Research Article

Multi-Power Beacon Empowered Secure In Iot Networks: Secrecy Outage Probability Analysis

Tran Cong HUNG[1], *Quang Sang NGUYEN*[2], *Bui Vu MINH*[3], *Thu-Quyen Thi NGUYEN*[4], *Ngoc-Long NGUYEN*[5,*]

[1]Dean of School of Computer Science & Engineering, The SaiGon International University, Ho Chi Minh City 70000, Vietnam
[2]Posts and Telecommunications Institute of Technology, Ho Chi Minh City 70000, Vietnam
[3]Faculty of Engineering and Technology, Nguyen Tat Thanh University, 300A-Nguyen Tat Thanh, Ward 13, District 4, Ho Chi Minh City 754000, Vietnam
[4]Faculty of Electrical and Electronics Engineering, Ton Duc Thang University, Ho Chi Minh City 70000, Vietnam.
[5]Faculty of Applied Sciences, Ton Duc Thang University, Ho Chi Minh City 70000, Vietnam.

tranconghung@siu.edu.vn, sangnq@ptit.edu.vn, bvminh@ntt.edu.vn, nguyenthithuquyen@tdtu.edu.vn, nguyenngoclong@tdtu.edu.vn

*Corresponding author: Ngoc-Long Nguyen; nguyenngoclong@tdtu.edu.vn

DOI: 10.15598/aeee.v23i2.241112

Article history: Received Nov 25, 2024; Revised Dec 20, 2024; Accepted Jan 15, 2025; Published Jun 30, 2025.

Abstract. *This paper investigates the physical-layer secure performance of a multi-power beacon-empowered wirelessly powered communication system in the surveillance of an external eavesdropper. Specifically, a limited-energy source harvests energy from multiple dedicated power beacons in the first time slot and reuses it to perform data transmission in the second time slot. However, its communication with the destination is wiretapped by a potentially idle untrusted user. Thus, to evaluate the secure performance of the considered system, we have derived closed-form expressions for the secrecy outage probability (SOP) metric in terms of both exact and asymptotic aspects. Through these formulas, we then provide a series of numerical discussions on how to configure the number setting of the power beacon, the energy harvesting parameters as well as scheduling time to improve the SOP performance, where the Monte-Carlo simulation method is used to verify the developed mathematical framework.*

Keywords

Energy harvesting; eavesdropper; secure outage probability; performance analysis.

1. Introduction

Over the past few years, wireless communication-based systems have significantly expanded beyond cellular services to encompass a wide range of integrated Internet-of-Things (IoT) applications, including smart homes, smart cities, smart healthcare services, learning-integrated networks, and the metaverse [1]. The rise of these services and applications introduces new security challenges in sharing sensitive information between IoT entities [2]. Consequently, developing effective security methods to protect communication over the air interface is becoming increasingly difficult. Besides traditional methods such as cryptography or authentication [2], implementing physical layer security (PLS) methods such as random signalling or coding is also important to confuse the adversary. Moreover, PLS can be further enhanced by cooperation models, where relay nodes not only act as cooperative relaying nodes but also jammers to confuse the eavesdropper by cooperatively generating artificial noise. Due to its benefits, research on PLS has attracted the attention of many scientists again in recent years, for example, cognitive radio [3, 4], cooperative relaying systems [5, 6], wireless sensor network [7, 8], device-to-device communication [9], multi-hop communication [10], de-

tecting the presence of fiber optic splitter-based eavesdropping [11], non-orthogonal multiple access (NOMA) with untrusted near-users [12,13], unmanned aerial vehicle communications [14], and short-packet communication [15,16].

On the other hand, the issue of energy consumption is also considered one of the ultimate concerns in IoT networking developments besides those of spectrum utilization [17–20], where IoT devices do not always guarantee a strong power budget. To tackle the energy scarcity issue in low-power nodes, an alternative energy source is needed to compensate for the energy demand in case of battery exhaustion. A common solution is to employ energy harvesting (EH) techniques, where energy from ambient sources like solar or wind is scavenged and converted into electricity to recharge IoT devices' batteries. However, the energy output from these sources can be insufficient due to irregular and spatial variations and uncontrolled characteristics, questioning new efficient mechanisms. This is when direct radio-frequency (RF) EH technologies become an effective alternative to facilitating energy issues for low-cost IoT devices. Instead of harvesting from surrounding unstable environments, RF-EH technologies suggest reusing the availability of the RF signals to prolong the lifetime for less-battery devices by two dominant technologies [21]: wireless powered communication network (WPCN) and simultaneous wireless information and power transfer (SWIPT). Compared to WPCN which relies on deployments of dedicated power stations–the so-called power beacon, WPCN refers to using the same RF signal of source information to charge energy for limited-energy devices. These models lay a solid foundation for the development of green technology shortly of 5G and future 6G wireless networks, where there is a wealth of discussion in the literature regarding the aspects of wirelessly powered issues in recent years. For example, Nguyen *et al* discussed the potential of RF-EH technologies in two-way relaying protocols for transceiver impairments [22,23], distinct relay selection strategies [24,25], cooperative user selection [26], and his research group also introduced a new mechanism of self-energy recycling [27]. Tin *et al* analyzed the upper bound ergodic capacity and symbol error probability (SEP) of two-way networks based on SWIPT-time-switching (TS) protocols [28]. Hoang *et al* provided useful guidelines on optimizing the TS protocols in full duplex multiple-input multiple-output systems to maximize the system throughput [29]. Van Nguyen *et al* investigated the impact of hardware impairment on the outage performance of NOMA users in the context of ambient backscatter-based systems [30].

To the best of the authors' knowledge, research on the performance of wirelessly powered communication systems has widely focused on single-power beacon deployments in the literature [21], while those of PLS aspects with multiple-power beacons have not been touched yet. This motivates us to conduct this research by providing a rigorous mathematical analysis framework for evaluating security performance. The main contributions of the paper include two-folds as follows:

- This work has developed exact and asymptotic mathematical frameworks for evaluating the secrecy outage probability (SOP), where the efficacy of the developed frameworks has been verified via the Monte-Carlo simulation method.
- Through numerical results, this work has demonstrated that: i) increasing secure rate gives rise to the SOP performance, making the legitimate transmission more leaked to the eavesdropper; ii) there exists an optimal region where optimizing the time splitting coefficient can minimize the SOP performance; iii) enhancing the quality of energy harvesting circuit design can improve the SOP performance; and iv) deploying the number of power beacon can only significantly enhance the SOP performance with 6 elements.

The remaining structure of the paper is organized as follows. Section 2. describes the system model and communication protocols. Section 3. provides guidelines on how to evaluate the secure performance and numerical resulting discussions. Section 4. concludes the paper with key new system design findings.

2. System Models & Communication Protocol

Let us study a wirelessly empowered communication system in Fig. 1, composed of N-dedicated power beacon nodes P, an information source S, a destination D, and an eavesdropper E. In terms of system setup, all nodes are assumed to be equipped with single antenna deployments and the communication channels h_{V}, with $\mathrm{V} \in \{\mathsf{PS}, \mathsf{SD}, \mathsf{SE}\}$, of links $\mathsf{P} \to \mathsf{S}$, $\mathsf{S} \to \mathsf{D}$, and $\mathsf{S} \to \mathsf{E}$ are experience to static Rayleigh block fading. This means that h_{V} remain constant during one transmission block and changes independently across different ones. Under this assumption, the squared amplitudes of the channel gains $|h_{\mathrm{V}}|^2$ are exponential random variables (RVs) whose cumulative distribution function (CDF) and probability density function (PDF) have the following forms, respectively, as

$$\begin{aligned} F_{|h_{\mathrm{V}}|^2} &= 1 - \exp\left(-\Omega_{\mathrm{V}} x\right), \\ f_{|h_{\mathrm{V}}|^2} &= \partial F_{|h_{\mathrm{V}}|^2}/\partial x = \Omega_{\mathrm{V}} \exp\left(-\Omega_{\mathrm{V}} x\right), \forall x \geq 0, \end{aligned} \quad (1)$$

where Ω_{V} is the mean of channel gain $|h_{\mathrm{V}}|^2$, i.e., $\Omega_{\mathrm{V}} = \mathbb{E}\{|h_{\mathrm{V}}|^2\}$. To take path-loss into account, Ω_{V} can be

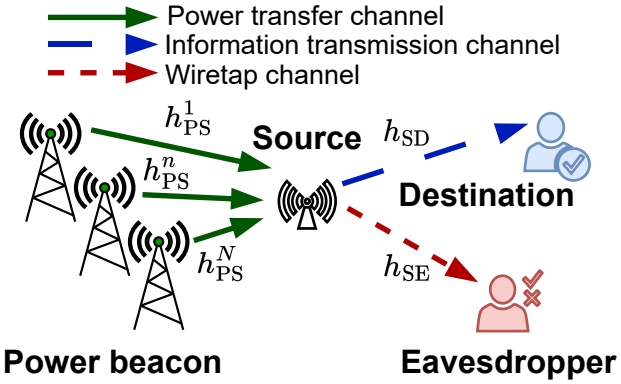


Fig. 1: Illustration of the considered system.

modeled by $\Omega_{\mathrm{V}} = (d_{\mathrm{V}})^{\theta}$, where d_{V} is the distance of links V while θ is the pathloss coefficient.

In terms of transmission, the system goes through two consecutive stages.

2.1. Energy Harvesting Phase

Initially, S exploits the period time αT of duration T to harvest energy from the power signals emitted by N power beacon, where $\alpha \in (0, 1)$ refers to the time splitting coefficient and its harvested energy is expressed as

$$E_{\mathsf{S}} = \eta \alpha T P_{\mathsf{P}} \sum_{n=1}^{N} |h_{\mathsf{PS}}^n|^2, \tag{2}$$

where η is the energy conversion efficiency and P_{P} is the average transmit power of P. Thus, the transmit power that S uses to serve communication can be derived as

$$\begin{aligned} P_{\mathsf{S}} &= \frac{E_{\mathsf{S}}}{(1-\alpha)T} = \frac{\eta \alpha T}{(1-\alpha)T} P_{\mathsf{P}} \sum_{n=1}^{N} |h_{\mathsf{PS}}^n|^2 \\ &= \kappa P_{\mathsf{P}} \sum_{n=1}^{N} |h_{\mathsf{PS}}^n|^2, \kappa \triangleq \frac{\eta \alpha}{(1-\alpha)}. \end{aligned} \tag{3}$$

2.2. Data Transmission Phase

In this phase, S transmits symbol s to D with transmission power P_{S} such that $\mathbb{E}\{|s|^2\} = 1$, where $\mathbb{E}\{\cdot\}$ is the expectation operator. However, due to broadcast wireless nature, not only D but also E receive the transmitted symbol s from S, and their received signals can be written accordingly as

$$y_{\mathsf{D}} = \sqrt{P_{\mathsf{S}}} x h_{\mathsf{SD}} + n_{\mathsf{D}}, \quad y_{\mathsf{E}} = \sqrt{P_{\mathsf{S}}} x h_{\mathsf{SE}} + n_{\mathsf{E}}, \tag{4}$$

where $n_{\mathsf{D}}, n_{\mathsf{E}} \sim \mathcal{CN}(0, N_0)$ are the additive white Gaussian noise with zero-mean and variance N_0 at D, E.

From the above signal observation, the received signal-to-noise ratio (SNR) at D and E for decoding symbol s can be calculated respectively as

$$\gamma_{\mathsf{D}} = \frac{P_{\mathsf{S}}}{N_0} |h_{\mathsf{SD}}|^2 = \kappa \frac{P_{\mathsf{P}}}{N_0} \sum_{n=1}^{N} |h_{\mathsf{PS}}^n|^2 |h_{\mathsf{SD}}|^2 = \Psi \kappa X Y, \tag{5}$$

$$\gamma_{\mathsf{E}} = \frac{P_{\mathsf{S}}}{N_0} |h_{\mathsf{SE}}|^2 = \kappa \frac{P_{\mathsf{P}}}{N_0} \sum_{n=1}^{N} |h_{\mathsf{PS}}^n|^2 |h_{\mathsf{SE}}|^2 = \Psi \kappa X Z. \tag{6}$$

where $\Psi = P_{\mathsf{S}}/N_0$ is the average transmit SNR, $X \triangleq \sum_{n=1}^{N} |h_{\mathsf{PS}}^n|^2$, $Y = |h_{\mathsf{SD}}|^2$, and $Z = |h_{\mathsf{SE}}|^2$. Note that since X can be expressed by summation of N independent and identical exponential random variables, the PDF of X is given by [5]

$$\begin{aligned} f_X(x) &= \frac{\Omega_{\mathsf{PS}}^N}{(N-1)!} x^{N-1} \exp\left(-\Omega_{\mathsf{PS}} x\right), \\ \Omega_{\mathsf{PS}} &= \Omega_{\mathsf{PS}}^n, \forall n = 1, 2, \cdots, N. \end{aligned} \tag{7}$$

On the foundation of the formulated SNRs above, we next move on evaluating the system's secure performance in the next section.

3. Performance Measurements & Results Discussions

In this section, we will evaluate the system's secure performance by first guiding how to measure the SOP metric in closed-form expressions and then providing numerical results based on Monte-Carlo simulation to verify the developed mathematical framework.

3.1. Performance Measurements

In the literature on physical layer security, such as [5], the researchers are interested in the possibility of conveying confidential messages at a positive rate, termed secrecy rate, between a source and a legitimate destination while keeping an eavesdropper ignorant if the source-destination channel is better than the relay-eavesdropper channel. In addition, the larger the difference in the channel strengths between the two channels, the higher the achieved secrecy rate. This secrecy rate is defined as

$$C_{\mathrm{sec}} = \max\left(C_{\mathsf{D}} - C_{\mathsf{E}}, 0\right), \tag{8}$$

where $C_{\mathsf{D}} = (1-\alpha)\log_2(1+\gamma_{\mathsf{D}})$ and $C_{\mathsf{E}} = (1-\alpha)\log_2(1+\gamma_{\mathsf{E}})$ are the achievable data rate at the destination and the eavesdropper, respectively. The secrecy outage event is said to occur when the secrecy capacity C_{sec} falls below a target secrecy rate $\overline{C}_{th}$. Therefore,

the SOP of the considered system can be given by

$$\begin{aligned}\mathsf{SOP} &= \Pr\left(C_{\text{sec}} < \overline{C}_{th}\right) \\ &= \Pr\left(\frac{1+\gamma_{\mathsf{D}}}{1+\gamma_{\mathsf{E}}} < \Psi_{th}\right),\ \Psi_{th} \triangleq 2^{\overline{C}_{th}/(1-\alpha)}. \quad (9)\end{aligned}$$

From (9), we can formulate the system SOP by the following theorem.

Theorem 1. *Exact closed-form SOP expressions for the considered system can be given as*

$$\begin{aligned}SOP = 1 - &\frac{2\Omega_{SE}\left(\Omega_{PS}\Omega_{SD}\widehat{\gamma}_{th}/[\kappa\Psi]\right)^{N/2}}{(N-1)!(\Omega_{SD}\Psi_{th}+\Omega_{SE})} \\ &\times \mathcal{K}_N\left(2\sqrt{\Omega_{PS}\Omega_{SD}\widehat{\gamma}_{th}/[\kappa\Psi]}\right), \quad (10)\end{aligned}$$

where $\widehat{\gamma}_{th} \triangleq \Psi_{th} - 1$ *while* $\mathcal{K}_N(\cdot)$ *is the modified Bessel function of the second kind and* N*-th order (See Eq. (8.432.1) in Ref. [31]).*

Proof. Substituting Ψ_{D} and Ψ_{E} into (9), we claim that

$$\begin{aligned}\mathsf{SOP} &= \Pr\left(\frac{1+\Psi\kappa XY}{1+\Psi\kappa XZ} < \Psi_{th}\right) \quad (11)\\ &= \Pr\left(\Psi\kappa XY < \widehat{\gamma}_{th} + \Psi_{th}\Psi\kappa XZ\right) \\ &= \int_0^\infty \underbrace{\Pr\left(\Psi\kappa xY < \widehat{\gamma}_{th} + \Psi_{th}\Psi\kappa xZ\right)}_{\Phi} f_X(x)dx,\end{aligned}$$

where Φ can be derived as

$$\begin{aligned}\Phi &= \Pr\left(Y < \frac{\widehat{\gamma}_{th} + \Psi_{th}\Psi\kappa xZ}{\Psi\kappa x}\right) \\ &= \int_0^\infty F_Y\left(\frac{\widehat{\gamma}_{th} + \Psi_{th}\Psi\kappa xz}{\Psi\kappa x}\right) f_Z(z)dz \\ &= \Omega_{\mathsf{SE}}\exp\left(-\frac{\Omega_{\mathsf{SD}}\widehat{\gamma}_{th}}{\Psi\kappa x}\right)\int_0^\infty \exp\left(-z\Omega_{\mathsf{SD}}\Psi_{th}\right) \\ &\quad \times \exp\left(-z\Omega_{\mathsf{SE}}\right)dz \\ &= \frac{\Omega_{\mathsf{SE}}}{\Omega_{\mathsf{SD}}\Psi_{th}+\Omega_{\mathsf{SE}}}\exp\left(-\Omega_{\mathsf{SD}}\frac{\widehat{\gamma}_{th}}{\Psi\kappa x}\right). \quad (12)\end{aligned}$$

Next, injecting (12) into (11), the SOP in (11) is reformulated as

$$\begin{aligned}\mathsf{SOP} &= \int_0^\infty \frac{\Omega_{\mathsf{SE}}}{\Omega_{\mathsf{SD}}\Psi_{th}+\Omega_{\mathsf{SE}}}\exp\left(-\Omega_{\mathsf{SD}}\frac{\widehat{\gamma}_{th}}{\Psi\kappa x}\right) f_X(x)dx \\ &= \frac{\Omega_{\mathsf{SE}}}{(N-1)!(\Omega_{\mathsf{SD}}\Psi_{th}+\Omega_{\mathsf{SE}})}\int_0^\infty \exp\left(-\frac{\Omega_{\mathsf{SD}}\widehat{\gamma}_{th}}{\Psi\kappa x}\right) \\ &\quad \times \Omega_{\mathsf{PS}}^N x^{N-1}\exp\left(-\Omega_{\mathsf{PS}}x\right)dx. \quad (13)\end{aligned}$$

Using Eq. (3.471.9) in Ref. [31], we can obtain the final SOP formula in (10). □

Theorem 1 shows that the system SOP can be efficiently expressed in a unique function that covers all the main system parameters and this function can be readily programmed with common software tools like Matlab, Mathematica, or Maple.

Next, to provide more insights into system designs, we turn to explore the system SOP behavior at high SNR regime. In detail, by setting $\Psi \to \infty$, we can approximate the SOP result in (9) as follows:

$$\begin{aligned}\widetilde{\mathsf{SOP}} &= \Pr\left(\frac{\gamma_{\mathsf{D}}}{\gamma_{\mathsf{E}}} < \Psi_{th}\right) = \Pr\left(\frac{Y}{Z} < \Psi_{th}\right) \\ &= \int_0^\infty F_Y\left(\Psi_{th}z\right) f_Z(z)dz \\ &= \Omega_{\mathsf{SE}}\int_0^\infty \exp(-z[\Omega_{\mathsf{SD}}\Psi_{th}+\Omega_{\mathsf{SE}}]) \\ &= 1 - \Omega_{\mathsf{SE}}/(\Omega_{\mathsf{SD}}\Psi_{th}+\Omega_{\mathsf{SE}}). \quad (14)\end{aligned}$$

The result in (14) states that the SOP trend does not depend on the transmit power, instead of dominating by three factors Ω_{SE}, Ω_{SD}, and Ψ_{th} when the transmit power of P becomes large enough. Moreover, since the SOP result in (14) is a simple function, it is particularly useful in designing the system performance. For example, if the system requires the SOP expectation $\mathsf{SOP}^\star$, the required rate should be

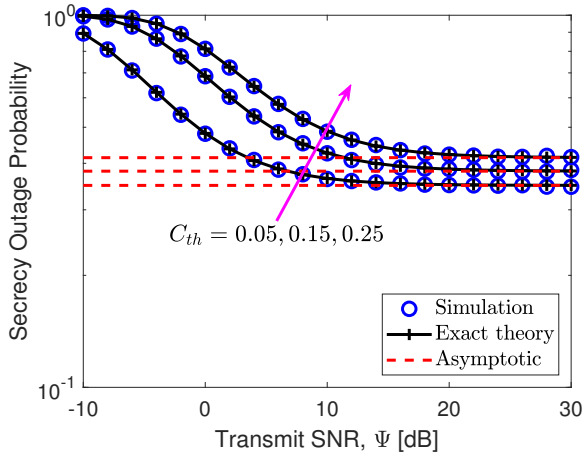
$$\begin{aligned}&\mathsf{SOP} \le \mathsf{SOP}^\star \Rightarrow \mathsf{SOP}^\star \le 1 - \Omega_{\mathsf{SE}}/(\Omega_{\mathsf{SD}}\Psi_{th}+\Omega_{\mathsf{SE}}) \\ &\Rightarrow \Psi_{th} \le \frac{1-\Omega_{\mathsf{SE}}-\mathsf{SOP}^\star\Omega_{\mathsf{SE}}}{\mathsf{SOP}^\star\Omega_{\mathsf{SD}}} \\ &\overline{C}_{th} \le (1-\alpha)\log_2\left(\frac{1-\Omega_{\mathsf{SE}}-\mathsf{SOP}^\star\Omega_{\mathsf{SE}}}{\mathsf{SOP}^\star\Omega_{\mathsf{SD}}}\right), \quad (15)\end{aligned}$$

where Ω_{SE} and Ω_{SD} can be efficiently computed by taking an average of channel gains, i.e., $\Omega_{\mathsf{SE}} = \mathbb{E}\{|h_{\mathsf{SE}}|^2\}$ and $\Omega_{\mathsf{SD}} = \mathbb{E}\{|h_{\mathsf{SD}}|^2\}$. Furthermore, since Ψ_{th} is proportional to C_{th} and α, we can rely on (14) to deduce that increasing C_{th} and α results in an increase in the SOP performance.

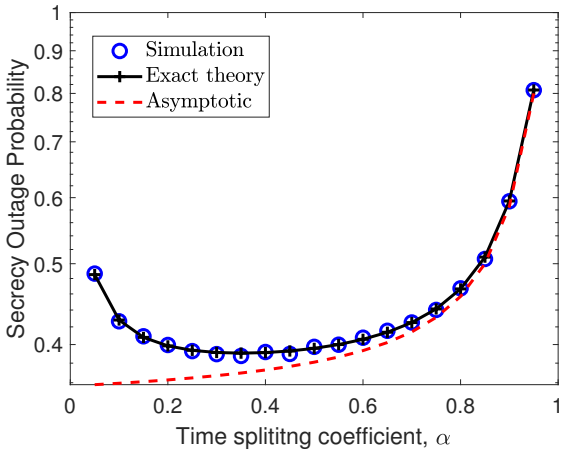
3.2. Results Discussions

To verify the above-developed mathematical framework, we next present some numerical results based on the Monte-Carlo Simulation method [32]. Specifically, for the sake of presentation, we list some fixed parameters used through the following figures as follows: $N = 4$, $\Omega_{\mathsf{PS}} = 2$, $\Omega_{\mathsf{SD}} = 4$, $\Omega_{\mathsf{SE}} = 8$, $T = 1$ (second), $\eta = 0.8$, $\alpha = 0.5$, $C_{th} = 0.1$, and $N = 4$, and the number of Monte-Carlo sample is 10^3.

Fig. 2 plots the system SOP performance as a function of SNR Ψ in dB and α using the developed expressions in (10) for the theory results and (14) for the asymptotic ones. As we can observe from Fig. 2(a), our developed mathematical frameworks are excellently matched with the simulation results. Besides, we can see that the SOP curves tend to first reduce with an increase of Ψ and then become saturated at high SNR and well aligns with the asymptotic

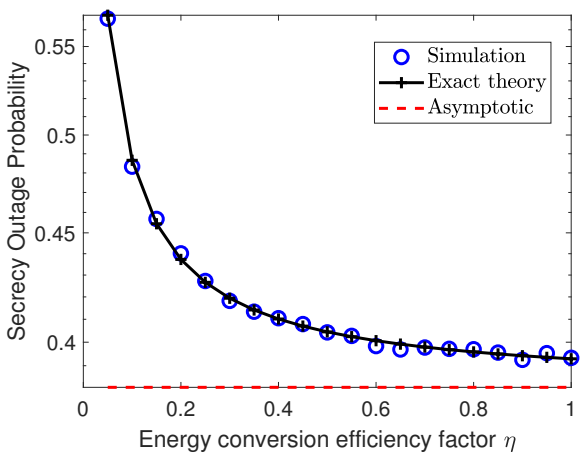


(a) Impact of Ψ.

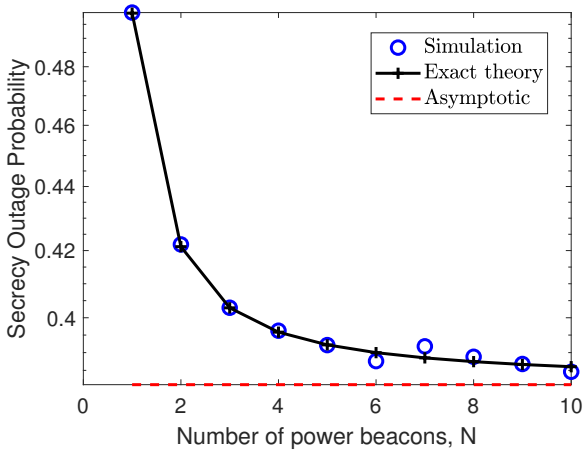


(b) Impact of α

Fig. 2: SOP versus SNR Ψ in dB and α. a) $\alpha = 0.5$ and b) $\Psi = 15$ dB.



(a) Impact of η



(b) Impact of N

Fig. 3: SOP versus η and N when the transmit SNR Ψ is 15 dB.

outcomes, which are almost true with our discussion from (14). Especially, the figure also verifies the correctness of our prediction based on the result in (14) that the higher the security rate the larger the SOP. On the other hand, we can observe from Fig. 2(b) that the SOP has a convex form, where it tends to reduce and then increase. This means that there is an optimal region at which $\alpha^\star$ can minimize the SOP performance.

Fig. 3 plots the system SOP performance as a function of η and N. From Fig. 3(a), we can observe that the SOP is improved significantly when S is equipped with an enhanced energy harvesting circuit. This is because S will have more chance to increase the transmit power, thereby improving SOP performance. Similarly, Fig. 3(b) also shows that the higher the number of power beacons, the better the SOP performance. However, we can recognize that the design of either $\eta > 0.6$ or $N > 6$ does not contribute to significant SOP improvement.

4. Conclusions

In this work, we developed mathematical frameworks in terms of exact and asymptotic closed-form expressions that allows us to efficiently evaluate the SOP performance without performing any simulation. From numerical results, we also found that there is a trade-off between the energy harvesting and information transmission phases, at which optimizing the time-splitting coefficient could result in the SOP minimization. Additionally, the configuration of the energy conversion efficiency factor attained the best improvement region from 0.1 to 0.6, while the remaining ranges are negligible to the practice implementations. Moreover, deploying the number of power beacons only benefits from 3 to 6 elements, while increasing more numbers does not yield significant SOP improvement.

Although this work provided an accurate mathematical framework for performance evaluation, it still has several empty rooms for future investigations, such as

multi-antennas sources, non-linear energy harvesting issues, channel imperfections, and hardware impairments.

Author Contributions

Tran Cong Hung and Ngoc Long Nguyen developed the system model while Quang Sang Nguyen and Bui Vu Minh performed the analytical calculations as well as numerical simulations. Finally, Thu-Quyen Thi Nguyen wrote the whole paper. All authors contributed to the final version of the manuscript.

References

[1] LE M., T. HUYNH-THE, T. DO-DUY, T. -H. VU, W. -J. HWANG, and Q. -V. PHAM. Applications of Distributed Machine Learning for the Internet-of-Things: A Comprehensive Survey. *IEEE Communications Surveys & Tutorials*. 2024. DOI: 10.1109/COMST.2024.3427324.

[2] AOUEDI O., et al. A Survey on Intelligent Internet of Things: Applications, Security, Privacy, and Future Directions. *IEEE Communications Surveys & Tutorials*. 2024. DOI: 10.1109/COMST.2024.3430368.

[3] PHU T. T., T. H. DANG, N. N. TAN, T. T. DUY, and V. MIROSLAV. Secrecy Performance Enhancement for Underlay Cognitive Radio Networks Employing Cooperative Multi-Hop Transmission with and without Presence of Hardware Impairments. *Entropy*. 2019, vol. 21, no. 2. DOI: 10.3390/e21020217.

[4] TIN P. T., PHAN, V.-D., NGUYEN, T. N., TU, L.-T., MINH, B. V., VOZNAK, M., and FAZIO, P. Outage Analysis of the Power Splitting Based Underlay Cooperative Cognitive Radio Networks. *Sensors*. 2021, vol. 21, no. 22. DOI: 10.3390/s21227653.

[5] HA D. -H., T. N. NGUYEN, M. H. Q. TRAN, X. LI, P. T. TRAN, and M. VOZNAK. Security and Reliability Analysis of a Two-Way Half-Duplex Wireless Relaying Network Using Partial Relay Selection and Hybrid TPSR Energy Harvesting at Relay Nodes. *IEEE Access*. 2020, vol. 8, pp. 187165-187181. DOI: 10.1109/ACCESS.2020.3030794.

[6] H. A. NGO, et al. Physical Layer Security in Hybrid TPSR Two-Way Half-Duplex Relaying Network over Rayleigh Fading Channel: Outage and Intercept Probability Analysis. *Electronics*.2020, vol. 9, no. 3, pp.1-16. DOI: 10.3390/electronics9030428.

[7] NGUYEN T. N., et al. Security–Reliability Tradeoff Analysis for SWIPT- and AF-Based IoT Networks With Friendly Jammers. *IEEE Internet of Things Journal*. 2022, vol. 9, no. 21, pp. 21662-21675. DOI: 10.1109/JIOT.2022.3182755.

[8] MINH T., et al. Security and Reliability Analysis of the Power Splitting-Based Relaying in Wireless Sensors Network. *Sensors*. 2024, vol. 24, no. 4. DOI: 10.3390/s24041300.

[9] BUI V. M., N.H.K.NHAN, T.H.T.PHAM, M.TRAN, and S-W KIM. Physical Layer Security in wireless sensors networks with friendly jammer: Secrecy Outage Probability Analysis. *Advances in Electrical and Electronic Engineering*. 2024, vol. 22, no. 4, pp. 387-398. DOI: 10.15598/aeee.v22i4.5840.

[10] CHU T. D., et al. Secrecy performance of multi-user multi-hop cluster-based network with joint relay and jammer selection under imperfect channel state information. *Performance Evaluation*. 2021, vol. 147. DOI: 10.1016/j.peva.2021.102193.

[11] DAVID G., J. FROLKA, K. SLAVICEK, O. DOSTAL, and M. KYSELAK. Network Physical Layer Attack in the Very High Capacity Networks. *Advances in Electrical and Electronic Engineering*. 2023, vol. 21, no. 1, pp. 37-47. DOI: 10.15598/aeee.v21i1.4973.

[12] VU T. -H., Q. -V. PHAM, D. B. D. COSTA, M. DEBBAH, and S. KIM. Physical-Layer Security in Short-Packet NOMA Systems with Untrusted Near Users. *2023 IEEE International Conference on Communications Workshops (ICC Workshops), Rome, Italy*. 2023, pp. 1830-1835. DOI: 10.1109/ICCWorkshops57953.2023.10283496.

[13] T.C. HUNG, et al. Performance analysis of dual-hop mixed RF-FSO systems combined with NOMA. *PloS ONE*. 2024, vol. 19, no. 12, pp. 1-19. DOI: 10.1371/journal.pone.0315123.

[14] NGUYEN N. T., et al. On the Dilemma of Reliability or Security in Unmanned Aerial Vehicle Communications Assisted by Energy Harvesting Relaying. *IEEE Journal on Selected Areas in Communications*. 2024, vol. 42, no. 1, pp. 52-67. DOI: 10.1109/JSAC.2023.3322756.

[15] NGUYEN T. -V., T. -H. VU, T. HUYNH-THE, and D. B. D. COSTA. Secrecy Performance of Short-Packet Communications in MultiHop IoT Networks With Imperfect CSI. *IEEE Wireless*

Communications Letters. 2024, vol. 13, no. 4, pp. 1093-1097. DOI: 10.1109/LWC.2024.3361379.

[16] C. FENG AND H. -M. WANG. Secure Short-Packet Communications at the Physical Layer for 5G and Beyond. *IEEE Communications Standards Magazine*. 2021, Vol. 5, no. 3, pp. 96-102. DOI: 10.1109/MCOMSTD.121.2100028.

[17] TIN P. T., T. L. NGUYEN, N. T. NGUYEN, M. TRAN, and T. T. DUY. Throughput enhancement for multi-hop decode-and-forward protocol using interference cancellation with hardware imperfection. *Alexandria Engineering Journal*. 2022, Vol. 61, Iss. 8, PP. 5837-5849. DOI: 10.1016/j.aej.2021.11.008.

[18] NGUYEN N. T., et al. Outage Performance of Satellite Terrestrial Full-Duplex Relaying Networks With Co-Channel Interference. *IEEE Wireless Communications Letters*. 2022, vol. 11, no. 7, pp. 1478-1482. DOI: 10.1109/LWC.2022.3175734.

[19] NGUYEN T. T. T., D.-T. DO. Exploiting Full-duplex and Fixed Power Allocation Approaches for Dual-hop Transmission in Downlink NOMA. *Advances in Electrical and Electronic Engineering*. 2021, vol. 19, no. 3, pp. 212–221. DOI: 10.15598/aeee.v19i3.4116.

[20] SUBHRA S. M., J. S. ROY. SC-FDMA uplink system in heavily faded areas with low signal-to-noise ratio. *Advances in Electrical and Electronic Engineering*. 2023, vol. 21, no. 3, pp. 206-215. DOI: 10.15598/aeee.v21i3.4987.

[21] VU T. -H., S. KIM. Performance Evaluation of Power-Beacon-Assisted Wireless-Powered NOMA IoT-Based Systems. *IEEE Internet of Things Journal*. 2021, vol. 8, no. 14, pp. 11655-11665. DOI: 10.1109/JIOT.2021.3058680.

[22] NGUYEN N. T., et al. Two-Way Half Duplex Decode and Forward Relaying Network with Hardware Impairment over Rician Fading Channel: System Performance Analysis. *Elektronika Ir Elektrotechnika*. 2018, vol. 24, no. 2, pp. 74-78. DOI: 10.5755/j01.eie.24.2.20639.

[23] NGUYEN N. T., Q. M. T. HOANG, T. T. PHUONG, and M. VOZNAK. Energy Harvesting over Rician Fading Channel: A Performance Analysis for Half-Duplex Bidirectional Sensor Networks under Hardware Impairments. *Sensors*. 2018, vol. 18, no. 6. DOI: 10.3390/s18061781.

[24] NGUYEN N. T., et al. Performance enhancement for energy harvesting based two-way relay protocols in wireless ad-hoc networks with partial and full relay selection methods. *Ad Hoc Networks*. 2019, vol. 81, pp. 178-187. DOI: 10.1016/j.adhoc.2018.10.005.

[25] NGUYEN T. N., M. TRAN, T. -L. NGUYEN, and M. VOZNAK. Adaptive relaying protocol for decode and forward full-duplex system over Rician fading channel: System performance analysis. *China Communications*. 2019, vol. 16, no. 3, pp. 92-102. DOI: 10.12676/j.cc.2019.03.009.

[26] NGUYEN N. T., M. TRAN, T. L. NGUYEN, , D. H. HA, and M. VOZNAK. Performance Analysis of a User Selection Protocol in Cooperative Networks with Power Splitting Protocol-Based Energy Harvesting Over Nakagami-m/Rayleigh Channels. *Electronics*. 2019, vol. 8, no. 4. DOI: 10.3390/electronics8040448.

[27] NGUYEN T. N., T. T. DUY, P. T. TRAN, M. VOZNAK, X. LI, and H. V. POOR. Partial and Full Relay Selection Algorithms for AF Multi-Relay Full-Duplex Networks With Self-Energy Recycling in Non-Identically Distributed Fading Channels. *IEEE Transactions on Vehicular Technology*. 2022, vol. 71, no. 6, pp. 6173-6188. DOI: 10.1109/TVT.2022.3158340.

[28] TIN P. T., N. T. NGUYEN, M. TRAN, T. T. THANH, and S. LUKAS. Exploiting Direct Link in Two-Way Half-Duplex Sensor Network over Block Rayleigh Fading Channel: Upper Bound Ergodic Capacity and Exact SER Analysis. *Sensors*. 2020, vol. 20, no. 4. DOI: 10.3390/s20041165.

[29] HOANG T. M., N. B. CAO, T. N. NHU, M. TRAN, and T. T. PHUONG. Performance and optimal analysis of time-switching energy harvesting protocol for MIMO full-duplex decode-and-forward wireless relay networks with various transmitter and receiver diversity techniques. *Journal of the Franklin Institute*. 2020, vol. 357, iss. 17, pp. 13205-13230. DOI: 10.1016/j.jfranklin.2020.09.037.

[30] SANG N. V. M., and H. P. DANG. Exploiting Performance of Ambient Backscatter Systems in Presence of Hardware Impairment. *Advances in Electrical and Electronic Engineering*. 2021, vol. 19, no. 4, pp. 313–321. DOI: 10.15598/aeee.v19i4.4198.

[31] GRADSHTEYN I. S., R. I. MOISEEVICH. Table of integrals, series, and products. 7th ed. San Diego, CA, USA, *Academic press*, 2007.

[32] T.N.NGUYEN, et al. Intelligent Reflecting Surface Aided Bidirectional Full-Duplex Communication System with Imperfect Self-Interference Cancellation and Hardware Impairments. *IEEE Systems Journal*. 2022, Vol. 17, No. 1, pp. 1352-1362. DOI: 10.1109/JSYST.2022.3167514.