resulted secrecy capacity from both approaches is not significant. (for example, at SNR = 15 dB). While at high SNR the increment rate in secrecy capacity for the null-steering approach decreases.

IV. Conclusion

This research studies the physical layer security of a cooperative NOMA in presence of an untrusted weak user case and an eavesdropper case. Based on the simulations, the increase of both the power allocation coefficient of the strong user ($user_1$) and the distances between the weak untrusted user ($user_2$) and the cooperative relay is beneficial to the security performance. Moreover, the results show that the proposed shared jamming signal outperforms the null-steering jamming scheme.

For future work, it is recommended to evaluate the secrecy performance of the cooperative NOMA system using different channels such as Rician fading channel.

Conflict of Interest

The authors declare no conflict of interest.

Author Contributions

Mohammed A. Salem conducted the research including formulating idea, performance evaluation to the final manuscript under the guidance of Azlan B. Abd. Aziz who is the corresponding author. Mohamad Y. Alias also spent time revising the manuscript. However, all of authors had approved the final version.

Acknowledgment

The supporter of this research is the TM Research and Development centre (TMRND).

References

[1] M. A. Salem, A. B. Abd. Aziz, M. Y. Bin Alias, and A. A. A. Rahman, "Secrecy performance on half-duplex two-way multi-relay transmission technique under wireless physical layer security," in *Proc. International Symposium on Information Theory and Its Applications (ISITA)*, Singapore, 2018, pp. 668-672.

[2] C. E. Shannon, "Communication theory of secrecy systems," *The Bell System Technical Journal*, vol. 28, no. 4, pp. 656-715, Oct. 1949.

[3] A. D. Wyner, "The wire-tap channel," *The Bell System Technical Journal*, vol. 54, no. 8, pp. 1355-1387, Oct. 1975.

[4] T. M. Hoang, T. Q. Duong, H. A. Suraweera, C. Tellambura, and H. V. Poor, "Cooperative beamforming and user selection for improving the security of relay-aided systems," *IEEE Transactions on Communications*, vol. 63, no. 12, pp. 5039-5051, Dec. 2015.

[5] E. Nosrati, X. Wang, A. Khabbazibasmenj, and A. M. Akhtar, "Secrecy enhancement via cooperative relays in multi-hop communication systems," in *Proc. IEEE 83rd Vehicular Technology Conference (VTC Spring)*, Nanjing, 2016, pp. 1-6.

[6] S. D. Roy, S. Kundu, A. Kumar, and S. Sharma, "Secrecy outage probability with destination assisted jamming in presence of an untrusted relay," in *Proc. IEEE Annual India Conference (INDICON)*, Bangalore, 2016, pp. 1-5.

[7] A. Yener and S. Ulukus, "Wireless physical-layer security: Lessons learned from information theory," *Proc. the IEEE*, vol. 103, no. 10, pp. 1814-1825, Oct. 2015.

[8] M. A. Salem, A. B. A. Aziz, M. Y. B. Alias, A. A. A. Rahman, and A. Mahmud, "Secrecy analysis on half-duplex two-way relay transmission using various transmission channels and jamming strategies," in *Proc. 7th International Conference on Computer and Communication Engineering (ICCCE)*, Kuala Lumpur, 2018, pp. 432-436.

[9] M. A. Salem, A. B. A. Aziz, M. Y. B. Alias, and A. A. A. Rahman, "Jamming power estimation technique under wireless physical layer security in presence of an eavesdropper," in *Proc. 7th International Conference on Smart Computing & Communications (ICSCC)*, Sarawak, Malaysia, Malaysia, 2019, pp. 1-4.

[10] Y. Zou, X. Wang, and W. Shen, "Physical-layer security with multiuser scheduling in cognitive radio networks," *IEEE Transactions on Communications*, vol. 61, no. 12, pp. 5103-5113, December 2013.

[11] M. Zhang and Y. Liu, "Energy harvesting for physical-layer security in OFDMA networks," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 1, pp. 154-162, Jan. 2016.

[12] Z. Ding, X. Lei, G. K. Karagiannidis, R. Schober, J. Yuan, and V. K. Bhargava, "A survey on non-orthogonal multiple access for 5G networks: Research challenges and future trends," *IEEE Journal on Selected Areas in Communications*, vol. 35, no. 10, pp. 2181-2195, Oct. 2017.

[13] J. Chen, L. Yang, and M. Alouini, "Physical layer security for cooperative NOMA systems," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 5, pp. 4645-4649, May 2018.

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

[15] Y. Liu, Z. Qin, M. Elkashlan, Y. Gao, and L. Hanzo, "Enhancing the physical layer security of non-orthogonal multiple access in large-scale networks," *IEEE Transactions on Wireless Communications*, vol. 16, no. 3, pp. 1656-1672, March 2017.

[16] M. Fadhil, N. F. Abdullah, M. Ismail, R. Nordin, A. Saif, and M. Al-Obaidi, "Power allocation in cooperative NOMA MU-MIMO beamforming based on maximal SLR precoding for 5G," *Journal of Communications*, vol. 14, no. 8, pp. 676-683, 2019.

[17] Y. Alsaba, C. Y. Leow, and S. K. Abdul Rahim, "A game-theoretical modeling approach for enhancing the physical

layer security of non-orthogonal multiple access system," *IEEE Access*, vol. 7, pp. 5896-5904, 2019.

Mohammed Ahmed Salem received the B.S. degree in Mechatronics Engineering from the Universiti Teknikal Malaysia Melaka (UTeM), Malaysia, in 2017. He is currently pursuing the master's degree in Telecommunication Engineering at Multimedia University (MMU), Malaysia. His research interest includes Wireless physical layer security, cooperative relay networks and non-orthogonal multi access network.

Azlan Bin Abd Aziz received the B.S. degree in electrical and computer engineering from Ohio State University, Columbus, Ohio, USA in 1998 and the M.S. degree in communication engineering from the University of Manchester, UK in 2004. In March 2012, he obtained a Ph.D. degree in engineering and computer science at Nagoya Institute of Technology. He has more than a decade industrial experience in telecommunication sectors and currently is attached to Multimedia University, Malaysia. His research interests cover from coding theory in communication systems, signal processing and deep learning for vehicular communication applications. His current research includes physical layer security for wireless networks, vehicular communications, and smart antenna applications.

Mohamad Yusoff Bin Alias received the B.S. degree in Electrical Engineering from the University of Michigan, Ann Arbor, in 1998. He then received his Ph.D. degree in December 2004 from the School of ECS, University of Southampton in the United Kingdom. He is currently a Professor at the Faculty of Engineering, Multimedia University in Malaysia. His research interests cover the field of wireless communications especially in OFDM, multiple antenna system, multiuser detection, genetic algorithms in communications, multimedia applications and visible light communications.