JTE HCMUTE
ISSN: 2615-9740

JOURNAL OF TECHNICAL EDUCATION SCIENCE
Ho Chi Minh City University of Technology and Education
Website: https://jte.edu.vn
Email: jte@hcmute.edu.vn

An Application of Physical Layer Security to Protect NOMA-Backscatter Communication

Truc Thanh Tran[1*], Diem-Phuc Tran[2]
[1]*Greenwich Vietnam, FPT University, Vietnam*
[2]*Duy Tan University, Vietnam*

[*]Corresponding author. *Email: tructt16@fe.edu.vn*

ARTICLE INFO

Received: 23/11/2024
Revised: 02/04/2025
Accepted: 15/05/2025
Published: 28/08/2025

KEYWORDS

NOMA;
Physical Layer Security;
Backscatter communication;
Baseband Signal Processing;
5G Technology.

ABSTRACT

This paper explores the enhancement of physical layer security in a communication model that integrates backscatter communication and Non-Orthogonal Multiple Access (NOMA) technology. The system involves two users sharing a common receiver, with a potential eavesdropper attempting to intercept the transmission. The study incorporates Rayleigh fading in backscatter channels and derives the theoretical probability of secure transmission capacity, providing a framework for analyzing security performance. To validate the theoretical results, Monte Carlo simulations are conducted, showing strong consistency between theoretical predictions and simulated outcomes. This research highlights the potential of combining backscatter communication with NOMA to improve data security and transmission efficiency, particularly in wireless environments prone to adversarial threats. The findings contribute to the understanding of how these technologies can work together to enhance security in next-generation communication systems, such as IoT and 5G networks, where secure and energy-efficient data transmission is critical. The paper offers new insights into physical layer security techniques and provides a foundation for future research in secure communication models involving emerging technologies.

Doi: https://doi.org/10.54644/jte.2025.1732

1. Introduction

Non-Orthogonal Multiple Access (NOMA) and backscatter communication are emerging technologies that play a critical role in advancing modern wireless communication systems. By addressing the challenges of spectrum efficiency, user connectivity, and energy efficiency, these technologies offer innovative solutions for next-generation networks, including the Internet of Things (IoT) and 5G ecosystems [1] – [4], [15].

NOMA enhances spectrum utilization by enabling multiple users to share the same time and frequency resources. Instead of assigning orthogonal resources as in traditional schemes, NOMA distinguishes users through power domain multiplexing, leveraging superposition coding at the transmitter and successive interference cancellation (SIC) at the receiver. This approach not only improves spectral efficiency but also facilitates better connectivity and fairness among users with varying channel conditions. Despite its potential, integrating NOMA into existing communication systems involves challenges such as managing inter-user interference, ensuring security, and increasing receiver complexity [1] – [4].

Backscatter communication is a low-power wireless communication technique that has gained attention for its ability to enable sustainable and energy-efficient networking. Unlike conventional systems that actively generate radio frequency (RF) signals, backscatter communication reflects existing RF signals to transmit data. This makes it an ideal choice for ultra-low-power applications, particularly in IoT, where energy-constrained devices need to communicate over extended periods [5], [6]. Backscatter communication systems typically involve three key entities: a source generating the RF signal, a backscatter device modulating the signal to encode data, and a receiver decoding the modulated signal. While energy efficiency is a significant advantage, backscatter communication faces challenges

JTE
HCMUTE
ISSN: 2615-9740

JOURNAL OF TECHNICAL EDUCATION SCIENCE
Ho Chi Minh City University of Technology and Education
Website: https://jte.edu.vn
Email: jte@hcmute.edu.vn

such as limited data rates, reliability under varying channel conditions, and vulnerability to security threats like eavesdropping [7] – [9].

With the rise of dense communication in 5G and beyond, wireless networks are becoming increasingly susceptible to unauthorized access and wiretapping by malicious nodes. The shared and open nature of wireless channels exacerbates the risk of information leakage, making physical layer security a critical concern. These challenges have triggered significant research into ensuring secure communication in new communication models, particularly those involving innovative technologies such as NOMA and backscatter communication. This pressing needs to address the vulnerabilities of dense wireless communication systems forms the primary motivation for this work [10] – [15].

This research is driven by the question: ***How can we evaluate the capacity of secure transmission in a communication model combining NOMA and backscatter communication?*** To address this, we begin with a simplified and commonly encountered fading scenario: slow Rayleigh fading. By focusing on this case, we aim to derive theoretical insights into the secure transmission capacity under realistic channel conditions and validate these findings through Monte Carlo simulations.

This paper investigates physical layer security in a NOMA-backscatter communication model involving two users and a common receiver, potentially wiretapped by an eavesdropper. In the proposed system, two transmitter devices employ backscatter technology to both save power and transmit data to the same receiver. By analyzing the system under slow Rayleigh fading, we compute the theoretical probability of secure transmission capacity and compare it with simulation results. This work highlights the potential of combining NOMA and backscatter communication to achieve secure and efficient wireless communication in next-generation networks.

The paper is structured as follows. The next section introduces the system model, detailing the wireless communication framework with NOMA and backscatter technology. Following this, the performance analysis derives theoretical expressions for secure transmission capacity under the proposed model. Numerical and simulation results are then presented to visualize and validate the findings, accompanied by a discussion of their implications. Finally, the conclusion highlights the key achievements of this research and suggests directions for future work.

2. System Model

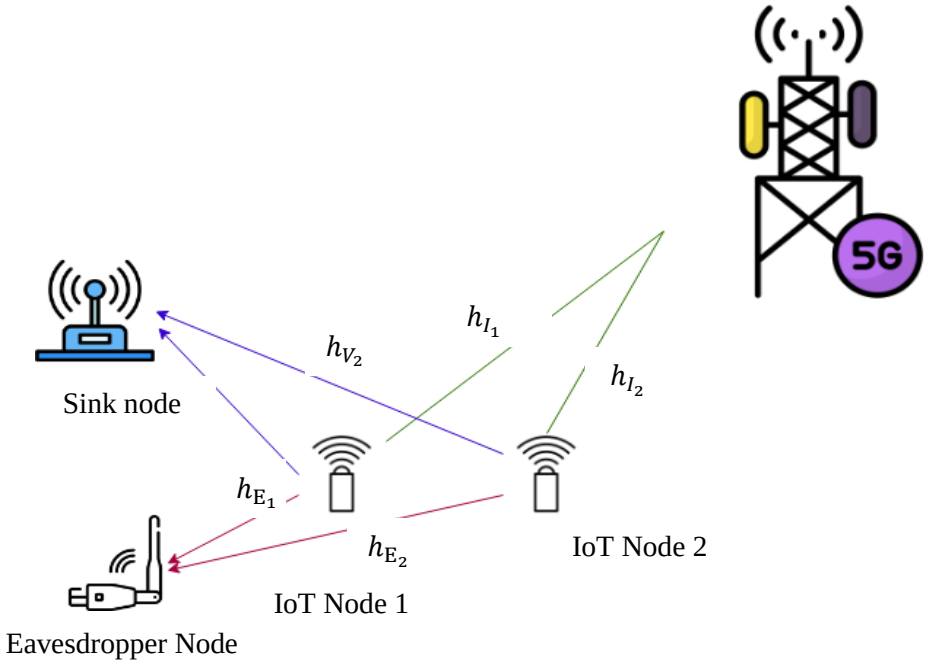

Figure 1. *System Model*

The proposed network is depicted in Figure 1 which consists of an RF station **I**, two NOMA-enabled IoT devices $\mathbf{V}_n$ where $n = \{1,2\}$, and a passive eavesdropper **E** . All devices operate in half-duplex mode and are equipped with single antennas. The RF station provides RF signals to the IoT devices for task offloading, while the passive eavesdropper attempts to intercept the transmitted information.

The channel coefficients for the links **I** $\rightarrow \mathrm{V}_n$, $\mathrm{V}_n \rightarrow \mathrm{V}_S$, and $\mathrm{V}_n \rightarrow$ E are denoted as h_{I_n}, h_{V_n}, and h_{E_n}, respectively. The transmitted signal from **I** interferes with the backscattered signal at the vehicles; however, perfect successive interference cancellation (pSIC) at the receiver ensures that this interference is eliminated.

The received signal at the IoT sink node S is given by:

$$y_{\mathrm{S}} = \sqrt{\frac{\varepsilon_1 \rho P_0}{\left(d_{\mathrm{I}_1} d_{\mathrm{V}_1}\right)^{\alpha}}} \epsilon_1 h_{\mathrm{I}_1} h_{\mathrm{V}_1} s_1 + \sqrt{\frac{\varepsilon_2 (1-\rho) P_0}{\left(d_{I_2} d_{V_2}\right)^{\alpha}}} \epsilon_2 h_{\mathrm{I}_2} h_{\mathrm{V}_2} s_2 + n_{\mathrm{S}} \tag{1}$$

and the received signal at the eavesdropper E is expressed as:

$$y_{\mathrm{E}} = \sqrt{\frac{\varepsilon_1 \rho P_0}{\left(d_{\mathrm{I}_1} d_{\mathrm{E}_1}\right)^{\alpha}}} \epsilon_1 h_{\mathrm{I}_1} h_{\mathrm{E}_1} s_1 + \sqrt{\frac{\varepsilon_2 (1-\rho) P_0}{\left(d_{I_2} d_{V_2}\right)^{\alpha}}} \epsilon_2 h_{\mathrm{I}_2} h_{\mathrm{E}_2} s_2 + n_{\mathrm{E}} \tag{2}$$

where:

- P_0 is the transmit power of I,
- ε_n $(0 \leq \varepsilon_n \leq 1)$ represents the backscattering reflection coefficient,
- ϵ_n, $\epsilon_n \in \{0,1\}$ denotes the transmitted data bit,
- h_{I_n}, h_{V_n}, and h_{E_n} are the distances from **I** $\rightarrow \mathrm{V}_n$, $\mathrm{V}_n \rightarrow \mathrm{V}_S$, and $\mathrm{V}_n \rightarrow$ E, respectively,
- n_{S} and n_{E} are the AWGN noise components, modeled as $n_{\mathrm{S}}, n_{\mathrm{E}} \sim (0,1)$ respectively.

The SINRs at S and E are expressed as follows. For the n-th IoT (V_n) at S:

$$\gamma_{\mathrm{V}_1} = \frac{\frac{\varepsilon_1 \rho\, \gamma_0}{\left(d_{\mathrm{I}_1} d_{\mathrm{V}_1}\right)^{\alpha}} \left|h_{\mathrm{I}_1}\right|^2 \left|h_{\mathrm{V}_1}\right|^2}{\frac{\varepsilon_2 (1-\rho)\, \gamma_0}{\left(d_{\mathrm{I}_2} d_{\mathrm{V}_2}\right)^{\alpha}} \left|h_{\mathrm{I}_2}\right|^2 \left|h_{\mathrm{V}_2}\right|^2 + 1} \tag{3}$$

Assume that $\rho > 0.5$, which indicates that the power allocated to signal s_1 is greater than that allocated to signal s_2.The decoding process employs successive interference cancellation (SIC), where s_2 is decoded after successfully canceling the interference from s_1.

$$\gamma_{\mathrm{V}_2} = \frac{\varepsilon_2 (1-\rho)\, \gamma_0}{\left(d_{\mathrm{I}_2} d_{\mathrm{V}_2}\right)^{\alpha}} \left|h_{\mathrm{I}_2}\right|^2 \left|h_{\mathrm{V}_2}\right|^2 \tag{4}$$

Similarly, at the eavesdropper (E):

$$\gamma_{\mathrm{E}_1} = \frac{\frac{\varepsilon_1 \rho\, \gamma_{\mathrm{E}}}{\left(d_{\mathrm{I}_1} d_{\mathrm{E}_1}\right)^{\alpha}} \left|h_{\mathrm{I}_1}\right|^2 \left|h_{\mathrm{E}_1}\right|^2}{\frac{\varepsilon_2 (1-\rho)\, \gamma_{\mathrm{E}}}{\left(d_{\mathrm{I}_2} d_{\mathrm{E}_2}\right)^{\alpha}} \left|h_{\mathrm{I}_2}\right|^2 \left|h_{\mathrm{E}_2}\right|^2 + 1} \tag{5}$$

$$\gamma_{\mathrm{E}_2} = \frac{\varepsilon_2 (1-\rho)\, \gamma_{\mathrm{E}}}{\left(d_{\mathrm{I}_2} d_{\mathrm{E}_2}\right)^{\alpha}} \left|h_{\mathrm{I}_2}\right|^2 \left|h_{\mathrm{E}_2}\right|^2 \tag{6}$$

To simplify the complexity of the SINR expressions, we define the a_1, a_2, b_1 and b_2 as follows:

$$a_1 = \frac{\varepsilon_1 \rho\, \gamma_0}{\left(d_{\mathrm{I}_1} d_{\mathrm{V}_1}\right)^{\alpha}} \tag{7}$$

$$b_1 = \frac{\varepsilon_2 (1-\rho)\, \gamma_0}{\left(d_{\mathrm{I}_2} d_{\mathrm{V}_2}\right)^{\alpha}} \tag{8}$$

$$a_2 = \frac{\varepsilon_1 \rho\, \gamma_{\mathrm{E}}}{\left(d_{\mathrm{I}_1} d_{\mathrm{E}_1}\right)^{\alpha}} \tag{9}$$

$$b_2 = \frac{\varepsilon_2 (1-\rho)\, \gamma_{\mathrm{E}}}{\left(d_{\mathrm{I}_2} d_{\mathrm{E}_2}\right)^{\alpha}} \tag{10}$$

To further simplify the expressions, we introduce the variables X_1, X_2, Y_1, Y_2, Z_1 and Z_2 representing the squared magnitudes of the respective channel coefficients:

$$X_n = \left|h_{\mathrm{I}_n}\right|^2, Y_n = \left|h_{\mathrm{V}_n}\right|^2, Z_n = \left|h_{\mathrm{E}_n}\right|^2 \text{ for } n \in \{1,2\} \tag{11}$$

These variables follow independent Rayleigh fading distributions. Using these definitions, the SINRs can be reformulated in terms of X_1, X_2, Y_1, Y_2, Z_1 and Z_2 significantly simplifying the mathematical expressions and subsequent analysis. The probability density function (PDF) for each variable is given by:

$$f_U(x) = \frac{1}{\lambda_U} \exp\left(-\frac{x}{\lambda_U}\right) \tag{12}$$

where $U \in \{X_1, X_2, Y_1, Y_2, Z_1, Z_2\}$ and λ_U is the mean of the corresponding exponential distribution. Typically, $\lambda_U = \mathbb{E}[U]$, which represents the average power of the respective channel. If the channels are normalized, we can assume $\lambda_U = 1$, simplifying the PDF to:

$$f_U(x) = \exp(-x), x \geq 0 \tag{13}$$

The transmission rate threshold is the minimum data rate required for reliable communication in the system. It serves as a benchmark to determine the efficiency of the transmission link, ensuring the data rate meets the system's performance requirements.

For the n-th IoT device (V_n), the transmission rate threshold is denoted as $R_s^{[n]}$ which is the minimum data rate required for successful task offloading. It is expressed in terms of the desired transmission efficiency.

3. Performance Analysis

3.1. Capacity at the Receiver

The capacity at the legitimate receiver (e.g., IoT sink node S) for the n-th IoT (V_n) is determined by the SINR γ_{V_n} of the legitimate channel. Using the Shannon capacity formula, the instantaneous capacity at the receiver is given by:

$$C_0^{[n]} = B \log_2\left(1 + \gamma_{\mathrm{V}_n}\right) \tag{14}$$

where:

- B is the channel bandwidth (Hz),
- γ_{V_n} is the SINR of the legitimate channel between the n-th vehicle and the IoT sink node.

This capacity represents the maximum achievable data rate under the current channel conditions for secure and reliable communication.

3.2. Capacity at the Eavesdropper

Similarly, the capacity at the eavesdropper E for the n-th IoT is determined by the SINR γ_{E_n} of the eavesdropper's channel. The instantaneous capacity at the eavesdropper is expressed as:

$$C_e^{[n]} = B \log_2\left(1 + \gamma_{\mathrm{E}_n}\right) \tag{15}$$

where:

- B is the channel bandwidth (Hz),
- γ_{E_n} is the SINR of the legitimate channel between the n-th vehicle and the IoT sink node.

This capacity quantifies the potential data rate the eavesdropper can achieve under current conditions, representing the vulnerability of the communication link.

3.3. The Secure Capacity

The secure capacity quantifies the rate at which confidential information can be transmitted reliably, ensuring that the eavesdropper cannot decode the information. It is defined as the non-negative difference between the capacity at the legitimate receiver and the capacity at the eavesdropper.

For the n-th IoT device V_n, the secure capacity $C_s^{[n]}$is expressed as:

$$C_s^{[n]} = \left[C_0^{[n]} - C_e^{[n]}\right]^+ \tag{16}$$

where $[x]^+ = \max(x, 0)$ ensures that the secure capacity is non-negative. If the legitimate channel capacity $C_s^{[n]}$ exceeds the eavesdropper's capacity $C_e^{[n]}$, then secure communication is possible, and $C_s^{[n]} > 0$. Otherwise, secure communication is not achievable, and $C_s^{[n]} = 0$.

In secure communication systems, ensuring that the data transmission rate meets a target transmission rate while remaining secure is a critical challenge. This involves satisfying conditions that maintain both reliability for the legitimate receiver and confidentiality against an eavesdropper.

To ensure secure communication at a target transmission rate $R_s^{[n]}$, the system must satisfy:

$$C_s^{[n]} = \left[C_0^{[n]} - C_e^{[n]}\right]^+ \geq R_s^{[n]} \tag{17}$$

This condition ensures that the legitimate channel is not only reliable but also capable of maintaining a secure data rate that the eavesdropper cannot decode.

If the secrecy capacity does not satisfy the target rate condition, $C_s^{[n]} < R_s^{[n]}$, the system fails to ensure secure communication at the desired transmission rate. This failure may occur under the following conditions:

- The quality of the legitimate channel deteriorates, leading to a low SINR for the legitimate receiver γ_{V_n}.
- The quality of the eavesdropper's channel improves, resulting in a high SINR for the eavesdropper γ_{E_n}

To address such scenarios, adaptive strategies can be employed, including reducing the target transmission rate $R_s^{[n]}$, increasing the transmit power, or enhancing the channel conditions through techniques such as relay-assisted communication or advanced channel coding. These measures aim to restore secure communication by ensuring that the secrecy condition is satisfied.

3.4. Probability of secure transmission

The probability of secure transmission quantifies the likelihood that the secrecy capacity of a communication system meets or exceeds the target transmission rate $R_s^{[n]}$. It is a critical metric for evaluating the security performance of a system under stochastic channel conditions.

The probability of secure transmission for the n-th IoT signal, denoted as $\Phi_s^{[n]}$, is defined as the probability that the secure capacity satisfies the target transmission rate $C_s^{[n]}$. Mathematically, it is expressed as:

$$\Phi_s^{[n]} = \Pr\left(C_s^{[n]} \geq R_s^{[n]}\right) \tag{18}$$

Substituting the definition of secure capacity:

$$\Phi_s^{[n]} = \Pr\left(C_0^{[n]} - C_e^{[n]} \geq R_s^{[n]}\right) \tag{19}$$

The secrecy condition can then be rewritten as:

$$\Phi_s^{[n]} = \Pr\left(B\log_2\left(1+\gamma_{\mathrm{V}_n}\right) - B\log_2\left(1+\gamma_{\mathrm{E}_n}\right) \geq R_s^{[n]}\right) \tag{20}$$

Simplifying further:

$$\Phi_s^{[n]} = \Pr\left(\frac{1+\gamma_{\mathrm{V}_n}}{1+\gamma_{\mathrm{E}_n}} \geq 2^{R_s^{[n]}/B}\right) \tag{21}$$

3.5. Probability of secure transmission

This section focuses on deriving the expression for the probability of secure transmission, which quantifies the likelihood that the secrecy condition is satisfied for a given target transmission rate.

The computation of $\Phi_s^{[1]}$ the probability of secure transmission for s_1 , is performed in Appendix A and showing the result as follows:

$$\begin{aligned}\Phi_s^{[1]} &= \mathbb{E}_U\left[\frac{b_2}{b_2+w_2a_2u}\right. \\ &\left. + \frac{a_1a_2u^2w_2\left(-1+\frac{a_1}{b_1}u-\frac{w_2a_2}{b_2}u+\left(1+\frac{w_2a_2}{b_2}u\right)\log\left(\frac{b_1\left(1+\frac{w_2a_2}{b_2}u\right)}{a_1u}\right)\right)}{b_1b_2\left(1+\frac{w_2a_2}{b_2}u\right)\left(-1+\frac{a_1}{b_1}u-\frac{w_2a_2}{b_2}u\right)^2}\right]\end{aligned} \tag{22}$$

The computation of $\Phi_s^{[2]}$ the probability of secure transmission for s_2 , is performed in Appendix B and showing the result as follows:

$$\Phi_s^{[2]} = \mathbb{E}_{\mathrm{X}_2}\left[\frac{b_1}{b_1+b_2w_1}\exp\left(-\frac{w_1-1}{b_1x_2}\right)\right] \tag{23}$$

4. Numerical and Simulation Results and Discussion

The simulation environment is configured to evaluate the system performance under realistic and controlled conditions. The free pathloss coefficient is set to $\alpha = 2$, and the carrier frequency is chosen as $f_c = 1$ GHz. A system bandwidth of $B = 1$MHz is used to ensure sufficient spectrum allocation for communication.

The base station is located at the origin, $[0, 0, 0]$, with a transmit power spectral density of 10^{-7} mW/Hz. Two reflectors (IoT users) are considered in the simulation, positioned at $[100, 0, 0]$, with identical reflection coefficients of 0.1. The target secrecy rate for each user is set to 10 kbps.

The receiver is placed at $(120,0,0)$ and operates under a noise power spectral density (PSD) of 3.98×10^{-18} mW/Hz. Similarly, the eavesdropper (EVE) is located at$(110,0,0)$ with a noise power of 3.98×10^{-18} mW/Hz.

These simulation parameters, as shown in Table 1, provide a well-defined framework for analyzing the system's secrecy performance, enabling the evaluation of the impact of pathloss, noise, reflection, and interference under realistic operating conditions.

Table 1. *Simulation parameters*

Parameters	Values
Free pathloss coefficient	$\alpha = 2$
Carrier frequency	1 GHz
Bandwidth	$B = 1$MHz
Transmit Power Spectral Density	10^{-7} mW/Hz
Base Station Locations	(0,0,0)
Number of reflector	$K = 2$
Locations of reflectors	(100,0,0); (100,0,0);
Reflect coefficients	$\varepsilon_1 = \varepsilon_2 = 0.1$
Target Secrecy Rate	$R_s^{[1]} = R_s^{[2]} = 10$ kbps
Receiver Locations	(120,0,0)
Noise PSD of Receiver	3.98×10^{-18} mW/Hz
Eavesdropper Locations	(110,0,0)
Noise PSD of Eavesdropper	3.98×10^{-18} mW/Hz

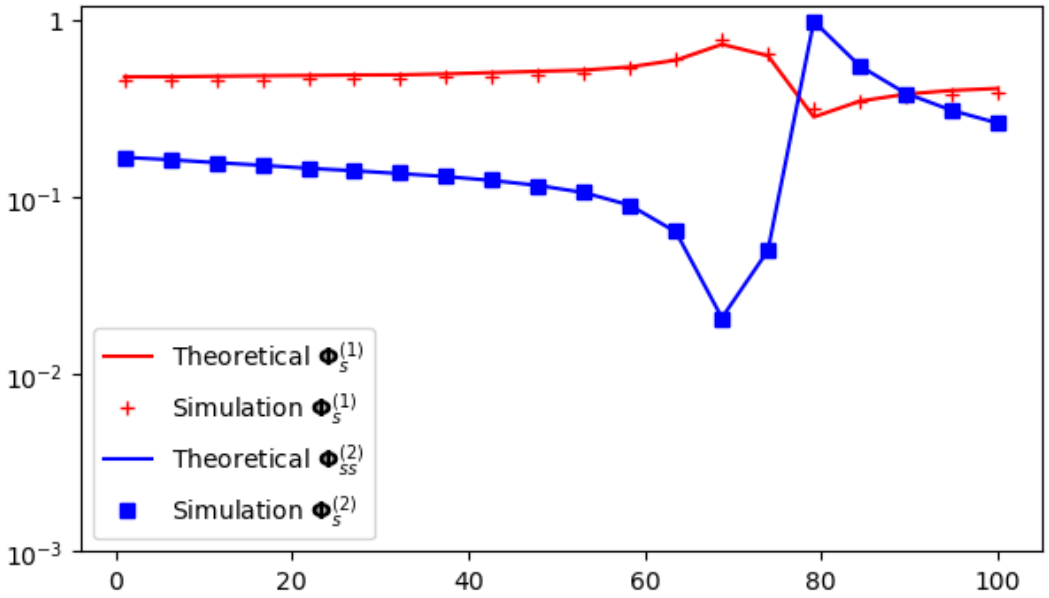

Figure 2. *Secrecy rate versus changes in positions of the IoT devices*

Figure 2 presents the probability of secure transmission $\Phi_s^{[1]}$ and $\Phi_s^{[2]}$as a function of the positions of the reflectors (IoT devices). The x-axis represents the reflectors' positions, while the y-axis, displayed on a logarithmic scale, indicates the secure transmission probability. Theoretical results are shown as solid lines, while simulation outcomes are represented by markers. The red curves and markers correspond to the first reflector $\Phi_s^{[1]}$, and the blue curves and markers represent the second reflector $\Phi_s^{[2]}$.

The results demonstrate a strong consistency between theoretical predictions and simulation data for both reflectors, validating the accuracy of the analytical model. Across the range of positions, the first reflector $\Phi_s^{[1]}$ exhibits a consistently higher secure transmission probability compared to the second reflector $\Phi_s^{[2]}$. This indicates that the first reflector benefits from more favorable channel conditions or a strategic placement advantage, leading to superior secrecy performance.

In contrast, the second reflector $\Phi_s^{[2]}$ shows significantly lower probabilities of secure transmission, which suggests weaker link conditions or a greater susceptibility to eavesdropping. Notably, the behavior of $\Phi_s^{[2]}$ is more sensitive to changes in position, as evidenced by sharp fluctuations in the probability, particularly between positions 60 and 80. During this interval, the probability experiences a noticeable dip and subsequent recovery, likely due to environmental factors or suboptimal positioning that adversely affect the channel's performance.

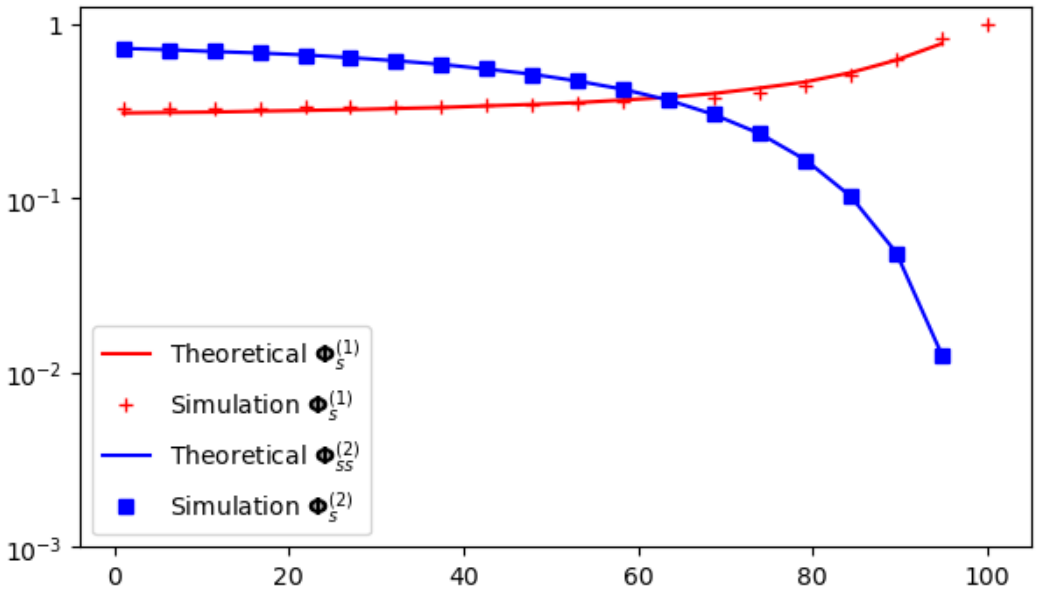

Figure 3. *Secrecy rate versus changes in positions of the Eavesdropper devices*

Figure 3 illustrates the probability of secure transmission $\Phi_s^{[1]}$ and $\Phi_s^{[2]}$ as a function of the eavesdropper's position. The x-axis represents the eavesdropper's position, while the y-axis, presented on a logarithmic scale, shows the secure transmission probability. Theoretical results are depicted with solid lines, while simulation results are represented with markers. The red curves and markers correspond to the first reflector $\Phi_s^{[1]}$, and the blue curves and markers represent the second reflector $\Phi_s^{[2]}$.

The results reveal a notable trend as the eavesdropper's position changes. For the first reflector $\Phi_s^{[1]}$, the secure transmission probability initially decreases slightly and then improves as the eavesdropper moves further away. This indicates that the channel conditions favor secure communication as the eavesdropper's position becomes less optimal for intercepting the transmitted signals. The consistency between theoretical predictions and simulation data validates the accuracy of the model for $\Phi_s^{[1]}$.

In contrast, the second reflector $\Phi_s^{[2]}$ exhibits a continuous and steep decline in the secure transmission probability as the eavesdropper's position approaches certain regions. This reflects the increasing vulnerability of the second reflector to eavesdropping due to unfavorable channel conditions or proximity effects. Notably, the secure transmission probability for $\Phi_s^{[2]}$ approaches zero in certain positions, highlighting the significant impact of the eavesdropper's location on secrecy performance for the second reflector.

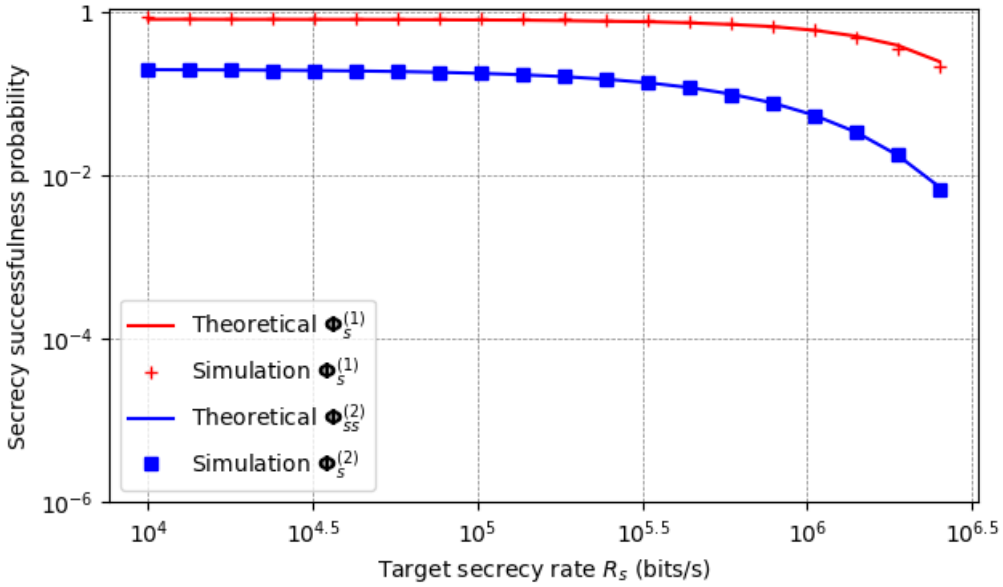

Figure 4. *Secrecy rate versus changes in target transmission rate*

Figure 4 illustrates the relationship between the probability of secure transmission $\Phi_s^{[1]}$ and $\Phi_s^{[2]}$ and the target secrecy rate R_s. The x-axis represents the target secrecy rate in bits per second R_s, plotted on a logarithmic scale, while the y-axis displays the secrecy success probability on a logarithmic scale. Theoretical results are shown as solid lines, and simulation results are represented by markers. The red curves and markers correspond to the first reflector $\Phi_s^{[1]}$, and the blue curves and markers represent the second reflector $\Phi_s^{[2]}$.

As the target secrecy rate increases, the figure reveals a clear degradation in the secure transmission probability for both reflectors. For the first reflector $\Phi_s^{[1]}$, the secrecy probability remains close to 1 for lower secrecy rates and decreases only slightly as $R_s$increases. This indicates a robust performance of the first reflector under higher target secrecy rate requirements, showcasing favorable channel conditions or better alignment with the legitimate receiver.

In contrast, the second reflector $\Phi_s^{[2]}$exhibits a more pronounced decline in secure transmission probability as the target secrecy rate increases. For higher values of R_s, the probability drops significantly, indicating increased difficulty in maintaining secure transmission under stringent secrecy rate requirements. This suggests that the second reflector is more susceptible to eavesdropping or channel inefficiencies as the required secrecy rate becomes more demanding.

The agreement between theoretical and simulation results is evident for both reflectors, confirming the accuracy of the analytical framework in predicting secure transmission probabilities under varying target secrecy rates.

This figure underscores the trade-off between higher target secrecy rates and the achievable probability of secure transmission. While the first reflector demonstrates resilience to increasing secrecy rate demands, the second reflector's performance diminishes significantly. These findings highlight the importance of optimizing system configurations and reflectors' placements to meet specific secrecy requirements in practical scenarios.

5. Conclusion

This study investigated the integration of Non-Orthogonal Multiple Access (NOMA) and backscatter communication to enhance physical layer security in wireless networks. By analyzing the theoretical and simulated probabilities of secure transmission, we demonstrated the feasibility and effectiveness of this model under various conditions, including changes in reflector positions, eavesdropper positions, and target secrecy rates.

The findings highlight that secure transmission probabilities are highly dependent on system parameters and environmental factors. For the first IoT device, secure communication is consistently robust, benefiting from favorable channel conditions and better alignment with the legitimate receiver. However, the second IoT device exhibited greater sensitivity to changes, particularly under stringent target secrecy rate requirements and eavesdropper proximity, resulting in significantly reduced secure transmission probabilities in certain scenarios.

The strong agreement between theoretical predictions and simulation results validates the accuracy of the proposed analytical framework, emphasizing its applicability for modeling secure communication in NOMA-backscatter systems. This research underscores the importance of optimizing key parameters such as reflector placement, transmission power, and secrecy rate thresholds to ensure reliable and confidential communication in adversarial environments.

Future research could extend this work by exploring more complex channel conditions, dynamic network configurations, and advanced techniques such as intelligent reflecting surfaces (IRS) to further improve system performance and security.

Conflict of Interest

The authors declare no conflict of interest.

Appendix A: Probability of Secure Transmission for s_1

The secure capacity for the first IoT device V_1 is defined as:

$$C_s^{[n]} = B\log_2\left(\frac{1+\gamma_{\mathrm{V}_n}}{1+\gamma_{\mathrm{E}_n}}\right) \tag{24}$$

where $C_0^{[n]} = B\log_2\left(1+\gamma_{\mathrm{V}_n}\right)$ and $C_e^{[n]} = B\log_2\left(1+\gamma_{\mathrm{E}_n}\right)$ are the capacities at the legitimate receiver and eavesdropper, respectively. The probability of secure transmission is expressed as:

$$\Phi_s^{[1]} = \Pr\left(\frac{1+\gamma_{\mathrm{V}_n}}{1+\gamma_{\mathrm{E}_n}} \geq 2^{R_s^{[1]}/B}\right) \tag{25}$$

The probability $\mathcal{M}_3$ for s_1 is given as:

$$\gamma_{\mathrm{V}_1} \approx \frac{a_1X_1Y_1}{b_1X_2Y_2}, \gamma_{\mathrm{E}_1} \approx \frac{a_2X_1Z_1}{b_2X_2Z_2}, w_2 = 2^{R_s^{[1]}/B} \tag{26}$$

Introducing the random variables $U = \frac{X_1}{X_2}, V = \frac{Y_1}{Y_2}$ and $W = \frac{Z_1}{Z_2}$ the probability simplifies to:

$$\mathcal{M}_3 \approx \mathbb{E}_U[\Pr(e_1V \geq e_2W - 1)] \tag{27}$$

Here:

$$e_1 = \frac{a_1}{b_1}u, e_2 = \frac{w_2a_2}{b_2}u \tag{28}$$

where u is a realization of U, and these random variables follow the PDF:

$$f_Z(z) = \frac{1}{(z+1)^2}, Z \in \{U, V, W\} \tag{29}$$

The term $\mathcal{M}_{31}$ is derived as:

$$\mathcal{M}_{31} = \int_0^{\frac{1}{e_2}} \Pr(V > 0)\, f_W(w)dw + \int_{\frac{1}{e_2}}^{\infty} \Pr(e_1 V \geq e_2 W - 1)\, f_W(w)dw \tag{30}$$

For $\mathcal{M}_{31A}$, the evaluation simplifies as:

$$\mathcal{M}_{31A} = \int_0^{\frac{1}{e_2}} \Pr(V > 0)\, f_W(w)dw = \int_0^{\frac{1}{e_2}} \frac{1}{(w+1)^2} dw = \frac{1}{1+e_2} \tag{31}$$

where , $e_2 = \frac{w_2 a_2}{b_2} u$. Substituting:

$$\mathcal{M}_{31A} = \frac{b_2}{b_2 + w_2 a_2 u} \tag{32}$$

For $\mathcal{M}_{31B}$, substituting $e_1 = \frac{a_1}{b_1} u$ and $e_2 = \frac{w_2 a_2}{b_2} u$, we have:

$$\begin{aligned} \mathcal{M}_{31B} &= \int_{\frac{1}{e_2}}^{\infty} \Pr(e_1 V \geq e_2 W - 1)\, f_W(w)dw \\ &= \int_{\frac{1}{e_2}}^{\infty} \frac{\frac{a_1}{b_1} u}{\left(\frac{w_2 a_2}{b_2} uw - 1 + \frac{a_1}{b_1} u\right)} \frac{1}{(w+1)^2} dw \\ &= \frac{a_1 a_2 u^2 w_2 \left(-1 + \frac{a_1}{b_1} u - \frac{w_2 a_2}{b_2} u + \left(1 + \frac{w_2 a_2}{b_2} u\right) \log\left(\frac{b_1 \left(1 + \frac{w_2 a_2}{b_2} u\right)}{a_1 u} \right) \right)}{b_1 b_2 \left(1 + \frac{w_2 a_2}{b_2} u\right) \left(-1 + \frac{a_1}{b_1} u - \frac{w_2 a_2}{b_2} u\right)^2} \end{aligned} \tag{33}$$

Appendix B: Probability of Secure Transmission for s_2

The second term, $\mathcal{M}_{32}$, represents the probability that the secure transmission condition for s_2 holds. It is defined as:

$$\mathcal{M}_{32} = \Pr\left[\frac{1 + \gamma_{\mathrm{V}_2}}{1 + \gamma_{\mathrm{E}_2}} > 2^{R_s^{[2]}/B} \right] \tag{34}$$

where

$$\gamma_{\mathrm{V}_2} = b_1 X_2 Y_2, \gamma_{\mathrm{E}_2} = b_2 X_2 Z_2, w_1 = 2^{R_s^{[2]}/B} \tag{35}$$

Expanding $\mathcal{M}_{32}$

$$\begin{aligned} \mathcal{M}_{32} &= \Pr\left[\frac{1 + b_1 X_2 Y_2}{1 + b_2 X_2 Z_2} > 2^{R_s^{[2]}/B} \right] = \Pr\left[\frac{b_1}{b_2 w_1} Y_2 - Z_2 > \frac{w_1 - 1}{b_2 w_1 X_2} \right] \\ &= \mathbb{E}_{\mathrm{X}_2} \left[\frac{b_1}{b_2 w_1} Y_2 - Z_2 > \frac{w_1 - 1}{b_2 w_1 x_2} \right] = \mathbb{E}_{\mathrm{X}_2} \left[\frac{b_1}{b_1 + b_2 w_1} \exp\left(-\frac{w_1 - 1}{b_1 x_2} \right) \right] \end{aligned} \tag{36}$$

REFERENCES

[1] X. Li *et al.*, "Physical-layer authentication for ambient backscatter-aided NOMA symbiotic systems," *IEEE Trans. Commun.*, vol. 71, no. 4, pp. 2288–2303, 2023.

[2] H. Wang *et al.*, "Physical layer security of two-way ambient backscatter communication systems," *Wireless Commun. Mobile Comput.*, vol. 2022, no. 1, pp. 5445676, 2022.

[3] Q. Zhang *et al.*, "Backscatter-NOMA: A symbiotic system of cellular and Internet-of-Things networks," *IEEE Access*, vol. 7, pp. 20000–20013, 2019.
[4] A. Farajzadeh, O. Ercetin, and H. Yanikomeroglu, "UAV data collection over NOMA backscatter networks: UAV altitude and trajectory optimization," in *Proc. IEEE Int. Conf. Commun. (ICC)*, 2019, pp. 1–7.
[5] G. Yang, X. Xu, and Y. Liang, "Resource allocation in NOMA-enhanced backscatter communication networks for wireless powered IoT," *IEEE Wireless Commun. Lett.*, vol. 9, no. 1, pp. 117–120, 2020.
[6] Y. Xu *et al.*, "Energy efficiency maximization in NOMA enabled backscatter communications with QoS guarantee," *IEEE Wireless Commun. Lett.*, vol. 10, no. 2, pp. 353–357, 2021.
[7] F. Pereira *et al.*, "When backscatter communication meets vehicular networks: Boosting crosswalk awareness," *IEEE Access*, vol. 8, pp. 34507–34521, 2020.
[8] J. Guo *et al.*, "Design of non-orthogonal multiple access enhanced backscatter communication," *IEEE Trans. Wireless Commun.*, vol. 17, no. 10, pp. 6837–6852, 2018.
[9] F. Jameel *et al.*, "NOMA-enabled backscatter communications: Toward battery-free IoT networks," *IEEE Internet Things Mag.*, vol. 3, no. 4, pp. 95–101, 2020.
[10] A. Ihsan *et al.*, "Energy-efficient backscatter aided uplink NOMA roadside sensor communications under channel estimation errors," *IEEE Trans. Intell. Transp. Syst.*, vol. 24, no. 5, pp. 4962–4974, 2023.
[11] C. Zhao *et al.*, "PEPA: Paillier cryptosystem-based efficient privacy-preserving authentication scheme for VANETs," *J. Syst. Archit.*, vol. 138, p. 102855, 2023.
[12] F. A. Akbar, "NOMA and 5G emerging technologies: A survey on issues and solution techniques," *Comput. Netw.*, vol. 190, p. 107950, 2021.
[13] T. Bai *et al.*, "Latency minimization for intelligent reflecting surface aided mobile edge computing," *IEEE J. Sel. Areas Commun.*, vol. 38, pp. 2666–2682, 2020.
[14] G. Chen *et al.*, "IRS-aided wireless powered MEC systems: TDMA or NOMA for computation offloading?," in *IEEE Transactions on Wireless Communications*, vol. 22, no. 2, pp. 1201-1218, Feb. 2023, doi: 10.1109/TWC.2022.3203158.
[15] Y. Cheng *et al.*, "Downlink and uplink intelligent reflecting surface aided networks: NOMA and OMA," *IEEE Trans. Wireless Commun.*, vol. 20, no. 6, 2021.

Truc Thanh Tran received the PhD certificate of Electrical and Information Communications Systems in Ulsan University, South Korea in 2014. In 2017, he was head of Post and Telecommunication Office which is apart of Information and Communications Department of Danang city. He also participated as a leader of a national level science project which was successfully conducted in 2019. From 2019 to March 2023, he held the position as director of the Danang city center of Information Infrastructure Development. His responsibilities were aimed at managing, exploiting and calling for investment to the Danang Software Park and operating the main IT infrastructures of Danang city government such as Data Center and MAN network. He starts as a lecturer, researcher in Computing Faculty in GreenWich Vietnam, FPT University in April 2023. His main researches are the studies of information theory, wireless communication technologies, networking, programing and digital signal processing.
Email: tructt16@fe.edu.vn. ORCID: https://orcid.org/0000-0001-9186-7504.

Diem-Phuc Tran is a Ph.D in Computer Science from Duy Tan University, Da Nang City, Vietnam. Now, he is working in Information and Communications department of Quang Binh province. His main research interests include artificial intelligence, image processing, computer vision, auto vehicle.
Email: trandiemphuc@dtu.edu.vn. ORCID: https://orcid.org/0000-0001-8335-6720