On the Performance of Power Beacon-Assisted D2D Communications in the Presence of Multi-Jammers and Eavesdropper

Tan N. NGUYEN[1,*], *Peppino FAZIO*[2,3], *Miroslav VOZNAK*[2]

[1]Communication and Signal Processing Research Group, Faculty of Electrical and Electronics Engineering, Ton Duc Thang University, Ho Chi Minh City, Vietnam
[2]Faculty of Electrical Engineering and Computer Science, Technical University of Ostrava, 70800 Ostrava, Czech Republic
[3]Department of Molecular Sciences and Nanosystems, Ca' Foscari University of Venice, Via Torino 155, 30123 Venezia VE, Italy

*Corresponding Author: Tan N. NGUYEN (email: nguyennhattan@tdtu.edu.vn)

(Received: 10-Sep-2021; accepted: 26-Oct-2021; published: 31-Dec-2021)
DOI: http://dx.doi.org/10.55579/jaec.202154.341

Abstract. *In this work, we investigate the performance analysis of a device-to-device (D2D) communication network under an eavesdropper E attack. Besides, we assume that E is located in the proximal region where it can overhear the information from the source S. Specifically, S transmits information to the destination D, adopting the power beacon's energy to surmount the limited energy budget. Moreover, to reduce the quality of the eavesdropping link, the cooperative jamming technique can be used, where the multi-friendly jammers are employed to generate the artificial noises to E continuously. As considering the above presentation, we derive the quality of system analysis in terms of the outage probability (OP), intercept probability (IP), and secrecy outage probability (SOP) of the proposed system model. Finally, the Monte-Carlo simulations are performed to corroborate the exactness of the mathematical analysis.*

Keywords

Friendly jammer, energy harvesting, intercept probability, outage probability, power beacon, secrecy outage probability.

1. Introduction

The Internet of things (IoT) has received substantial attention from academia and industry because it is a promising communications paradigm that can potentially boost the quality of life with advances in smart transportation, manufacturing, smart cities, energy, health care, agriculture, and retail [1, 2]. Especially, it has become a crucial research direction to accelerate the evolution of the fifth-generation (5G) and beyond [3–6]. Besides many benefits, the massive number of IoT users proposes new communication challenges due to the limited resources, i.e., frequency, power. Fortunately, to improve network performance by increasing the coverage region, D2D communication has emerged as a solution and allows the IoT devices to share the content, as well as other users in close proximity, [7].

Recently, wireless energy harvesting (EH) [8–10] has emerged as a potential solution to prolong the lifetime of WSNs. In wireless EH, the energy-constrained devices can harvest energy from radio frequency signals generated by ambient nodes. In [8], the authors studied the EH Decode-and-Forward (DF) by applying a time-switching (TS) scheme in a cooperative Full-Duplex (FD) network, wherein a single-antenna source wants to transmit its signal to a multi-antenna destination with the help of a two-antenna relay was investigated. Different with [8], in [10], the authors employed a static/dynamic power splitting (PS) scheme at the relay, the outage probability and the diversity gain of the dual-hop DF relay systems were analyzed in the presence of a direct link with simultaneous wireless information and power transfer (SWIPT). By combining the TS and PS schemes, the hybrid TS-PS named HTPSR was studied to evaluate the quality of cooperative half-duplex (HD) network in [11]. In [12–14], the authors presented the EH relaying cooperative network with PS protocol with power beacon (PB)-assisted to charge energy for wireless devices and enhance the ability to exchange information between the nodes. The PB-aided wireless power transfer models are suitable for large-scale WSNs or ad-hoc wireless networks. More specifically, the authors in [15,16] proposed novel multi-hop multi-path PB-assisted cooperating networks with path selection methods to enhance the system performance.

In addition, physical-layer security (PLS) [17–19] has also attracted much attention from researchers as an efficient method to obtain security. Due to its simple implementation, i.e., exploiting only wireless medium characteristics such as link distance and channel state information (CSI), PLS can be effectively implemented in wireless sensor networks (WSNs), internet-of-things (IoT) networks, etc. [20–22]. In [22], the secrecy performance of transmit antenna selection/selection combining(TAS/SC)-based multi-hop harvest-to-transmit cognitive WSNs under the joint impact of interference constraint, limited-energy source, and hardware impairments was investigated. The authors derived new exact and asymptotic expressions of the end-to-end secrecy outage probability (SOP) and probability of non-zero secrecy capacity (PNSC) over the Rayleigh fading channel. In [17], Tin et al. also used TAS and harvest-to-jam techniques to improve security and energy efficiency. Specifically, they derived the closed-form expressions of the probability of successful and secure communication (SS), outage probability (OP), and intercept probability (IP) for the system by considering both co-channel interference and hardware impairments. Despite many fruitful results obtained from the literature to improve the PLS in IoT networks [23–25], none of these works considered jammer in their system model. Therefore, to reduce quality of the eavesdropping channels and increase the credibility of the legitimate channels, in [26–28], the authors proposed cooperative jamming (CJ) techniques, where friendly jammers are adopted to generate artificial noises on the eavesdropper, and the legitimate receivers must cooperate with the jammers to cancel the interference in the received signals.

Motivated by the above discussions, this paper proposed and investigated the performance analysis of the D2D network under power beacon assistance in the presence of eavesdropper and multi-friendly jammers. Furthermore, the source node, which is equipped with an EH circuit, harvests energy from a power beacon. The main contributions are listed as follows:

- We consider a single-input single-output D2D system model in which the source node harvests energy from a power beacon and helps S transfer information to the destination in the presence of an eavesdropper. Moreover, multi-friendly jammers are adopted to reduce the ability to eavesdrop on information from E.

- For the SWIPT technique, a time-switching scheme is considered in our work to illustrate the EH process at the source node. Specifically, we derive the closed-form expressions in terms of OP, IP, and SOP to evaluate the quality of the proposed system. On the other hand, the indept security-reliability trade-off analysis is investigated.

- Simulation results are performed to corroborate the exactness of our analysis. The simulation results show the influences of different parameters on the system perfor-

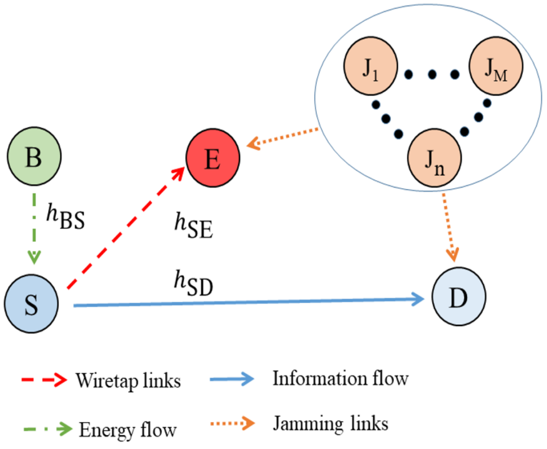

Fig. 1: SWIPT-based cooperative D2D networks in the presence of an eavesdropper and multi friendly jammers.

mance and how to select these parameters appropriately to eliminate the eavesdropper's impacts.

2. System model

As shown in Fig.1, a source node S harvests energy from a power beacon B. Then, S will transmit the information to the destination by using this energy, and eavesdropper E will overhear this signal in the broadcast phase. Furthermore, there are M multiple friendly jammers denoted by $\mathrm{J}_1, \mathrm{J}_2, ..., \mathrm{J}_M$ that generate artificial noises on the eavesdropper and the legitimate users must cooperate with jammers to remove these noises in their received information. Please noticed that in our proposed model, we assume that the jammers are located very far from the power beacon B and can not harvest the energy. The EH and information processing are shown in Fig. 2 . During the first time slot αT, S will harvest the energy from B, and it adopts this energy to transmit its signal to the destination D in the second time slot $(1-\alpha)$T, wherein T is the total time for whole processing. In our model, we assume that the channels between nodes are block Rayleigh fading. The reason that we choose the Rayleigh fading channel is simple and very easy to encounter in densely populated environments,

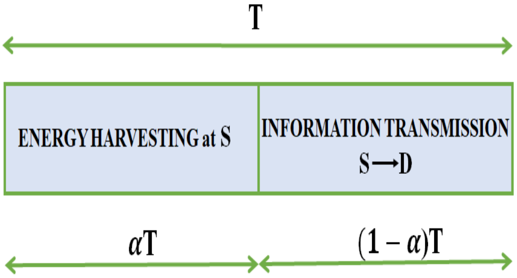

Fig. 2: Energy Harvesting and Information transmission processing.

especially in environments covered by buildings and trees. Moreover, Rayleigh fading channel will be worse than Rician or Nakagami-m channel and if we examine the quality of the system in a Rayleigh environment that it meets the needs of the users, then of course in a Rician or Nakagami-m environment it will satisfy. Thus, the squared amplitudes of the channel gains such as $|h_{\mathrm{BS}}|^2 = \gamma_{\mathrm{BS}}, |h_{\mathrm{SD}}|^2 = \gamma_{\mathrm{SD}}$, etc. are exponential random variables (RVs) whose cumulative distribution function (CDF) and probability density function (PDF) have the following forms, respectively:

$$F_X(x) = 1 - \exp\left(-\lambda x\right), \tag{1}$$

$$f_X(x) = \lambda \exp\left(-\lambda x\right), x \geq 0. \tag{2}$$

where λ is the mean of the exponential random variable X.

As mentioned above, in the first phase, the source S employs all harvested energy to transmit the signal to the destination D. By applying the time-switching (TS) scheme, the average transmit power at S can be given as [29]

$$P_S = \frac{E_S}{(1-\alpha)\mathrm{T}} = \frac{\eta\alpha\mathrm{T}P_{\mathrm{B}}|h_{\mathrm{BS}}|^2}{(1-\alpha)\mathrm{T}} = \mu P_{\mathrm{B}}\gamma_{\mathrm{BS}}, \tag{3}$$

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

In the broadcast phase, the received signal at the destination D can be expressed as

$$y_{\mathrm{D}} = h_{\mathrm{SD}} x_S + \sum_{n=1}^{M} x_{\mathrm{J}_n} h_{\mathrm{J}_n\mathrm{D}} + n_{\mathrm{D}}, \qquad (4)$$

where x_S is the transmitted signal at the source S and $\mathrm{E}\left\{|x_S|^2\right\} = P_S$; n_{D} is the zero-mean additive white Gaussian noise (AWGN) with variance N_0 and $\mathrm{E}\{\bullet\}$ is the expectation operator.

For simplicity, we assume that all the friendly jammers have the same transmit power P_{J}, i.e., $\underbrace{\mathrm{E}\left\{|x_{\mathrm{J}_n}|^2\right\}}_{n=1,2,\ldots,M} = P_{\mathrm{J}}$.

Because D have to cooperate with the jammers to remove the artificial noises which are generated by jammers in its received signal. Hence, (4) can be re-written by

$$y_{\mathrm{D}} = h_{\mathrm{SD}} x_S + n_{\mathrm{D}}, \qquad (5)$$

Next, the received signal at the eavesdropper E can be expressed as

$$y_{\mathrm{E}} = h_{\mathrm{SE}} x_S + \sum_{n=1}^{M} x_{\mathrm{J}_n} h_{\mathrm{J}_n\mathrm{D}} + n_{\mathrm{E}}, \qquad (6)$$

Based on (3), (5) and (6), the signal to noise (SNR) at D and E can be given as, respectively.

$$\gamma_{\mathrm{D}} = \mu\Psi\gamma_{\mathrm{SD}}\gamma_{\mathrm{BS}}, \qquad (7)$$

$$\gamma_{\mathrm{E}} = \frac{\mu|h_{SE}|^2|h_{BS}|^2\Psi}{\Delta\sum\limits_{n=1}^{M}|h_{I_nE}|^2+1} = \frac{\mu\gamma_{\mathrm{SE}}\gamma_{\mathrm{BS}}\Psi}{\Phi\mathrm{X}+1}, \qquad (8)$$

where $\Psi = \frac{P_{\mathrm{B}}}{N_0}$, $\Phi = \frac{P_{\mathrm{J}}}{N_0}$ and $\mathrm{X} = \sum\limits_{n=1}^{M}|h_{\mathrm{J}_n\mathrm{E}}|^2$.

Next, the data rate expressions at D and E can be obtained by, respectively.

$$\begin{aligned} C_{\mathrm{D}} &= (1-\alpha)\log_2(1+\gamma_{\mathrm{D}}),\\ C_{\mathrm{E}} &= (1-\alpha)\log_2(1+\gamma_{\mathrm{E}}), \end{aligned} \qquad (9)$$

Remark 1. *Based on [30, eq.35], the PDF of RV X can be computed as*

$$f_{\mathrm{X}}(x) = \frac{(\lambda_{\mathrm{JE}})^M}{(M-1)!}x^{M-1}\exp(-\lambda_{\mathrm{JE}}x), \qquad (10)$$

3. Performance analysis

3.1. Outage probability (OP) analysis

Based on (7) and (9), the OP of system can be calculated by [31]

$$\begin{aligned} &\mathrm{OP} = \Pr\left(C_{\mathrm{D}} < C_{th}\right) = \Pr\left(\mu\Psi\gamma_{\mathrm{SD}}\gamma_{\mathrm{BS}} < \gamma_{th}\right)\\ &= \Pr\left(\gamma_{\mathrm{SD}} < \frac{\gamma_{th}}{\mu\Psi\gamma_{\mathrm{BS}}}\right) = \int\limits_0^\infty F_{\gamma_{\mathrm{SD}}}\left(\frac{\gamma_{th}}{\mu\Psi x}\right) f_{\gamma_{\mathrm{BS}}}(x)dx\\ &= 1 - \lambda_{\mathrm{BS}}\int\limits_0^\infty \exp\left(-\frac{\gamma_{th}\lambda_{\mathrm{SD}}}{\mu\Psi x} - \lambda_{\mathrm{BS}}x\right)dx, \end{aligned} \qquad (11)$$

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

By using [32, eq.3.324.1], (11) can be reformulated as

$$\mathrm{OP} = 1 - 2\sqrt{\frac{\gamma_{th}\lambda_{\mathrm{BS}}\lambda_{\mathrm{SD}}}{\mu\Psi}} \times K_1\left(2\sqrt{\frac{\gamma_{th}\lambda_{\mathrm{BS}}\lambda_{\mathrm{SD}}}{\mu\Psi}}\right). \qquad (12)$$

where $K_v(\bullet)$ is the modified Bessel function of the second kind and v-th order.

3.2. Intercept probability (IP) analysis

Destination will be intercepted if eavesdropper can successfully wiretap signal, i.e. $C_{\mathrm{E}} \geq C_{th}$. Therefore, the IP can be defined as [33–35]

$$\begin{aligned} &\mathrm{IP} = \Pr\left(C_{\mathrm{E}} \geq C_{th}\right) = \Pr\left(\gamma_{\mathrm{E}} \geq \gamma_{th}\right)\\ &= 1 - \Pr\left(\gamma_{\mathrm{E}} < \gamma_{th}\right), \end{aligned} \qquad (13)$$

By substituting (8) into (13), we obtain:

$$\begin{aligned} &\mathrm{IP} = 1 - \Pr\left(\frac{\mu\gamma_{\mathrm{SE}}\gamma_{\mathrm{BS}}\Psi}{\Phi\mathrm{X}+1} < \gamma_{th}\right)\\ &= 1 - \int\limits_0^\infty F_{\gamma_{\mathrm{SE}}\gamma_{\mathrm{BS}}}\left(\frac{\gamma_{th}[\Phi x+1]}{\mu\Psi}\right) \times f_{\mathrm{X}}(x)dx, \end{aligned} \qquad (14)$$

First, by using the result from (12) to calculate the product of two variables $\gamma_{\mathrm{SE}}\gamma_{\mathrm{BS}}$ as following

$$\begin{aligned}&F_{\gamma_{\mathrm{SE}}\gamma_{\mathrm{BS}}}\left(\tfrac{\gamma_{th}[\Phi x+1]}{\mu\Psi}\right)=\Pr\left(\gamma_{\mathrm{SE}}\gamma_{\mathrm{BS}}<\tfrac{\gamma_{th}[\Phi x+1]}{\mu\Psi}\right)\\&=\int\limits_0^\infty F_{\gamma_{\mathrm{SE}}}\left(\tfrac{\gamma_{th}[\Phi x+1]}{\mu\Psi y}\right)\times f_{\gamma_{\mathrm{BS}}}(y)dy\\&=1-\lambda_{\mathrm{BS}}\int\limits_0^\infty\exp\left(-\tfrac{\gamma_{th}\lambda_{\mathrm{SE}}[\Phi x+1]}{\mu\Psi y}-\lambda_{\mathrm{BS}}y\right)dy\\&=1-2\sqrt{\tfrac{\gamma_{th}\lambda_{\mathrm{SE}}\lambda_{\mathrm{BS}}[\Phi x+1]}{\mu\Psi}}\\&\times K_1\left(2\sqrt{\tfrac{\gamma_{th}\lambda_{\mathrm{SE}}\lambda_{\mathrm{BS}}[\Phi x+1]}{\mu\Psi}}\right),\end{aligned}\tag{15}$$

By substituting (10) and (15) into (14), the IP can be re-computed as (16) shown in the next top page.

In order to find the closed-form expression for (16), firstly, we denote $y=\Phi x+1$, (16) can be re-written by

$$\begin{aligned}&\mathrm{IP}=1-\tfrac{2(\lambda_{\mathrm{JE}})^M\sqrt{\gamma_{th}\lambda_{\mathrm{SE}}\lambda_{\mathrm{BS}}}}{(M-1)!\Phi^M\sqrt{\mu\Psi}}\times\exp\left(\tfrac{\lambda_{\mathrm{JE}}}{\Phi}\right)\\&\times\int\limits_1^\infty\left\{\begin{array}{l}(y-1)^{M-1}y^{1/2}\\ \exp\left(-\tfrac{\lambda_{\mathrm{JE}}y}{\Phi}\right)K_1\left(2\sqrt{\tfrac{\lambda_{\mathrm{SE}}\lambda_{\mathrm{BS}}\gamma_{th}y}{\mu\Psi}}\right)dy\end{array}\right\},\end{aligned}\tag{17}$$

Next, for ease of analysis, we apply the Maclaurin series as following

$$\begin{aligned}&\exp\left(-\tfrac{\lambda_{\mathrm{JE}}y}{\Phi}\right)=\sum_{k=0}^{\infty}\frac{\left(-\frac{\lambda_{\mathrm{JE}}y}{\Phi}\right)^k}{k!}\\&=\sum_{k=0}^{\infty}(-1)^k\frac{\left(\frac{\lambda_{\mathrm{JE}}}{\Phi}\right)^k}{k!}y^k,\end{aligned}\tag{18}$$

By substituting (18) into (17), and then by applying [32, eq.6.592.4], the closed-form expression of IP can be claimed by

$$\begin{aligned}&\mathrm{IP}=1-\sum_{k=0}^{\infty}\frac{(-1)^k\left(\frac{\lambda_{\mathrm{JE}}}{\Phi}\right)^{k+M}\exp\left(\frac{\lambda_{\mathrm{JE}}}{\Phi}\right)}{k!\left(\frac{\lambda_{\mathrm{SE}}\lambda_{\mathrm{BS}}\gamma_{th}}{\mu\Psi}\right)^k}\\&\times G_{1,3}^{3,0}\left(\frac{\lambda_{\mathrm{SE}}\lambda_{\mathrm{BS}}\gamma_{th}}{\mu\Psi}\middle|\begin{array}{l}0\\-M,k+1,k\end{array}\right).\end{aligned}\tag{19}$$

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

3.3. Secrecy outage probability (SOP) analysis

For a general communication system, the secrecy rate is determined as the maximum between zero and the value of the difference between the channel rate at the destination and eavesdropper [19]. The secrecy capacity can be thus expressed by

$$C_{\mathrm{sec}}=\max\left(C_{\mathrm{D}}-C_{\mathrm{E}},0\right),\tag{20}$$

The SOP can be determined as following if the secrecy capacity is lower than the threshold of system

$$\mathrm{SOP}=\Pr\left(C_{\mathrm{Sec}}<C_{th}\right)=\Pr\left(\frac{1+\gamma_{\mathrm{D}}}{1+\gamma_{\mathrm{E}}}<\tilde{\gamma}_{th}\right),\tag{21}$$

where $\tilde{\gamma}_{th}=\gamma_{th}+1$.

Based on (7) and (8), the SOP can be reformulated by

$$\mathrm{SOP}=\Pr\left(\frac{1+\mu\Psi\gamma_{\mathrm{SD}}\gamma_{\mathrm{BS}}}{1+\frac{\mu\gamma_{\mathrm{SE}}\gamma_{\mathrm{BS}}\Psi}{\Phi\mathrm{X}+1}}<\tilde{\gamma}_{th}\right),\tag{22}$$

It is easy to observe that the closed-form expression of SOP in (22) is unsolvable due to the difficulty of deriving its probability distribution. To address this issue, we have used the approximation $\frac{1+a}{1+b}\approx\frac{a}{b}$ which is widely adopted in [36, 37]. Therefore, (22) can be derived as

$$\begin{aligned}&\mathrm{SOP}\approx\Pr\left(\tfrac{\Phi\mathrm{X}\gamma_{\mathrm{SD}}}{\gamma_{\mathrm{SE}}}<\tilde{\gamma}_{th}\right)=\Pr\left(\Omega<\tfrac{\tilde{\gamma}_{th}}{\Phi\mathrm{X}}\right)\\&=\int\limits_0^\infty F_\Omega\left(\tfrac{\tilde{\gamma}_{th}}{\Phi x}\right)\times f_{\mathrm{X}}(x)dx,\end{aligned}\tag{23}$$

where $\Omega=\frac{\gamma_{\mathrm{SD}}}{\gamma_{\mathrm{SE}}}$.

From (23), the CDF of Ω can be computed by

$$\begin{aligned}&F_\Omega\left(\tfrac{\tilde{\gamma}_{th}}{\Phi x}\right)=\Pr\left(\Omega<\tfrac{\tilde{\gamma}_{th}}{\Phi x}\right)=\Pr\left(\tfrac{\gamma_{\mathrm{SD}}}{\gamma_{\mathrm{SE}}}<\tfrac{\tilde{\gamma}_{th}}{\Phi x}\right)\\&=\int\limits_0^\infty F_{\gamma_{\mathrm{SD}}}\left(\tfrac{\tilde{\gamma}_{th}y}{\Phi x}\right)f_{\gamma_{\mathrm{SE}}}(y)dy\\&=1-\lambda_{\mathrm{SE}}\int\limits_0^\infty\exp\left(-\tfrac{\lambda_{\mathrm{SD}}\tilde{\gamma}_{th}y}{\Phi x}-\lambda_{\mathrm{SE}}y\right)dy\\&=\tfrac{\lambda_{\mathrm{SD}}\tilde{\gamma}_{th}}{\lambda_{\mathrm{SD}}\tilde{\gamma}_{th}+\Phi x\lambda_{\mathrm{SE}}},\end{aligned}\tag{24}$$

$$\mathrm{IP} = 1 - \frac{2(\lambda_{\mathrm{JE}})^M\sqrt{\lambda_{\mathrm{SE}}\lambda_{\mathrm{BS}}}}{(M-1)!}\int\limits_0^\infty x^{M-1}\exp\left(-\lambda_{\mathrm{JE}}x\right)\times\sqrt{\frac{\gamma_{th}\left(\Phi x+1\right)}{\mu\Psi}}\times K_1\left(2\sqrt{\frac{\lambda_{\mathrm{SE}}\lambda_{\mathrm{BS}}\gamma_{th}\left(\Phi x+1\right)}{\mu\Psi}}\right)dx, \tag{16}$$

By substituting (10) and (24) into (23), we obtain:

$$\mathrm{SOP} = \frac{\lambda_{\mathrm{SD}}\tilde{\gamma}_{th}(\lambda_{\mathrm{JE}})^M}{(M-1)!\Phi\lambda_{\mathrm{SE}}}\int\limits_0^\infty \frac{x^{M-1}\exp(-\lambda_{\mathrm{JE}}x)}{x+\frac{\lambda_{\mathrm{SD}}\tilde{\gamma}_{th}}{\Phi\lambda_{\mathrm{SE}}}}dx, \tag{25}$$

Finally, with the help of [32, eq.3.383.10], the SOP can be thus found by

$$\begin{aligned}\mathrm{SOP} =& \frac{\lambda_{\mathrm{SD}}\tilde{\gamma}_{th}(\lambda_{\mathrm{JE}})^M}{\Phi\lambda_{\mathrm{SE}}}\times\left(\frac{\lambda_{\mathrm{SD}}\tilde{\gamma}_{th}}{\Phi\lambda_{\mathrm{SE}}}\right)^{M-1}\\ &\times\exp\left(\frac{\lambda_{\mathrm{SD}}\lambda_{\mathrm{JE}}\tilde{\gamma}_{th}}{\Phi\lambda_{\mathrm{SE}}}\right)\Gamma\left(1-M,\frac{\lambda_{\mathrm{SD}}\lambda_{\mathrm{JE}}\tilde{\gamma}_{th}}{\Phi\lambda_{\mathrm{SE}}}\right).\end{aligned} \tag{26}$$

where $\Gamma\left(\alpha,x\right)=\int\limits_x^\infty e^{-t}t^{\alpha-1}dt$ is the incomplete gamma function.

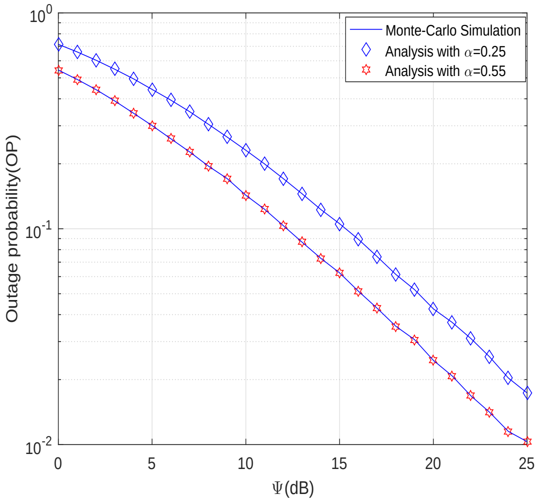

Fig. 3: OP versus Ψ with C_{th}=0.25 bps/Hz and η=0.8.

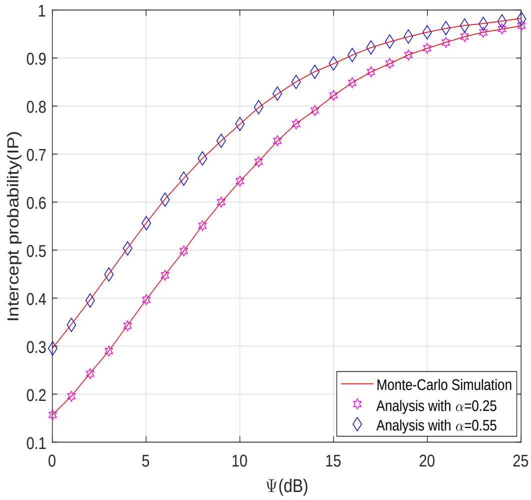

Fig. 4: IP versus Ψ with C_{th}=0.25 bps/Hz, η=0.8, M=1 and Φ = 1 dB.

4. Numerical results

In this section, Monte-Carlo simulations are furnished to verify the theoretical expressions and the effects of various parameters on the system performance. To obtain the OP, IP and SOP for the proposed schemes, we perform 10^5 independent trials, and the channel coefficients are randomly generated as Rayleigh fading in each trial.

In Figs. 3 and 4, we sketch the OP and IP as functions of Ψ(dB) with different α values, where C_{th}=0.25 bps/Hz, η=0.8, M=1 and Φ=1dB. First, in Fig. 3, we can see that if the Ψ is higher, the better OP can be obtained. On the other hand, in Fig. 4, the IP is also proportional to the Ψ value. This is easy to explain since when we increase the value of transmit power, the possibility to receive transmitted information from the source at the destination will be higher, so OP will decrease. Moreover, based on observation in (3), when α=0.25 case, the transmit power will be lower than α=0.55

case. Furthermore, in (11), the OP is a linear function of the transmit power Ψ, hence, the OP with α=0.55 is better than the OP with α=0.25. Besides, when increasing the transmit power, the possibility of E eavesdropping data from the source is also very high. As the same explaination for OP case, the IP is the better if α=0.55 and the transmit power Ψ increases gradually. So, the problem is that we have to trade off between OP and IP. It means that if we want the system to work well, we must accept high eavesdropping information and vice versa. In more detail, for example in Fig. 3, with Ψ=12 dB, the OP is 0.1 while the IP is approximately 0.75 in Fig. 4. Hence, with the choice of simulation parameters as shown above, the overhear ability of E is still very high and in order to reduce the IP value, we can increase the number of jammers as shown in Fig. 5.

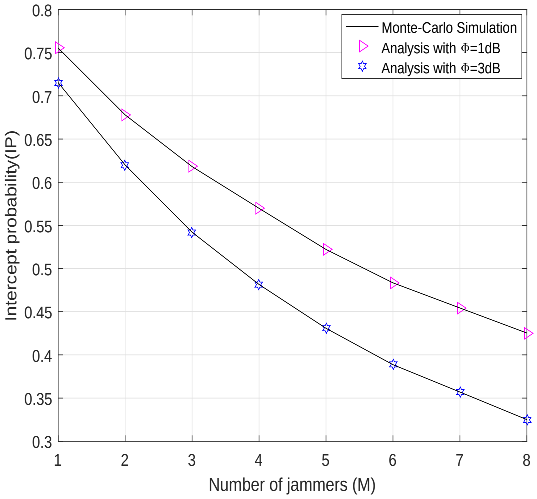

Fig. 5: IP versus M with C_{th}=0.25 bps/Hz, η=0.8, α=0.5 and Ψ = 10 dB.

In order that the system works well, we have to find solutions which reduce E's eavesdropping ability. So, as the same parameter such as C_{th}=0.25 bps/Hz, η=0.8 for OP analysis, we can observe in Fig. 3, the OP is very close the 0.1 value when Ψ=12dB. If want to hold this value, we will choose to increase the transmit power of the jammer as well as choose a large number of jammers to decrease the IP value where is illustrated in Fig. 5.

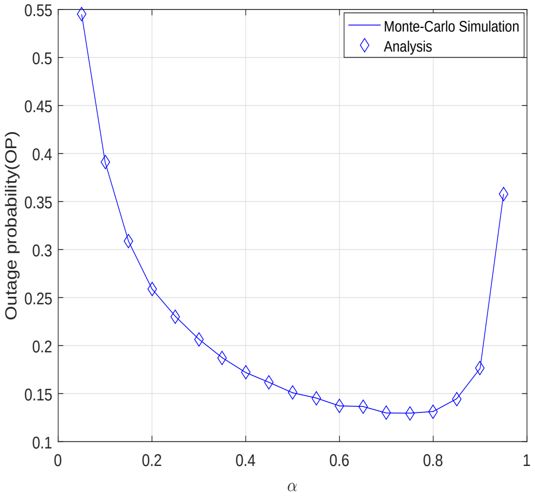

Fig. 6: OP versus α with C_{th}=0.25 bps/Hz, η=0.8 and Ψ = 10 dB.

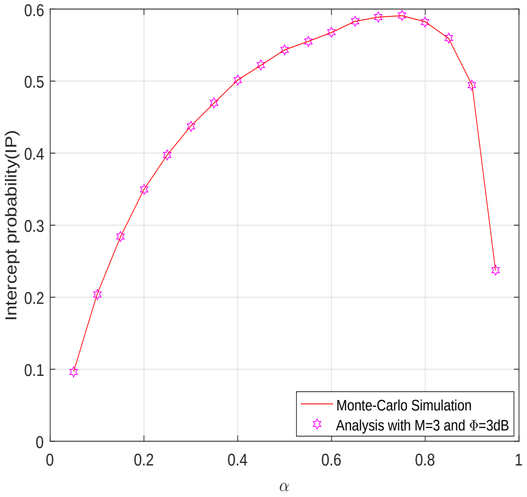

Fig. 7: IP versus α with C_{th}=0.25 bps/Hz, η=0.8, M = 3, Φ = 3 dB and Ψ = 10 dB.

In Figs. 6 and 7, we plot the OP and IP as functions of α, where C_{th}=0.25 bps/Hz, η=0.8, Ψ = 10 dB, M=3 and Φ = 3 dB. By observing the results, the optimal α can be found when the OP is minimum in Fig. 6 and IP is maximum in Fig. 7. This optimal α value varies between 0.7 and 0.8. In both figures, once again, the trade-off between OP and IP is described clearly where the α value that makes the OP minimize will make the IP maximally. Therefore, the chosen α value must guarantee trade-off condition between OP and IP in practice. The recommendation α value in both Figs. 6 and 7 is approximately 0.2 with specific values set as above.

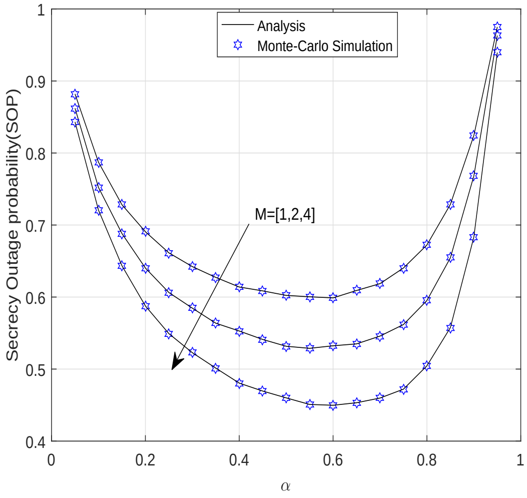

Fig. 8: SOP versus α with C_{th}=0.25 bps/Hz, η=0.8, Φ = 1 dB and Ψ = 5dB.

For a general analysis, finally, the SOP versus α with different number of jammers is investigated shown in Fig. 8, where C_{th}=0.25 bps/Hz, η=0.8, Ψ = 5 dB and Φ = 1 dB. Similar to Figs. 6 and 7, there also exists an optimal value of α to minimize SOP. For instance, when M equals 1, the SOP performance converges to the optimal α value equals 0.6, then SOP value increases when α varies from 0.6 to 1 and decreases when α varies from 0 to 0.6. Moreover, it is easily observed that the higher value of Φ is, the the lower the secrecy performance can be achieved. Because of the higher Φ at the jammers, it will increase the power of artificial noises on the eavesdropper and make the received capacity C_{E} to decrease.

5. Conclusions

In this paper, we studied a D2D network that is assisted by a power beacon, an EH source, a destination under the impact of an eavesdropper, and multi-friendly jammers. The source node can harvest energy from a power beacon and used this energy to transmit its data to the destination. At the same time, other sources transfer information or noises using the same frequency. As mentioned above, we derive the performance analysis of the OP, IP, and SOP to estimate the system quality. Finally, the Monte-Carlo simulation is carried out to confirm the rightness of the mathematical analysis. The results also express the trade-off between the OP and IP. For future work, it is of interest to extend the average secrecy capacity (ASC) analysis and investigate to the case of a more generalized model such as investigating multi-sources, multi destinations models,i.e., and Rician or Weibull fading channels.

Acknowledgement

This research was supported by the Ministry of Education, Youth and Sports of the Czech Republic under the grant SP2021/25 and e-INFRA CZ (ID:90140).

References

[1] Nguyen, T.V., Tran, T.N., Shim, K., Huynh-The, T., & An, B. (2021). A Deep-Neural-Network-Based Relay Selection Scheme in Wireless-Powered Cognitive IoT Networks. *IEEE Internet of Things Journal*, *8*(9), 7423–7436.

[2] Mao, B., Kawamoto, Y., & Kato, N. (2020). AI-Based Joint Optimization of QoS and Security for 6G Energy Harvesting Internet of Things. *IEEE Internet of Things Journal*, *7*(8), 7032–7042.

[3] Liu, X. & Zhang, X. (2019). Rate and Energy Efficiency Improvements for 5G-Based IoT With Simultaneous Transfer. *IEEE Internet of Things Journal*, *6*(4), 5971–5980.

[4] Moudoud, H., Khoukhi, L., & Cherkaoui, S. (2021). Prediction and Detection of FDIA

and DDoS Attacks in 5G Enabled IoT. *IEEE Network*, *35*(2), 194–201.

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

[6] Nguyen, P.X., Tran, D.H., Onireti, O., Tin, P.T., Nguyen, S.Q., Chatzinotas, S., & Vincent Poor, H. (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.

[7] Yang, Y., Xu, J., Xu, Z., Zhou, P., & Qiu, T. (2020). Quantile Context-Aware Social IoT Service Big Data Recommendation With D2D Communication. *IEEE Internet of Things Journal*, *7*(6), 5533–5548.

[8] Tin, P.T., Nguyen, T.N., Tran, D.H., Voznak, M., Phan, V.D., & Chatzinotas, S. (2021). Performance Enhancement for Full-Duplex Relaying with Time-Switching-Based SWIPT in Wireless Sensors Networks. *Sensors*, *21*(11).

[9] Hieu, T.D., Duy, T.T., Choi, S.G. *et al.* (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.

[10] Ye, Y., Li, Y., Zhou, F., Al-Dhahir, N., & Zhang, H. (2019). Power Splitting-Based SWIPT With Dual-Hop DF Relaying in the Presence of a Direct Link. *IEEE Systems Journal*, *13*(2), 1316–1319.

[11] Tran, P., Nguyen, T., & Voznak, M. (2018). Performance Analysis of General Hybrid TSR-PSR Energy Harvesting Protocol for Amplify-and-Forward Half-Duplex Relaying Networks. *Journal of Advanced Engineering and Computation*, *2*(2).

[12] Tin, P.T., Dinh, B.H., Nguyen, T.N., Ha, D.H., & Trang, T.T. (2020). Power Beacon-Assisted Energy Harvesting Wireless Physical Layer Cooperative Relaying Networks: Performance Analysis. *Symmetry*, *12*(1).

[13] Xu, C., Zheng, M., Liang, W., Yu, H., & Liang, Y.C. (2017). End-to-End Throughput Maximization for Underlay Multi-Hop Cognitive Radio Networks With RF Energy Harvesting. *IEEE Transactions on Wireless Communications*, *16*(6), 3561–3572.

[14] Hieu, T.D., Duy, T.T., Dung, L.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).

[15] Dinh Hieu, T., Duy, T.T., & Choi, S.G. (2018). Performance enhancement for harvest-to-transmit cognitive multi-hop networks with best path selection method under presence of eavesdropper. In *2018 20th International Conference on Advanced Communication Technology (ICACT)*, 323–328.

[16] 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 Sensors Journal*, *18*(12), 5173–5186.

[17] Tran Tin, P., 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).

[18] Hoang An, N., Tran, M., Nguyen, T.N., & Ha, D.H. (2020). Physical Layer Security in a Hybrid TPSR Two-Way Half-Duplex Relaying Network over a Rayleigh Fading Channel: Outage and Intercept Probability Analysis. *Electronics*, *9*(3).

[19] Ha, D.H., Nguyen, T.N., Tran, M.H.Q., Li, X., Tran, P.T., & Voznak, M. (2020). Security and Reliability Analysis of a Two-Way Half-Duplex Wireless Relaying Network Using Partial Relay Selection and Hy-

brid TPSR Energy Harvesting at Relay Nodes. *IEEE Access*, *8*, 187165–187181.

[20] Phan, V.D., Nguyen, T.N., Le, A.V., & Voznak, M. (2021). A Study of Physical Layer Security in SWIPT-Based Decode-and-Forward Relay Networks with Dynamic Power Splitting. *Sensors*, *21*(17).

[21] Sun, L. & Du, Q. (2018). A Review of Physical Layer Security Techniques for Internet of Things: Challenges and Solutions. *Entropy*, *20*(10).

[22] Tin, P.T., Minh Nam, P., Trung Duy, T., Tran, P.T., & Voznak, M. (2019). Secrecy Performance of TAS/SC-Based Multi-Hop Harvest-to-Transmit Cognitive WSNs Under Joint Constraint of Interference and Hardware Imperfection. *Sensors*, *19*(5).

[23] Yan, P., Yang, J., Liu, M., Sun, J., & Gui, G. (2020). Secrecy Outage Analysis of Transmit Antenna Selection Assisted With Wireless Power Beacon. *IEEE Transactions on Vehicular Technology*, *69*(7), 7473–7482.

[24] Wang, H.M., Zhang, Y., Zhang, X., & Li, Z. (2020). Secrecy and Covert Communications Against UAV Surveillance via Multi-Hop Networks. *IEEE Transactions on Communications*, *68*(1), 389–401.

[25] Chu, Z., Nguyen, H.X., & Caire, G. (2018). Game Theory-Based Resource Allocation for Secure WPCN Multiantenna Multicasting Systems. *IEEE Transactions on Information Forensics and Security*, *13*(4), 926–939.

[26] Cao, K., Cai, Y., Wu, Y., & Yang, W. (2017). Cooperative Jamming for Secure Communication With Finite Alphabet Inputs. *IEEE Communications Letters*, *21*(9), 2025–2028.

[27] Kang, J.M., Yang, J., Ha, J., & Kim, I.M. (2017). Joint Design of Optimal Precoding and Cooperative Jamming for Multiuser Secure Broadcast Systems. *IEEE Transactions on Vehicular Technology*, *66*(11), 10551–10556.

[28] Zhang, G., Xu, J., Wu, Q., Cui, M., Li, X., & Lin, F. (2018). Wireless Powered Cooperative Jamming for Secure OFDM System. *IEEE Transactions on Vehicular Technology*, *67*(2), 1331–1346.

[29] Voznak, M., Tran, H.Q.M., & Nguyen, N.T. (2018). The System Performance of Half-Duplex Relay Network under Effect of Interference Noise. *Journal of Advanced Engineering and Computation*, *2*(1).

[30] Duy, T.T., Duong, T.Q., Thanh, T.L., & Bao, V.N.Q. (2015). Secrecy Performance Analysis with Relay Selection Methods under Impact of Co-channel Interference. *IET Communications*, *9*(11), 926–939.

[31] Ha, D.H., Dong, S.T.C., Nguyen, T.N., Trang, T.T., & Voznak, M. (2019). Half-Duplex Energy Harvesting Relay Network over Different Fading Environment: System Performance with Effect of Hardware Impairment. *Applied Sciences*, *9*(11).

[32] Gradshteyn, I.S. & Ryzhik, I.M. (2014). *Table of integrals, series, and products*. Academic press.

[33] Li, X., Zhao, M., Liu, Y., Li, L., Ding, Z., & Nallanathan, A. (2020). Secrecy Analysis of Ambient Backscatter NOMA Systems Under I/Q Imbalance. *IEEE Transactions on Vehicular Technology*, *69*(10), 12286–12290.

[34] Zou, Y., Champagne, B., Zhu, W.P., & Hanzo, L. (2015). Relay-Selection Improves the Security-Reliability Trade-Off in Cognitive Radio Systems. *IEEE Transactions on Communications*, *63*(1), 215–228.

[35] Zou, Y. (2018). Intelligent Interference Exploitation for Heterogeneous Cellular Networks Against Eavesdropping. *IEEE Journal on Selected Areas in Communications*, *36*(7), 1453–1464.

[36] Jeon, H., Kim, N., Choi, J., Lee, H., & Ha, J. (2011). Bounds on Secrecy Capacity Over Correlated Ergodic Fading Channels at High SNR. *IEEE Transactions on Information Theory*, *57*(4), 1975–1983.

[37] Bankey, V. & Upadhyay, P.K. (2019). Physical Layer Security of Multiuser Multirelay Hybrid Satellite-Terrestrial Relay Networks. *IEEE Transactions on Vehicular Technology*, *68*(3), 2488–2501.

About Authors

Tan N. NGUYEN (M'18) was born at Nha Trang City, Vietnam, in 1986. He received B.S. and M.S. degrees in electronics and telecommunications engineering from Ho Chi Minh University of Natural Sciences, a member of Vietnam National University at Ho Chi Minh City (Vietnam) in 2008 and 2012, respectively. He is currently pursuing his Ph.D. degree in electrical engineering at VSB Technical University of Ostrava, Czech Republic. He got his Ph.D. degree in computer science, communication technology and applied mathematics at VSB Technical University of Ostrava, Czech Republic, in 2019. In 2013, he joined the Faculty of Electrical and Electronics Engineering of Ton Duc Thang University, Vietnam and have been working as lecturer since then. His major interests are cooperative communications, cognitive radio, and physical layer security.

Peppino FAZIO was born in Catanzaro in 1977 and took master's degree in Computer Engineering in 2004 at University of Calabria (UNICAL) with his thesis named "A New Algorithm of Rate Adaptation and Call Admission Control for QoS Optimization in Wireless Networks with a Slow Fading Channel". At the end of 2004, he started my Ph.D. activity in Electronics and Communications Engineering at UNICAL on mobility prediction, channel modeling, resource reservation and vehicular communications. He took my Ph.D. in 2008 with his thesis titled "Resource Reservation Protocol and Predictive Algorithms for QoS support in Wireless Environments". In the middle of 2008, he has been at the "Universidad Politecnica" of Valencia (UPV) for several months, in order to make some post-doc research on vehicular networks and, in particular, the multi-channel structure of MAC in VANETs. His research interests include also mobile communication networks, QoS architectures and internetworking.

Miroslav VOZNAK (M'09-SM'16) received his PhD in telecommunications in 2002 from the Faculty of Electrical Engineering and Computer Science at VSB – Technical University of Ostrava, and achieved habilitation in 2009. He was appointed Full Professor in Electronics and Communications Technologies in 2017. His research interests generally focus on ICT, especially on quality of service and experience, network security, wireless networks, and big data analytics. He has authored and co-authored over one hundred articles indexed in SCI/SCIE journals. According to the Stanford University study released in 2020, he is one of the World's Top 2% of scientists in Networking & Telecommunications and Information & Communications Technologies. He served as a general chair of the 11th IFIP Wireless and Mobile Networking Conference in 2018 and the 24th IEEE/ACM International Symposium on Distributed Simulation and Real Time Applications in 2020. He participated in six projects funded by EU in programs managed directly by European Commission. Currently, he is a principal investigator in the research project QUANTUM5 funded by NATO, which focuses on the application of quantum cryptography in 5G campus networks.