D2D Communication Network with the Assistance of Power Beacon under the Impact of Co-channel Interferences and Eavesdropper: Performance Analysis

Bui Vu MINH[1], *Tran Hoang Quang MINH*[2], *Van-Duc PHAN*[3], *Hieu T. NGUYEN*[4]

[1]Faculty of Engineering and Technology, Nguyen Tat Thanh University, 300A-Nguyen Tat Thanh, Ward 13, District 4, Ho Chi Minh City 754000, Vietnam
[2]Communication and Signal Processing Research Group, Faculty of Electrical and Electronics Engineering, Ton Duc Thang University, Ho Chi Minh City, Vietnam
[3]Faculty of Automotive Engineering, School of Technology, Van lang University, Ho Chi Minh city, Vietnam
[4]Posts and Telecommunications Institute of Technology, Ha Noi, Vietnam

bvminh@ntt.edu.vn, tranhoangquangminh@tdtu.edu.vn, duc.pv@vlu.edu.vn, hieunt@ptit.edu.vn

DOI: 10.15598/aeee.v21i4.5495

Article history: Received Oct 16, 2023; Revised Dec 06, 2023; Accepted Dec 21, 2023; Published Dec 31, 2023.

Abstract. *In this paper, we study and demonstrate the performance analysis of a device-to-device (D2D) communication network. Specifically, a source node transmits data to the destination node using the power beacon's harvested energy in order to overcome the limited energy budget. Besides, an eavesdropper located in the proximal region of a source is trying to overhear secure information. Notably, both eavesdropper and destination are affected by co-channel interferences from other sources when they utilize the same frequency. By considering the above discussions, we derived the closed-form expressions for outage probability (OP), intercept probability (IP), and secrecy outage probability (SOP) in connection with using the system model. The derived analytical expressions are then verified by utilizing both simulation and numerical results. Finally, the intensive parameters' influences on the OP, IP, and SOP are also investigated.*

Keywords

Co-channel interference, energy harvesting, device-to-device, outage probability, intercept probability, secrecy outage probability

1. Introduction

Recently, in connection with the evolution of the fifth-generation (5G), the research of Internet of Things (IoT) is the main research work in over the world [1, 2, 3, 4, 5, 6, 7]. Fortunately, a device-to-device (D2D) communication network has emerged as a solution to enhance network performance (i.e., throughput) by increasing the coverage region. Specifically, D2D communication employing non-orthogonal multiple access (NOMA) is expected to play an important role in the 5G networks [8].

Further, IoT communications are also restricted by their limited on-board energy. The replaced or recharged battery is not always convenient or even impossible because it depends on weather conditions or terrain, etc. Consequently, energy harvesting (EH) is a technology for enabling autonomous, sustainable, and green IoT communications. Recent research shows radio frequency (RF.) EH's benefits in wireless networks [9, 10, 11, 12, 13, 14, 15, 16, 17]. In addition, the co-channel interference also significantly influences the system performance of the IoT networks. Moreover, interference becomes an indispensable factor in wireless communications, and it has been received significant attention from researchers [18, 19, 20, 21, 22]. Duy et al. [18] investigated the secrecy performance of a cooperative network consisting of multiple sources, one

destination, and one eavesdropper under the impact of co-channel interference. In [19], the authors adopted transmit antenna selection (TAS) and harvest-to-jam techniques to improve security and energy efficiency. Eunhye et al. [20] maximized the achievable spectral efficiency of a full-duplex system under the presence of inherent interference caused by self-interference and co-channel interference. In [21], the authors studied the end-to-end performance of dual-hop cooperative networks under the presence of co-channel interference and hardware impairments. Concretely, they derived the closed-form for the average channel capacity and OP for the N-th best partial and opportunistic relay methods. In [22], the authors investigated the outage probability (OP) in satellite communication networks under co-channel interference. Different from [18, 19, 20, 21, 22] that only investigated interference in a cooperative system, the authors in [23] studied the influence of co-channel interference in a PSK-chirp-BOK multiuser system.

Besides the restriction on energy capacity and co-channel interference, IoT communications are vulnerable to eavesdropping attacks because of wireless networks' broadcast nature. Consequently, physical layer security (PLS) becomes a promising solution due to its simplicity and effectiveness [24, 25, 26, 27]. Hieu et al. [24] proposed a novel generalized partial relay selection (PRS) protocol to improve a cooperative cognitive radio network's secrecy performance in terms of non-zero secrecy capacity and SOP. In [25], the authors investigated the PLS of reflecting intelligent surface (RIS) on the downlink. Specifically, they derived the closed-formed optimal transmit beamforming of the BS at a fixed RIS phase shift. Nguyen et.al. [26] investigated the security-reliability trade-off in satellite communication relaying networks in terms of OP and IP. Unlike [24, 25, 26], which only studied the PLS in two-hop relaying networks, [27] examined the PLS of multi-hop multi-path cooperative wireless sensor networks.

Motivated by the above discussions, this paper proposed and investigated the secrecy performance analysis of a power beacon-assisted D2D network in the presence of an eavesdropper. Besides, the source node is equipped with an energy harvesting circuit, and it can harvest energy from a power beacon. The contributions of this paper are listed as follows:

- We model a novel D2D communication for IoT networks in the presence of an eavesdropper and co-channel interference. Specifically, a source receives RF EH from a power beacon, and then it uses the harvested energy to transmit data to the destination. The eavesdropper is trying to intercept the information from a source. Particularly, both eavesdropper and destination are under the influence of multiple interference sources.
- By considering the above system model, we derive the performance analysis for outage probability (OP), intercept probability (IP), and secrecy outage probability (SOP) to evaluate the trade-off as well as the quality of the proposed system.
- Then, the mathematical results are validated through simulations.

The rest of this paper is organized as follows. In Section 2. , the system model of the D2D communication for IoT networks is described in detail. Then, the OP, IP, and SOP are analyzed in Sections 3. . The simulation results to clarify our analysis are indicated in Section 4. . Finally, we conclude the important points of the paper in Section 5. .

2. SYSTEM MODEL

As described in Fig. 1, a source is equipped with an energy harvesting circuit, and its energy can be harvested from a power beacon. Then, the harvested energy is utilized to transmit information from the source to the destination in the presence of an eavesdropper E. Notably, eavesdropper E is able to overhear information from source S. Moreover, there are M interference sources denoted by $I_1, \ldots, I_n, \ldots, I_M$ that make additional noises to the eavesdropper and the destination. The energy harvesting and information transmission at the source S are presented in Fig. 2. Concretely, the source can harvest energy during αT, and it transmits data to the destination during $(1-\alpha)T$. We assume that the channels between two random users are block Rayleigh fading.

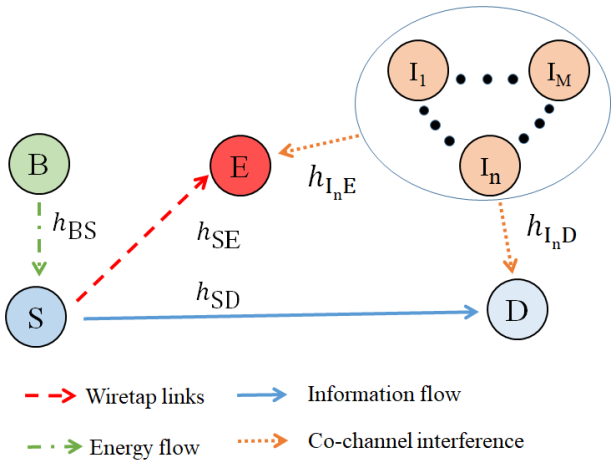

Fig. 1: System model.

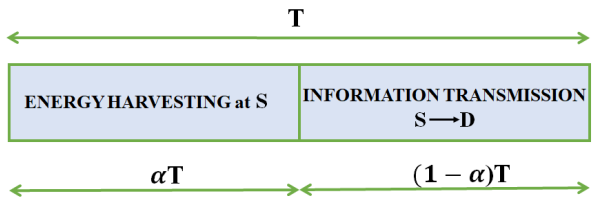

Fig. 2: IT and EH processes

2.1. Energy harvesting phase

Consequently, the average transmit power at S can be found by

$$P_S = \frac{E_S}{(1-\alpha)T} = \frac{\eta\alpha T P_B \left|h_{BS}\right|^2}{(1-\alpha)T} = \mu P_B \left|h_{BS}\right|^2, \quad (1)$$

where P_B is the average transmit power at the power beacon B, $\mu = \frac{\eta\alpha}{1-\alpha}$, and $0 < \eta \leqslant 1$ is the energy conversion efficiency.

2.2. Information transmission phase

In this phase, the received signal at D and E can be figured out as, respectively.

$$y_D = h_{SD}x_S + \sum_{n=1}^{M} x_{I_n} h_{I_n D} + n_D, \quad (2)$$

$$y_E = h_{SE}x_S + \sum_{n=1}^{M} x_{I_n} h_{I_n D} + n_E. \quad (3)$$

From (1), (2), and (3), the signal to interference and noise ratio (SINR) at the destination D and eavesdropper E can be respectively given by:

$$\begin{aligned} \gamma_D &= \frac{\mu \left|h_{SD}\right|^2 \left|h_{BS}\right|^2 \Psi}{\Delta \sum\limits_{n=1}^{M} \left|h_{I_n D}\right|^2 + 1} = \frac{\mu X \Psi}{\Delta Z + 1}, \\ \gamma_E &= \frac{\mu \left|h_{SE}\right|^2 \left|h_{BS}\right|^2 \Psi}{\Delta \sum\limits_{n=1}^{M} \left|h_{I_n E}\right|^2 + 1} = \frac{\mu Y \Psi}{\Delta T + 1}, \end{aligned} \quad (4)$$

where $\Psi = \frac{P_B}{N_0}, \Delta = \frac{P_I}{N_0}$, $X = \left|h_{SD}\right|^2 \left|h_{BS}\right|^2, Y = \left|h_{SE}\right|^2 \left|h_{BS}\right|^2$, $Z = \sum\limits_{n=1}^{M} \left|h_{I_n D}\right|^2$, and $T = \sum\limits_{n=1}^{M} \left|h_{I_n E}\right|^2$.

Next, the received capacity at D and E can be thus expressed as, respectively.

$$\begin{aligned} C_D &= (1-\alpha)\log_2(1+\gamma_D), \\ C_E &= (1-\alpha)\log_2(1+\gamma_E). \end{aligned} \quad (5)$$

Remark 1: As in [18], the probability density function (PDF) of random variables (RVs) Z and T can be obtained as, respectively.

$$\begin{aligned} f_Z(t) &= \frac{(\lambda_{ID})^M}{(M-1)!} t^{M-1} \exp(-\lambda_{ID} t), \\ f_T(t) &= \frac{(\lambda_{IE})^M}{(M-1)!} t^{M-1} \exp(-\lambda_{IE} t), \end{aligned} \quad (6)$$

where λ_{ID} and λ_{IE} are the mean of RVs Z and T, respectively.

3. PERFORMANCE ANALYSIS

3.1. Outage probability (OP)

The OP at the destination can be calculated by:

$$\begin{aligned} OP &= \Pr\left(C_D < C_{th}\right) = \Pr\left[\frac{\mu X \Psi}{\Delta Z + 1} < \gamma_{th}\right] \\ &= \Pr\left[\mu X \Psi < \gamma_{th}\left(\Delta Z + 1\right)\right] \\ &= \int_0^{\infty} F_X\left[\frac{\gamma_{th}\left(\Delta t + 1\right)}{\mu\Psi}\right] \times f_Z(t) dt. \end{aligned} \quad (7)$$

where $\gamma_{th} = 2^{\frac{C_{th}}{(1-\alpha)}} - 1$ is the SINR threshold and C_{th} is the target rate.

As a result like in [28, 29], $F_X(x)$ can be found by:

$$F_X(x) = 1 - 2\sqrt{\lambda_{SD}\lambda_{BS}x} \times K_1\left(2\sqrt{\lambda_{SD}\lambda_{BS}x}\right) \quad (8)$$

where λ_{SD} and λ_{BS} are the mean of RVs $\left|h_{SD}\right|^2$ and $\left|h_{BS}\right|^2$, respectively, and $K_v(\bullet)$ is the modified Bessel function of the second kind with v^{th} order.

By substituting (6) and (8) into (7), the OP can be derived as:

$$\begin{aligned} OP = 1 - &\frac{2(\lambda_{ID})^M \sqrt{\lambda_{SD}\lambda_{BS}}}{(M-1)!} \times \\ &\int_0^{\infty} \left\{ \begin{array}{l} t^{M-1} \exp\left(-\lambda_{ID} t\right) \times \sqrt{\frac{\gamma_{th}(\Delta t+1)}{\mu\Psi}} \\ \times K_1\left(2\sqrt{\frac{\lambda_{SD}\lambda_{BS}\gamma_{th}(\Delta t+1)}{\mu\Psi}}\right) dt \end{array} \right\}. \end{aligned} \quad (9)$$

By changing the variable $y = \Delta t + 1$, (9) can be rewritten by:

$$\begin{aligned} OP = 1 - &\frac{2(\lambda_{ID})^M \sqrt{\gamma_{th}\lambda_{SD}\lambda_{BS}}}{(M-1)!\Delta^M\sqrt{\mu\Psi}} \times \exp\left(\frac{\lambda_{ID}}{\Delta}\right) \\ \times &\int_1^{\infty} \left\{ \begin{array}{l} \sqrt{y}(y-1)^{M-1} \exp\left(-\frac{\lambda_{ID} y}{\Delta}\right) \\ \times K_1\left(2\sqrt{\frac{\lambda_{SD}\lambda_{BS}\gamma_{th} y}{\mu\Psi}}\right) dy \end{array} \right\}. \end{aligned} \quad (10)$$

Here, we employ the Taylor series as following:

$$\begin{aligned} \exp\left(-\frac{\lambda_{ID} y}{\Delta}\right) &= \sum_{k=0}^{\infty} \frac{\left(-\frac{\lambda_{ID} y}{\Delta}\right)^k}{k!} \\ &= \sum_{k=0}^{\infty} (-1)^k \frac{\left(\frac{\lambda_{ID}}{\Delta}\right)^k}{k!} y^k. \end{aligned} \quad (11)$$

By substituting (11) into (10), we have:

$$OP = 1 - \frac{2(\lambda_{ID})^M \sqrt{\gamma_{th}\lambda_{SD}\lambda_{BS}}}{(M-1)!\Delta^M\sqrt{\mu\Psi}} \times \exp\left(\frac{\lambda_{ID}}{\Delta}\right) \sum_{k=0}^{\infty}(-1)^k \frac{\left(\frac{\lambda_{ID}}{\Delta}\right)^k}{k!} \int_1^{\infty} y^{k+1/2}(y-1)^{M-1} \times K_1\left(2\sqrt{\frac{\lambda_{SD}\lambda_{BS}\gamma_{th}y}{\mu\Psi}}\right)dy. \tag{12}$$

By applying [33, 6.592.4], the closed-form expression of OP in (12) can be given by:

$$OP = 1 - \sum_{k=0}^{\infty} \frac{(-1)^k\left(\frac{\lambda_{ID}}{\Delta}\right)^{k+M}\exp\left(\frac{\lambda_{ID}}{\Delta}\right)}{k!} \times\left(\sqrt{\frac{\lambda_{SD}\lambda_{BS}\gamma_{th}}{\mu\Psi}}\right)^{-2k} \times G_{1,3}^{3,0}\left(\frac{\lambda_{SD}\lambda_{BS}\gamma_{th}}{\mu\Psi}\middle| \begin{matrix}0\\ -M, k+1, k\end{matrix}\right), \tag{13}$$

where $\mathrm{G}_{p,q}^{m,n}\left(z\middle| \begin{matrix}a_1,...,a_p\\ b_1,...,b_q\end{matrix}\right)$ is the Meijer G-function.

3.2. Intercept probability (IP)

The IP can be defined as [30]:

$$IP = \Pr\left(C_E \geq C_{th}\right) = \Pr\left(\gamma_E \geq \gamma_{th}\right) = 1 - \Pr\left(\gamma_E < \gamma_{th}\right). \tag{14}$$

Similar proof as OP case, the IP can be obtained by:

$$IP = \sum_{k=0}^{\infty}\left\{\begin{matrix}\frac{(-1)^k\left(\frac{\lambda_{ID}}{\Delta}\right)^{k+M}\exp\left(\frac{\lambda_{ID}}{\Delta}\right)}{k!}\\ \times\left(\sqrt{\frac{\lambda_{SE}\lambda_{BS}\gamma_{th}}{\mu\Psi}}\right)^{-2k}\\ \times G_{1,3}^{3,0}\left(\frac{\lambda_{SE}\lambda_{BS}\gamma_{th}}{\mu\Psi}\middle| \begin{matrix}0\\ -M, k+1, k\end{matrix}\right)\end{matrix}\right\}, \tag{15}$$

where λ_{SE} is the mean of RV $|h_{SE}|^2$.

3.3. Secrecy outage probability (SOP)

As in [31, 32], the achievable secrecy capacity can be computed as follows:

$$C_{\text{sec}} = \max\left(C_D - C_E, 0\right), \tag{16}$$

where C_D and C_E represent the received capacity at the D and E, respectively. A secrecy outage occurs if the achievable secrecy capacity is lower than the capacity threshold:

$$SOP = \Pr\left(C_{\text{Sec}} < C_{th}\right) = \Pr\left(\frac{1+\gamma_D}{1+\gamma_E} < \gamma_{th}\right) = \Pr\left(\frac{1+\frac{\mu X\Psi}{\Delta Z+1}}{1+\frac{\mu Y\Psi}{\Delta T+1}} < \gamma_{th}\right). \tag{17}$$

To address this issue, we will investigate SOP in an approximate form. When $\Psi \to +\infty$, SOP in (17) can be approximated as follows:

$$SOP_{\Psi\to\infty} \approx \Pr\left(\frac{\frac{\tilde{X}}{\Delta Z}}{\frac{\tilde{Y}}{\Delta T}} < \gamma_{th}\right) = \Pr\left(\frac{\tilde{X}}{Z} \times \frac{T}{\tilde{Y}} < \gamma_{th}\right), \tag{18}$$

where $\tilde{X} = |h_{SD}|^2, \tilde{Y} = |h_{SE}|^2$.

Let us denote $\Omega = \frac{\tilde{X}}{Z}$ and $\Phi = \frac{T}{\tilde{Y}}$, equation (18) can be re-calculated by:

$$SOP_{\Psi\to\infty} = \Pr\left(\Omega \times \Phi < \gamma_{th}\right) = \Pr\left(\Omega < \frac{\gamma_{th}}{\Phi}\right) = \int_0^{\infty} F_{\Omega}\left(\frac{\gamma_{th}}{x}\right) f_{\Phi}(x)dx. \tag{19}$$

At first, we will find the CDF of Ω and PDF of Φ as follows

$$F_{\Omega}(y) = \Pr\left(\Omega < y\right) = \Pr\left(\frac{\tilde{X}}{Z} < y\right) = \int_0^{\infty} F_{\tilde{X}}(yt) f_Z(t)dt. \tag{20}$$

Substituting (6) into (21), we have:

$$F_{\Omega}(y) = 1 - \frac{(\lambda_{ID})^M}{(M-1)!}\int_0^{\infty} t^{M-1}\exp\left(-\lambda_{SD}yt - \lambda_{ID}t\right)dt. \tag{21}$$

By applying [33, 3.351.3], (22) can be formulated as:

$$F_{\Omega}(y) = 1 - \left(\frac{\lambda_{ID}}{\lambda_{SD}y + \lambda_{ID}}\right)^M. \tag{22}$$

Similar to $F_{\Omega}(y)$, the CDF of Φ can be defined as:

$$F_{\Phi}(x) = \Pr\left(\frac{T}{\tilde{Y}} < x\right) = \Pr\left(T < \tilde{Y}x\right) = 1 - \Pr\left(\tilde{Y} < \frac{T}{x}\right) = 1 - \int_0^{\infty} F_{\tilde{Y}}\left(\frac{t}{x}\right) f_T(t)dt = \frac{(\lambda_{IE})^M}{(M-1)!}\int_0^{\infty} t^{M-1}\exp\left(-\frac{\lambda_{SE}t}{x} - \lambda_{IE}t\right)dt = \left(\frac{\lambda_{IE}}{\frac{\lambda_{SE}}{x} + \lambda_{IE}}\right)^M. \tag{23}$$

From (23), the PDF of Φ can be expressed as:

$$f_{\Phi}(x) = \frac{\partial F_{\Phi}(x)}{\partial x} = \frac{M\lambda_{SE}}{\lambda_{IE}x^2}\left(\frac{\lambda_{IE}x}{\lambda_{IE}x + \lambda_{SE}}\right)^{M+1}. \tag{24}$$

Finally, by substituting (23) and (24) into (18), the $SOP_{\Psi\to\infty}$ can be rewritten as:

$$SOP_{\Psi\to\infty} = 1 - \frac{M\lambda_{SE}}{\lambda_{IE}} \times \int_0^\infty x^{2M-1}\left(x + \frac{\lambda_{SD}\gamma_{th}}{\lambda_{ID}}\right)^{-M}\left(x + \frac{\lambda_{SE}}{\lambda_{IE}}\right)^{-M-1} dx. \quad (25)$$

By applying [33, 3.197.1], the closed-form expression of $SOP_{\Psi\to\infty}$ can be claimed by:

$$SOP_{\Psi\to\infty} = 1 - M\left(\frac{\lambda_{SE}}{\lambda_{IE}}\right)^{-M}\left(\frac{\lambda_{SD}\gamma_{th}}{\lambda_{ID}}\right)^{M} B(2M,1) \times {}_2F_1\left(M+1, 2M; 2M+1; 1 - \frac{\lambda_{SD}\lambda_{IE}\gamma_{th}}{\lambda_{ID}\lambda_{SE}}\right), \quad (26)$$

where $B(x,y)$ is the Beta function, and ${}_2F_1(\alpha,\beta;\gamma;z)$ is the Gauss hypergeometric function.

4. NUMERICAL RESULTS

This section introduces the results by using Monte Carlo simulation as in [34, 35, 36] to validate the accuracy of the mathematic analysis, i.e., OP, IP, and SOP. Concretely, the results are achieved by running 10^6 Rayleigh fading channels. The simulation parameters are listed in Table 1.

Tab. 1: Simulation parameters.

Symbol	Parameter name	Value
C_{th}	Target rate	0.25
η	EH efficiency	0.8
α	time-switching factor	0.5; 0 to 1
d_{BS}	Distance between B and S	1m
d_{SE}	Distance between R and D	1m
d_{SD}	Distance between S and D	1m
d_{IE}	Distance between I and E	1m
d_{ID}	Distance between I and D	1m
M	Number of interference sources	1;3;6
Δ	Transmit power to noise ratio at interference source	1;3;5 (dB)
Ψ	Transmit power to noise ratio at source	0 to 25 (dB)

In Figs. 3 and 4, we plot the OP and IP as functions of $\Psi(dB)$ with different number of interference sources, where $C_{th} = 0.25bps/Hz, \alpha = 0.5, \eta = 0.8,$ and$\Delta = 1dB$. First, as we can observe that the higher the Ψ value is, the better the OP can be claimed. Besides, the IP is also proportional to the Ψ value. It will lead to easy understanding since when we allocate more transmit power for the source, both the destination and eavesdropper can improve the reception rate. Therefore, they have more chance to pass the rate threshold to decode the signal successfully. Second, we also observe that increasing interference sources significantly influences the OP and IP. Concretely, both outage and intercept performance are degraded with a higher value of M.

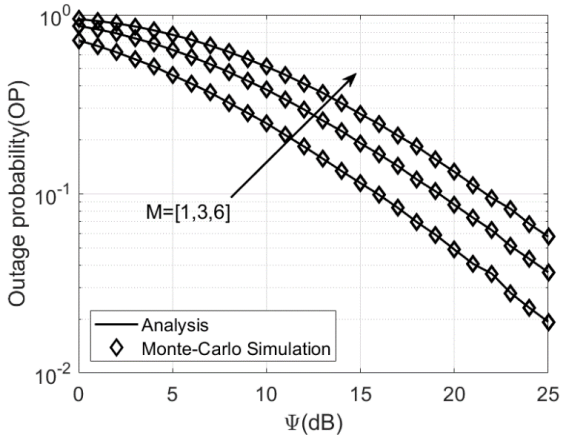

Fig. 3: OP versus $\Psi(dB)$.

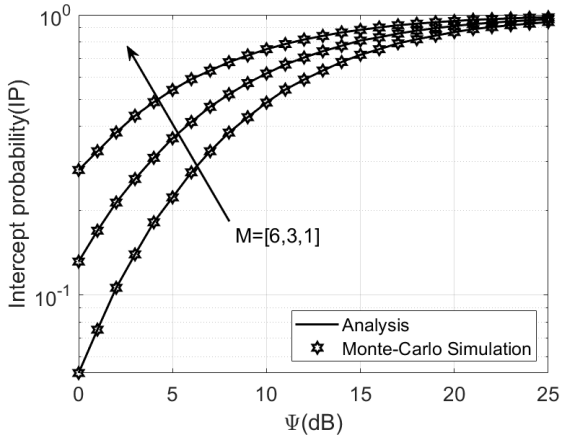

Fig. 4: IP versus $\Psi(dB)$.

Figs. 5 and 6 show the OP and IP as functions of α factor. The time-splitting ratio plays an important factor α, where $C_{th} = 0.25\frac{bps}{Hz}, \Psi = 3dB, \eta = 0.8,$ and$M = 1$. since it impacts the allocated time for energy harvesting and data transmission at the source node. It can be seen that the outage performance is improved to an optimal point with the increase of value, then it becomes worse. It can be explained by the fact that the higher α is, the more time is allocated for EH, but it will lead to less time for information transmission from source S to destination D, and vice versa. Thus, there exists an optimal value of α value to maximize the OP. Moreover, when the α value changes from 0.65 to 0.8, the OP and IP are both improved. The higher Δ means more power is transmitted from sources of interference, causing more critical effects directly on the channel to the destination and eavesdropper.

With the generally analytical, Fig. 7 plots the SOP as a function of α , where $C_{th} = 0.25\frac{bps}{Hz}$, $\eta = 0.8$, Ψ=5

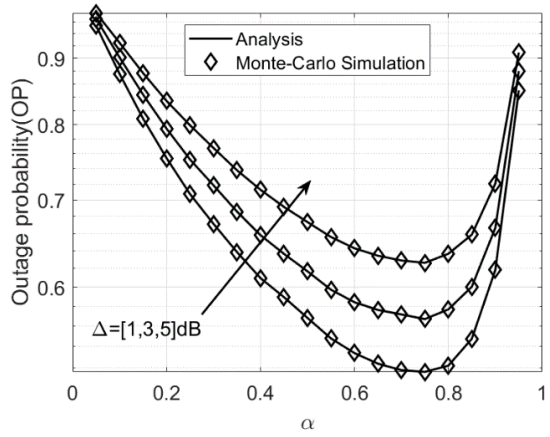

Fig. 5: OP versus α .

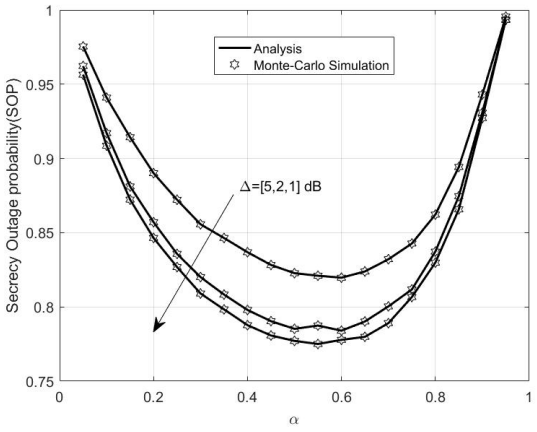

Fig. 7: SOP versus α .

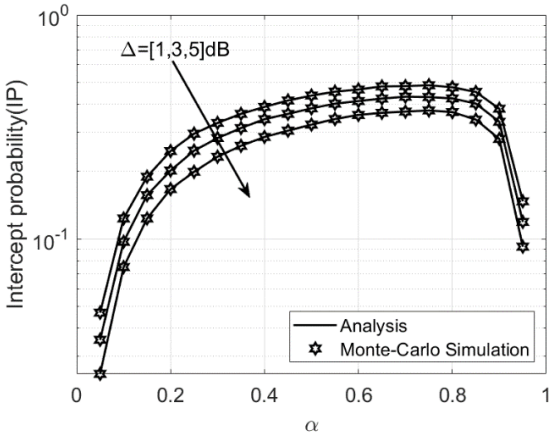

Fig. 6: IP versus α .

dB, and $M = 1$. Like as Figs. 5 and 6, an optimal value of α can be found to minimize SOP. For example, when Δ=5 dB, the performance of SOP will converge to the optimal value at α approximates 0.6, and then the SOP value significantly increases when α extends from 0.6 to 1. It can be understood that the value of the difference between the received capacity at the destination and eavesdropper is maximized at around α equals 0.6, and then it will decrease. Further, it is also observed that the higher the value of Δ is, the poorer the secrecy performance will be obtained. It can be explained that the higher the transmit power at the interference sources, the lower the destination's data rate is claimed.

5. CONCLUSIONS

This work explored a cooperative relaying network with a PB, an EH source, a destination under the presence of an eavesdropper, and multiple interference sources. Further, the energy of the source node can be harvested from a PB to overcome the limited energy budget. Simultaneously, when the source transmits data to the destination, the other sources also transfer information using the same frequency, which creates more interferences to the destination and the eavesdropper. By considering the above discussions, the closed-form expressions of OP, IP, and SOP will be derived at the receiver to evaluate the performance of the proposed system. Then, the Monte Carlo simulations are performed to confirm the accuracy of the mathematical analysis. The results show the trade-off between the IP and OP. Specifically, the better the outage performance is, the higher chance the eavesdropper can overhear the information.

Author Contributions

Both B.V.Minh and T.H.Q.Minh performed the analytic calculations and performed the numerical simulations. T.H.Q.Minh wrote the whole paper while Van-Duc Phan and Hieu T. Nguyen checked the simulation results by MATLAB as well as the grammar and typos.

References

[1] Abbas H.F (2021). Management of Network Service Orchestration and 5G Networks. *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, *12*(10), 1109-1114. DOI: 10.17762/turcomat.v12i10.4297.

[2] D.T.Vo, T.V.Chien, T.N. Nguyen, D.H.Tran, M.Voznak, B.S.KIM, and L.T.Tu. SWIPT-Enabled Cooperative Wireless IoT Networks with Friendly Jammer and Eavesdropper: Outage and Intercept Probability Analysis. *IEEE*

Access, *11*, 86165-86177. DOI: 10.1109/ACCESS.2023.3303369.

[3] Naraiah R (2021). Spectral Efficiency Improvement Techniques In Massive Mimo For 5G Communications. *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, *12*(2), 1457-1565. DOI: 10.17762/turcomat.v12i2.1374.

[4] Liu X, Zhang X (2018). Rate and energy efficiency improvements for 5G-based IoT with simultaneous transfer. *IEEE Internet of Things Journal*, *6*(4), 5971-80. DOI: 10.1109/JIOT.2018.2863267.

[5] Tran D.H, Nguyen V.D, Gautam S, Chatzinotas S, Vu T.X, Ottersten B. Resource Allocation for UAV Relay-Assisted IoT Communication Networks (2020). *In 2020 IEEE Globecom Workshops (GC Wkshps 2020 Dec 7)*, 1-7. DOI: 10.1109/GCWkshps50303.2020.9367522.

[6] Moudoud H, Khoukhi L, Cherkaoui S (2020). Prediction and Detection of FDIA and DDoS Attacks in 5G Enabled IoT. *IEEE Network*, *35*(2), 194-201. DOI: 10.1109/MNET.011.2000449.

[7] Nguyen P.X, Tran D.H, Onireti O, Tin P.T, Nguyen S.Q, Chatzinotas S, Poor H.V (2021). Backscatter-Assisted Data Offloading in OFDMA-Based Wireless-Powered Mobile Edge Computing for IoT Networks. *IEEE Internet of Things Journal*, *8*(11), 9233-9243. DOI: 10.1109/JIOT.2021.3057360.

[8] S.P.Dash, S.Joshi. Performance analysis of a cooperative D2D communication network with NOMA (2020). *IET Communications*, *14*(16), 2731-2739. DOI: 10.1049/iet-com.2020.0265.

[9] Phu T. T., Dang T. H., Nguyen T. N., Tran T. D., M. Voznak. Secrecy Performance Enhancement for Underlay Cognitive Radio Networks Employing Cooperative Multi-hop Transmission With and Without Presence of Hardware Impairments (2019). *Entropy*, *21*(2), 217. DOI: 10.3390/e21020217.

[10] Nguyen, T. N., Tran, M., Nguyen, T. L., Ha, D. H., & Voznak, M. (2019). Performance Analysis of a User Selection Protocol in Cooperative Networks with Power Splitting Protocol-Based Energy Harvesting Over Nakagami-m/Rayleigh Channels. *Electronics*, *8*(4), 448. DOI: 10.3390/electronics8040448.

[11] Abou-Rjeily C, Kaddoum G (2020). Free space optical cooperative communications via an energy harvesting harvest-store-use relay. *IEEE Transactions on Wireless Communications*,*19*(10), 6564-6577. DOI: 10.1109/TWC.2020.3003811.

[12] Nguyen, T. N., Tran, M., Nguyen, T. L., Ha, D. H., & Voznak, M. (2019). Multisource power splitting energy harvesting relaying network in half-duplex system over block Rayleigh fading channel: System performance analysis. *Electronics*, *8*(1), 67. DOI: 10.3390/electronics8010067.

[13] Nguyen T.N., Phuong T.T., Voznak M. 2018). Power-splitting-based energy harvesting protocol for wireless powered communication networks with a bidirectional relay. *International Journal on Communication Systems*, *31*(13), e3721. DOI: 10.1002/dac.3721.

[14] Van D.P., Nguyen T.N., VU A.L.,Voznak M. (2021). A Study of Physical Layer Security in SWIPT-Based Decode-And-Forward Relay Networks with Dynamic Power Splitting. *Sensors*, *21*(17), 5692. DOI: 10.3390/s21175692.

[15] Gong.S, Zou Y, Hoang D.T, Xu.J, Cheng.W, Niyato.D (2020). Capitalizing backscatter-aided hybrid relay communications with wireless energy harvesting. *IEEE Internet of Things Journal*,*7*(9), 8709-8721. DOI: 10.1109/JIOT.2020.2995512.

[16] Nguyen, T. N., Tran, T.Duy, Phuong, T.Tran., & Voznak, M. (2016). Performance Evaluation Of User Selection Protocols In Random Networks With Energy Harvesting And Hardware Impairments. *Advances in Electrical and Electronic Engineering*, *14*(4), 372-377. DOI: 10.15598/aeee.v14i4.1783.

[17] Hieu T.D., Duy T.T., Choi S.G. (2018). Performance evaluation of relay selection schemes in beacon-assisted dual-hop cognitive radio wireless sensor networks under impact of hardware noises. *Sensors*, *18*(6), 1843. DOI: 10.3390/s18061843.

[18] Duy T.T., Duong T.Q., Thanh T.L., Bao V.N. (2015). Secrecy performance analysis with relay selection methods under impact of co-channel interference. *IET Communications*. *9*(11), 1427-1435. DOI: 10.1049/iet-com.2014.1128.

[19] Phu T.T., Nguyen T.N., Sang N.Q., Trung Duy T., Tran P.T., Voznak M. (2019). Rateless Codes-Based Secure Communication Employing Transmit Antenna Selection and Harvest-To-Jam under Joint Effect of Interference and Hardware Impairments. *Entropy*, *21*(7), 700. DOI: 10.3390/e21070700.

[20] Park E., Bae J., Ju H., Han Y. (2019). Resource allocation for full-duplex systems with imperfect co-channel interference estimation. *IEEE Transactions on Wireless Communications*, *18*(4), 2388-23400. DOI: 10.1109/TWC.2019.2903803.

[21] Duy T.T., Duong T.Q., da Costa D.B., Bao V.N., Elkashlan M (2015). Proactive relay selection with joint impact of hardware impairment and co-channel interference. *IEEE Transactions on Communications*, *63*(5), 1594-1606. DOI: 10.1109/TCOMM.2015.2396517.

[22] Nguyen T.N., Thanh L.T., Dinh H.T., Duc V.P., Voznak M., Chatzinotas S., & Ding Z. (2022). Outage Performance of Satellite Terrestrial Full-Duplex Relaying Networks with Co-Channel Interference. *IEEE Wireless Communications Letters*, *11*(7), 1478-1482. DOI: 10.1109/LWC.2022.3175734.

[23] Roy A., Nemade H.B., Bhattacharjee R. Multiuser PSK-Chirp-BOK Communication System Under Co-Channel Interference. *IEEE Transactions on Circuits and Systems II: Express Briefs*, *67*(3), 465-569. DOI: 10.1109/TCSII.2019.2914056.

[24] Dinh Tran H., Trung Tran D., Choi S.G. (2018). Secrecy performance of a generalized partial relay selection protocol in underlay cognitive networks. *International Journal on Communication Systems*, *31*(17), e3806. DOI: 10.1002/dac.3806.

[25] Feng K, Li X, Han Y, Jin S, Chen Y (2020). Physical layer security enhancement exploiting intelligent reflecting surface. *IEEE Communication Letter*, *25*(3), 734-738. DOI: 10.1109/LCOMM.2020.3042344.

[26] Nguyen T.N., Dinh H.T., Chien T.V., Duc P.V., Voznak M., Tin P.T., Chatzinotas S., Derrick W.K.N., & Poor H.V. (2022). Security-Reliability Trade-Off Analysis for SWIPT- and AF-Based IoT Networks with Friendly Jammers. *IEEE Internet of Things Journal*, *9*(21), 21662-21675. DOI: 10.1109/JIOT.2022.3182755.

[27] Hieu T.D., Duy T.T., Kim B.S. (2018). Performance enhancement for multihop harvest-to-transmit WSNs with path-selection methods in presence of eavesdroppers and hardware noises. *IEEE Sens Journal*, *18*(12), 5173-5186. DOI: 10.1109/JSEN.2018.2829145.

[28] Tan N.N., Duy T.T., Phuong T.T., Voznak M., Xingwang L., & Poor H.V. (2022). 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*, *71*(6), 6173-6188. DOI: 10.1109/TVT.2022.3158340.

[29] Tan N.N., Dinh H.T., Duc P.V., Voznak M., Chatzinotas S., Ottersten B., & Poor H.V. (2021). Throughput Enhancement in FD and SWIPT-enabled IoT Networks over Non-Identical Rayleigh Fading Channels. *IEEE Internet of Things Journal*, *9*(12), 10172-10186. DOI: 10.1109/JIOT.2021.3120766.

[30] Tan N.N., Dinh H.T., Chien T.V., Duc P.V., Tien N.N., Voznak M., Chatzinotas S., Ottersten B., & Poor H.V. (2021). Physical Layer Security in AF-Based Cooperative SWIPT Sensor Networks. *IEEE Sensors Journal*, *23*(1), 689-705. DOI: 10.1109/JSEN.2022.3224128.

[31] Ha D.H., Nguyen T.N., Minh T., Li X., Phuong T.T., & Voznak M. (2020). 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*, 8, 187165-18781. DOI: 10.1109/ACCESS.2020.3030794.

[32] Makarf A.U., Rabie K.M., Kaiwartya O., Adhikari K., Nauryzbayev G., Li X., & Kharel R. (2021). Toward Physical-Layer Security for Internet of Vehicles: Interference-Aware Modeling. *IEEE Internet of Things Journal*, *8*(1), 443-457. DOI: 10.1109/JIOT.2020.3006527.

[33] Gradshteyn, I.S., & Ryzhik, I.M. *Table of integrals, series, and products. Elsevier/Academic Press*, 2007. ISBN 978-0-12-384933-5.

[34] Nguyen T. N., Lam T.T., Fazio P., Chien T.V., Cuong V. L., Binh H.T.T., & Voznak, M. (2023). On the Dilemma of Reliability or Security in Unmanned Aerial Vehicle Communications Assisted by Energy Harvesting Relaying. *IEEE Journal on Selected Areas in Communications*, *Early Access*. DOI: 10.1109/JSAC.2023.3322756.

[35] Phuoc T. H., Son P. N., & Voznak M. (2017). Exact Throughput Analyses of Energy-Harvesting Cooperation Scheme with Best Relay Selections Under I/Q Imbalance. *Advances in Electrical and Electronic Engineering*, *15*(4), 585-590. DOI: 10.15598/aeee.v15i4.2302.

[36] Nhu H. N., Huu P. D., Si P. L., Thanh D. L., Dinh T. D., Voznak M., & Zdralek J. (2018). Enabling D2D Transmission Mode with Energy Harvesting and Information Transfer in Heterogeneous Networks. *Advances in Electrical and Electronic Engineering*, *16*(2), 178-184. DOI: 10.15598/aeee.v16i2.2393.

About Authors

Bui Vu MINH was born on March 02, 1991, in Dong Nai, Vietnam. He graduated in Electrical and

Electronic Engineering in 2015 from Nguyen Tat Thanh University, Ho Chi Minh City, Vietnam. End of 2014, he joined the Faculty of Engineering and Technology of Nguyen Tat Thanh University as a laboratory practice management, and then he became a lecturer in 2017. In 2019, he received a Master's degree in Electrical Engineering from Ho Chi Minh City University of Technology and Education, Ho Chi Minh City, Vietnam. His major research interests are Wireless Networks, Robot, Artificial Neural Networks, and Power Electronics.

Tran Hoang Quang MINH received his Ph.D. from Tomsk Polytechnic University, Tomsk City, Russian Federation. His research interests include high-voltage power systems, optoelectronics, wireless communications, and network information theory. He serves as a Lecturer in the Faculty of Electrical and Electronics Engineering, Ton Duc Thang University, Ho Chi Minh City, Vietnam.

Van-Duc PHAN (corresponding author) was born in 1975 in Long An province, Vietnam. He received the M.Sc. degree from the Department of Electric, Electrical and Telecommunications Engineering, Ho Chi Minh City University of Transport, Ho Chi Minh City, Vietnam, and the Ph.D. degree from the Department of Mechanical and Automation Engineering, Da-Yeh University, Changhua, Taiwan. His current research interests include sliding mode controls, nonlinear systems and active magnetic bearings, flywheel energy storage systems, power system optimization, optimization algorithms, renewable energies, energy harvesting enabled cooperative networks, optical property improvement, lighting performance of white LEDs, energy efficiency LED driver integrated circuits, novel radio access technologies, and physical security in communications networks.

Hieu T. NGUYEN received the B.S. and M.Sc. degrees in electronics and telecommunications, and the Ph.D. degree in electronics engineering from Posts and Telecommunications Insti tute of Technology, Hanoi, Vietnam, in 2006, 2010, and 2018, respectively. From 2006 to present, he was with the Faculty of Electron ics Engineering, Hanoi, Vietnam. He is currently Head of the Department of Electronics and Computer Engineering. His research interests include coding theory, signal processing, IoT devices and embedded systems, electronics design, and computer-aided design.