Bulletin of Electrical Engineering and Informatics
Vol. 15, No. 3, June 2026, pp. 2150∼2161
ISSN: 2302-9285, DOI: 10.11591/eei.v15i3.10207

Exact outage and intercept analysis of physical layer security in half-duplex energy harvesting relay systems

The-Anh Ngo[1], Xuan-Truong Tran[1], Viet-Thanh Le[2], Thien P. Nguyen[3], Duy-Hung Ha[4]
[1]Division of Electrical-Electronic Engineering, Campus in Ho Chi Minh City, University of Transport and Communications, Ho Chi Minh City, Vietnam
[2]Faculty of Information Technology, Ton Duc Thang University, Ho Chi Minh City, Vietnam
[3]Faculty of Electrical and Electronics Engineering, Ton Duc Thang University, Ho Chi Minh City, Vietnam
[4]Wireless Communications Research Group, Faculty of Electrical and Electronics Engineering, Ton Duc Thang University, Ho Chi Minh City, Vietnam

Article Info

Article history:

Received Mar 4, 2025
Revised Mar 28, 2026
Accepted Apr 19, 2026

Keywords:

Amplify-and-forward
Energy harvesting
Half-duplex
Intercept probability
Outage probability
Power beacon
Relay networks

ABSTRACT

This paper investigates physical layer security (PLS) in a half duplex (HD) relay network with radio frequency energy harvesting (EH). We consider an amplify and forward (AF) protocol in which both the source and the relay harvest energy from a dedicated power beacon, while a passive eavesdropper attempts to intercept the confidential message. Unlike prior studies that rely on asymptotic analysis or numerical integration, we derive exact closed form expressions for the outage probability (OP) and the intercept probability (IP). The proposed expressions characterize the reliability and secrecy trade-off in energy limited cooperative relaying and enable efficient performance evaluation. Monte Carlo simulations validate the analysis and match the theoretical results. Moreover, the closed form results reveal how channel conditions and harvesting duration jointly shape outage and interception behaviors. We further quantify the impacts of normalized transmit power, the time allocation factor between harvesting and information transmission, and the EH efficiency. The results provide practical guidance for selecting system parameters to meet target reliability and secrecy levels, and they show that the time allocation factor must be carefully chosen to balance harvested energy and transmission time.

Corresponding Author:

Duy-Hung Ha
Wireless Communications Research Group, Faculty of Electrical and Electronics Engineering
Ton Duc Thang University
Ho Chi Minh City, Vietnam
Email: haduyhung@tdtu.edu.vn

1. INTRODUCTION

Recent advancements in wireless communication have increasingly focused on solving the energy constraints of battery-powered devices with limited energy resources [1], [2]. Radio frequency (RF) energy harvesting (EH) has emerged as a promising solution to address this issue, gaining significant attention in both academic research and industrial applications [3]–[7]. RF EH enables devices to harvest energy from ambient RF signals, thus reducing their reliance on traditional power sources, making it an attractive option for powering internet of things (IoT) devices and other battery-operated equipment.

In parallel, ensuring the confidentiality and integrity of transmitted information in wireless networks remains a critical challenge [8], [9]. Physical layer security (PLS) plays a pivotal role in safeguarding data against potential eavesdroppers by enhancing the security of wireless communication systems [10]–[13]. The integration of EH with PLS techniques has gained substantial interest in recent years, aiming to enhance both the energy sustainability and security of wireless networks [14]–[17]. Several studies have investigated simultaneous wireless information and power transfer (SWIPT), where both energy harvesting and data transmission occur simultaneously [18], [19]. In relay-assisted EH systems, relays harvest RF energy from the source signal or co-channel interference to enhance both network energy efficiency and sustainability [20], [21]. However, the practical deployment of SWIPT models faces significant challenges, especially when long-range communication is needed, as the transmission power required to cover long distances often exceeds the available energy harvested from RF signals.

Another emerging technology that shows promise in enhancing energy harvesting systems is reconfigurable intelligent surfaces (RIS), which can improve both energy harvesting and signal quality by controlling the propagation of electromagnetic waves [22]–[26]. Although RIS holds significant potential for improving energy efficiency and communication quality, its real-world deployment faces difficulties due to the assumption of perfect channel state information (CSI) in many studies [27]–[29]. Moreover, several existing studies, including those in [28], [29], rely on approximate closed-form solutions, which may not accurately reflect real-world scenarios, emphasizing the need for more precise analytical models in RIS-based EH systems.

Furthermore, many existing optimization algorithms introduce high computational complexity, which limits their applicability in large-scale or real-time wireless systems due to prohibitive runtime and resource demands [30]. These limitations underscore the need for further research to develop secure and energy-efficient cooperative networks that operate under practical system constraints.

Motivated by these considerations, this paper investigates the problem of PLS in half-duplex (HD) relay networks over Rayleigh fading channels. In the proposed system, both the source (S) and relay (R) harvest RF energy from a dedicated power beacon (PB) while transmitting confidential information to the destination (D) in the presence of a passive eavesdropper (E). We employ an amplify-and-forward (AF) relaying protocol to enable secure communication within this energy-constrained cooperative system. The main contributions of this paper are as follows:

- We propose a comprehensive analytical framework for evaluating PLS in HD relay systems operating over Rayleigh fading channels with integrated EH capabilities. Specifically, we derive exact closed-form expressions for the outage probability (OP) and intercept probability (IP), which serve as key performance indicators for assessing the security of wireless communication systems.
- We introduce an innovative EH model in which both the source and relay nodes harvest RF energy from a dedicated PB. This model effectively addresses the challenge of energy constraints in wireless networks, ensuring a continuous energy supply for relay-assisted communication, even in environments with limited energy resources.
- The accuracy of the derived analytical results is rigorously validated through extensive Monte Carlo simulations. The validation confirms that our closed-form expressions for OP and IP provide accurate and reliable predictions of the system's performance under practical operating conditions.
- We conduct a detailed analysis of the impact of several key system parameters, including energy conversion efficiency, normalized transmit power, and time allocation factor, on the OP and IP performance. This analysis provides valuable insights for optimizing the design of energy-efficient and secure relay systems.

The remainder of this paper is organized as follows. Section 2 presents the system model, including the time-splitting relay protocol and EH process. Section 3 provides the detailed performance analysis and derivation of OP and IP. Section 4 discusses the simulation results and their implications. Finally, section 5 concludes the paper and outlines potential directions for future research.

2. SYSTEM MODEL

We consider a dual-hop wireless communication system, as shown in Figure 1, where the source (S) communicates with the destination (D) through an intermediate relay (R) in the presence of a passive eavesdropper (E). Unlike conventional relaying systems with fixed power supplies [31], both S and R are energy-constrained and rely solely on wireless energy harvested from a dedicated PB. This design models practical scenarios such as IoT or sensor networks where devices operate without batteries. Moreover, in contrast to [32], which only considered relay-side EH, our framework enables simultaneous EH at both source and relay and derives closed-form expressions for OP and IP under this novel setup.

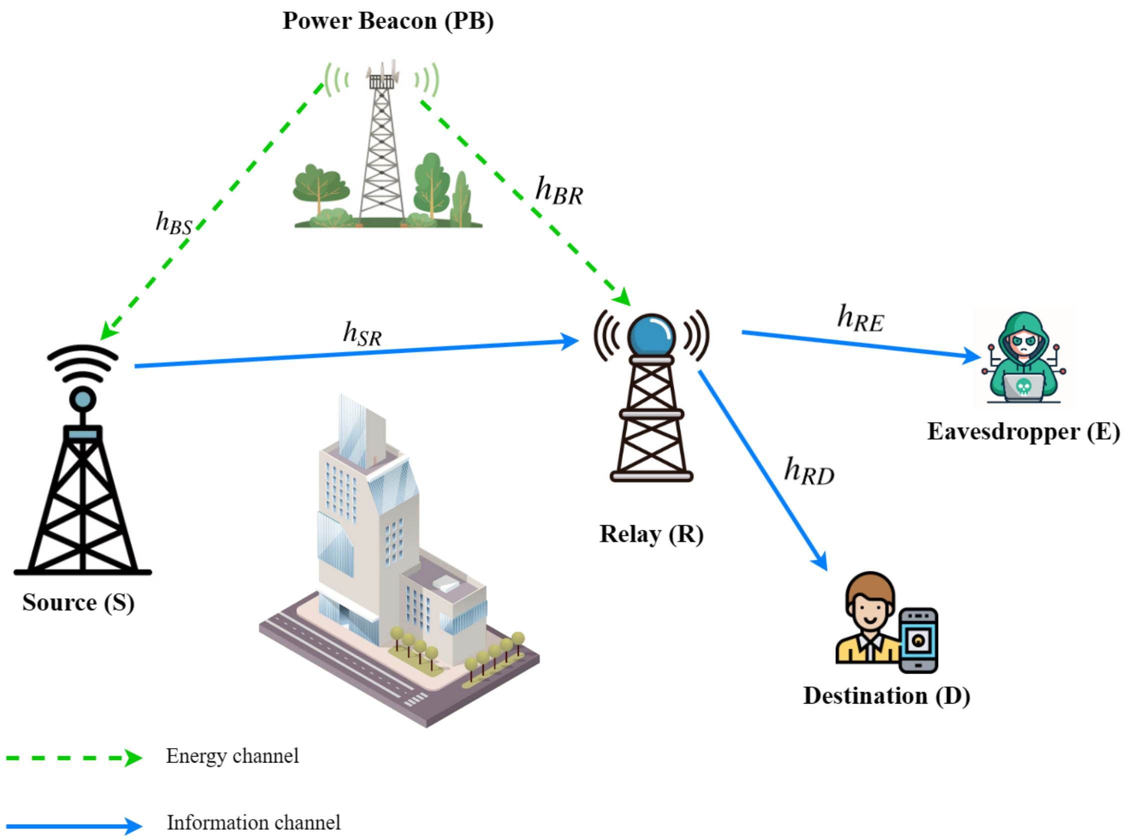


Figure 1. Proposed system model with EH-enabled source and relay

The transmission follows the time-switching relaying (TSR) protocol [33], [34] illustrated in Figure 2. Each block of duration T is divided into three phases. In the first phase, with duration αT $(0 < \alpha < 1)$, both S and R harvest wireless energy from the PB. The harvested energies are given by:

$$E_S = \eta P_{\mathrm{B}} |h_{BS}|^2 \alpha T, \quad (1)$$

$$E_R = \eta P_{\mathrm{B}} |h_{BR}|^2 \alpha T, \quad (2)$$

where P_{B} denotes the PB transmit power, $\eta \in (0, 1]$ is the energy conversion efficiency, and h_{BS} and h_{BR} represent the complex channel coefficients of the B–S and B–R links. Physically, $|h_{BS}|^2$ and $|h_{BR}|^2$ capture the fading-induced power attenuation. All wireless links are modeled as independent Rayleigh fading channels, which appropriately characterize non-line-of-sight rich-scattering environments typically encountered in urban and indoor deployments, where no dominant line-of-sight component exists. The AF protocol is adopted due to its low computational complexity and minimal processing delay, which are particularly desirable for energy-constrained relays, thereby ensuring practical feasibility in EH-assisted systems. A linear energy harvesting model is considered to preserve analytical tractability while accurately approximating practical direct current (RF-to-DC) conversion behavior in moderate input power regimes. Perfect CSI at the receivers is assumed to establish an analytical performance upper bound and enable coherent detection, which is a standard benchmark in theoretical physical layer security studies.

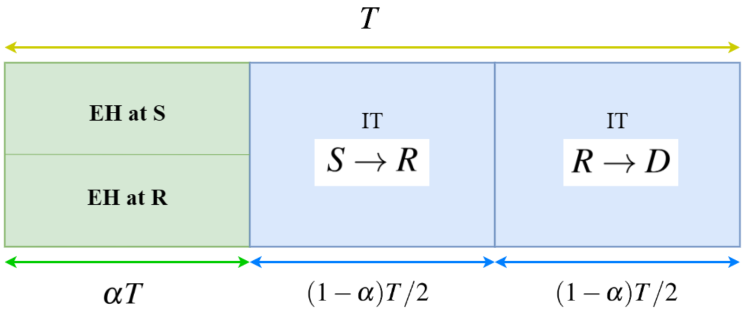


Figure 2. TSR protocol

During the remaining two slots, each of length $(1-\alpha)T/2$, information transmission takes place. Using (1) and (2), the average transmit powers at S and R are:

$$P_S = \frac{E_S}{(1-\alpha)T/2} = \kappa P_B |h_{BS}|^2, \tag{3}$$

$$P_R = \frac{E_R}{(1-\alpha)T/2} = \kappa P_B |h_{BR}|^2, \tag{4}$$

with $\kappa = \frac{2\eta\alpha}{1-\alpha}$. These expressions highlight the key difference from battery-powered systems: the instantaneous transmit powers of both nodes now fluctuate with the harvested energy, making the performance analysis fundamentally different.
In the second time slot, the signal received at R is:

$$y_R = h_{SR} x_S + n_R, \tag{5}$$

where h_{SR} is the channel coefficient of the S–R link, x_S is the transmit signal from S with average power P_S, and n_R is additive white Gaussian noise (AWGN) with variance N_0. In the third slot, R forwards the signal to D, which receives:

$$y_D = h_{RD} x_R + n_D, \tag{6}$$

where h_{RD} is the R–D channel coefficient, x_R is the relay's transmit signal with power P_R, and n_D is AWGN with variance N_0.

To process the received signal, R employs the AF protocol. AF is particularly suitable for EH systems because it avoids the energy-intensive decoding process required in decode-and-forward (DF), thereby reducing complexity and energy consumption. The amplification factor is:

$$\beta = \sqrt{\frac{P_R}{P_S |h_{SR}|^2 + N_0}}, \tag{7}$$

and substituting (5) into (6) yields:

$$y_D = h_{RD}\beta(h_{SR}x_S + n_R) + n_D = \underbrace{h_{SR}h_{RD}\beta x_S}_{\text{desired signal}} + \underbrace{h_{RD}\beta n_R + n_D}_{\text{equivalent noise}}. \tag{8}$$

3. SYSTEM PERFORMANCE ANALYSIS

From (8), the end-to-end signal-to-noise ratio (SNR) of the S-R-D link is given by:

$$\gamma_{SRD} = \frac{\mathbb{E}\left\{|\text{signal}|^2\right\}}{\mathbb{E}\left\{|\text{noise}|^2\right\}} = \frac{|h_{SR}|^2 |h_{RD}|^2 \beta^2 P_S}{|h_{RD}|^2 \beta^2 N_0 + N_0}. \tag{9}$$

By substituting $\beta^2 = \dfrac{P_R}{P_S|h_{SR}|^2 + N_0}$ into (9), one obtains:

$$\gamma_{SRD} = \frac{|h_{SR}|^2|h_{RD}|^2 P_S P_R}{P_R|h_{RD}|^2 N_0 + N_0 P_S |h_{SR}|^2 + N_0^2}. \tag{10}$$

Substituting (3) and (4) into (10), and defining:

$$\Psi = \frac{P_B}{N_0}, \qquad X = |h_{BR}|^2|h_{RD}|^2, \qquad Y = |h_{BS}|^2|h_{SR}|^2, \tag{11}$$

the SNR at D can be rewritten as (12):

$$\gamma_{SRD} = \frac{\kappa^2\Psi^2 XY}{\kappa\Psi(X+Y)+1} = \frac{\kappa\Psi XY}{X + Y + \dfrac{1}{\kappa\Psi}}. \tag{12}$$

At high SNR, i.e., $\kappa\Psi \gg 1$, (12) can be approximated as (13):

$$\gamma_{SRD} \approx \frac{\kappa\Psi XY}{X+Y}. \tag{13}$$

The received signal at the eavesdropper during the forwarding phase is expressed as (14):

$$y_E = h_{RE} x_R + n_E, \tag{14}$$

where h_{RE} denotes the channel coefficient of the R-E link and n_E is the AWGN with variance N_0. Since the relay adopts the AF protocol, the forwarded signal is:

$$x_R = \beta y_R = \beta\left(h_{SR} x_S + n_R\right). \tag{15}$$

Hence, (14) can be rewritten as (16):

$$y_E = h_{RE}\beta\left(h_{SR} x_S + n_R\right) + n_E. \tag{16}$$

Accordingly, the SNR at the eavesdropper is given by:

$$\gamma_E = \frac{|h_{RE}|^2|h_{SR}|^2\beta^2 P_S}{|h_{RE}|^2\beta^2 N_0 + N_0}. \tag{17}$$

Substituting $\beta^2 = \dfrac{P_R}{P_S|h_{SR}|^2 + N_0}$ into (17), we obtain:

$$\gamma_E = \frac{|h_{RE}|^2|h_{SR}|^2 P_S P_R}{P_R|h_{RE}|^2 N_0 + N_0 P_S |h_{SR}|^2 + N_0^2}. \tag{18}$$

By substituting (3) and (4) into (18), and defining:

$$U = |h_{BR}|^2|h_{RE}|^2, \qquad V = |h_{BS}|^2|h_{SR}|^2, \tag{19}$$

the SNR at the eavesdropper can be expressed as (20):

$$\gamma_E = \frac{\kappa^2\Psi^2 UV}{\kappa\Psi(U+V)+1} = \frac{\kappa\Psi UV}{U + V + \dfrac{1}{\kappa\Psi}}. \tag{20}$$

Similarly, at high SNR, (20) reduces to:

$$\gamma_E \approx \frac{\kappa\Psi UV}{U+V}. \tag{21}$$

Lemma 1

Since all channels are assumed to follow Rayleigh fading, the squared channel magnitude $|h_i|^2$ is exponentially distributed with the probability density function (PDF):

$$f_{|h_i|^2}(x) = \lambda_i e^{-\lambda_i x}, \qquad x \geq 0, \tag{22}$$

for $i \in \{SR, RD, BS, BR, RE\}$, where λ_i denotes the *rate parameter* of the exponential random variable $|h_i|^2$. Therefore, the corresponding cumulative distribution function (CDF) is:

$$F_{|h_i|^2}(x) = 1 - e^{-\lambda_i x}. \tag{23}$$

Lemma 2

The random variables X, Y, U, and V are defined as products of two independent exponential random variables. Using the standard result for the product of two independent exponential random variables [35], the CDFs of X and Y are respectively given by:

$$F_X(a) = 1 - 2\sqrt{\lambda_{BR}\lambda_{RD}a}\, K_1\left(2\sqrt{\lambda_{BR}\lambda_{RD}a}\right), \tag{24}$$

$$F_Y(b) = 1 - 2\sqrt{\lambda_{BS}\lambda_{SR}b}\, K_1\left(2\sqrt{\lambda_{BS}\lambda_{SR}b}\right), \tag{25}$$

where $K_\nu(\cdot)$ denotes the modified Bessel function of the second kind of order ν.
By differentiating (24) and (25), the corresponding PDFs are obtained as (26) and (27):

$$f_X(a) = 2\lambda_{BR}\lambda_{RD}K_0\left(2\sqrt{\lambda_{BR}\lambda_{RD}a}\right), \tag{26}$$

$$f_Y(b) = 2\lambda_{BS}\lambda_{SR}K_0\left(2\sqrt{\lambda_{BS}\lambda_{SR}b}\right). \tag{27}$$

Similarly, the CDFs and PDFs of U and V are respectively given by:

$$F_U(u) = 1 - 2\sqrt{\lambda_{BR}\lambda_{RE}u}\, K_1\left(2\sqrt{\lambda_{BR}\lambda_{RE}u}\right), \tag{28}$$

$$f_U(u) = 2\lambda_{BR}\lambda_{RE}K_0\left(2\sqrt{\lambda_{BR}\lambda_{RE}u}\right), \tag{29}$$

$$F_V(v) = 1 - 2\sqrt{\lambda_{BS}\lambda_{SR}v}\, K_1\left(2\sqrt{\lambda_{BS}\lambda_{SR}v}\right), \tag{30}$$

$$f_V(v) = 2\lambda_{BS}\lambda_{SR}K_0\left(2\sqrt{\lambda_{BS}\lambda_{SR}v}\right). \tag{31}$$

3.1. Outage probability

The OP is defined as (32):

$$\text{OP} = \Pr\left(\gamma_{SRD} < \gamma_{th}\right), \tag{32}$$

where $\gamma_{th} = 2^{2R} - 1$, and R denotes the source transmission rate.
Substituting (12) into (32), the outage event can be written as (33):

$$\frac{\kappa\Psi XY}{X + Y + \frac{1}{\kappa\Psi}} < \gamma_{th}. \tag{33}$$

After straightforward manipulations, this condition is equivalent to:

$$X\left(\kappa\Psi Y - \gamma_{th}\right) < \gamma_{th}Y + \frac{\gamma_{th}}{\kappa\Psi}. \tag{34}$$

It follows that:

$$\text{OP} = F_Y\left(\frac{\gamma_{th}}{\kappa\Psi}\right) + \int_{\frac{\gamma_{th}}{\kappa\Psi}}^{\infty} F_X\left(\frac{\gamma_{th}\left(y + \frac{1}{\kappa\Psi}\right)}{\kappa\Psi y - \gamma_{th}}\right) f_Y(y)\, dy. \tag{35}$$

Substituting (24) and (27) into (35), and applying the integral identity in [36, equation (6.561.16)6.561.16)], yields the exact OP expression given in (36):

$$\mathrm{OP} = 1 - 4\lambda_{BS}\lambda_{SR} \int_{\frac{\gamma_{th}}{\kappa\Psi}}^{\infty} \sqrt{\lambda_{BR}\lambda_{RD}\frac{\gamma_{th}\left(y+\frac{1}{\kappa\Psi}\right)}{\kappa\Psi y-\gamma_{th}}} \times K_1\left(2\sqrt{\lambda_{BR}\lambda_{RD}\frac{\gamma_{th}\left(y+\frac{1}{\kappa\Psi}\right)}{\kappa\Psi y-\gamma_{th}}}\right) K_0\left(2\sqrt{\lambda_{BS}\lambda_{SR}y}\right)\, dy. \quad (36)$$

3.2. Intercept probability

The IP is defined as (37):

$$\mathrm{IP} = \Pr\left(\gamma_E \geq \gamma_{th}\right). \quad (37)$$

By substituting (20) into (37), the interception event is equivalently written as (38):

$$\frac{\kappa\Psi UV}{U+V+\frac{1}{\kappa\Psi}} \geq \gamma_{th}, \quad (38)$$

which can be rearranged as (39):

$$U\left(\kappa\Psi V-\gamma_{th}\right) \geq \gamma_{th}V + \frac{\gamma_{th}}{\kappa\Psi}. \quad (39)$$

Therefore, the exact IP is obtained as (40):

$$\mathrm{IP} = \int_{\frac{\gamma_{th}}{\kappa\Psi}}^{\infty} \overline{F}_U\left(\frac{\gamma_{th}\left(v+\frac{1}{\kappa\Psi}\right)}{\kappa\Psi v-\gamma_{th}}\right) f_V(v)\, dv, \quad (40)$$

where $\overline{F}_U(u) = 1 - F_U(u)$.
Substituting (28) and (31) into (40), we obtain:

$$\mathrm{IP} = 4\lambda_{BS}\lambda_{SR} \int_{\frac{\gamma_{th}}{\kappa\Psi}}^{\infty} \sqrt{\lambda_{BR}\lambda_{RE}\frac{\gamma_{th}\left(v+\frac{1}{\kappa\Psi}\right)}{\kappa\Psi v-\gamma_{th}}} \times K_1\left(2\sqrt{\lambda_{BR}\lambda_{RE}\frac{\gamma_{th}\left(v+\frac{1}{\kappa\Psi}\right)}{\kappa\Psi v-\gamma_{th}}}\right) K_0\left(2\sqrt{\lambda_{BS}\lambda_{SR}v}\right)\, dv. \quad (41)$$

4. SIMULATION RESULTS

In this section, we present the results of Monte Carlo simulations to validate the analytical expressions for the OP and IP derived in (36) and (41). The main findings are discussed, providing a comprehensive understanding of the system's behavior and offering physical interpretations for the results.

4.1. Simulation setup

Table 1 summarizes the key simulation parameters used in the Monte Carlo simulations. These parameters are chosen to reflect practical values for energy harvesting systems, and the simulations are performed over 10^6 iterations to ensure statistical reliability.

Table 1. Summary of parameters and simulation setup

Symbol	Description	Value/unit
Ψ	Normalized transmit power	-10 to 20 dB
α	Time-switching factor	$0 < \alpha < 1$
η	Energy harvesting efficiency	$0 < \eta \leq 1$
R	Target transmission rate	0.5 to 1.55 bps/Hz
N_{sim}	Monte Carlo iterations	10^6

4.2. Outage probability and intercept probability analysis

Figure 3 shows the OP as a function of Ψ for $\eta = 0.9$ and $R = 0.8$ bps/Hz under various values of α. As expected, OP decreases with increasing Ψ because higher normalized transmit power improves the SNR at the destination. Additionally, a larger α allocates more time for energy harvesting, which boosts the transmit power of both the source and the relay. This enhancement strengthens the legitimate link, leading to lower OP. For instance, $\alpha = 0.75$ results in a significantly higher reliability compared to $\alpha = 0.25$. The close match between the analytical and simulation results confirms the correctness of (36).

Figure 4 presents the IP for the same simulation setup. Contrary to OP, IP increases with Ψ, as higher transmit power not only enhances the legitimate link but also improves the eavesdropper's received SNR. This opposite trend illustrates the fundamental reliability–secrecy trade-off, which has been widely recognized in physical layer security literature. Specifically, increasing the transmit power enhances the main channel capacity while simultaneously improving the eavesdropper channel, thereby enlarging the secrecy outage region [13], [14]. While increasing Ψ improves the legitimate link, it simultaneously makes interception easier for the eavesdropper. The role of α is crucial in strengthening the relay transmission, which improves reliability but also increases the likelihood of interception. Thus, the choice of α is a fundamental design trade-off between OP and IP.

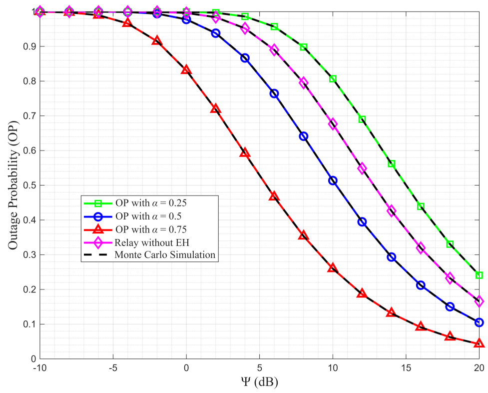


Figure 3. OP vs. normalized transmit power for different values of α

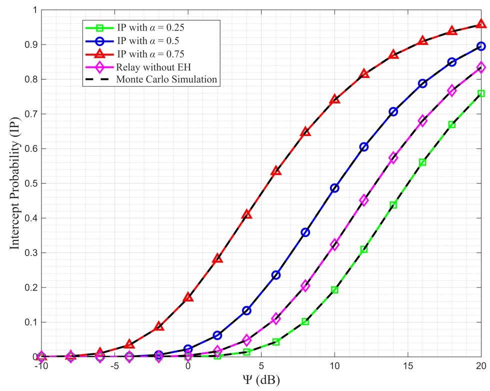


Figure 4. IP vs. normalized transmit power for different values of α

Moreover, the results clearly demonstrate the advantage of the exact closed-form analysis, as the analytical curves perfectly overlap with the Monte Carlo simulation results over the entire SNR range. This exact agreement confirms the accuracy of the derived expressions and contrasts with prior studies that rely on approximate analytical methods, where noticeable discrepancies between analytical and simulation results may occur (e.g., [28], [29]). Additionally, in Figures 3 and 4, we also compare the proposed EH-enabled scheme with a conventional relay without energy harvesting. The results show that when the time allocation factor is sufficiently large, the EH-based system achieves superior intercept and outage performance due to the additional harvested energy that enhances the relay transmit power. In contrast, when the harvesting duration is limited, the EH scheme may underperform the non-EH relay since the harvested energy is insufficient to offset the loss in information transmission time. This observation reveals a fundamental tradeoff between energy harvesting and data transmission, emphasizing the importance of properly selecting the time allocation factor.

4.3. Effect of time-switching factor α

Figures 5 and 6 explore the effect of α at a fixed normalized transmit power $\Psi = 10$ dB and energy harvesting efficiency $\eta = 0.9$. In Figure 5, OP monotonically decreases as α increases. More harvesting time allows greater transmit powers at both the source and relay, thereby reducing the probability of falling below the target SNR threshold. The performance gap between different target rates is more significant at larger R, where stricter SNR requirements result in more frequent outage events.

In contrast, Figure 6 shows that IP increases with α, as stronger relay transmissions make the signal more decodable at the eavesdropper. Interestingly, the IP is not always highest at larger R. For example, a target rate of $R = 1.5$ bps/Hz achieves the lowest IP, as the higher secrecy threshold makes successful interception more difficult. This result is consistent with the findings reported in [16].

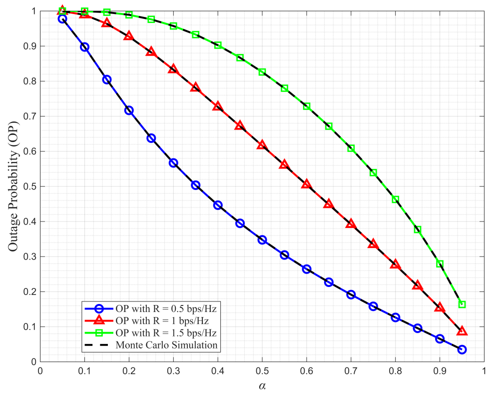


Figure 5. OP vs. energy harvesting time for different target rates

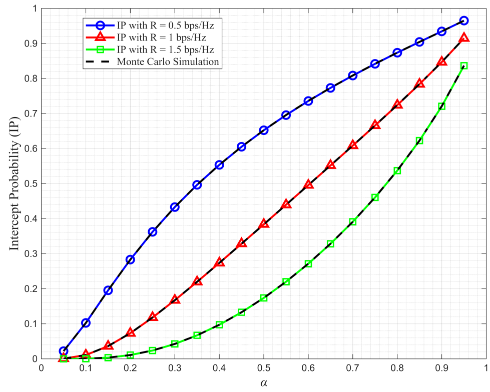


Figure 6. IP vs. energy harvesting time for different target rates

4.4. Impact of energy harvesting efficiency η

Figures 7 and 8 illustrate the influence of energy harvesting efficiency η on OP and IP. As η increases, the harvested energy improves linearly, which enhances the relay's forwarding capability and reduces OP (Figure 7). However, this improvement in reliability comes at the expense of secrecy, as stronger relay transmission benefits both the legitimate link and the eavesdropper, thereby increasing IP (Figure 8). Such behavior aligns with prior studies on EH-assisted relaying systems, where higher harvesting efficiency linearly scales the relay transmit power under the linear EH model, improving reliability but also strengthening the wiretap channel [20]. These results demonstrate the dual role of EH efficiency: it enhances reliability but simultaneously poses a risk to confidentiality.

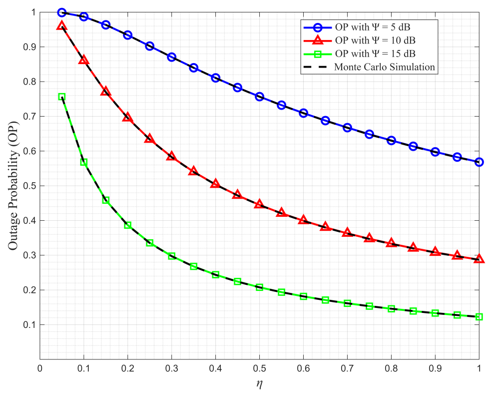


Figure 7. OP vs. energy harvesting efficiency for different normalized transmit power

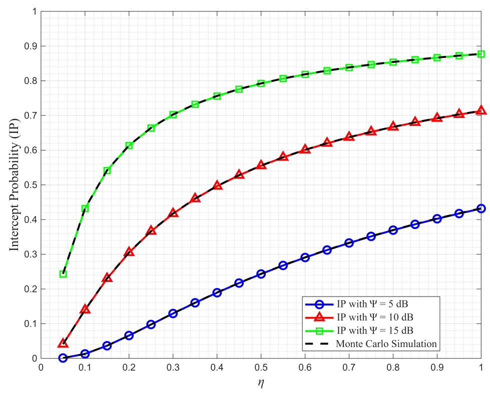


Figure 8. IP vs. energy harvesting efficiency for different normalized transmit power

4.5. Summary of key insights

The numerical results yield three key insights for the design of energy-harvesting secure relaying systems:

– The normalized transmit power Ψ and harvesting time α both improve system reliability but degrade secrecy, highlighting the inherent OP–IP trade-off.
– Higher transmission rates amplify the outage effect but can reduce the interception probability, suggesting that R plays a non-trivial role in balancing reliability and secrecy.
– The energy harvesting efficiency η acts as a double-edged sword: while it improves reliability by strengthening relaying capabilities and reducing OP, it simultaneously increases the eavesdropping risk by enhancing the eavesdropper's SNR, thereby increasing IP.

These findings provide useful design guidelines for energy-harvesting secure relaying systems, where both reliability and confidentiality must be jointly optimized to achieve the best performance in real-world deployments.

5. CONCLUSION

In this paper, we have presented a comprehensive analysis of the performance of a cooperative wireless network, focusing on OP and IP. The proposed analytical framework, supported by closed-form expressions, was validated through extensive Monte Carlo simulations. The close alignment between the analytical and numerical results confirms the validity and robustness of the proposed model in evaluating and optimizing the performance of secure energy-harvesting relay systems.

While the current study is based on idealized assumptions, such as Rayleigh fading, future research can extend the framework to more realistic fading models, including Rician and Nakagami-m channels, to better capture the complexities of real-world environments. Additionally, practical deployments in IoT networks, unmanned aerial vehicle (UAV-assisted) communication, and multi-hop cooperative systems may introduce new challenges, including hardware impairments, circuit non-linearities, antenna misalignment, and adaptive eavesdropping techniques. These challenges highlight the need for the development of more robust and low-complexity solutions.

The findings from this work lay a strong foundation for the design of secure and energy-efficient cooperative communication systems. Furthermore, the paper outlines several promising directions for future research, which include the exploration of advanced fading models, hardware imperfection mitigation strategies, and the application of the proposed framework in emerging communication networks.

FUNDING INFORMATION

This research received no external funding.

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
The-Anh Ngo	✓	✓	✓	✓	✓	✓		✓	✓	✓		✓	✓	
Xuan-Truong Tran		✓			✓	✓		✓		✓				
Viet-Thanh Le			✓	✓		✓		✓		✓				
Thien P. Nguyen		✓	✓		✓	✓	✓	✓		✓	✓			
Duy-Hung Ha	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	

C : **C**onceptualization
M : **M**ethodology
So : **So**ftware
Va : **Va**lidation
Fo : **Fo**rmal Analysis
I : **I**nvestigation
R : **R**esources
D : **D**ata Curation
O : Writing - **O**riginal Draft
E : Writing - Review & **E**diting
Vi : **Vi**sualization
Su : **Su**pervision
P : **P**roject Administration
Fu : **Fu**nding Acquisition

CONFLICT OF INTEREST STATEMENT

Authors state no conflict of interest.

DATA AVAILABILITY

The data that support the findings of this study are available from the corresponding author [initials: Duy-Hung Ha] upon reasonable request.

REFERENCES

[1] O. Abusaid and M. Showaia, “Consideration of energy efficiency into wireless communication systems,” in *Proc. 2024 IEEE 7th Int. Conf. Advanced Technologies, Signal and Image Processing (ATSIP)*, Sousse, Tunisia, 2024, pp. 34–39, doi: 10.1109/ATSIP62566.2024.10638852.

[2] K. L. Ranganayagi, S. P. Kumar, D. Lingaraja, T. Aravind, S. Ramya, and G. D. Ram, “Energy-efficient communication protocols for 6G wireless sensor network,” in *Proc. 2024 IEEE 2nd Int. Conf. Netw. Commun. (ICNWC)*, 2024, pp. 1–6, doi: 10.1109/ICNWC60771.2024.10537356.

[3] O. L. A. López and K. Suto, "RF energy harvesting and wireless power transfer for IoT," *Sensors*, vol. 24, no. 23, 2024, doi: 10.3390/s24237567.

[4] G. Moloudian *et al.*, "RF energy harvesting techniques for battery-less wireless sensing, industry 4.0, and Internet of Things: A review," *IEEE Sens. J.*, vol. 24, no. 5, pp. 5732–5745, 2024, doi: 10.1109/JSEN.2024.3352402.

[5] B. Y. L. Ávila, C. A. G. Vázquez, O. P. Baluja, D. T. Cotfas, and P. A. Cotfas, "Energy harvesting techniques for wireless sensor networks: A systematic literature review," *Energy Strategy Rev.*, vol. 57, 2025, doi: 10.1016/j.esr.2024.101617.

[6] T. N. Nguyen, T. H. Quang Minh, P. T. Tran, and M. Vozňák, "Energy harvesting over Rician fading channel: A performance analysis for half-duplex bidirectional sensor networks under hardware impairments," *Sensors*, vol. 18, no. 6, pp. 1781, 2018.

[7] A. Rauniyar, P. E. Engelstad, and O. N. Østerbø, "Performance analysis of RF energy harvesting and information transmission based on NOMA with interfering signal for IoT relay systems," *IEEE Sens. J.*, vol. 19, no. 17, pp. 7668–7682, 2019, doi: 10.1109/JSEN.2019.2914796.

[8] C. Li, Y. Tang, and F. Luo, "Research on internet regional security based on 5G wireless communication technology," in *Proc. 2022 Int. Conf. Int. Conf. Smart City Green Energy (ICSCGE)*, 2022, pp. 1–4, doi: 10.1109/ICSCGE58152.2022.00008.

[9] P. Porambage, G. Gür, D. P. M. Osorio, M. Livanage, and M. Ylianttila, "6G security challenges and potential solutions," in *Proc. 2021 Joint Eur. Conf. Netw. Commun. 6G Summit (EuCNC/6G Summit)*, 2021, pp. 622–627, doi: 10.1109/EuCNC/6GSummit51104.2021.9482609.

[10] R. Zhao, Y. Huang, W. Wang, and V. K. N. Lau, "Ergodic achievable secrecy rate of multiple-antenna relay systems with cooperative jamming," *IEEE Trans. Wireless Commun.*, vol. 15, no. 4, pp. 2537–2551, 2016, doi: 10.1109/TWC.2015.2504526.

[11] A. Pradhan, S. Das, M. J. Piran, and Z. Han, "A survey on physical layer security of ultra/reliable low latency communication in 5G and 6G networks: Recent advancements, challenges, and future directions," *IEEE Access*, vol. 12, pp. 112320–112353, 2024, doi: 10.1109/ACCESS.2024.3429285.

[12] I. Ara and B. Kelley, "Physical layer security for 6G: Toward achieving intelligent native security at layer-1," *IEEE Access*, vol. 12, pp. 82800–82824, 2024, doi: 10.1109/ACCESS.2024.3413047.

[13] Y. Li, Z. Liu, J. Su, and Y. Yuan, "Physical layer security scheme with AoI-awareness for industrial IoT based on covert communications," *IEEE/CAA J. Autom. Sinica*, vol. 12, no. 1, pp. 276–278, 2025, doi: 10.1109/JAS.2024.124770.

[14] A. Salem, K. A. Hamdi, and K. M. Rabie, "Physical layer security with RF energy harvesting in AF multi-antenna relaying networks," *IEEE Trans. Commun.*, vol. 64, no. 7, pp. 3025–3038, 2016, doi: 10.1109/TCOMM.2016.2573829.

[15] K. Ho-Van, "Energy harvesting-assisted wireless transmission secured with jamming: Performance analysis," *Comput. Electr. Eng.*, vol. 119, 2024, doi: 10.1016/j.compeleceng.2024.109496.

[16] P. Yan *et al.*, "EH cognitive network with NOMA: Perspective on impact of passive and active eavesdropping," *IEEE Internet of Things J.*, vol. 11, no. 3, pp. 5050–5062, 2024, doi: 10.1109/JIOT.2023.3301631.

[17] R. Lin, H. Qiu, J. Wang, Z. Zhang, L. Wu, and F. Shu, "Physical-layer security enhancement in energy-harvesting-based cognitive Internet of Things: A GAN-powered deep reinforcement learning approach," *IEEE Internet of Things J.*, vol. 11, no. 3, pp. 4899–4913, 2024, doi: 10.1109/JIOT.2023.3300770.

[18] P. Nezhadmohammad, M. Abedi, M. J. Emadi, and R. Wichman, "SWIPT-enabled multiple access channel: Effects of decoding cost and non-linear EH model," *IEEE Trans. Commun.*, vol. 70, no. 1, pp. 306–316, 2022, doi: 10.1109/TCOMM.2021.3121035.

[19] N. Ashraf, S. A. Sheikh, M. Mahrukh, and S. A. Khan, "Performance analysis of SWIPT-assisted cooperative NOMA network with non-linear EH, interference, and imperfect SIC," *IEEE Access*, vol. 13, pp. 77481–77492, 2025, doi: 10.1109/ACCESS.2025.3563111.

[20] G. Wang, C. Peng, and Y. Huang, "The power allocation for SWIPT-based cognitive two-way relay networks with rate fairness consideration," in *Proc. 2022 IEEE Int. Conf. Trust, Security Privacy Comput. Commun. (TrustCom)*, 2022, pp. 60–65, doi: 10.1109/TrustCom56396.2022.00019.

[21] J. L. Bing, Y. Rong, L. Gopal, and C. W. R. Chiong, "Transceiver design for SWIPT MIMO relay systems with hybridized power-time splitting-based relaying protocol," *IEEE Access*, vol. 8, pp. 190922–190933, 2020, doi: 10.1109/ACCESS.2020.3032120.

[22] M. Ahmed *et al.*, "A survey on RIS advances in terahertz communications: Emerging paradigms and research frontiers," *IEEE Access*, vol. 12, pp. 173867–173901, 2024, doi: 10.1109/ACCESS.2024.3482564.

[23] G. Huang, A. Zappone, G. C. Alexandropoulos, M. Debbah, and C. Yuen, "Reconfigurable intelligent surfaces for energy efficiency in wireless communication," *IEEE Trans. Wireless Commun.*, vol. 18, no. 8, pp. 4157–4170, 2019, doi: 10.1109/TWC.2019.2922609.

[24] Y. Liu *et al.*, "Reconfigurable intelligent surfaces: Principles and opportunities," *IEEE Commun. Surveys Tutorials*, vol. 23, no. 3, pp. 1546–1577, 2021, doi: 10.1109/COMST.2021.3077737.

[25] C. Pan *et al.*, "Reconfigurable intelligent surfaces for 6G systems: Principles, applications, and research directions," *IEEE Commun. Mag.*, vol. 59, no. 6, pp. 14–20, 2021, doi: 10.1109/MCOM.001.2001076.

[26] M. ElMossallamy *et al.*, "Reconfigurable intelligent surfaces for wireless communications: Principles, challenges, and opportunities," *IEEE Trans. Cogn. Commun. Networking*, vol. 6, no. 3, pp. 990–1002, 2020, doi: 10.1109/TCCN.2020.2992604.

[27] F. R. Ghadi, M. Kaveh, K. Wong, and D. Martín, "Physical layer security performance of cooperative dual-RIS-aided V2V NOMA communications," *IEEE Syst. J.*, vol. 18, no. 4, pp. 2074–2084, 2024, doi: 10.1109/JSYST.2024.3476447.

[28] T. P. Nguyen, D. T. Vo, Q.-S. Vu, M. Tran, Q.-S. Nguyen, and T. Kim, "RIS-aided multi-antenna IoT systems: Performance evaluation under MRC combining," *Adv. Elect. Electron. Eng.*, vol. 23, no. 3, pp. 227–236, 2025, doi: 10.15598/aeee.v23i3.250801.

[29] J. Liu, S. Wang, B. Ji, R. Zheng, H. Li, and G. Zheng, "Energy-harvesting relay-assisted STAR-RIS-enhanced vehicular NOMA networks," *Vehicular Commun.*, vol. 55, 2025, doi: 10.1016/j.vehcom.2025.100960.

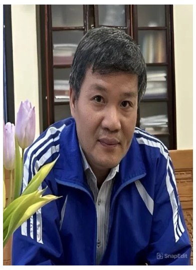
[30] M. Liaq, S. Sharif, S. Zeadally, and W. Ejaz, "Utilization of machine learning in future wireless networks for resource optimization: A survey," *Ad Hoc Netw.*, vol. 178, 2025, doi: 10.1016/j.adhoc.2025.103983.

[31] J. N. Laneman, D. N. C. Tse, and G. W. Wornell, "Cooperative diversity in wireless networks: Efficient protocols and outage behavior," *IEEE Trans. Inf. Theory*, vol. 50, no. 12, pp. 3062–3080, 2004, doi: 10.1109/TIT.2004.838089.

[32] F. Gholami, H. Meghdadi, and A. Shahzadi, "Throughput analysis for decode-and-forward relaying protocol with wireless energy harvesting and information processing," in *Proc. 2018 Int. Conf. Internet of Things, Embedded Syst. Commun. (IINTEC)*, 2018, pp. 132–135, doi: 10.1109/IINTEC.2018.8695285.

[33] H. A. Suraweera, G. K. Karagiannidis, and P. J. Smith, "Performance analysis of the dual-hop asymmetric fading channel," *IEEE Trans. Wireless Commun.*, vol. 8, no. 6, pp. 2783–2788, 2009, doi: 10.1109/TWC.2009.080420.
[34] G. Zhang *et al*., "Hybrid time-switching and power-splitting EH relaying for RIS-NOMA downlink," *IEEE Trans. Cogn. Commun. Networking*, vol. 9, no. 1, pp. 146–158, 2023, doi: 10.1109/TCCN.2022.3216406.
[35] C. Zhong, S. Jin, K.-K. Wong, and M. R. McKay, "Ergodic mutual information analysis for multi-keyhole MIMO channels," *IEEE Trans. Wireless Commun.*, vol. 10, no. 6, pp. 1754–1763, 2011, doi: 10.1109/TWC.2011.041311.091011.
[36] J. Wimp, "Table of Integrals, Series and Products: CD-ROM Version 1.0. By I. S. Gradshteyn and I. M. Ryzhik," *Am. Math. Mon.*, vol. 104, no. 4, pp. 373–376, 1997, doi: 10.1080/00029890.1997.11990651.

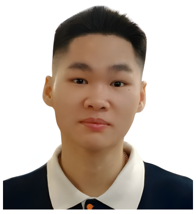
BIOGRAPHIES OF AUTHORS



The-Anh Ngo received B.S. degree at first grade in Telecommunications Engineering from University of Transport and Communications (UTC), Vietnam in 1997, and then he joined the Telecommunications Engineering Department and moved to Electrical and Electronics Engineering Division in Campus in Ho Chi Minh City of UTC as a lecturer. In 2012, he received M.Eng. degree in Telecommunications Engineering from University of South Australia, Australia. In 2024, he received Ph.D. degree in Telecommunications Engineering from Posts and Telecommunications Institute of Technology (PTIT), Vietnam. His major interests are wireless communications, cooperative communications, and physical-layer security. He can be contacted at email: anhnt_ph@utc.edu.vn.

Xuan-Truong Tran received B.S. degree at first grade in Telecommunications Engineering from University of Transport and Communications (UTC), Vietnam in 1997, and then he joined Department of Telecommunications Engineering and moved to Electrical and Electronics Engineering Division in Campus in Ho Chi Minh City of UTC as a lecturer. In 2003, he received M.Eng. degree in Electronics and Telecommunications Engineering from Ho Chi Minh City University of Technology. In 2012, he received Ph.D. degree in Automation from University of Transport and Communications (UTC), Vietnam. His major interests are switching techniques and optical communications. He can be contacted at email: truongtx_ph@utc.edu.vn.

Viet-Thanh Le is a lecturer at the Faculty of Information Technology, Ton Duc Thang University, Vietnam. He received his Bachelor's degree in Mathematics and Computer Science from the University of Sciences in 2000 and a Master's degree in Computer Science from Saigon University in 2022. Currently, in 2023, he is a Ph.D. candidate at Duy Tan University, Da Nang, Vietnam. His main research area includes wireless sensor networks. He has published several articles in international journals and participated in scientific conferences in his field. He can be contacted at email: levietthanh@tdtu.edu.vn.



Thien P. Nguyen is a fourth-year undergraduate student majoring in Electronics and Telecommunications at Ton Duc Thang University, Vietnam. As a dedicated member of the Wireless Communications Research Group, he focuses on advanced topics such as wireless communication systems, artificial intelligence, and the IoT. Despite being in the early stages of his academic journey, Thien has co-authored several international conference papers, demonstrating his strong commitment to innovation in wireless communications. With a passion for integrating AI and IoT into future networks, he strives to contribute to the development of cutting-edge telecommunication technologies. He can be contacted at email: nguyenphucthien999@gmail.com.

Duy-Hung Ha received B.S. and M.S. degrees in Electronics and Telecommunications Engineering from Institute of Post and Telecommunication, Vietnam; University of Transport and Communications, Hanoi, Vietnam in 2007 and 2014. In 2017, he joined the Faculty of Electrical and Electronics Engineering, Ton Duc Thang University, Vietnam as a lecturer. In 2021, he received a Ph.D. in communication technology at VSB-Technical University of Ostrava, Czech Republic. His major interests are cooperative communications and physical-layer security. He can be contacted at email: haduyhung@tdtu.edu.vn.