

# Empowering secure transmission for downlink of multiple access system relying non-orthogonal signal multiplexing

Dinh-Thuan Do , Minh-Sang Van Nguyen

Department of Electronics and Telecommunications, Faculty of Electronics Technology Industrial University of Ho Chi Minh City (IUH), Ho Chi Minh, Vietnam

## Article Info

### Article history:

Received Mar 9, 2022

Revised May 9, 2022

Accepted Jun 8, 2022

### Keywords:

Decode and forward  
Non-orthogonal multiple access  
Physical layer security

## ABSTRACT

The growth of internet-of-things (IoT) inspired use cases in different run of the mill environments such as cities, industries, healthcare, agriculture, and transportation, has led to a greater desire for safer IoT data gathering and storage. However, securing IoT is challenging due to form-factor, complexity, energy, and connectivity limitations. Conventional coding-based security techniques are unsuitable for ultra-reliable low-latency and energy-efficient communication in IoT. Numerous research studies on physical layer security (PLS) techniques for fifth generation (5G) have emerged recently, but not all of the solutions can be used in IoT networks due to complexity limitations. Non-orthogonal multiple access (NOMA) is billed as a possible technology to solve connectivity and latency requirements in IoT. In this study, we exploit the power allocation characteristics of NOMA to enhance security in a downlink device-to-device (D2D) decode and forward (DF) IoT network infiltrated by an eavesdropper. Our performance metric of choice is the secrecy outage probability (SOP). We formulate exact SOP results for different users. Simulation results demonstrate the positive impact of NOMA on SOP in a D2D IoT-NOMA network.

This is an open access article under the [CC BY-SA](#) license.



## Corresponding Author:

Minh-Sang Van Nguyen

Department of Electronics and Telecommunications, Faculty of Electronics Technology, Industrial University of Ho Chi Minh City (IUH)

12 Nguyen Van Bao, Phuong 4, Go Vap, Thanh pho Ho Chi Minh 7000, Vietnam

Email: nguyenvanminhsang@iuh.edu.vn

## 1. INTRODUCTION

The promise of 10x spectral efficiency and connectivity in fifth generation (5G), has driven the adoption and development of internet-of-things (IoT) in different scenarios ranging from agriculture to transportation. Consequently, the transmission security of IoT networks is now an urgent requirement as public and government scrutiny has increased on data collection and security habits of IoT applications. Physical layer security (PLS) technology is an alternative to conventional cryptography-based security technologies in IoT networks as it does not affect latency nor increase packet lengths [1]. However, not every PLS technique can be introduced into IoT networks because of the unique characteristics of IoT devices which tend to have small form-factors, energy constraints and limited signal processing capability [1], [2].

To speedup spectral efficiency in next generation wireless system, non-orthogonal multiple access (NOMA) can be recommended as the leading technology since it exhibits higher connectivity and low latency demands as well [3]–[8]. These are features important for the next generation support of IoT communication functions [9]. NOMA is an advance on orthogonal multiple access, as its supreme feature is power-domain

multiplexing which exploits and allows interference amongst users. Also, message superposition coding and successive interference cancellation (SIC) are tools it relies on to mitigate interference in the network [4], [10].

There have been several studies on the security of NOMA-assisted IoT networks [11]–[15]. The author study the use of NOMA in improving security and quality of service (QoS) of IoT networks hosting a passive eavesdropper by taking advantage of NOMA's power allocation ability [16]. The authors develop an anti-eavesdropping security scheme for the cooperative NOMA-IoT network [17]. The authors formulated closed-form secrecy outage probability (SOP) results. The author investigated secure transmission in a NOMA-IoT network consisting of latency and security-sensitive devices [18]–[20]. Furthermore, [21]–[23] investigated SIC NOMA in full-duplex device-to-device (D2D) IoT and derived sum-throughput expressions, and closed-form outage probability (OP) and secrecy rate expressions.

The main advantages of NOMA is the concept of perfect and imperfect SIC, and resource allocation as seen in [1], [10], [19], [20]. Inspired by these ideas, we exploit NOMA's power allocation strategy to enhance security in a downlink D2D IoT network invaded by an eavesdropper, to reduce the SOP at the intended users. Based on the above ideas, we introduce brief findings as the key results as shown in:

- We try to figure out outage behavior of the system by computing closed-form formula. These expressions are dedicated to evaluate performance of different users since these users are assigned with Rayleigh fading channel conditions.
- We plot the relationship of SOP under different scenarios such as power allocation variation, residual interference, transmitter interference, and change in target data rate. We especially show that the inherent characteristics of power-domain NOMA improve the SOP of IoT-NOMA networks. All the results are validated using Monte Carlo simulations.

The rest of this study is organized as follows. In section 2, the secure transmission for D2D can be deployed for downlink IoT system. Then, section 3 is main part conducting secrecy outage performance analysis by finding closed-form expressions. In section 4, we discuss the significance of the obtained results. While we conclude main findings and important remarks in section 5.

## 2. THE MODEL OF D2D IOT-ASSISTED NOMA SYSTEM

In Figure 1, a downlink secure transmission originated from a base station (BS) which serve two users, i.e. near user  $D_1$  and the far user  $D_2$  while an eavesdropper wants to overhear signal from link  $BS-D_1$ . To transmit signals from the BS, two superimposed signals are conducted,  $x_i$ , ( $i = 1, 2$ ) are unit power signals which target destinations  $D_i$ . We call  $P_1$  as the transmit power from the BS. To easy compute outage performance, fixed power allocation factors are employed in this scenario, i.e.  $\psi_i$  with  $0 < \psi_i < 1$  and  $\psi_1 + \psi_2 = 1$ ,  $\psi_1 < \psi_2$ . Following the principle of NOMA, the coded signal is processed at the BS is given by:

$$x = \sqrt{\psi_1 P_1} x_1 + \sqrt{\psi_2 P_1} x_2. \quad (1)$$

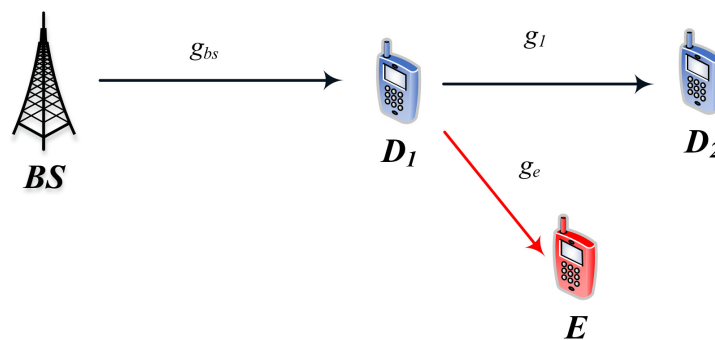


Figure 1. System model of D2D NOMA reliant IoT network

To look at imperfect CSI,  $\eta_1$  is characterized as the error term. It is assumed as complex Gaussian distributed random variable and it follows  $CN(0, \kappa_1)$  [24]. The received signals at user  $D_1$  can thus, be written as [24]:

$$y_{B-D_1} = (g_{bs} + \eta_1)x + \sigma_1, \quad (2)$$

where  $\sigma_1$  is the complex Gaussian noise at User  $D_1$  with  $\sigma_1 \sim CN(0, N_0)$ .  $g_{bs}$  denotes the channel responses from the BS to  $D_1$  with  $g_{bs} \sim CN(0, \lambda_{bs})$ . At the receiving nodes, we assume channel state information (CSI) is not known perfectly, thus, the CSI (estimated channel) at each node is given by  $g_{bs}$ . Conducting SIC operation, the user  $D_1$  first decodes  $x_2$ , then  $x_1$ . By decoding  $x_2$ , the signal-to-interference-plus-noise ratio (SINR) could be computed by:

$$\gamma_{1,2} = \frac{\psi_2 \rho_1 |g_{bs}|^2}{\psi_1 \rho_1 |g_{bs}|^2 + \rho_1 \kappa_1 + 1}, \quad (3)$$

where  $\rho_1 = \frac{P_1}{N_0}$ . After performing SIC, the interference is deleted at user  $D_1$ . We compute SNR which is intended to have own signal  $x_1$  for the user  $D_1$  and SNR is formulated by:

$$\gamma_1 = \frac{\psi_1 \rho_1 |g_{bs}|^2}{\rho_1 \kappa_1 + 1}. \quad (4)$$

After  $D_1$  successfully decodes  $x_2$ , the received signal at  $D_2$  can given by [24]:

$$y_{D_2} = (g_1 + \eta_2) \sqrt{P_2} x_2 + \sigma_2, \quad (5)$$

where  $P_2$  is the total transmit power of the  $D_1$ .  $\sigma_2$  is the complex Gaussian noise at user  $D_2$  with  $\sigma_2 \sim CN(0, N_0)$ .  $g_1$  denotes the channel responses from the  $D_1$  to  $D_2$  with  $g_1 \sim CN(0, \lambda_1)$ .  $\eta_2$  is the error term, which is typically modeled as a complex Gaussian distributed random variable with  $CN(0, \kappa_2)$  [24]. The SINR to detect  $x_2$  at  $D_2$  is:

$$\gamma_2 = \frac{\rho_2 |g_1|^2}{\rho_2 \kappa_2 + 1}, \quad (6)$$

where  $\rho_2 = \frac{P_2}{N_0}$ . The received signal at  $E$  from  $D_1$  is:

$$y_E = g_e \left( \sqrt{\psi_1 P_2} x_1 + \sqrt{\psi_2 P_2} x_2 \right) + \sigma_e, \quad (7)$$

where  $\sigma_e$  is the complex Gaussian noise at  $E$  with  $\sigma_e \sim CN(0, N_e)$ ,  $g_e$  denotes the channel responses from the  $D_1$  to  $E$  is given as [25];

$$\gamma_{E_i} = \psi_i \rho_e |g_e|^2, \quad (8)$$

where  $\rho_e = \frac{P_2}{N_e}$ . In the next step, we should mention capacity to measure how information is processed from the source to  $D_1$  and from  $D_1$  to  $D_2$ , respectively. These expressions of channel capacity are given by:

$$C_{D_1} = \frac{1}{2} \log_2 (1 + \min(\gamma_{1,2}, \gamma_1)), \quad (9)$$

and

$$C_{D_2} = \frac{1}{2} \log_2 (1 + \min(\gamma_{1,2}, \gamma_2)). \quad (10)$$

Also, we deal with channel to eavesdropper, and we can compute the capacity related to the eavesdropping channel as:

$$C_{E_i} = \frac{1}{2} \log_2 (1 + \gamma_{E_i}). \quad (11)$$

Finally, the secrecy capacity for  $D_i$  can be expressed as

$$C_i = [C_{D_i} - C_{E_i}]^+, \quad (12)$$

where  $[x]^+ = \max(0, x)$ .

### 3. ANALYSIS OF SECRECY OUTAGE PROBABILITY

It is noted that all channels follow the Rayleigh distribution with cumulative distribution function (CDF) and probability density function (PDF) can be:

$$F_{|g_Q|^2}(x) = 1 - \exp\left(-\frac{x}{\lambda_Q}\right), \quad (13)$$

and

$$f_{|g_Q|^2}(x) = \frac{1}{\lambda_Q} \exp\left(-\frac{x}{\lambda_Q}\right), \quad (14)$$

where  $Q = \{bs; 1; e\}$ . In this section, we pay attention on SOP performance which is necessary to evaluate security of the considered system. Therefore, in this section, the analytic expressions could be computed based on some provided distributions of related channels.

#### 3.1. SOP of $D_1$

The SOP of  $D_1$  can be expressed as [24]:

$$\begin{aligned} SOP_1 &= 1 - \Pr\left(\frac{1+\gamma_{1,2}}{1+\gamma_{E_2}} \geq \zeta_2, \frac{1+\gamma_1}{1+\gamma_{E_1}} \geq \zeta_1\right) \\ &= 1 - \underbrace{\Pr\left(\frac{1+\gamma_{1,2}}{1+\gamma_{E_2}} \geq \zeta_2\right)}_{A_1} \underbrace{\Pr\left(\frac{1+\gamma_1}{1+\gamma_{E_1}} \geq \zeta_1\right)}_{A_2}, \end{aligned} \quad (15)$$

where  $\zeta_i = 2^{2R_i}$ ,  $R_i$  is the target data rate for user  $D_i$ . From (15), we can observe that the variables  $\gamma_{1,2}$  is correlated with  $\gamma_1$ , making exact analysis of  $SOP_1$  intractable. Hence, we focus on the analysis for high SNR regime and adopt the following upper bounds  $\gamma_{1,2} < \frac{\psi_2}{\psi_1}$ . Then, an upper bound of  $A_1$  can be obtained as:

$$\begin{aligned} A_1 &= \Pr\left(\frac{1+\gamma_{1,2}}{1+\gamma_{E_2}} \geq \zeta_2\right) \\ &= \Pr(\gamma_{1,2} \geq \zeta_2 - 1 + \zeta_2 \gamma_{E_2}) \\ &= \Pr(\gamma_{1,2} \geq \zeta_2 + \zeta_2 \gamma_{E_2}) \\ &\approx \Pr\left(\frac{\psi_2}{\psi_1} \geq \zeta_2 + \zeta_2 \psi_2 \rho_e |g_e|^2\right) \\ &\approx 1 - \Pr\left(|g_e|^2 \geq \frac{\psi_2 - \zeta_2 \psi_1}{\zeta_2 \psi_1 \psi_2 \rho_e}\right) \\ &\approx 1 - \exp\left(-\frac{\psi_2 - \zeta_2 \psi_1}{\zeta_2 \psi_1 \psi_2 \rho_e \lambda_e}\right), \end{aligned} \quad (16)$$

where  $\bar{\zeta}_2 = \zeta_2 - 1$ . From (15),  $A_2$  can be obtained as:

$$\begin{aligned} A_2 &= \Pr\left(\frac{1+\gamma_1}{1+\gamma_{E_1}} \geq \zeta_1\right) \\ &= \Pr(\gamma_1 \geq \bar{\zeta}_1 + \zeta_1 \gamma_{E_1}) \\ &= \Pr\left(|g_{bs}|^2 \geq \frac{(\bar{\zeta}_1 + \zeta_1 \psi_1 \rho_e |g_e|^2)(\rho_1 \kappa_1 + 1)}{\psi_1 \rho_1}\right) \\ &= \int_0^\infty \left(1 - F_{|g_{bs}|^2}\left(\frac{(\bar{\zeta}_1 + \zeta_1 \psi_1 \rho_e x)(\rho_1 \kappa_1 + 1)}{\psi_1 \rho_1}\right)\right) f_{|g_e|^2}(x) dx \\ &= \frac{1}{\lambda_e} \exp\left(-\frac{(\rho_1 \kappa_1 + 1) \bar{\zeta}_1}{\psi_1 \rho_1 \lambda_{bs}}\right) \int_0^\infty \exp\left(-\left(\frac{(\rho_1 \kappa_1 + 1) \zeta_1 \rho_e}{\rho_1 \lambda_{bs}} + \frac{1}{\lambda_e}\right)x\right) dx \\ &= \frac{\rho_1 \lambda_{bs}}{(\rho_1 \kappa_1 + 1) \zeta_1 \rho_e \lambda_e + \rho_1 \lambda_{bs}} \exp\left(-\frac{(\rho_1 \kappa_1 + 1) \bar{\zeta}_1}{\psi_1 \rho_1 \lambda_{bs}}\right), \end{aligned} \quad (17)$$

where  $\bar{\zeta}_1 = \zeta_1 - 1$ . Finally, from (16) and (17) into (15), the SOP for  $D_1$  is given by:

$$\begin{aligned} SOP_1 &= 1 - \left[1 - \exp\left(-\frac{\psi_2 - \bar{\zeta}_2 \psi_1}{\zeta_2 \psi_1 \psi_2 \rho_e \lambda_e}\right)\right] \\ &\quad \times \frac{\rho_1 \lambda_{bs}}{(\rho_1 \kappa_1 + 1) \zeta_1 \rho_e \lambda_e + \rho_1 \lambda_{bs}} \exp\left(-\frac{(\rho_1 \kappa_1 + 1) \bar{\zeta}_1}{\psi_1 \rho_1 \lambda_{bs}}\right). \end{aligned} \quad (18)$$

### 3.2. SOP of $D_2$

The SOP of  $D_2$  is written as:

$$\begin{aligned} SOP_2 &= 1 - \Pr\left(\frac{1+\gamma_{1,2}}{1+\gamma_{E_2}} \geq \zeta_2, \frac{1+\gamma_2}{1+\gamma_{E_2}} \geq \zeta_2\right) \\ &= 1 - \underbrace{\Pr\left(\frac{1+\gamma_{1,2}}{1+\gamma_{E_2}} \geq \zeta_2\right)}_{B_1} \underbrace{\Pr\left(\frac{1+\gamma_2}{1+\gamma_{E_2}} \geq \zeta_2\right)}_{B_2}. \end{aligned} \quad (19)$$

From (19),  $B_1$  is calculated similarly to  $A_1$ . On the other hand,  $B_2$  can be obtained as:

$$\begin{aligned} B_2 &= \Pr\left(\frac{1+\gamma_2}{1+\gamma_{E_2}} \geq \zeta_2\right) \\ &= \Pr\left(\gamma_2 \geq \zeta_2 + \zeta_2 \gamma_{E_2}\right) \\ &= \Pr\left(|g_1|^2 \geq \frac{(\zeta_2 + \zeta_2 \psi_2 \rho_e |g_e|^2)(\rho_2 \kappa_2 + 1)}{\rho_2}\right) \\ &= \int_0^\infty \left(1 - F_{|g_1|^2}\left(\frac{(\zeta_2 + \zeta_2 \psi_2 \rho_e x)(\rho_2 \kappa_2 + 1)}{\rho_2}\right)\right) f_{|g_e|^2}(x) dx \\ &= \frac{1}{\lambda_e} \exp\left(-\frac{(\rho_2 \kappa_2 + 1)\zeta_2}{\rho_2 \lambda_1}\right) \int_0^\infty \exp\left(-\left(\frac{(\rho_2 \kappa_2 + 1)\zeta_2 \psi_2 \rho_e}{\rho_2 \lambda_1} + \frac{1}{\lambda_e}\right)x\right) dx \\ &= \frac{\rho_2 \lambda_1}{(\rho_2 \kappa_2 + 1)\zeta_2 \psi_2 \rho_e \lambda_e + \rho_2 \lambda_1} \exp\left(-\frac{(\rho_2 \kappa_2 + 1)\zeta_2}{\rho_2 \lambda_1}\right). \end{aligned} \quad (20)$$

Finally, from (16), (20) into (19), the SOP for  $D_2$  is given by:

$$\begin{aligned} SOP_2 &= 1 - \left[1 - \exp\left(-\frac{\psi_2 - \zeta_2 \psi_1}{\zeta_2 \psi_1 \psi_2 \rho_e \lambda_e}\right)\right] \\ &\quad \times \frac{\rho_2 \lambda_1}{(\rho_2 \kappa_2 + 1)\zeta_2 \psi_2 \rho_e \lambda_e + \rho_2 \lambda_1} \exp\left(-\frac{(\rho_2 \kappa_2 + 1)\zeta_2}{\rho_2 \lambda_1}\right). \end{aligned} \quad (21)$$

## 4. NUMERICAL AND SIMULATION RESULTS

The system parameters in our evaluations are as follows:  $\psi_1 = 0.2$ ,  $R_1 = R_2 = 0.2$  (bps/Hz),  $\kappa_1 = \kappa_2 = 0.001$ ,  $\rho_1 = 30$  (dB),  $\rho_e = 1$  (dB),  $\lambda_{bs} = \lambda_1 = 1$ , and  $\lambda_e = 0.01$ . We assume  $\rho_2 = 0.5\rho_1$ . Monte Carlo simulations are used to verify the performance results.

Figure 2 shows the relationship between SOP and transmit  $\rho_e$ , with different values of  $\psi_1$ . In (18) and (21) are necessary to computed and verified via simulation and the analytical lines can be seen. Furthermore, we notice the gaps between the SOP lines at different intervals of  $\rho_e$ , with  $D_1$  at  $\psi_1 = 0.4$  intersecting  $D_1$  at  $\psi_1 = 0.2$  at about  $\rho_e = 12$  (dB). Also,  $D_1$  at  $\psi_1 = 0.4$  and  $D_2$  at  $\psi_1 = 0.4$  at  $\rho_e = 10$  (dB) start to deteriorate rapidly and converge at  $\rho = 15$  (dB). It can be observed from Figure 2, the SOP of  $D_1$  and  $D_2$  become weaker with the increase in  $\rho_e$  regardless of the value of  $\psi_1$ . The reason being that as  $\rho_e$  increases beyond 15 (dB) the capacity of eavesdropper channel  $C_{E_i}$  in (11) also increases, thus, reducing the secrecy capacity  $C_i$  in (12).

Figure 3 highlights the relationship between SOP and transmit  $\rho_2$ , with different values of  $\kappa_1 = \kappa_2$ . In (18) and (21) are used to obtain the analytical lines. From Figure 3, we see that increasing  $\rho_2$  improves the SOP regardless of the values of  $\kappa_1 = \kappa_2$ . This is due to the capacity of the eavesdropper channel  $C_{E_i}$  in (11) decreasing, thereby, improving the secrecy capacity  $C_i$  in (12). We also observe that increasing  $\kappa_1 = \kappa_2$  from 0.001 to 0.005 improves the SOP of  $D_1$  and  $D_2$  significantly.  $D_2$  at  $\kappa_1 = \kappa_2 = 0.001$  has the best SOP performance compared to the other lines, because the residual interference at  $D_2$  is less than  $D_1$  as it further away from the base station. We also observe that the SOP of  $D_1$  at  $\kappa_1 = \kappa_2 = 0.001$  and  $D_2$  at  $\kappa_1 = \kappa_2 = 0.005$  converge at  $\rho_e = 40$  (dB), highlighting the impact of residual interference on SOP for both  $D_1$  and  $D_2$ .

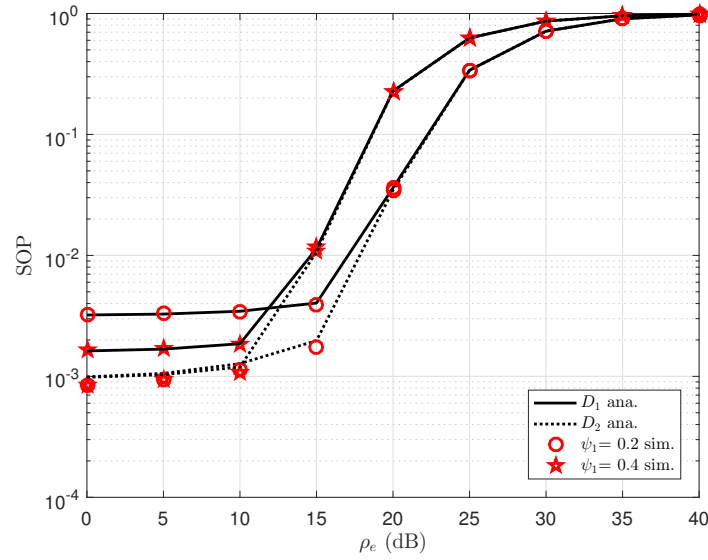
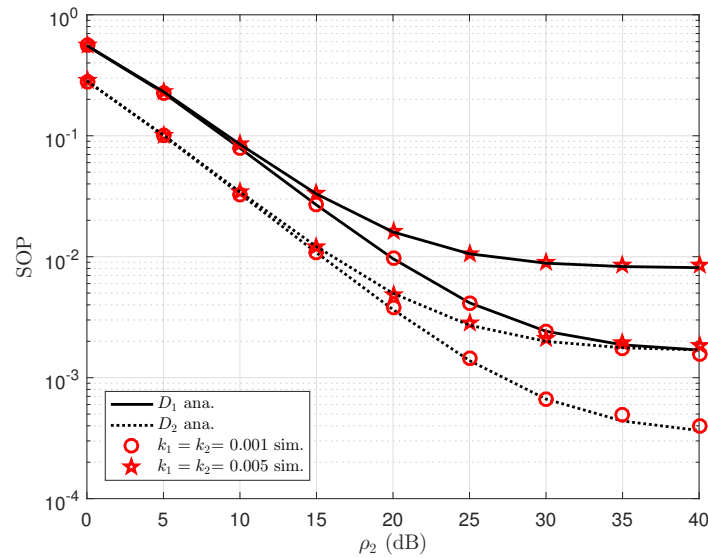
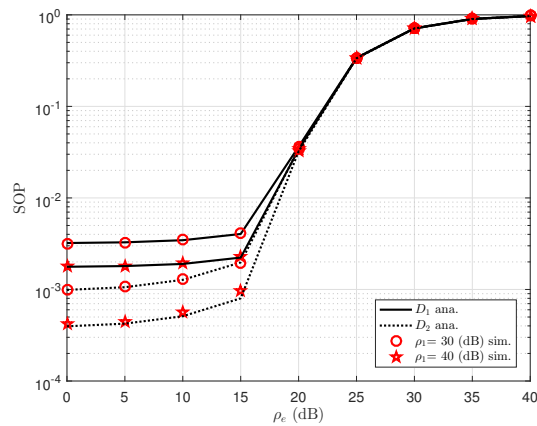
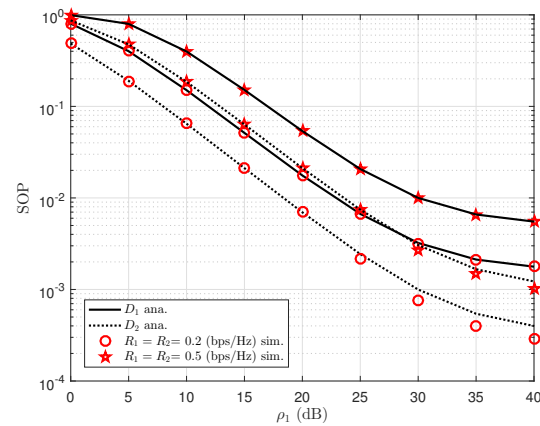
Figure 2. SOP vs transmit  $\rho_e$  with different  $\psi_1$ Figure 3. SOP vs transmit  $\rho_2$  with different  $\kappa_1 = \kappa_2$ 

Figure 4 demonstrates the relationship between SOP and transmit  $\rho_e$ , with different values of  $\rho_1$ . In (18) and (21) are used to obtain the analytical lines. From Figure 4, we observe that increasing  $\rho_1$  weakens the SOP of both  $D_1$  and  $D_2$ . This is due to the capacity of the eavesdropper channel  $C_{E_i}$  in (11) increasing, thus, decreasing the secrecy capacity  $C_i$  in (12). We also observe the convergence of the different SOP lines at  $\rho_e = 20dB$ , demonstrating that after this dB value,  $D_1$  and  $D_2$  lose any benefits of a change in transmit  $\rho_1$  value.

Figure 5 depicts the relationship between SOP and transmit  $\rho_1$ , with different values of  $R_1 = R_2$ . In (18) and (21) are used to obtain the analytical lines. From Figure 5, we visualize that increasing  $\rho_1$  improves the SOP of both  $D_1$  and  $D_2$ . We also observe the intersection of the SOP of  $D_1$  at  $R_1 = R_2 = 0.2bps/Hz$  line and the SOP of  $D_2$  at  $R_1 = R_2 = 0.5bps/Hz$  at  $\rho_1 = 30dB$ . Figure 5 demonstrates the impact of target rate  $R_1$  and  $R_2$  on SOP.

Figure 4. SOP vs transmit  $\rho_e$  with different  $\rho_1$ Figure 5. SOP vs transmit  $\rho_1$  with different  $R_1 = R_2$ 

## 5. MAIN FINDINGS ANALYSIS AND CONCLUSION

We have demonstrated how secrecy outage probability is necessary to evaluate secure performance of a device-to-device IoT network with power-domain NOMA assistance. We also derived expressions of secrecy outage probability for different users. Our results showed the secrecy outage performance of the IoT network users under different network conditions such as power allocation variation, residual interference, transmitter interference, and target data rate changes. Finally, simulation results verified the correctness of the formulated results and proved that the inherent characteristics of power-domain NOMA can secure downlink device-to-device IoT-NOMA networks against eavesdroppers.





## REFERENCES

- [1] Z. Xiang, W. Yang, Y. Cai, Z. Ding, Y. Song, and Y. Zou, "NOMA-Assisted Secure Short-Packet Communications in IoT," in *IEEE Wireless Communications*, vol. 27, no. 4, pp. 8–15, Aug. 2020, doi: 10.1109/MWC.01.1900529.
- [2] B. Ji, Y. Li, D. Cao, C. Li, S. Mumtaz, and D. Wang, "Secrecy Performance Analysis of UAV Assisted Relay Transmission for Cognitive Network With Energy Harvesting," in *IEEE Transactions on Vehicular Technology*, vol. 69, no. 7, pp. 7404–7415, Jul. 2020, doi: 10.1109/TVT.2020.2989297.
- [3] X. Li et al., "Physical Layer Security of Cooperative NOMA for IoT Networks Under I/Q Imbalance," *IEEE Access*, vol. 8, pp. 51189–51199, 2020, doi: 10.1109/ACCESS.2020.2980171.
- [4] K. Chandra, A. S. Marciano, S. Mumtaz, R. V. Prasad, and H. L. Christiansen, "Unveiling Capacity Gains in Ultradense Networks: Using mm-Wave NOMA," in *IEEE Vehicular Technology Magazine*, vol. 13, no. 2, pp. 75–83, Jun. 2018, doi: 10.1109/MVT.2018.2814822.
- [5] D.-T. Do, Anh-Tu Le, Y. Liu, and A. Jamalipour, "User Grouping and Energy Harvesting in UAV-NOMA System with AF/DF Relaying," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 11, pp. 11855–11868, Nov. 2021, doi: 10.1109/TVT.2021.3116101.
- [6] D.-T. Do, M.-S. V. Nguyen, M. Voznak, A. Kwasinski, and J. N. de Souza, "Performance Analysis of Clustering Car-Following V2X System with Wireless Power Transfer and Massive Connections," *IEEE Internet of Things Journal*, 2021, doi: 10.1109/IJOT.2021.3070744.
- [7] D.-T. Do, C.-B. Le, and F. Afghah, "Enabling Full-Duplex and Energy Harvesting in Uplink and Downlink of Small-Cell Network Relying on Power Domain Based Multiple Access," *IEEE Access*, vol. 8, pp. 142772–142784, doi: 10.1109/ACCESS.2020.3013912.
- [8] D.-T. Do, T.-T. T. Nguyen, C.-B. Le, M. Voznak, Z. Kaleem, and K. M. Rabie, "UAV Relaying Enabled NOMA Network with Hybrid Duplexing and Multiple Antennas," *IEEE Access*, vol. 8, pp. 186993–187007, 2020, doi: 10.1109/ACCESS.2020.3030221.
- [9] Z. Ding, X. Lei, G. K. Karagiannis, 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, doi: 10.1109/JSAC.2017.2725519.
- [10] M. Vaezi, Z. Ding, and H. V. Poor, eds *Multiple access techniques for 5G wireless networks and beyond*, Cham: Springer, vol. 159, 2019, doi: 10.1007/978-3-319-92090-0.
- [11] X. Li, J. Li, Y. Liu, Z. Ding, and A. Nallanathan, "Residual Transceiver Hardware Impairments on Cooperative NOMA Networks," in *IEEE Transactions on Wireless Communications*, vol. 19, no. 1, pp. 680–695, Jan. 2020, doi: 10.1109/TWC.2019.2947670.
- [12] X. Li et al., "Hardware Impaired Ambient Backscatter NOMA System: Reliability and Security," in *IEEE Transactions Communications*, vol. 69, no. 4, pp. 2723–2736, Apr. 2021, doi: 10.1109/TCOMM.2021.3050503.
- [13] I. Budhiraja, N. Kumar, S. Tyagi, S. Tanwar and M. S. Obaidat, "URJA: Usage Jammer as a Resource Allocation for Secure Transmission in a CR-NOMA-Based 5G Femtocell System," *IEEE Systems Journal*, vol. 15, no. 2, pp. 1776–1785, June 2021, doi: 10.1109/JSYST.2020.2999474.





- [14] X. Li, M. Zhao, Y. Liu, L. Li, Z. Ding, and A. Nallanathan, "Secrecy Analysis of Ambient Backscatter NOMA Systems under I/Q Imbalance," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 10, pp. 12286–12290, Oct. 2020, doi: 10.1109/TVT.2020.3006478.
- [15] X. Li *et al.*, "Cooperative Wireless-Powered NOMA Relaying for B5G IoT Networks With Hardware Impairments and Channel Estimation Errors," in *IEEE Internet of Things Journal*, vol. 8, no. 7, pp. 5453–5467, Apr. 2021, doi: 10.1109/JIOT.2020.3029754.
- [16] W. Khalid and H. Yu, "Security Improvement With QoS Provisioning Using Service Priority and Power Allocation for NOMA-IoT Networks," in *IEEE Access*, vol. 9, pp. 9937–9948, 2021. doi: 10.1109/ACCESS.2021.3049258.
- [17] H. Li *et al.*, "Secrecy Outage Probability of Relay Selection Based Cooperative NOMA for IoT Networks," in *IEEE Access*, vol. 9, pp. 1655–1665, 2021, doi: 10.1109/ACCESS.2020.3047136.
- [18] Z. Xiang, W. Yang, Y. Cai, J. Xiong, Z. Ding, and Y. Song, "Secure Transmission in a NOMA-Assisted IoT Network With Diversified Communication Requirements," *IEEE Internet of Things Journal*, vol. 7, no. 11, pp. 11157–11169, Nov. 2020. doi: 10.1109/JIOT.2020.2995609.
- [19] X. Yue, Y. Liu, Y. Yao, X. Li, R. Liu, and A. Nallanathan, "Secure Communications in a Unified Non-Orthogonal Multiple Access Framework," *IEEE Transactions on Wireless Communications*, vol. 19, no. 3, pp. 2163–2178, Mar. 2020, doi: 10.1109/TWC.2019.2963181.
- [20] M. Li, H. Yuan, X. Yue, S. Muhaidat, C. Maple, and M. Dianati, "Secrecy Outage Analysis for Alamouti Space-Time Block Coded Non-Orthogonal Multiple Access," *IEEE Communications Letters*, vol. 24, no. 7, pp. 1405–1409, Jul. 2020, doi: 10.1109/LCOMM.2020.2980825.
- [21] Q. Li, P. Ren, and D. Xu, "Security Enhancement and QoS Provisioning for NOMA-Based Cooperative D2D Networks," *IEEE Access*, vol. 7, pp. 129387–129401, 2019, doi: 10.1109/ACCESS.2019.2939783.
- [22] A. Kilzi, J. Farah, C. A. Nour, and C. Douillard, "Optimal Resource Allocation for Full-Duplex IoT Systems Underlying Cellular Networks with Mutual SIC NOMA," *IEEE Internet of Things Journal*, vol. 8, no. 24, pp. 17705–17723, 15 Dec. 15, 2021, doi: 10.1109/JIOT.2021.3082428.
- [23] W. Duan, Y. Ji, J. Hou, B. Zhuo, M. Wen, and G. Zhang, "Partial-DF Full-Duplex D2D-NOMA Systems for IoT With/Without an Eavesdropper," *IEEE Internet of Things Journal*, vol. 8, no. 8, pp. 6154–6166, Apr. 2021, doi: 10.1109/JIOT.2020.3034271.
- [24] S. Arzykulov, T. A. Tsiftsis, G. Nauryzbayev, and M. Abdallah, "Outage Performance of Cooperative Underlay CR-NOMA With Imperfect CSI," *IEEE Communications Letters*, vol. 23, no. 1, pp. 176–179, Jan. 2019, doi: 10.1109/LCOMM.2018.2878730.
- [25] 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, doi: 10.1109/TVT.2017.2789223.

## BIOGRAPHIES OF AUTHORS



**Dinh-Thuan Do**     (Senior Member, IEEE) received the M.Eng., and Ph.D. degrees in communications engineering from Vietnam National University (VNU-HCM), in 2007 and 2013, respectively. His research interests include signal processing in wireless communications networks, cooperative communications, non-orthogonal multiple access, full-duplex transmission, and energy harvesting. He has served as a guest editor for eight prominent SCIE journals. He can be contacted at email: dodinhthuan@iuh.edu.vn and dodinhthuan@gmail.com.



**Minh-Sang Van Nguyen**     was born in Ben Tre, Vietnam. He received a B.S. from the Industrial University of Ho Chi Minh City (IUH) in 2019. He is currently pursuing the master's degree in wireless communications. He has worked with the Industrial University of Ho Chi Minh City, Vietnam. He has authored or co-authored over 22 technical papers published in peer-reviewed international journals (SCIE), one book chapter and one conference paper. His research interests include electronic design, signal processing in wireless communications networks, non-orthogonal multiple access, reconfigurable intelligent surfaces and physical layer security. He was a reviewer for WCNC conferences, IEEE access, international journal of electronics, eurasip journal on wireless communications and networking. He can be contacted at email: nguyenvanminhsang@iuh.edu.vn.