On the Performance of Transmit Antenna Selection for Physical-Layer Security of NOMA Systems Under Untrusted Users

Jones Márcio Nambundo, Samuel Mafra and Samuel Montejo-Sánchez

Abstract— **In this paper, the physical layer security for a two-user downlink NOMA cluster, between a near trusted user and a far untrusted user, subject to Nakagami- m fading is investigated. It is considered a scenario with a multiple antenna base station, in which the antenna with best channel for the near user is selected. The pair outage probability and secrecy outage probability are analyzed to verify the system performance gain. Results show improvements in the pair outage probability and secrecy outage probability when the relative distance between the trusted user and the BS decreases, its link has direct line of sight and/or the number of base station antennas increases.**

Keywords— **Non-orthogonal multiple access; Physical-layer security; Secrecy outage probability; Untrusted users.**

I. Introduction

The non-orthogonal multiple access (NOMA), introduced by Saito *et al.* in [1], is one of the most promising techniques of the new generation of wireless network due to the significantly increasing number of wireless users and devices, low latency and higher quality of service [2], [3].

The NOMA schemes can be divided in two categories: power-domain NOMA and code-domain NOMA [4]. Similar to the code-domain multiple access (CDMA), in code-domain NOMA, the users communicate at the same time and frequency but with different codes. In power-domain NOMA, multiple users are encouraged to transmit messages at the same frequency and time, but with different power levels. In particular, this strategy allocates less power to users with better channel conditions, and these users can decode their own information by applying successive interference cancellations (SIC), offering better performance and spectral efficiency compared to other techniques.

The multiple antenna systems in wireless networks, can provide spatial diversity improving system performance and simplifying detection in users by mitigating the effects of multi-path fading. The NOMA techniques has been proposed in different scenarios with use of multiple antennas [5]–[8].

In [5] are proposed new design of precoding and detection matrices for a NOMA scenario in which all nodes are equipped with multiple antennas. In [6]–[8], the transmission antenna selection (TAS) technique has been proposed and has been recognized as an effective solution. In [6], the authors design NOMA for downlink energy harvesting (EH) multiple-antenna relaying networks with simultaneous wireless information and power transfer. In [7], efficient antenna selection and user scheduling algorithms are investigated to maximize the sum rate in two MIMO-NOMA scenarios. In [8], the authors propose antenna selection algorithms for scenarios: NOMA with fixed power allocation (F-NOMA) and NOMA with cognitive radio-inspired power allocation (CR-NOMA). The algorithms achieve a significant computational complexity reduction in comparison with other schemes of literature.

Achieving security in NOMA systems is a critical issue due to the broadcast nature of these systems and the process of successive interference cancellation, the users can decode the messages of other paired users. The conventional solutions are based on cryptography. However, the networks of new generation can impose difficulties for implementation of cryptography due to the decentralized, heterogeneous organization, power and processing constraints for instance in internet of things (IoT) networks [9]. In [10], Wyner proposed the concept of physical layer security (PLS) in order to improve network security as a complementary approach to cryptographic techniques. The physical layer security techniques exploit the dynamic resources of wireless networks, such as random channel, fading, noise interference and others to prevent the eavesdropper decode the data.

The physical layer security technique has been demonstrated as a sustainable way to deal with security problems in NOMA networks [11]. In [12], the authors analyze the physical layer security for an downlink NOMA network with an untrusted far user, i.e. the user tries to obtain the message of the other user after decoding its own message by acting as an eavesdropper. The authors analyze the proposed scheme in terms of pair outage probability (OP) and the secrecy outage performance (SOP). Due to the relevance to the topic, similar analyzes are performed here. El Halawany and Wu. show that is possible to obtain an lower pair outage probability at same time that the security level of the strong user is under a certain threshold.

In [14], three different schemes are investigated for a multiple-input single-output energy harvesting internet of

Jones Márcio Nambundo and Samuel Mafra are with Instituto Nacional de Telecomunições Santa Rita Sapucai , Minas Gerais, E-mails:(jonesnambundo@mtel.inatel.br,samuelbmafra@inatel.br).

S. Montejo-Sánchez is with *Programa Institucional de Fomento a la I+D+i*, Universidad Tecnológica Metropolitana, Santiago, Chile. E-mail: smontejo@utem.cl.

This work was partially supported by FADCOM (Fundo de Apoio ao Desenvolvimento das Comunicações), presidential decree No. 264/10, November 26, 2010, Republic of Angola in partnership with INATEL (Instituto Nacional de Telecomunicações), Brazil, as well as by RNP, with resources from MCTIC, Grant No. 01250.075413/2018-04, under the CRR (Centro de Referência em Radiocomunicações) project of INATEL. The authors wish also acknowledge the financial support from and FONDECYT Regular No. 1201893, FONDECYT Iniciación No. 11200659 and SCC-PIDi-UTEM FONDEQUIP-EQM180180,Chile.

things systems, in which a multi-antenna base station transmits signals to IoT devices (IoTDs) with the help of untrusted relays.

In [13], the authors investigate the secrecy outage probability of an untrusted relaying energy-harvesting system in the presence of an eavesdropper network. In order to decrease the overhearing capacity of the untrusted relay, the destination sends artificial noise signals during the communication.

In [15], the authors propose two relay selection schemes termed decode-and-forward and amplify-and-forward protocols based optimal relay selection schemes for a NOMA network under untrusted users.

In [16], the authors investigate secrecy outage probability for cooperative NOMA systems with antenna selection schemes, where the base station communicates with the far user through the use of a full-duplex relay. The proposed scheme has a best performance in comparison with single-antenna systems and without antenna selection.

In this work, we extend the scenario of [12] for a network with a multiple antenna base station and under a Nakagami-m fading. A transmit antenna selection scheme is employed, in which the antenna with best channel for the near user is selected. The pair outage probability and secrecy outage probability are analyzed to guarantee a certain level of quality of service in the network, i.e. the base station can achieve a reliable communication for both users and a acceptable level of security for the near user. We derive closed-form expressions for the pair outage considering the number of antennas and Nakagami-m fading. Results show improvements in the pair outage probability and secrecy outage probability when a some line of sight is present and with a multiple antenna base station.

The remainder of this paper is organized as follows: Section II introduces the system model. In Section III the pair outage probability and secrecy outage probablity are analyzed for the proposed scheme. In Section IV representative numerical results are provided and insightful discussions are drawn. Finally, Section V concludes the paper.

II. System Model

We consider a NOMA downlink network composed of two single antenna users and a multiple antenna base station (BS) located in the center of the cell, as shown in Figure 1. The near user U_1 needs highest security clearance to be protected of the far user U_2, which is an untrusted user by means of physical layer security.

The quasi-static fading channel between the selected antenna ϱ of BS and user i is denoted by h_i^{ϱ}, $i \in \{1,2\}$, where $\{1,2\}$ represent the near user U_1 and the far user U_2, respectively. h_i^{ϱ} follows a Nakagami-m distribution with fading parameter m_i and average power $\lambda_i \triangleq \mathbb{E}\left[|h_i^{\varrho}|^2\right] \triangleq d_i^{-\nu}$, where d_i represents the distance between the base station and the user i and ν is the path-loss exponent ($\nu \geq 2$).The transmit power of BS is denoted by P.

In order to improve the security of the U_1, we employ a transmit antenna selection scheme, in which the base station chooses the antenna that has the best channel to the near user. The channel among BS and U_2 is independent of the selected channel h_1, i.e. the best channel for U_1 could not be the best for U_2. The index of the best antenna can be obtained by:

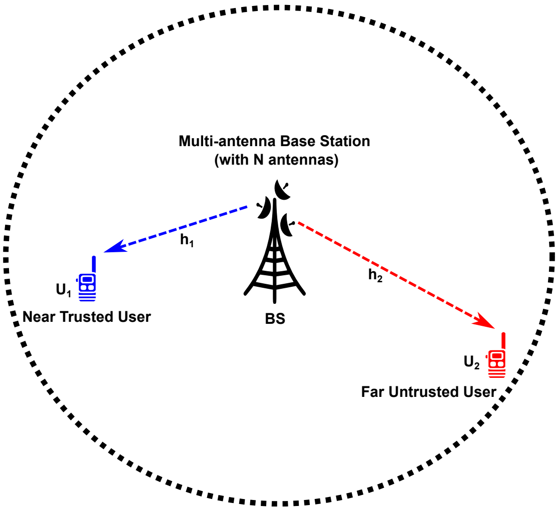


Fig. 1: System model composed by a multi-antenna base station (BS) with N antennas, a near trusted user (U_1) and a far untrusted user (U_2), both single-antenna users.

$$\varrho = \underset{k=1,\ldots,N}{\arg\max}\; h_1^k, \tag{1}$$

where N represents the number of antennas at the base station. The estimation of the channels can be done through the pilot symbol transmitted by the near user. Then for means of simplicity, we assume hereinafter the channel among BS and U_2 as h_2.

The BS broadcasts the superimposed signal, $x = \sqrt{a}x_1 + \sqrt{1-a}x_2$, where x_1 and x_2 are the unit power signals received by users U_1 and U_2, respectively, and a is the power allocation coefficient for the near user where $(0 < a < 1)$. The received signal at users U_1 and U_2 can be given by

$$y_1 = h_1^{\varrho} x \sqrt{P} + n_1, \tag{2}$$

$$y_2 = h_2^{\varrho} x \sqrt{P} + n_2, \tag{3}$$

where n_1 and n_2 are additive white Gaussian noise with variance $N_0/2$ per dimension, while without loss of generality we assume hereinafter that $N_0 = 1$.

Considering a power-domain NOMA scheme, the deconding process occurs as:

1) First, U_1 tries to decode the signal of the far user, considering its message as interference and then decodes its own signal after applies SIC.
2) U_2 has assigned more power, thus it tries to decode its own signal assuming the U_1 signal as a interference.
3) Finally, the user U_2 is an untrusted user and tries to decode the near user signal after decoding its own signal using SIC.

The signal-to-interference-plus-noise ratio (SINR) of U_2 decoded by U_i is given by:

$$\gamma_2^i = \frac{(1-a)P\left|h_i^{\varrho}\right|^2}{aP\left|h_i^{\varrho}\right|^2 + N_0}, \tag{4}$$

while, the signal-to-noise ratio (SNR) of U_1 after the SIC process at U_i is:

$$\gamma_1^i = \frac{aP\left|h_i^{\varrho}\right|^2}{N_0}. \tag{5}$$

III. Performance Analysis

In this section, we first derive the closed form expression of the OP, followed by the derivation of the SOP of user U_1.

A. Pair Outage Probability Analysis

The pair outage probability is defined as the probability of at least one of users do not correctly decode its message. Thus, the pair outage probability can written as:

$$\begin{aligned} P_0 &= 1 - P_r\left\{\gamma_2^2 > \epsilon, \gamma_2^1 > \epsilon, \gamma_1^1 > \epsilon\right\}, \\ &= 1 - P_r\left\{\gamma_2^2 > \epsilon\right\} \times P_r\left\{\gamma_2^1 > \epsilon, \gamma_1^1 > \epsilon\right\}, \\ &= 1 - \underbrace{P_r\left\{\left|h_2\right|^2 > \frac{N_0\epsilon}{P\left(1-(\epsilon+1)a\right)}\right\}}_{\text{A}} \times \\ &\quad \underbrace{P_r\left\{\left|h_1^{\varrho}\right|^2 > \frac{N_0\epsilon}{P\min((1-(\epsilon+1)a, Pa))}\right\}}_{\text{B}}, \end{aligned} \tag{6}$$

where $\epsilon = 2^R - 1$ is the attempted rate of the users.

The term (A) in (6) represents the probability that the user U_2 correctly decodes its own signal considering the signal of U_1 as a interference. The term (B) in (6) represents the probability that the user U_1 correctly decoded the signal of U_2 considering its own signal as a interference and then U_1 decoded its own signal after performing successive interference cancellation in the received signal.

The probabilities of the terms (A) and (B) are given by:

$$\begin{aligned} \text{A} &= P_r\left\{\left|h_2\right|^2 > \frac{N_0\epsilon}{P\left(1-(\epsilon+1)a\right)}\right\} \\ &= 1 - P_r\left\{\left|h_2\right|^2 \le \frac{N_0\epsilon}{P\left(1-(\epsilon+1)a\right)}\right\} \\ &= 1 - \int_0^{\frac{N_0\epsilon}{P(1-(\epsilon+1)a)}} \frac{e^{-\frac{m_2 z}{\lambda_2}}\left(\frac{m_2 z}{\lambda_2}\right)^{m_2}}{z\Gamma(m_2)}dz \\ &= \begin{cases} 1 - \frac{\gamma\left(m_2, \frac{m_2\epsilon N_0}{\lambda_2 P(1-(\epsilon+1)a)}\right)}{\Gamma(m_2)} & \text{for } 0 \le a \le \frac{1}{1+\epsilon} \\ 1, \quad \text{otherwise.} \end{cases} \end{aligned} \tag{7}$$

where $\gamma(a,b) = \int_0^b y^{a-1}\exp(-y)dy$ and $\Gamma(a) = \int_0^\infty y^{a-1}\exp(-y)dy$ are, respectively, the lower incomplete Gamma function and the complete Gamma function.

$$\begin{aligned} \text{B} &= P_r\left\{\left|h_1^{\varrho}\right|^2 > \frac{N_0\epsilon}{P\min((1-(\epsilon+1)a, a))}\right\} \\ &= P_r\left\{\max_{k=1,\ldots,N}\left|h_1^k\right|^2 > \frac{N_0\epsilon}{P\min((1-(\epsilon+1)a, a))}\right\} \\ &= 1 - \left(P_r\left\{\left|h_1\right|^2 \le \frac{N_0\epsilon}{P\min((1-(\epsilon+1)a, a))}\right\}\right)^N \\ &= 1 - \left(\int_0^{\frac{N_0\epsilon}{P\min((1-(\epsilon+1)a,a))}} \frac{e^{-\frac{m_1 z}{\lambda_1}}\left(\frac{m_1 z}{\lambda_1}\right)^{m_1}}{z\Gamma(m_1)}dz\right)^N, \\ &= \begin{cases} 1 - \left(\frac{\gamma\left(m_1, \frac{m_1\epsilon N_0}{\lambda_1 P(1-(\epsilon+1)a)}\right)}{\Gamma(m_1)}\right)^N, & \text{for } 0 \le a \le \frac{1}{2+\epsilon} \\ 1 - \left(\frac{\gamma\left(m_1, \frac{m_1\epsilon N_0}{\lambda_1 Pa}\right)}{\Gamma(m_1)}\right)^N, & \text{for } \frac{1}{2+\epsilon} \le a \le \frac{1}{1+\epsilon} \\ 1, \quad \text{otherwise.} \end{cases} \end{aligned} \tag{8}$$

Finally, the pair outage probability can be obtained by replacing the terms (A) and (B) in Eq. (6) by Eq. (7) and (8), respectively.

B. Secrecy Outage Probability Analysis

The Secrecy Outage Probability (SOP) is defined as the probability that the BS cannot reliably and securely transmit the message of the user U_1, without the interception by the untrusted user U_2. Hence, the Secrecy Outage Probability of U_1 can be written as:

$$\begin{aligned} SOP &= \Pr[\log_2(1+\gamma_1^1) - \log_2(1+\gamma_1^2) < R_s] \\ &= \Pr\left[\log_2\left(\frac{1+\gamma_1^1}{1+\gamma_1^2}\right) < R_s\right] \end{aligned} \tag{9}$$

where R_s is the secure data rate. This probability has not a general closed-form expression. The expression of the SOP was derived in [12, Eq. 17] for the scenario with a single antenna base station and Rayleigh fading, which is given by:

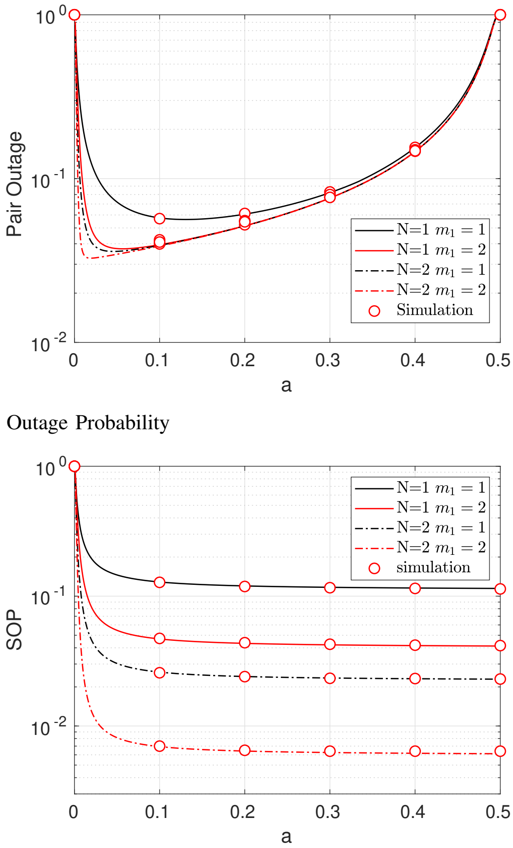
$$SOP = 1 - \frac{\lambda_1}{\lambda_1 + \lambda_2\epsilon_s}e^{-\frac{\epsilon_s - 1}{aP\lambda_1}}, \tag{10}$$

where $\epsilon_s = 2^{R_s}$. For the more general scenarios we calculate the SOP by means of numerical integration.

IV. Numerical Results

In this section we present some numerical results in order to evaluate the performance of the proposed scheme. We compare the proposed scheme with the scenario of one antenna base station and Rayleigh fading that correspond to analysis of ElHalawany and Wu in [12]. Monte Carlo simulations have been carried out to verify the accuracy of the analytical derivations. Monte Carlo simulations are represented by red circles. We evaluate the pair outage outage probability and secrecy outage probability for a two-user NOMA downlink network with $d_1 = 1/2$, $d_2 = 1$, $N_0 = 1$, $\nu = 4$, attempted transmission rate $R = 1$ bit per channel use (bpcu), secure data rate $R_s = 1$ bit per channel use (bpcu), $P = 15$ dB.

In Fig. 2, we evaluate the effect of the fading parameter of the channel among base station and near user (m_1), the pair outage probability and the secrecy outage probability as a function of a are analyzed for different number of antennas $N \in \{1, 2\}$, $m_1 = \{1, 2\}$ and $m_2 = 1$.



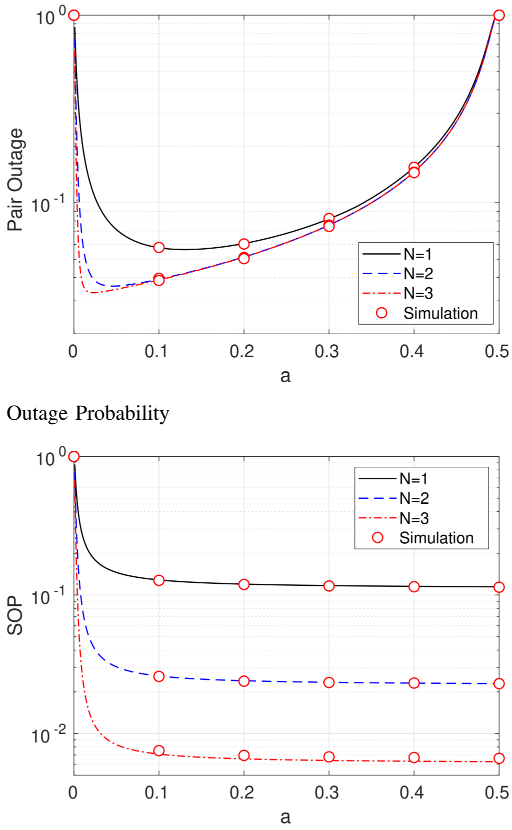
(a) Pair Outage Probability

(b) Secrecy Outage Probability

Fig. 2: Pair outage probability/secrecy outage probability versus the power allocation factor for different number of antennas and fading parameter m_1

By the Fig. 2a, we can see that the pair outage probability decreases when there is some line of sight in the $BS \to U_1$ link. Moreover, the best value of the power allocation factor tends to smaller values with the increment in m_1 and in the number of antennas. For instance, the best value of a is approximately 0.15 when $m_1 = 1$ and $N = 1$ while for $m_1 = 2$, $N = 1$ and $m_1 = 1$, $N = 2$ cases, the best value of a is 0.05. The best scenario occurs when it is possible to increase the number of antennas and there is a some light of sight in the $BS \to U_1$ link as demonstrated for the case with $N = 2$, $m_1 = 2$. It is possible to note in Fig. 2b, that the secrecy outage probability considerably decreases when there is a some light of sight in the $BS \to U_1$ link as well as with the increment in the number of antennas. Considering the best values of a in Fig. 2a, one can observe that the SOP of U_1 is approximately 0.11 for $m_1 = 1$, $N = 1$, while for $m_1 = 1$, $N = 2$ is equal to 7×10^{-3}. Finally, it is possible to see that there is an optimal number of antennas in order to guarantee a certain level of security for the user U_1 at same time with the best value of pair outage probability. When the best value of a approaches to zero the secrecy outage probability tends to one.

In order to evaluate the effect of the number of antennas at the base station, we analyze the pair outage probability and the secrecy outage probability as a function of a for different number of antennas $N \in \{1, 2, 3\}$, $m_1 = m_2 = 1$ in Fig. 3.



(a) Pair Outage Probability

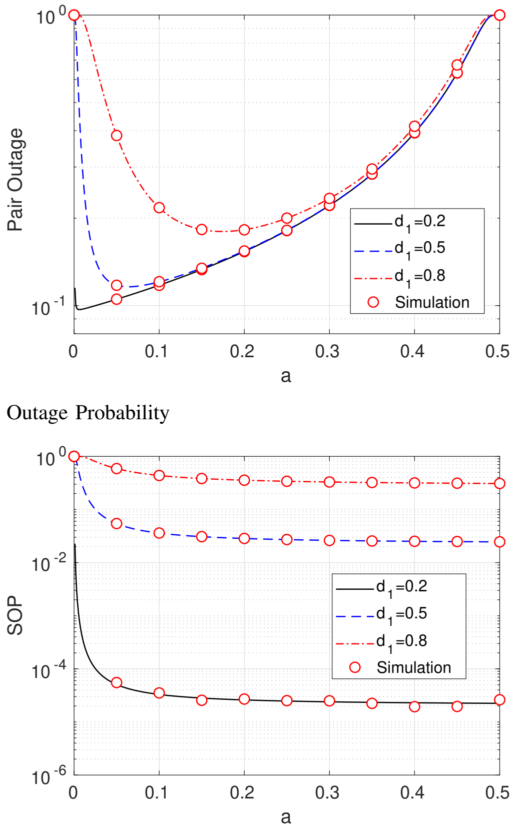
(b) Secrecy Outage Probability

Fig. 3: Pair outage probability/secrecy outage probability versus the power allocation factor for different number of antennas

By the Fig. 3, for this specific scenario one can see as expected the performance of both both metrics improve with the increment of antennas. The best number of antennas is two if the objective is transmit with low values of both metrics. If the objective is only to guarantee the security of U_1 with a certain range for the pair outage probability, then it is possible to obtain lowest values with the increment of antennas.

In Fig. 4, we analyze the performance of the proposed scheme for different positions of U_1 with $R = 1$ bpcu, $N = 2$, $m_1 = m_2 = 1$, $P = 10$ dB.

By the Fig. 4, one can see that the best value of a changes with the position of U_1. When the user is closer to the base station, a tends to zero, and in this case, it is not possible to obtain the best values of the metrics simultaneously. In this case, BS needs to allocate more power to the U_1 at the cost of increasing the pair outage probability. While for the scenario with U_1 closer to U_2, it is possible to transmit the optimal a of the pair outage, however the secrecy outage probability is very high in this region. Finally, by the above analyses, one can see that the choices of the power allocation factor and the number of antennas depend of the scenario of application and the objectives for the pair performance and security of U_1.



(a) Pair Outage Probability

(b) Secrecy Outage Probability

Fig. 4: Pair outage probability/secrecy outage probability versus the power allocation factor for different positions of the user U_1

V. Conclusion

We evaluated the performance of transmit antenna selection for physical-layer security of a two user downlink NOMA network in presence of an untrusted user under Nakagami-m fading. The results show that the proposed scheme has improvements performance in terms of pair outage probability and secrecy outage probability, when compared with a single antenna scenario. We analyzed the proposed scheme considering the effect of different parameters. By the analyses, we observe that there is an optimum number of antennas when the objective is to minimize the pair outage probability and at same time to guarantee the security of the near user. As a future works, we intend to analyze a scenario when the base station has imperfect channel state information of the channels. Moreover, we intend to extend the analysis for a scenario with multiple untrusted users.

References

[1] Y. Saito, Y. Kishiyama, A. Benjebbour, T. Nakamura, A. Li and K. Higuchi, "Non-Orthogonal Multiple Access (NOMA) for Cellular Future Radio Access," *2013 IEEE 77th Vehicular Technology Conference (VTC Spring)*, Dresden, 2013, pp. 1-5,

[2] S. M. R. Islam, N. Avazov, O. A. Dobre and K. Kwak, "Power-Domain Non-Orthogonal Multiple Access (NOMA) in 5G Systems: Potentials and Challenges," in *IEEE Communications Surveys & Tutorials*, vol. 19, no. 2, pp. 721-742, Secondquarter 2017

[3] L. Dai, B. Wang, Z. Ding, Z. Wang, S. Chen and L. Hanzo, "A Survey of Non-Orthogonal Multiple Access for 5G," in *IEEE Communications Surveys & Tutorials*, vol. 20, no. 3, pp. 2294-2323, thirdquarter 2018

[4] L. Dai, B. Wang, Y. Yuan, S. Han, C. I and Z. Wang, "Non-orthogonal multiple access for 5G: solutions, challenges, opportunities, and future research trends," in *IEEE Communications Magazine*, vol. 53, no. 9, pp. 74-81, September 2015

[5] Ding, Z., Adachi, F., Poor, H.: 'The application of MIMO to non-orthogonal multiple access', *IEEE Trans. Wireless Commun.*, 2016, 15, (1), pp. 537–552

[6] W. Han, J. Ge, and J. Men, "Performance analysis for NOMA energy harvesting relaying networks with transmit antenna selection and maximal- ratio combining over Nakagami-m fading," *IET Commun.*, vol. 10, no. 18, pp. 2687-2693, Dec. 2016.

[7] X. Liu and X. Wang, "Eficient antenna selection and user scheduling in 5G massive MIMO-NOMA system," in *Proc. IEEE 83rd Veh. Technol. Conf. (VTC Spring)*, Nanjing, China, May 2016, pp. 1-5.

[8] Y. Yu, H. Chen, Y. Li, Z. Ding, L. Song and B. Vucetic, "Antenna Selection for MIMO Nonorthogonal Multiple Access Systems," in *IEEE Transactions on Vehicular Technology*, vol. 67, no. 4, pp. 3158-3171, April 2018

[9] M. Frustaci, P. Pace, G. Aloi and G. Fortino, "Evaluating Critical Security Issues of the IoT World: Present and Future Challenges," in *IEEE Internet of Things Journal*, vol. 5, no. 4, pp. 2483-2495, Aug. 2018

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

[11] H. M. Furqan, J. M. Hamamreh, and H. Arslan, "Physical layer security for NOMA: Requirements, merits, challenges, and recommendations," 2019, arXiv:1905.05064. [Online]. Available: http://arxiv.org/abs/1905.05064

[12] B. M. ElHalawany and K. Wu, "Physical-Layer Security of NOMA Systems Under Untrusted Users," 2018 IEEE Global Communications Conference (GLOBECOM), Abu Dhabi, United Arab Emirates, 2018, pp. 1-6,

[13] Tuan, V.P., Kong, H.Y. Secrecy Outage Analysis of an Untrusted Relaying Energy Harvesting System with Multiple Eavesdroppers. *Wireless Pers Commun* 107, 797–812 (2019).

[14] V. N. Vo et al., "On Security and Throughput for Energy Harvesting Untrusted Relays in IoT Systems Using NOMA," in *IEEE Access*, vol. 7, pp. 149341-149354, 2019

[15] K. Cao, B. Wang, H. Ding, T. Li and F. Gong, "Optimal Relay Selection for Secure NOMA Systems Under Untrusted Users," in *IEEE Transactions on Vehicular Technology*, vol. 69, no. 2, pp. 1942-1955, Feb. 2020

[16] X. Pei, H. Yu, M. Wen, Q. Li and Z. Ding, "Secure Outage Analysis for Cooperative NOMA Systems With Antenna Selection," in *IEEE Transactions on Vehicular Technology*, vol. 69, no. 4, pp. 4503-4507, April 2020, doi: 10.1109/TVT.2020.2973726.