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

Intercept Probability Analysis of the Energy Harvesting Enabled Multisource Half-Duplex Relaying Network with Receiver Diversity Techniques

Tan N. Nguyen[1], Pham Ngoc Son[2], Lam-Thanh Tu[1*]
[1]Ton Duc Thang University, Ho Chi Minh City, Vietnam
[2]Ho Chi Minh City University of Technology and Education, Vietnam

[*]Corresponding author. *Email: tulamthanh@tdtu.edu.vn*

ARTICLE INFO

Received: 24/08/2023
Revised: 15/09/2023
Accepted: 18/09/2023
Published: 28/04/2024

KEYWORDS

Amplify-and-forward;
Energy Harvesting;
Outage Probability;
Relaying network;
Time Switching.

ABSTRACT

In this paper, the performance of a multisource half-duplex relaying network utilizing the time-switching approach is investigated. Particularly, the relay simply relies on the harvested energy from the selected source to perform its operations such as amplifying and forwarding the source signals. The selected source is chosen according to the channel gain of the legitimate link from all source nodes to the relay. Under this context, the intercept probability (IP) of the considered system model with both maximal ratio combining (MRC) and selection combining (SC) is analyzed and presented in the integral-form and closed-form expressions. Monte Carlo simulations are deployed to confirm the accuracy of the analytical framework as well as to find out the impact of the main system parameters. The outcomes indicate that the simulation and analytical values are the same in all cases. It also unveils that the MRC is always superior to the SC scheme. Additionally, the IP is a concave function with respect to the time-switching ratio while the IP is a monotonic function regarding the number of source nodes, transmit power, etc.

Doi: https://doi.org/10.54644/jte.2024.1458

1. Introduction

With the exponential growth of the number of wirelessly connected devices towards the Internet of Things (IoTs), cyber security has become one of the most important issues that need to be tackled along with conventional problems like spectral efficiency (SE) and energy efficiency (EE) [1]. Yet, another problem is how to scale up the EE of the networks since the number of connected devices is ultra-large. To overcome such an issue, a recently proposed technique called simultaneous wireless information and power transfer (SWIPT) has been considered a promising solution since it allows devices to operate without connecting to the electrical grid thus ameliorating the EE of the networks [2]-[4]. To realize such advanced techniques, three popular protocols have been proposed in the literature such as time switching, power splitting, and antenna splitting protocols. The last approach, however, requires at least two antennae at the receiver while the first two methods require only a single antenna combined with the power splitter and switching circuits. On the other hand, relaying networks has proven itself as one of the most effective ways to enhance the SE of the networks. Particularly, by shortening the transmission distance combined with advanced signal processing such as decode and forward (DF) and amplify and forward (AF) protocol. The system reliability will significantly improve.

The performance of the EH-enabled relaying networks was investigated in [5]-[11]. Particularly, Tan and other authors studied the performance of the full-duplex relaying networks under the imperfect channel state information (CSI) [5]. A novel architecture and trade-off between rate and energy was investigated in [6]. Kashef et. al. derived the optimal partial relaying selection in the EH-enabled networks [7]. The system-level performance of the SWIPT-enabled cellular networks was addressed in [8]. The impact of co-channel satellite-terrestrial full-duplex relaying networks was given in [9] while the outage probability (OP) of power splitting-based cooperative cognitive radio networks (CRNs) was derived in [10]. The OP performance of the incremental underlay CRNs with imperfect CSI was provided in [11].

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

Different from the above-mentioned works, in the present paper, we study the security aspects of EH-enabled relaying networks. Particularly, we consider the SWIPT-based networks via the time-switching protocol. The main contributions and novelties of this manuscript can be drawn as follows:

1. We consider a multisource half-duplex SWIPT-enabled relaying network based on the time-switching protocol.
2. We adopt both maximal ratio combining (MRC) and selection combining (SC) diversity techniques at the eavesdropper to take advantage of multiple available replicas of the main link signals.
3. We derive the intercept probability (IP) of the considered systems in the closed-form expression.
4. We confirm the correctness of the analytical framework with Monte Carlo simulations and find out the impact of some main parameters on the performance of the IP.

2. System model

Let us consider an EH-enabled relaying network as shown in Fig. 1. It comprises M sources having information to transmit to the destination D. Owing to the long transmission distance, the direct transmission from all S to D is not available. They can only exchange information via the help of relay R. Nonetheless, the relay is not connected to the power grid, it simply counts on the harvested energy from the source node. The whole transmission is taken place in three phases. In the first and second phases, the source that has the largest channel coefficient to relay R is selected to transmit. At the relay, in the first phase, it will harvest energy from the incoming signals sent by the selected source. It, then, in the second phase will decode information from S. In the last phase, the relay employs amplify-and-forward (AF) protocol to amplify and forward source signals to the destination as illustrated in Fig. 2. The considered network also comprises an active eavesdropper denoted by E who attempts to wiretap the secure information in the main link. All nodes are equipped with a single antenna. We also consider block fading where the fading is stable for the whole transmission but varies between transmissions.

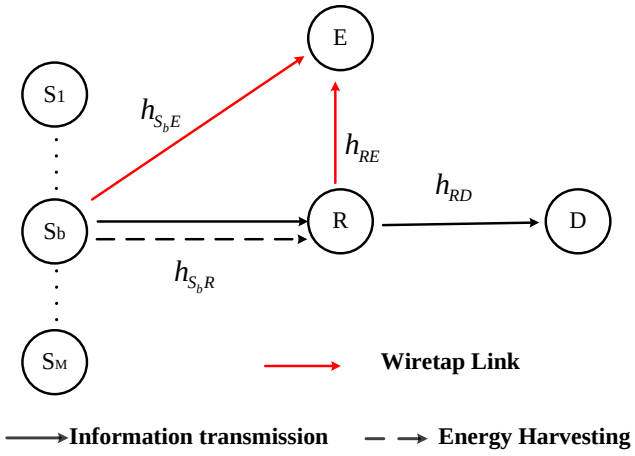

Figure 1. *System model*

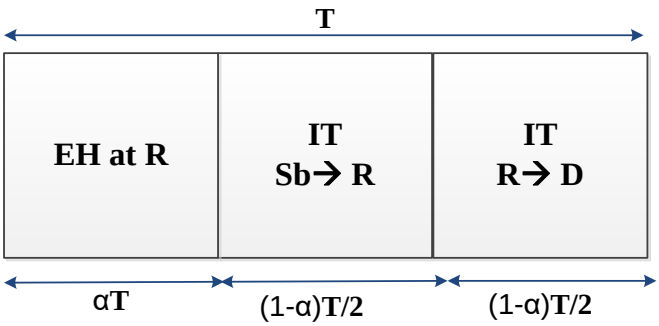

Figure 2. *Time splitting protocol*

In the first transmission phase, the received signal at the relay can be given by

$$y_r = h_{S_bR} x_{S_b} + n_r \tag{1}$$

where $b \in (1,2,...,M)$; x_{S_b} is the transmitted signal at the source, n_r is the additive white Gaussian noise (AWGN) with variance N_0 and $\mathrm{E}\left\{\left|x_{S_b}\right|^2\right\} = P_{S_b}$, $\mathrm{E}\{\bullet\}$: is the expectation operator, P_{S_b} is the transmit power of the bth source). h_{S_bR} is the channel coefficient from the selected source to the relay. The harvested power at the relay R can be obtained as:

$$P_r = \frac{E_h}{(1-\alpha)T/2} = \frac{\eta\alpha T P_{S_b}\left|h_{S_bR}\right|^2}{(1-\alpha)T/2} = \kappa P_{S_b}\left|h_{S_bR}\right|^2 \tag{2}$$

where $\kappa = \frac{2\eta\alpha}{1-\alpha}$ and $0 < \eta \le 1$ are the shorthand and the energy conversion efficiency which takes into account the energy loss by harvesting circuits and by decoding and processing circuits. T is the whole transmission duration and $\left|h_{S_bR}\right|^2$ is the channel gain from b-th source to the relay. The received signal at the eavesdropper from the source and relay in the second and third phases are given as follows:

$$\begin{aligned} y_E^2 &= h_{S_bE} x_{S_b} + n_E^2, \\ y_E^3 &= h_{RE} x_r + n_E^3 \end{aligned} \tag{3}$$

where h_{RE}, h_{S_bE} are channel coefficient from the relay and selected source to the eavesdropper; n_E^2, n_E^3 and n_E are the zero-mean AWGN with the same variance N_0, and $\mathrm{E}\left\{\left|x_r\right|^2\right\} = P_r$.

Since the AF protocol is considered, the relay will amplify the source signals and forward them to the destination with the following amplification factor [12]

$$\beta = \frac{x_r}{y_r} = \sqrt{\frac{P_r}{P_{S_b}\left|h_{S_bR}\right|^2 + N_0}} \tag{4}$$

From (3) and (4), the received signal at E in the third phase can be rewritten by

$$\begin{aligned} y_E^3 &= h_{RE}\beta y_r + n_E^3 \\ &= h_{RE}\beta\left[h_{S_bR}x_{S_b} + n_r\right] + n_E^2 \\ &= \underbrace{h_{S_bR}x_{S_b}h_{RE}\beta}_{signal} + \underbrace{h_{RE}\beta n_r + n_E^2}_{noise} \end{aligned} \tag{5}$$

Hence, the signal to noise ratio (SNR) at E in this phase can be obtained by

$$\gamma_E^3 = \frac{\mathrm{E}\left\{\left|signal\right|^2\right\}}{\mathrm{E}\left\{\left|noise\right|^2\right\}} = \frac{P_{S_b}\left|h_{S_bR}\right|^2\left|h_{RE}\right|^2\beta^2}{\left|h_{RE}\right|^2\beta^2 N_0 + N_0} = \frac{P_{S_b}\left|h_{S_bR}\right|^2\left|h_{RE}\right|^2}{\left|h_{RE}\right|^2 N_0 + \frac{N_0}{\beta^2}} = \frac{\kappa\Psi\left|h_{S_bR}\right|^2\left|h_{RE}\right|^2}{\kappa\left|h_{RE}\right|^2 + 1} \tag{6}$$

Here $\Psi = P_{S_b}/N_0$, after some manipulations and using the fact that N_0<<Pr, we have

$$\gamma_D^2 = \frac{P_{S_b}P_r\left|h_{S_bR}\right|^2\left|h_{RE}\right|^2}{\left|h_{RE}\right|^2 P_r N_0 + P_{S_b}\left|h_{S_bR}\right|^2 N_0} \tag{7}$$

the SNR at eavesdropper in the second phase is computed as

$$\gamma_E^2 = \Psi\left|h_{S_bE}\right|^2 \tag{8}$$

Since the E receives two versions of the transmitted signals sent by S. It, as a consequence, can employ different receiver techniques to maximize the wiretap chances. More precisely, two popular receiver techniques, namely, maximal ratio combining and selection combining are used in the present work[1].

The best source S_b is selected to maximize the end-to-end (e2e) signal-to-noise-ratio (SNR) at the destination to maximize the system performance. The criteria to choose the best source are given below

$$\omega_1 = \max_{b=1,2,...,M} \left(\left| h_{S_b R} \right|^2 \right) \tag{9}$$

Here the cumulative distribution function (CDF) of ω_1 is given as [13]

$$F_{\omega_1}(x) = \sum_{n=0}^{M} (-1)^n C_M^n \times e^{-\lambda_1 n x} = 1 + \sum_{n=1}^{M} (-1)^n C_M^n \times e^{-\lambda_1 n x} \tag{10}$$

where $C_M^n = \dfrac{M!}{n!(M-n)!}$ and λ_1 are the mean of a random variable (RV) ω_1. The corresponding probability density function (PDF) of ω_1 is then given as [13]

$$f_{\omega_1}(x) = \lambda_1 \sum_{n=0}^{M-1} (-1)^n C_{M-1}^n M \times e^{-\lambda_1 (n+1) x} \tag{11}$$

Intercept probability (IP) analysis

The IP of the system is defined as the probability that the eavesdropper successfully wiretaps the secure information from the source to the destination. Mathematical speaking, it is formulated as [14]

$$IP = \Pr\left(\gamma_{AF}^i > \gamma_{th} \right) \tag{12}$$

where γ_{th} is the predefined threshold of the system and $i \in (MRC, SC)$.

3. The System Performance

3.1. MRC diversity technique

In this technique, the e2e SNR at E is given as following with the help from (7) and (8)

$$\gamma_{AF}^{MRC} = \gamma_E^2 + \gamma_E^3 = \frac{\kappa \Psi \omega_1 \omega_2}{\kappa \omega_2 + 1} + \Psi \omega_3 \tag{13}$$

where $\omega_2 = \left| h_{RE} \right|^2, \omega_3 = \left| h_{S_j E} \right|^2$. Substituting (13) into (12), the IP, under the MRC technique, is given as [15]

$$\begin{aligned} IP_{MRC} &= 1 - \Pr\left(\frac{\kappa \Psi \omega_1 \omega_2}{\kappa \omega_2 + 1} + \Psi \omega_3 < \gamma_{th} \right) \\ &= 1 - \Pr\left(X + Y < \gamma_{th} \right) = 1 - \int_0^{\gamma_{th}} F_X(\gamma_{th} - y) \times f_Y(y) dy \end{aligned} \tag{14}$$

where $X = \dfrac{\kappa \Psi \omega_1 \omega_2}{\kappa \omega_2 + 1}$, and $Y = \Psi \omega_3$. Next, we are going to derive the CDF of X and PDF of Y as follows:

[1] It is noted that relying on the applications and/or cost, one can consider either MRC or SC scheme. In particular, if reliability is preferred, the MRC is a better choice. On the other hand, if reliability is not the highest priority but the cost, i.e., the receiver is a low-cost device, a SC scheme should be considered in this circumstance.

$$F_X(x)=\Pr\left(\frac{\kappa\Psi\omega_1\omega_2}{\kappa\omega_2+1}<x\right)=\Pr\left(\omega_1<\frac{x(\kappa\omega_2+1)}{\kappa\Psi\omega_2}\right)$$
$$=\Pr\left(\omega_1<\frac{x}{\Psi}+\frac{x}{\kappa\Psi\omega_2}\right)=\int_0^{\infty}F_{\omega_1}\left(\frac{x}{\Psi}+\frac{x}{\kappa\Psi\omega}\right)\times f_{\omega_2}(\omega)d\omega \quad (15)$$

By using (10), (15) can be rewritten as

$$F_X(x)=1+\sum_{n=1}^{M}(-1)^n C_M^n\times\lambda_2\exp\left(-\frac{\lambda_1 nx}{\Psi}\right)\int_0^{\infty}\exp\left(\frac{-\lambda_1 nx}{\kappa\Psi\omega}-\lambda_2\omega\right)d\omega \quad (16)$$

where λ_2 is the mean of RV ω_2. With the help of [16, 3.324.1], $F_X(x)$ is derived as

$$F_X(x)=1+2\sum_{n=1}^{M}(-1)^n C_M^n\times\sqrt{\frac{\lambda_1\lambda_2 nx}{\kappa\Psi}}\times\exp\left(-\frac{\lambda_1 nx}{\Psi}\right)\times K_1\left(2\sqrt{\frac{\lambda_1\lambda_2 nx}{\kappa\Psi}}\right) \quad (17)$$

where $K_1(\bullet)$ is the modified Bessel function of second kind with 1[th] order.

On the other hand, the CDF of Y can be computed by

$$F_Y(y)=\Pr(Y<y)=\Pr(\Psi\omega_3<y)=\Pr\left(\omega_3<\frac{y}{\Psi}\right)=1-\exp\left(\frac{-\lambda_3 y}{\Psi}\right) \quad (18)$$

where λ_3 is the mean of RV ω_3. Hence, the PDF of Y can be obtained as

$$f_Y(y)=\frac{\partial F_Y(y)}{\partial y}=\frac{\lambda_3}{\Psi}\exp\left(-\frac{\lambda_3 y}{\Psi}\right) \quad (19)$$

Finally, substituting (17) and (19) into (14), the IP_{MRC} can be claimed by

$$IP_{MRC}=1-\frac{\lambda_3}{\Psi}\int_0^{\gamma_{th}}\left\{\begin{array}{l}1+2\sum_{n=1}^{M}(-1)^n C_M^n\times\sqrt{\frac{\lambda_1\lambda_2 n(\gamma_{th}-y)}{\kappa\Psi}}\\ \times\exp\left(-\frac{\lambda_1 n(\gamma_{th}-y)}{\Psi}\right)\times K_1\left(2\sqrt{\frac{\lambda_1\lambda_2 n(\gamma_{th}-y)}{\kappa\Psi}}\right)\end{array}\right\}\times\exp\left(\frac{-\lambda_3 y}{\Psi}\right)dy \quad (20)$$

3.2. SC diversity technique

Under the SC technique, the end-to-end SNR at E is given as [17]

$$\gamma_{AF}^{SC}=\max\left(\gamma_E^1,\gamma_E^2\right)=\max\left(\frac{\kappa\Psi\omega_1\omega_2}{\kappa\omega_2+1},\Psi\omega_3\right)=\max(X,Y) \quad (21)$$

The IP, in this case, can be calculated by

$$IP_{SC}=1-\Pr\left(\gamma_{AF}^{SC}<\gamma_{th}\right)=1-\Pr\left(\max(X,Y)<\gamma_{th}\right)$$
$$=1-\Pr(X<\gamma_{th})\Pr(Y<\gamma_{th})$$
$$=1-F_X(\gamma_{th})\times F_Y(\gamma_{th}) \quad (22)$$

Using the results from (17) and (18), the IP_{SC} can be obtained as

$$IP_{SC}=1-\left\{1+2\sum_{n=1}^{M}(-1)^n C_M^n\times\sqrt{\frac{\lambda_1\lambda_2 n\gamma_{th}}{\kappa\Psi}}\times\exp\left(-\frac{\lambda_1 n\gamma_{th}}{\Psi}\right)\times K_1\left(2\sqrt{\frac{\lambda_1\lambda_2 n\gamma_{th}}{\kappa\Psi}}\right)\right\}\times\left(1-\exp\left(-\frac{\lambda_3\gamma_{th}}{\Psi}\right)\right) \quad (23)$$

Remark 1. By direct inspection (23), we observe that increasing γ_{th} will monotonically decrease the IP since both terms $\left\{1+2\sum_{n=1}^{M}(-1)^n C_M^n\times\sqrt{\frac{\lambda_1\lambda_2 n\gamma_{th}}{\kappa\Psi}}\times\exp\left(-\frac{\lambda_1 n\gamma_{th}}{\Psi}\right)\times K_1\left(2\sqrt{\frac{\lambda_1\lambda_2 n\gamma_{th}}{\kappa\Psi}}\right)\right\}$ and $\left(1-\exp\left(-\frac{\lambda_3\gamma_{th}}{\Psi}\right)\right)$

are getting larger and approaching 1. For the MRC scheme, we experience the same trend since scaling up γ_{th} will increase the integration thus reducing the IP. Regarding the impact of λ_3 on the IP under the SC scheme, we experience that raising λ_3 will obviously decline the IP. By inspecting (20), a similar conclusion about the impact of λ_3 on the IP under the MRC scheme can be drawn.

4. Numerical Results and Discussion

Here, the effects of ψ on the IP are shown in Fig. 3 with ψ=5 dB, ρ=0.5, R=0.5, and 1. As shown in Fig. 3, we can see that the IP is a monotonic increasing function with respect to (w.r.t.) ψ. Additionally, we observe good agreements between the derived mathematical framework and Monte-Carlo simulations. It is obvious that the MRC scheme is better than the SC scheme. However, the gap between the two schemes is minor under the figure setup. It is noted that the impact of the transmit power of the source node P_S or $\left(\Psi = \frac{P_S}{N_0}\right)$ on the performance of the IP is considered the most important. The rationale behind this statement is that the higher the transmit power of the source, P_S, the higher the SNR from the source to the eavesdropper, γ_E^2. Second, as the transmit power of the relay is proportional to the transmit power of the source node, it signifies that the higher the transmit power of the source node the better the SNR from the relay to the eavesdropper as well. Finally, since the e2e SNR at the eavesdropper is the combination of two SNRs, i.e., MRC or SC diversity techniques. It, as a result, significantly improves the intercept probability of the eavesdropper.

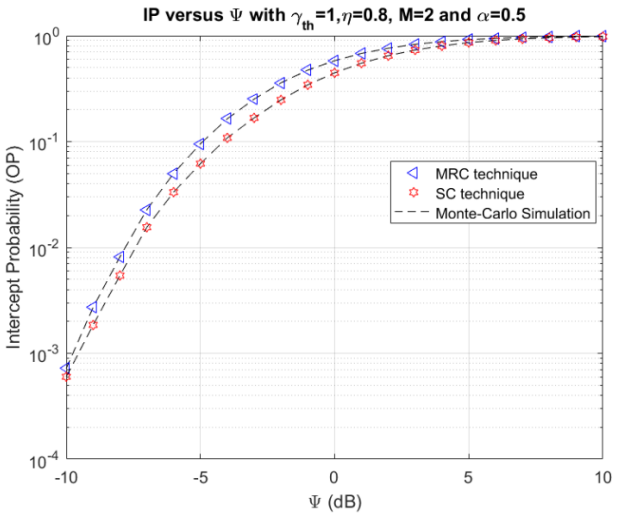

Figure 3. *IP versus ψ.*

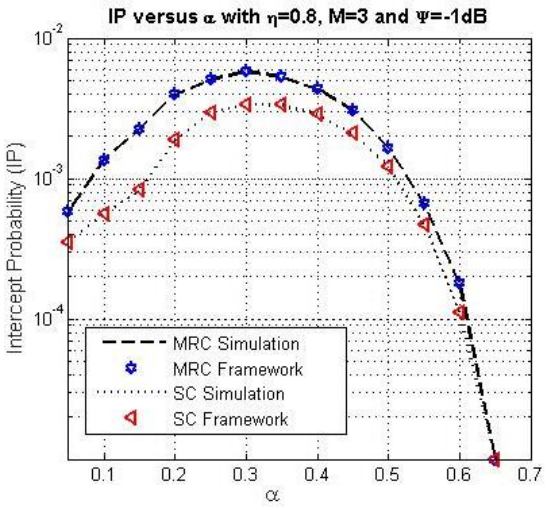

Figure 4. *IP versus α.*

Fig. 4 addresses the performance of the IP as a function of the time switching ratio α. It is expected that the IP is a parabola function since increasing α will improve the transmit power of the relay thus scaling up the IP performance. Nonetheless, if α approaches 1, it means that the amount of duration for information decoding is little. As a consequence, the probability that eavesdropper successfully wiretaps the secure information is smaller. It is certain that the IP of the MRC scheme is always higher than the counterpart. The rationale behind this statement is that the MRC is defined as the sum of γ_E^2, γ_E^3, i.e., $\gamma_E^2 + \gamma_E^3$ while the SC refers to the maximum of these RVs. It is certain that the sum of two RVs will always be greater than the maximum, i.e., $\gamma_E^2 + \gamma_E^3 > \max\left(\gamma_E^2, \gamma_E^3\right)$.

Fig. 5 investigates the performance of the IP w.r.t. the number of source nodes *M*. It is evident that the larger the number of source nodes the higher the intercept probability. This can be explained that the higher the number of sources the better the channel gain to both relay and eavesdropper thus degrading the security aspect of the system. We see again that the analytical framework aligns with the Monte-Carlo simulations and the MRC outperforms the SC scheme.

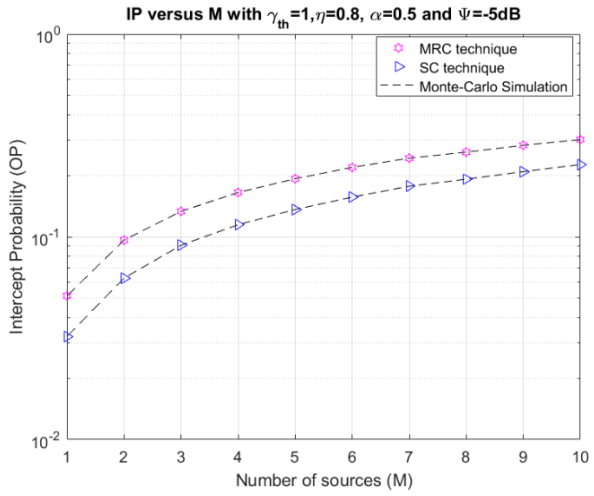

Figure 5. *IP versus M.*

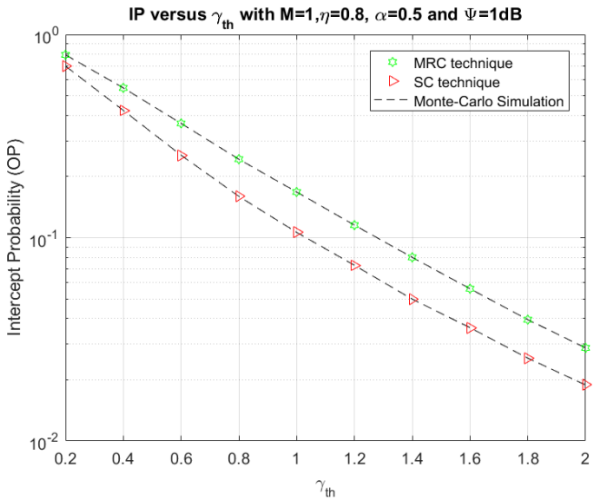

Figure 6. *IP versus γ_{th}.*

Fig. 6 stretches the performance of the IP regarding γ_{th}. We experience that IP is a monotonic decrease function w.r.t. the predefined threshold. This can be straightforwardly elaborated from the definition of the IP that the higher the γ_{th} the smaller the IP. Nonetheless, this is beneficial for the system from the viewpoint of the security aspect.

5. Conclusions

In this paper, we presented the multisource half-duplex relaying network employing the time-switching protocol. The intercept probability (IP) of the system model with maximal receiver ratio combining (MRC) and selection combining (SC) was derived in the integral-form and closed-form expressions. The Monte Carlo simulations were given to study the correctness of the developed framework and to unveil the impact of some vital parameters on the system performance. We revealed that among all parameters, the transmit power of the source node has a larger impact on the performance of the IP. Particularly, the IP had already approached one when Ψ approximately 8 dB. Additionally, the IP is a parabolic function w.r.t. the time switching ratio, and the maximum is attained at α around 0.3. The paper can be extended in several directions such as reconfigurable intelligent surfaces, Fountain codes, LoRa networks, and covert communications.

Acknowledgments

No funding has been reported for this work.

Conflict of Interest

The authors declare no conflict of interest.

Data Availability Statement

The data that support the findings of this study are available from the corresponding author upon reasonable request.

REFERENCES

[1] C. X. Ming, D. W. K. Ng, and H. H. Chen, "Secrecy Wireless Information and Power Transfer: Challenges and Opportunities," *IEEE Wireless Communications*, vol. 23, no. 2, pp. 54-61, 2016, doi: 10.1109/mwc.2016.7462485.

[2] S. Bi, C. K. Ho, and R. Zhang, "Wireless powered communication: Opportunities and challenges," *IEEE Communications Magazine*, vol. 53, no. 4, pp. 117-125, 2015, doi: 10.1109/mcom.2015.7081084.

[3] D. Niyato, D. I. Kim, M. Maso, and Z. Han, "Wireless Powered Communication Networks: Research Directions and Technological Approaches," *IEEE Wireless Communications*, pp. 2-11, 2017, doi: 10.1109/mwc.2017.1600116.

[4] A. A. Nasir, X. Zhou, S. Durrani, and R. A. Kennedy, "Relaying Protocols for Wireless Energy Harvesting and Information Processing," *IEEE Transactions on Wireless Communications*, vol. 12, no. 7, pp. 3622-636, 2013, doi: 10.1109/twc.2013.062413.122042.

[5] T. N. Nguyen, D. T. Do, P. T. Tran, and M. Voznak, "Time Switching for Wireless Communications with Full-Duplex Relaying in Imperfect CSI Condition," *KSII Transactions on Internet and Information Systems*, 2016, doi:10.3837/tiis.2016.09.011.

[6] Z. Xun, R. Zhang, and C. K. Ho, "Wireless Information and Power Transfer: Architecture Design and Rate-energy Tradeoff," in *2012 IEEE Global Communications Conference (GLOBECOM)*, doi: 10.1109/glocom.2012.6503739.

[7] K. Mohamed, and A. Ephremides, "Optimal Partial Relaying for Energy-Harvesting Wireless Networks," *IEEE/ACM Transactions on Networking 24*, no. 1, pp. 113-22, 2016, doi: 10.1109/tnet.2014.2361683.
[8] L. T. Tu, M. D. Renzo, and J. P. Coon, "System-Level Analysis of SWIPT MIMO Cellular Networks," *IEEE Communications Letters*, vol. 20, no. 10, pp. 2011-2014, Oct. 2016, doi: 10.1109/LCOMM.2016.2590424.
[9] T. N. Nguyen *et al.*, "Outage Performance of Satellite Terrestrial Full-Duplex Relaying Networks With co-Channel Interference," *IEEE Wireless Communications Letters*, vol. 11, no. 7, pp. 1478-1482, 2022, doi: 10.1109/LWC.2022.3175734.
[10] P. T. Tin *et al.*, "Outage Analysis of the Power Splitting Based Underlay Cooperative Cognitive Radio Networks," *Sensors*, vol. 21, no. 22, p. 7653, Nov. 2021, doi: 10.3390/s21227653.
[11] L. T. Tu, P. L. Tung, T. V. Chien, T. T. Duy, and N. T. Hoa, "Performance Evaluation of Incremental Relaying in Underlay Cognitive Radio Networks with Imperfect CSI," in *2020 IEEE Eighth International Conference on Communications and Electronics (ICCE)*, Phu Quoc Island, Vietnam, 2021, pp. 472-477, doi: 10.1109/ICCE48956.2021.9352039.
[12] P. N. Son and H. Y. Kong, "Cooperative communication with energy-harvesting relays under physical layer security," *IET Commun.*, vol. 9, pp. 2131-2139, 2015, doi: 10.1049/iet-com.2015.0186.
[13] T. S. Le, N. T. Pham, D. Q. H. Thieu, and N. S. Pham, "Analyses of transmit antenna selection to enhance security performance in cooperative radio communication networks under wiretap channel," *Journal of Technical Education Science*, no. 55, pp. 32–40, Dec. 2019.
[14] D. T. Vo *et al.*, "SWIPT-Enabled Cooperative Wireless IoT Networks With Friendly Jammer and Eavesdropper: Outage and Intercept Probability Analysis," *IEEE Access*, vol. 11, pp. 86165-86177, 2023, doi: 10.1109/ACCESS.2023.3303369.
[15] T. N. Ha, N. V. Phuc, D. P. H. Trang, and P. T. N. Hieu, "Performance analysis in multi-hop communication", *Journal of Technical Education Science*, no. 61, pp. 9–16, Dec. 2020.
[16] D. Zwillinger and V. Moll, *Table of Integrals, Series, and Products*, 2015, doi:10.1016/c2010-0-64839-5.
[17] D. T. Do, M. Le, V. P. Nguyen, M. T. Le, and P. H. T. Dang, "Queue length-based opportunistic relay selection for cooperative wireless networks," *Journal of Technical Education Science*, no. 59, pp. 85–92, Aug. 2020.

Nguyen Nhat Tan (member IEEE) was born in 1986 in Nha Trang City, Vietnam. He received a BS degree in electronics in 2008 from Ho Chi Minh University of Natural Sciences and an MS degree in telecommunications engineering in 2012 from Vietnam National University. He received a Ph.D. in communications technologies in 2019 from the Faculty of Electrical Engineering and Computer Science at VSB – Technical University of Ostrava, Czech Republic. He joined the Faculty of Electrical and Electronics Engineering of Ton Duc Thang University, Vietnam, in 2013, and since then has been lecturing. He started as the Editor-in-Chief of Advances in Electrical and Electronic Engineering (AEEE) journal in 2023. His major interests are cooperative communications, cognitive radio, signal processing, satellite communication, UAV, and physical layer security. Email address: nguyennhattan@tdtu.edu.vn.

Pham Ngoc Son received the B.E. degree (2005) and M.Eng. degree (2009) in Electronics and Telecommunications Engineering from Post and Telecommunication Institute of Technology, Ho Chi Minh City and Ho Chi Minh City University of Technology, Vietnam, respectively. In 2015, he received the Ph.D. degree in Electrical Engineering from University of Ulsan, South Korea. He is currently a Lecturer in the Faculty of Electrical and Electronics Engineering of Ho Chi Minh City University of Technology and Education (HCMUTE). His major research interests are cooperative communication, cognitive radio, physical layer security, energy harvesting, non-orthogonal multiple access, intelligent reflecting surface and short packet communications. Email address: sonpndtvt@hcmute.edu.vn.

Tu Lam Thanh received the B.Eng. degree in electronics and telecommunications engineering from the Ho Chi Minh City University of Technology, Vietnam, in 2009, the M.Sc. degree in telecommunications engineering from the Posts and Telecommunications Institute of Technology, Vietnam, in 2014, and the Ph.D. degree from the University of Paris Sud, Paris-Saclay University, France, in 2018. From 2015 to 2018, he was with the French National Center for Scientific Research (CNRS), Paris, as an Early Stage Researcher of the European-Funded Project H2020 ETN-5Gwireless. From 2019-2021, he was with the Xlim Research Institute, University of Poitiers, France as a postdoctoral research fellow. From 2022, he has been with the Faculty of Electrical and Electronics Engineering, at Ton Duc Thang University, Vietnam. His research interests include stochastic geometry, LoRa networks, reconfigurable intelligent surfaces, covert communications, and artificial intelligence applications for wireless communications. Email address: tulamthanh@tdtu.edu.vn. ORCID: https://orcid.org/0000-0001-5735-4641