Research Article

Physical Layer Security in wireless sensors networks with friendly jammer: Secrecy Outage Probability Analysis

Bui Vu MINH[1], *N.H.K. NHAN*[2,*], *Thu-Ha Thi PHAM*[3], *Minh Tran*[2], *Sung-Won KIM*[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 Electrical and Electronics Engineering, Ton Duc Thang University, Ho Chi Minh City, Vietnam.
[4]Information and Communication Engineering Department, Yeungnam University, Gyeongsan 38541, Republic of Korea.

bvminh@ntt.edu.vn, nguyenhuukhanhnhan@tdtu.edu.vn, 42101299@student.tdtu.edu.vn, tranhoangquangminh@tdtu.edu.vn, swon@yu.ac.kr.

[*]Corresponding author: N.H.K. NHAN; nguyenhuukhanhnhan@tdtu.edu.vn

DOI: 10.15598/aeee.v22i4.5840

Article history: Received Mar 10, 2024; Revised Jun 12, 2024; Accepted Jul 3, 2024; Published Dec 31, 2024.

Abstract. *In this paper, we addressed improving the physical layer security (PLS) of an energy harvesting (EH)-based wireless network composed of a source node, which is operated by the harvested energy from the power beacon and sends secure information to a destination in the presence of an eavesdropper and a cooperative jammer (CJ). In particular, we provided an explicit transmit design for minimizing the secrecy outage probability (SOP), subject to a minimum secrecy rate constraint. The results show that support from a friendly jammer can significantly improve the reliability and security performance of the system. Additionally, we described the effects of particular factors on the optimal possible temporal distribution between information transmission and energy harvesting. As a result, when considering the SOP, we concluded that there exists an optimal value of the time switching factor for the system to function well. The analytical formulas were verified by Monte Carlo simulation.*

Keywords

Physical layer security (PLS), energy harvesting (EH), cooperative jamming (CJ), secrecy outage probability (SOP).

1. Introduction

The term "Internet of Things" (IoT) generally refers to situations in which network connectivity and computing capability extend to ordinary items, sensors, and objects not typically thought of as computers, enabling these devices to generate, exchange, and use data with minimal human intervention [1, 2]. In recent years, a wide range of IoT applications and next-generation communication (5G and beyond) have been deployed in areas such as smart cities, crowd dynamics management, spatial crowdsourcing, security surveillance, and environment monitoring [3]. However, as most IoT devices have limited battery life, one of the most commonly acknowledged challenges is figuring out how to autonomously maintain connectivity and network longevity. While it is possible to replace or recharge the

battery, there are certain deployments and conditions, such as dangerous situations, remote or underground locations, and places devastated by natural disasters, that make these methods unfeasible, costly, or impossible [4].

Recently, as opposed to waiting for a breakthrough in energy storage technology, an epoch-making technique, the wireless power transfer (WPT) technique is garnering more attention as a way around the present technological limitations with batteries. This apparently magical method has the ability to alter our customary procedures for energy use in a variety of applications, including integrated circuits, solar-powered satellites, electric vehicles, unmanned aerial vehicles, portable electronics, implanted medical devices, wireless sensor networks, and more [5, 6]. Two varieties of WPT-based networks exist. First, there is simultaneous wireless information and power transmission (SWIPT) [7], where radio frequency (RF) signals are utilized to charge the energy-harvesting (EH) receiver in addition to transmitting information. Because both the EH circuit and the decoding circuit are part of the transceiver, this type of SWIPT-enabled receiver has a symmetric structure. The maximizing problem of energy efficiency (EE) of the SWIPT-Enabled IoT Network system under the limitations of quality of service and transmission power was examined by the authors in [8]. Furthermore, three widely-used protocols—time switching (TS), power splitting (PS), and antenna splitting (if the receiver has two or more antennae)—are suggested in the literature to implement a technique like this. In particular, the performance of random networks with three user protocols of selection under the PS protocol was examined by the authors in [9]. The outage probability (OP) of the cooperative cognitive radio network operating under the PS protocol was examined in [10]. Furthermore, Tan and other writers calculated the IoT networks' throughput over independent and non-idential distribution (i.n.i.d.) Rayleigh fading using SWIPT [11]. Throughput analysis of the optimal relay selection network with in-phase and quadrature-phase imbalances under the TS protocol was examined by the authors of [12]. The second kind of this network is known as the wireless-powered communications network (WPCN), wherein specialized power stations like a power beacon (PB) or a hybrid access point are the only sources of power for the batteries of the EH-based devices. As well, it is recommended that PB-based WPCN be considered as a viable option for energizing wireless networks and facilitating a great deal of applications that demand high EE [13]. In [14], intelligent reflecting surface-assisted user cooperation in a WPCN was considered, where two users harvest wireless energy and transmit information to a common hybrid access point. The authors investigated the performance analysis and presented the algorithms for the PB-assisted wirelessly powered non-orthogonal multiple access (NOMA) IoT-based systems in [15]. The exact close-form expressions for the OP, throughput, the optimal sum throughput, and EE were derived. The related works on WPCN concentrated on its applications to cognitive radio networks [16], cellular networks [17], and relaying networks [18]. In particular, the authors of [17] looked into the EE of two-tier cellular networks, in which one tier of the base station (BS) operates on renewable resources. To capture the randomness of the wireless networks, other BSs and end users are modeled according to the Poison Point Process. Their findings show that there exists a transmit power value that is ideal for optimizing the multitier cellular network.

Additionally, it is anticipated that the next generation of mobile networks (5G, 6G, etc.) will significantly increase the global penetration of IoT. In recent years, there has been a noticeable increase in the deployment and performance optimization of IoT networks, as well as their integration with both existing and future cellular networks, thanks to the efforts of wireless standardization organizations across the globe. However, due to wireless communications' openness and the anticipated surge in linked devices, there will be previously unheard-of security breaches and vulnerabilities. Because wireless communications include broadcasting, which makes them vulnerable to various forms of wiretapping, information security has grown to be a major concern. Even more of a security risk exists in IoT networks. This is because unlicensed bands are used by the majority of IoT networks, including WiFi HaLow, SigFox, and LoRa. Furthermore, the exponential annual growth in IoT device connections to wireless networks makes them increasingly susceptible to wiretapping attempts, even from intranet networks. Plenty of research has been done recently to pave the way for the integration of physical layer security into modern and futuristic networks. When it comes to wireless networks, PLS algorithms have twice the benefits of traditional cryptography techniques in the context of 5G and beyond. The first advantage of PLS over higher-layer cryptography is its independence from computational complexity, especially since it exploits the characteristics of the wireless channel instead of cryptography to secure communications [19, 20]. Thus, even with highly capable computational eavesdroppers, secure and reliable communications can be guaranteed. The second is that PLS approaches exhibit extraordinary scalability [21]. It is important to remember that PLS can be applied as an extra security layer on top of the ones that are already in place. PLS can be used in conjunction with other security technologies to offer private and secure communication data in wireless networks that are capable of supporting 5G [22, 23]. Relay networks [24], cellular networks [25, 26], cognitive ra-

dio networks [27], the IoT [28], massive multiple-input multiple-output networks [29], and intelligent reflecting surface-based NOMA networks in the downlink and uplink scenarios with a pernicious eavesdropper[30], etc. have all used PLS. Various techniques have been devised to lower the quality of the wiretapped signals at the eavesdropper, such as multi-antenna-creating beams, cooperative beamforming, and artificial noise. PLS in two-way energy-constraint relaying networks has been implemented by the authors in [31] with three secret cooperative transmission protocols, including secure two-way communication, secure two-way communication with network coding, and secure two-way communication with cooperative jamming and network coding. To enhance outage performance in two-way relaying networks under PLS, binary jamming message solutions for source-wiretapping [32] or combining binary jamming and network coding [33] are used. In addition, numerous studies have improved our knowledge of the physics layer's basic capacity to maintain secure communications and shown its ensuing limitations[34].

One of the main technologies of 5G cellular communications is device-to-device (D2D) communication, which allows adjacent user pairs to connect directly instead of via the BS [35]. This technology has drawn a lot of interest. Increased cellular coverage, reduced transmission latency, improved energy economy, and improved spectrum efficiency are just a few of the benefits of D2D communications [36]. Additionally, D2D communication provides new benefits for mobile services for a number of proximity-based applications, including social networking, content sharing, and multiplayer gaming [37]. D2D communication can be divided into two categories based on the spectrum band utilized: in-band D2D and out-band D2D communications. In the first approach, D2D communication and the cellular network share the same frequency band [36], while in the second approach, the D2D network uses the unlicensed spectrum band [37]. The interference caused by the sharing of spectrum between D2D and cellular communications is one of the most important issues in cellular networks that have in-band underlay D2D communication. Such interference is traditionally considered a negative that impairs cellular network performance. Therefore, the previous D2D communication efforts concentrated on using interference management strategies to reduce the interference impacts in cellular networks. These works are predicated on the negative notion that the interference generated by spectrum sharing must be avoided, controlled, or mitigated by a variety of means. Nonetheless, as recently suggested in [38, 39], such interference may be advantageous from a PLS standpoint since it may be used as artificial noise in CJ to paralyze malicious eavesdroppers and assist cellular users in avoiding eavesdropping. As long as there is less interference from the cognitive users than there is from the eavesdroppers, this is feasible. Spurred by this observation, recent studies have examined in-band D2D communication from the PLS perspective [40, 41].

Especially, the idea of EH, which is the direct use of available energy in the environment through energy conversion from a specific physical domain into electricity, was raised a decade ago and is now an intensive research and application field [42]. In fact, spectral efficiency and quality of service limitations have become less important considerations for wireless networks in favor of EE and green communication [43, 44]. This is particularly true for generational communication in 5G and beyond networks, which aim to minimize power consumption.Green and inexhaustible energy resources, including solar, wind, thermal, and mechanical vibrations, are being explored as ways to increase the EE of networks with limited resources, including wireless sensor networks. Regretfully, the environment has a major influence on how these energy sources are collected. Unlike the techniques mentioned above, EH using RF signals has gained a lot of interest and emerged as a promising alternative in recent years, particularly because RF signals can be used for simultaneous energy and information transmission. RF EH performance in a range of wireless networks and communication schemes has been studied recently, including wireless sensor networks [45], mobile networks [46], the NOMA scheme [47], cognitive radio networks [48], bidirectional relay networks [49], multiple-antenna networks [50], and multi-hop relay networks [51]. In 2020, in particular, Duy et al. [52] examined two-way half-duplex wireless relay networks in a Rayleigh fading environment with partial relay selection and hybrid-TPSR-based EH at the relay node, in which there is an eavesdropper in the vicinity of one source node. The closed-form formulas for the outage probability and intercept probability in the authors' model have been developed.

In addition, the closed-form expression of the secrecy outage probability (SOP) and the SOP-constrained secrecy rate are often adopted as performance metrics in models. To increase the security of a cooperative relay network, the authors of [24] suggested a generalized multi-relay selection strategy. In order to reduce the SOP, they concurrently optimized the power allocation factor and the number of relays using a semi-closed-form definition of the SOP. The secrecy outage performance of satellite-to-terrestrial downlink transmissions with one authorized receiver and one eavesdropper dispersed randomly over the satellite's footprint was examined by the authors in [53]. In [54], SOP and a viable secrecy rate for a vehicle relay network were investigated using CJ and superposition coding techniques. Phu et al. [55] studied an EH-aided underlay single-input, multiple-output cognitive radio network

in the presence of eavesdroppers. The channels within the network are assumed to follow Nakagami-M distribution, and the system SOP performance is evaluated under colluding eavesdropping and non-colluding eavesdropping scenarios. Various techniques have been suggested to lower the quality of wiretapped communications at the eavesdroppers, such as reconfigurable intelligent surfaces [56] and co-channel interference [57].

On the other hand, research on the integration of PLS with energy harvesting is scarce [58, 59, 60]. More precisely, we looked at the scenario of totally wireless networks, whereas the authors in Ghosh et al. in [58] examined the secrecy performance of an undersea optical communication - RF network. Furthermore, they took into account the relay's ability to assist in converting optical signals into electrical signals, but we do not use relays to change the signal's form. Moreover, we utilize EH-enabled communications at the source node to enhance the network's overall EE, while they do not take this method into account in their work. Contrarily, Nguyen and other researchers in T. N. Nguyen et al. in [59] determined the OP and intercept probability, while the SOP is the subject of our current work, which is more difficult due to the numerous correlated variables from both the legitimate and wiretap links. Another difference between the two works is that our approach considers the PB to power the wireless devices, whereas theirs uses SWIPT. The study conducted by Tuan et al. [60] examined the secrecy performance of a two-way relaying SWIPT network that included a hidden eavesdropper. Specifically, the power splitting ratio, uplink transmission power, and downlink beamforming vectors were all concurrently optimized.

Different from some of the above-related works, in this paper we investigate the performance of EH-based wireless networks where a source is charged by harvested energy from a PB in the presence of eavesdroppers. Besides, to stop eavesdroppers from deciphering the secret communication, a cooperative jammer sends out jamming signals. In addition, a CJ scheme is proposed to further enhance PLS. Specifically, we provide a transmission design that is expected to minimize SOP, and we hope that applying our approach will be effective and thus serve as a basis for application to our other work in the future. This paper's main contributions and novelties are summarized as follows:

- We considered an EH-based wireless network comprising a source, a destination, a PB, a CJ, and an eavesdropper. More precisely, the source's operations only respond to the energy that is captured from the PB, thereby increasing the EE of the networks under consideration.
- The security performance of the networks under consideration was examined by us. The closed-form expression of the SOP is provided.

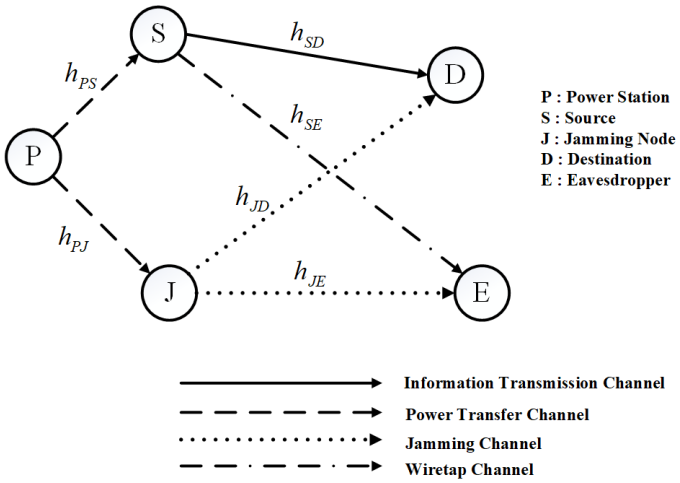

Fig. 1: System Model

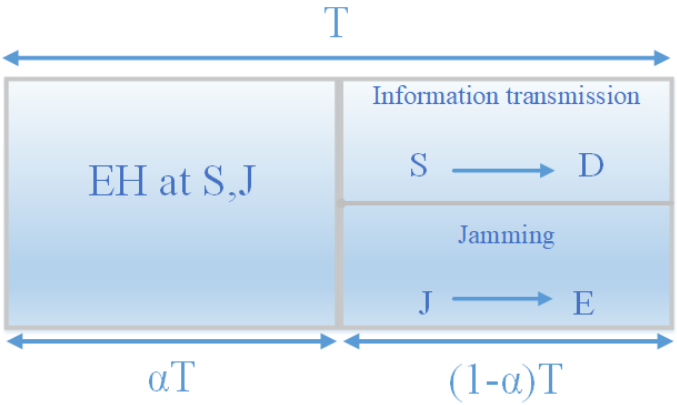

Fig. 2: System Model

- We presented Monte Carlo simulations to assess the reliability of our framework and conclusions. To provide more insights into the physical meaning, the effect of a few critical parameters on its performance is also explored.

2. System Model

In this paper, we consider a wirelessly powered network that includes a source (S) that communicates with one destination user (D), and an eavesdropper (E) that also receives the information signal and wants to decode it, as shown in Figure 1. However, if a jammer (J) transmits a jamming signal to make the information signal's SNR poor at the E receiver, the jamming creates interference at it and deteriorates the strength of the information signal. We also assume that before, D and S could know the jamming signal of J, which can be considered harmless to both of them. Furthermore, we also have a PB (denoted by P), which is replenished by the battery of the source node S. In our research,

we assume that the system model is working in the TS-based protocol, as displayed in Figure 2. In the first half interval αT time, the source S harvests energy from the PB signals, in which α is the TS factor and $0 < \alpha < 1$. In the remaining half-interval time $(1-\alpha)$T, the S node spends all the harvested energy at the first phase to send data to the D by virtue of the harvest-then-use protocol being employed at the S node, and at the same time, J also broadcasts the jamming signal, which is known by D.

Let's refer to the links among these nodes as the given channel coefficients $h_{\rm PS}$, $h_{\rm PJ}$, $h_{\rm SD}$, $h_{\rm SE}$, and $h_{\rm JE}$ as well as the links P $\rightarrow$ S, P $\rightarrow$ J, S $\rightarrow$ D, S $\rightarrow$ E, J $\rightarrow$ E, respectively. Assume that $h_{\rm X}$ (X $\in \{\rm PS, PJ, SD, SE, JE\}$) are Rayleigh fading channels, the channel gains $\gamma_{\rm X} = |h_{\rm X}|^2$ are exponential random variables (RVs) whose cumulative distribution function (CDF) are given as:

$$F_{\rm X}(x) = 1 - \exp\left(-\tfrac{x}{\lambda_{\rm X}}\right). \tag{1}$$

To take into account the simple path loss model, we can formulate the parameters as follows:

$$\lambda_{\rm X} = (d_{\rm X})^{-\omega}. \tag{2}$$

where ω is the path-loss exponent and $d_{\rm X}$ is the distance between two respective nodes.

Then, probability density function (PDF) of $\gamma_{\rm Y}$ is given by:

$$f_{\gamma_{\rm Y}}(x) = \tfrac{1}{\xi}\exp\left(\tfrac{-x}{\xi}\right). \tag{3}$$

where $\xi \in \{\lambda_{\rm PS}, \lambda_{\rm PJ}, \lambda_{\rm SD}, \lambda_{\rm SE}, \lambda_{\rm JE}\}$.

In the EH phase, P transmits energy signals to S for a period of time αT, and T is the time duration for the whole procedure, as shown in Figure 2. The harvested energy at S and J is given as follows:

$$E_S = \alpha T \eta P_P \gamma_{PS}, \tag{4}$$

$$E_J = \alpha T \eta P_P \gamma_{PJ}, \tag{5}$$

where P_P represents P's transmit power and η is the energy conversion efficiency in the interval $\eta \in (0, 1)$. Thus, at the second phase, the transmit power of S and J is calculated as:

$$P_S = \tfrac{E_S}{(1-\alpha)T} = \tfrac{\alpha\eta P_P \gamma_{PS}}{1-\alpha} = \chi P_P \gamma_{PS} \tag{6}$$

$$P_J = \tfrac{E_J}{(1-\alpha)T} = \tfrac{\alpha\eta P_P \gamma_{PJ}}{1-\alpha} = \chi P_P \gamma_{PJ} \tag{7}$$

where $\chi = \frac{\alpha\eta}{1-\alpha}$. In the data transmission phase, S transmits unit power signals x to D, i.e., $\mathrm{E}\left\{|x|^2\right\} = 1$. Where $\mathrm{E}\{.\}$ is the expectation operator. Especially when the jamming signal is issued by J, the legitimate channels S are already aware of the interference signal and can easily remove the interference using successive interference cancellation. Thus, the received signals at D are given as follows:

$$y_D = \sqrt{P_S} h_{SD} x_S + n_D. \tag{8}$$

Here, n_D is the additive white Gaussian noise of the destination and N_0 is the noise variance. The SNR at D is then computed as follows:

$$\gamma_D = \tfrac{\mathrm{E}\{|signal|^2\}}{\mathrm{E}\{|noise|^2\}} = \tfrac{\gamma_{SD} P_S}{N_0}. \tag{9}$$

With the help of (6), the SNR at D is rewritten as:

$$\gamma_D = \tfrac{\chi P_p \gamma_{PS} \gamma_{SD}}{N_0} = \chi\psi\gamma_{PS}\gamma_{SD} \tag{10}$$

where $\psi = \frac{P_p}{N_0}$. At the same time, when the signal from S is transmitted to the destination, the jammer also emits an interference signal to the thief, E. From there, the signal received at E is calculated as follows:

$$y_E = \sqrt{P_S} h_{SE} x_S + \sqrt{P_J} h_{JE} x_J + n_E. \tag{11}$$

where n_E is the additive white Gaussian noise of the destination and the SNR at E is then computed as follows:

$$\gamma_E = \tfrac{\mathrm{E}\{|signal|^2\}}{\mathrm{E}\{|noise|^2\}} = \tfrac{\gamma_{SE} P_S}{\gamma_{JE} P_J + N_0}. \tag{12}$$

Using the fact that $N_0 << P_P$, then by doing some algebra, and finally by substituting (6) into (7) , we have:

$$\gamma_E = \tfrac{\chi\gamma_{SE}\gamma_{PS}P_p}{\chi\gamma_{JE}\gamma_{PJ}P_p + N_0} \approx \tfrac{\gamma_{SE}\gamma_{PS}}{\gamma_{JE}\gamma_{PJ}}. \tag{13}$$

The instantaneous capacity of D and E is given by

$$C_D = (1-\alpha)\log_2(1+\gamma_D) \tag{14}$$

$$C_E = (1-\alpha)\log_2(1+\gamma_E) \tag{15}$$

By substituting (10), (13) into (14) and (15), then by doing some algebra, the instantaneous capacity of D and E can be rewritten as:

$$C_D = (1-\alpha)\log_2(1+\chi\psi\gamma_{PS}\gamma_{SD}) \tag{16}$$

$$C_E = (1-\alpha)\log_2(1+\tfrac{\gamma_{SE}\gamma_{PS}}{\gamma_{JE}\gamma_{PJ}}) \tag{17}$$

The secrecy capacity of individual signal is defined as:

$$C_{\rm Sec} = \max\left[0; C_D - C_E\right]. \tag{18}$$

It can be seen that if $C_D > C_E$, or if $C_{\rm Sec} = C_D - C_E$, then our suggested method makes sense, and vice versa.

3. Performance Analysis

The probability of secrecy capacity falling below the target secrecy rate is known as the SOP. In particular, the SOP is the probability that the instantaneous capacity of the main link divided by the instantaneous capacity of the eavesdropper link is smaller than a given threshold R_{th}, which is expressed as follows:

$$\begin{aligned} SOP &= \Pr\left(C_{\text{Sec}} < R_{th}\right) = \Pr\left(C_D - C_E < R_{th}\right) \\ &= \Pr\left[(1-\alpha)\left(\log_2(1+\gamma_D) - \log_2(1+\gamma_E)\right) < R_{th}\right] \\ &= \Pr\left[\log_2\left(\frac{1+\gamma_D}{1+\gamma_E}\right) < \frac{R_{th}}{1-\alpha}\right] \\ &= \Pr\left[\frac{1+\gamma_D}{1+\gamma_E} < 2^{\frac{R_{th}}{1-\alpha}}\right] \end{aligned} \tag{19}$$

We assume that the P's transmit power and that the SNR at destinations is large enough. Therefore, an approximate formula to apply to SOP to make the calculation less complicated is calculated as follows:

$$SOP \approx \Pr\left[\frac{\gamma_D}{\gamma_E} < 2^{\frac{R_{th}}{1-\alpha}}\right] \tag{20}$$

By substituting (10), (13) and $\gamma_{th} = 2^{\frac{R_{th}}{1-\alpha}}$ into (20) , then by doing some algebra, the SOP can be rewritten as:

$$\begin{aligned} SOP &= \Pr\left[\frac{\chi\psi\gamma_{PS}\gamma_{SD}}{\frac{\gamma_{SE}\gamma_{PS}}{\gamma_{JE}\gamma_{PJ}}} < \gamma_{th}\right] \\ &= 1 - \Pr\left[\frac{\chi\psi\gamma_{PS}\gamma_{SD}}{\frac{\gamma_{SE}\gamma_{PS}}{\gamma_{JE}\gamma_{PJ}}} > \gamma_{th}\right] \end{aligned} \tag{21}$$

So (21) is calculated where $\gamma_{PJE} = \gamma_{PJ}\gamma_{JE}$ as follows:

$$\begin{aligned} SOP &= 1 - \Pr\left(\gamma_{PJE} > \frac{\gamma_{th}\gamma_{SE}}{\chi\psi\gamma_{SD}}\right) \\ &= 1 - \int_0^\infty f_{\gamma_{SE}}(x) \int_0^\infty f_{\gamma_{SD}}(y) \\ &\times \left[1 - F_{\gamma_{PJE}}\left(\frac{\gamma_{th}x}{\chi\psi y}\right)\right] dxdy \end{aligned} \tag{22}$$

With the help of [[61], Eq. 3.324.1], we claim:

$$\begin{aligned} SOP &= 1 - \int_0^\infty f_{\gamma_{SE}}(x) \int_0^\infty f_{\gamma_{SD}}(y) \sqrt{\frac{4\gamma_{th}x}{\chi\psi y\lambda_{PJ}\lambda_{JE}}} \\ &\times K_1\left(\sqrt{\frac{4\gamma_{th}x}{\chi\psi y\lambda_{PJ}\lambda_{JE}}}\right) dxdy \\ &= 1 - \int_0^\infty \int_0^\infty \frac{\exp\left(\frac{-x}{\lambda_{SE}} - \frac{y}{\lambda_{SD}}\right)}{\lambda_{SE}\lambda_{SD}} \sqrt{\frac{4\gamma_{th}x}{\chi\psi y\lambda_{PJ}\lambda_{JE}}} \\ &\times K_1\left(\sqrt{\frac{4\gamma_{th}x}{\chi\psi y\lambda_{PJ}\lambda_{JE}}}\right) dxdy \\ &= 1 - \int_0^\infty \frac{\exp\left(-\frac{y}{\lambda_{SD}}\right)}{\lambda_{SE}\lambda_{SD}} \sqrt{\frac{4\gamma_{th}}{\chi\psi y\lambda_{PJ}\lambda_{JE}}} \\ &\times \int_0^\infty x^{1-\frac{1}{2}} \exp\left(\frac{-x}{\lambda_{SE}}\right) K_1\left(2\sqrt{\frac{\gamma_{th}x}{\chi\psi y\lambda_{PJ}\lambda_{JE}}}\right) dxdy \end{aligned} \tag{23}$$

With the help of [[61], Eq. 6.643.3], we have:

$$\begin{aligned} SOP &= 1 - \int_0^\infty \frac{1}{\lambda_{SD}} W_{-1,\frac{1}{2}}\left(\frac{\gamma_{th}\lambda_{SE}}{\chi\psi y\lambda_{PJ}\lambda_{JE}}\right) \\ &\times \exp\left(\frac{-y}{\lambda_{SD}} + \frac{\gamma_{th}\lambda_{SE}}{2\chi\psi y\lambda_{PJ}\lambda_{JE}}\right) dy \end{aligned} \tag{24}$$

However, the integral in equation (24) is a tough task to find a closed-form expression. Hence, by applying the Gaussian-Chebyshev quadrature in [62], SOP can be approximated . As a result, with $\phi_n = \cos\left(\frac{2n-1}{2N}\pi\right)$, SOP can be given as:

$$\begin{aligned} SOP &\approx 1 - \frac{\pi^2}{4N}\sum_{n=1}^{N}\sqrt{1-\Phi_n^2} \\ &\times \left[\begin{array}{l} \frac{1}{\lambda_{SD}} W_{-1,\frac{1}{2}}\left(\frac{\gamma_{th}\lambda_{SE}}{\chi\psi\lambda_{PJ}\lambda_{JE}\tan\left[(\Phi_n+1)\frac{\pi}{4}\right]}\right) \\ \times \exp\left(\frac{-\tan\left[(\Phi_n+1)\frac{\pi}{4}\right]}{\lambda_{SD}} + \frac{\gamma_{th}\lambda_{SE}}{2\chi\psi\lambda_{PJ}\lambda_{JE}\tan\left[(\Phi_n+1)\frac{\pi}{4}\right]}\right) \\ \times \sec^2\left[(\Phi_n+1)\frac{\pi}{4}\right] \end{array}\right] \end{aligned} \tag{25}$$

4. Numerical results

In this section, we provide numerical results to not only verify the accuracy of the proposed mathematical frameworks but also discuss the insights of the SOP with respect to some key parameters by using the Monte Carlo approach [63, 64, 65]. The simulation parameters are listed in Table 1.

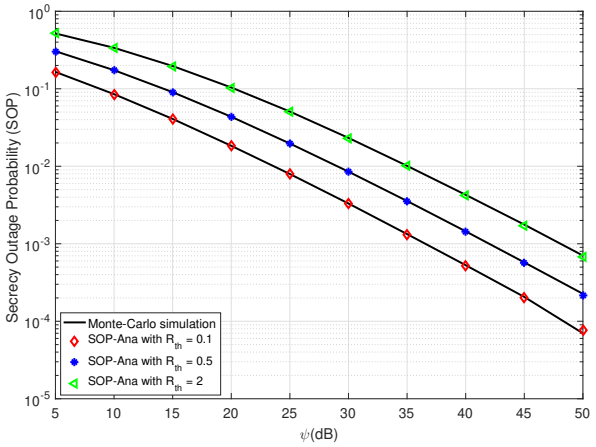

Fig. 3: The SOP versus ψ (dB) with varying R_{th} and $\eta = 0.8$, $\alpha = 0.5$

With varying R_{th}, the fixed values $\eta = 0.8$ and $\alpha = 0.5$, Figure 3 displayed the SOP versus $\psi(dB)$. The curves of SOP match the Monte Carlo simulation findings exactly, as can be seen. By observing in Figure 3, an increase in ψ will result in a drop in SOP. Because the higher ψ is applied, the higher harvested energy at the source will be obtained, and the received SNR will be greatly improved when ψ is large. In addition, when R_{th} is decreased, better SOP performance will be claimed. It can be explained that the higher R_{th} leads to a higher system threshold based on the definition of SOP as in equation (19). At the same time, when versus $\psi(dB)$, Figure 4 shows SOP with varying

Tab. 1: Simulation parameters.

Symbol	Parameter name	Value
R_{th}	Target rate	0.1; 0.5; 2 1(bps/Hz)
η	EH efficiency	0.8
α	Time switching ratio	0.5
d_{PS}	Distance between P and S	1m
d_{PJ}	Distance between P and J	1m
d_{SD}	Distance between S and D	1m
d_{SE}	Distance between S and E	2m
d_{JE}	Distance between J and E	0.5m
ω	Path-loss exponent	2.2
ψ	Transmit power to noise ratio at source	5 to 50 (dB)

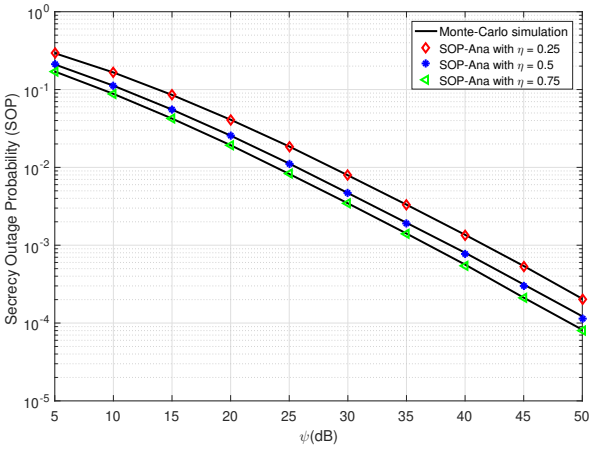

Fig. 4: The SOP versus ψ (dB) with varying η and $\mathrm{R_{th}} = 0.1$, $\alpha = 0.5$

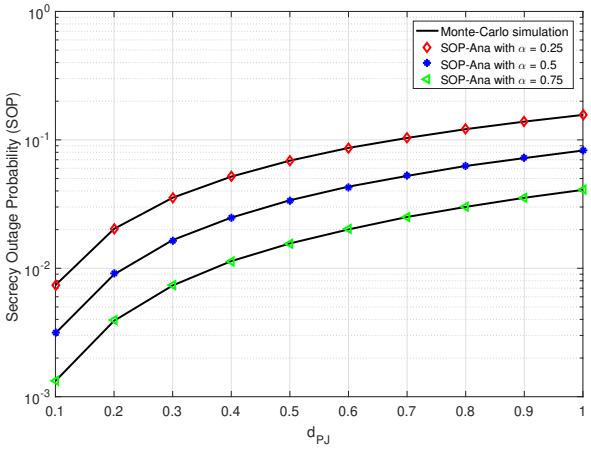

Fig. 5: The SOP versus $\mathrm{d_{PJ}}$ with varying α and $\eta = 0.8$, $\mathrm{R_{th}} = 0.1$, ψ (dB) $= 10$

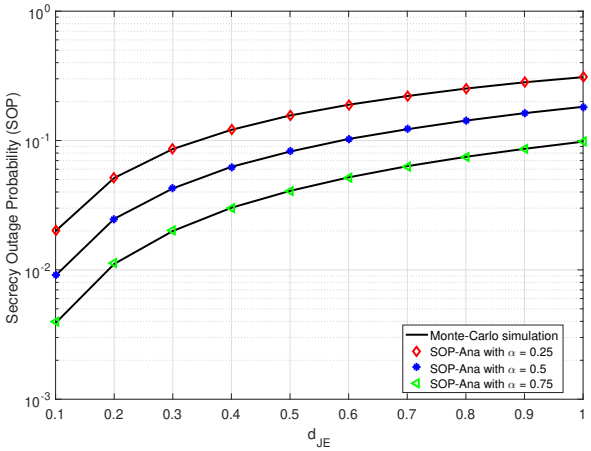

Fig. 6: The SOP versus $\mathrm{d_{JE}}$ with varying α and $\eta = 0.8$, $\mathrm{R_{th}} = 0.1$, ψ (dB) $= 10$

η, the fixed values $R_{th} = 0.1$ and $\alpha = 0.5$. Here, when increasing the energy conversion efficiency, η leads to higher energy obtained at S and J, and this is specifically proven through the formulas (4) and (5). This means that the larger η is, the smaller the SOP is, thus increasing the security of the systems under consideration.

Using fixed parameters $\eta = 0.5$, $\Psi(dB) = 10$, and R_{th} = 0.1 (bps/hz), we sequenced the SOP versus d_{PJ} and d_{JE} with different α in Figures 5 and 6. As a result, the performance of the SOP regarding the distance between the nodes of the power transfer and jamming links. Specifically, in Figure 5, we observe that if the distance from P to J of the power transmission link is smaller, the SOP is significantly improved. It can be explained that when d_{PJ} is smaller, λ_{PJ} in (2) is larger, thereby leading to a larger channel gain, $|h_{\mathrm{PJ}}|^2$. This leads to an increase in the collected energy and the output power at J. Furthermore, increasing the time switching factor α also supports SOP improvement. All this is clearly shown in formulas (5) and (7). In particular, the improved SOP in Figure 6 may explain that when the distance between J and E is smaller, the gain of channel $|h_{\mathrm{JE}}|^2$ is larger. At this point, the eavesdropper E is impacted by the jamming signal at J, which lessens the signal that E steals. Equation (13) provides evidence for this.

Finally, Figures 7 displayed the OP versus α, with varying $\Psi(dB)$, the fixed values $\eta = 0.8$, and $R_{th} = 1$. The curves of SOP match the Monte Carlo simulation findings exactly. The time switching factor η plays an important role because it affects the portion of the time used for energy collection and data transmission. As a result, the higher the value of η, the more energy is collected at S and J. However, the received data at D and the possibility of interference at E will decrease, and vice versa. This is shown in Figure 2. Thus, SOP will result in a concave function; hence, SOP can obtain the best value at the optimal point of η, and after that, the performance deteriorates. By observing in Figure 7,

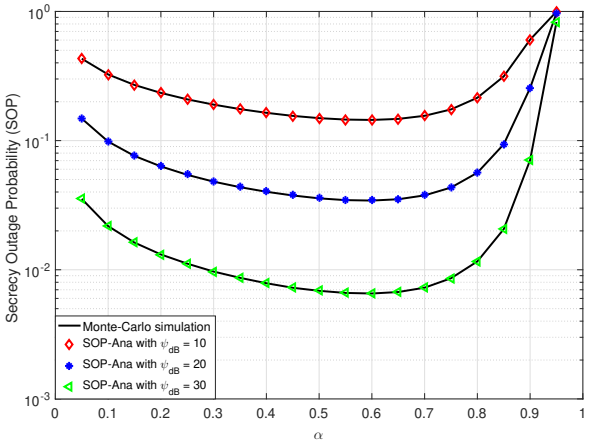

Fig. 7: The SOP versus α with varying ψ (dB) and $\eta = 0.8$, $R_{th} = 1$

SOP with $\Psi(dB) = 10, 20, 30$ can obtain the best values, respectively, at point $\eta = 0.6$. Furthermore, when the value of η is $\eta < 0.6$, the SOP is incremental, and the SOP with all values varying $\Psi(dB)$ will converge to 1, and the system is not able to transmit securely. In addition, the increasing $\Psi(dB)$ also improved SOP, as discussed in Figures 3 and 4. Once again, when considering the SOP, selecting suitable parameters plays an important role in order for the system to work well.

5. Conclusion

In this paper, we discussed enhancing the PLS of an EH-based wireless network composed of a source node, which is operated by the harvested energy from the power beacon and sends secure information to a destination in the presence of an eavesdropper and a cooperative jammer. In particular, we provided an explicit transmit design for minimizing the SOP, subject to a minimum secrecy rate constraint. From the numerical results, we show that friendly device assistance can significantly improve the reliability and security performance of the system. Not only that, increasing the signal that causes interference from thieves improves the SOP. Moreover, we characterized the impacts of specific parameters on the optimal time allocation between energy harvesting and transmitting information. Based on our in-depth theoretical analysis in Figure 7, we concluded that there exists an optimal value of time switching factor $\alpha = 0.6$ for the system to function well. That is, with our system given in this article, $0.6T$ time is needed for collecting energy at the source and $0.4T$ time for transmitting information to the destination so that the system can operate optimally (based on the time division in Figure 2). Furthermore, via the use of Monte Carlo simulation, the precision of the analytical formulations and the effect of system parameters on network performance were verified and examined. In the future, we will apply the findings of this to deploy multiple antennae at the source, destination, and/or multiple jammers so that a diversity of transmitting and receiving techniques can be used to boost the secrecy performance as well. To evaluate system performance more realistically, additional transmission channels, such as the Rician and Nakagami-m channels, will also be considered.

Author Contributions

Analytical computations and numerical simulations were carried out by both Bui Vu Minh and Thu-Ha Thi Pham. N.H.K. Nhan and Thu-Ha Thi Pham wrote the whole paper. Sung-won Kim helps us to revise the manuscript.

References

[1] Rose, Karen and Eldridge, Scott and Chapin, Lyman. The internet of things: An overview. In: *The internet society (ISOC)*. 80 (2015): 1-50.

[2] Li, Shancang and Xu, Li Da and Zhao, Shanshan. The internet of things: a survey. *Information systems frontiers*. 17 (2015): 243-259. DOI: 10.1007/s10796-014-9492-7.

[3] Hu, Lin and Wen, Hong and Wu, Bin and Pan, Fei and Liao, Run-Fa and Song, Huanhuan and Tang, Jie and Wang, Xiumin. Cooperative jamming for physical layer security enhancement in Internet of Things. In: *IEEE Internet of Things Journal*. vol. 5, no. 1, pp. 219-228, Feb. 2018. DOI: 10.1109/JIOT.2017.2778185.

[4] Al Hajj, Maarouf, Shanshan Wang, Lam Thanh Tu, Soumaya Azzi, and Joe Wiart. A Statistical Estimation of 5G Massive MIMO Networks' Exposure Using Stochastic Geometry in mmWave Bands. In: *Applied Sciences*. 2020, 10, 8753. DOI: 10.3390/app10238753.

[5] Zhao, Nan and Lu, Weidang and Sheng, Min and Chen, Yunfei and Tang, Jie and Yu, F Richard and Wong, Kai-Kit. UAV-assisted emergency networks in disasters. In: *IEEE Wireless Communications*. vol. 26, no. 1, pp. 45-51, February 2019. DOI: 10.1109/MWC.2018.1800160z.

[6] Z. Zhang, H. Pang, A. Georgiadis and C. Cecati. Wireless Power Transfer—An Overview. In: *IEEE Transactions on Industrial Electronics*. vol. 66, no. 2, pp. 1044-1058, Feb. 2019. DOI: 10.1109/TIE.2018.2835378.

[7] Chien, Wei, Chien-Ching Chiu, Po-Hsiang Chen, Yu-Ting Cheng, Eng Hock Lim, Yue-Li Liang, and Jia-Rui Wang. Different Object Functions for SWIPT Optimization by SADDE and APSO. In: *Symmetry* . vol. 13, no. 8: 1340. DOI: 10.3390/sym13081340.

[8] Cao, Yang, Ye Zhong, Chunling Peng, Xiaofeng Peng, and Song Pan. Energy Efficiency Optimization for SWIPT-Enabled IoT Network with Energy Cooperation. In: *Sensors*. 2022; 22(13):5035. DOI: 10.3390/s22135035.

[9] Nguyen. T N, Duy. T T, Tran. P T and Voznak, Miroslav. Performance evaluation of user selection protocols in random networks with energy harvesting and hardware impairments. In: *Advances in Electrical and Electronic Engineering*. 14 (4) (2016), pp. 372-377. DOI: 10.15598/aeee.v14i4.1783.

[10] Tin. P T, Phan. V D, Nguyen. T N, Tu. L T, Minh. B V, Voznak. M and Fazio. P. Outage Analysis of the Power Splitting Based Underlay Cooperative Cognitive Radio Networks. In: *Sensors*. vol. 21, no. 22, pp. 7653, 2021. DOI: 10.3390/s21227653.

[11] Nguyen. T N, Tran. D-H, Phan. V-D, Voznak. Miroslav, Chatzinotas. Symeon, Ottersten. Björn and Poor, H. Vincent. Throughput Enhancement in FD- and SWIPT-Enabled IoT Networks Over Nonidentical Rayleigh Fading Channels. In: *IEEE Internet of Things Journal*. vol. 9, no. 12, pp. 10172-10186, 15 June15, 2022. DOI: 10.1109/JIOT.2021.3120766.

[12] Huynh. T P, Son. P N and Voznak, Miroslav. Exact Throughput Analyses of Energy-Harvesting Cooperation Scheme with Best Relay Selections Under I/Q Imbalance. In: *Advances in Electrical and Electronic Engineering*. vol. 15, no. 4, pp. 585-590, 2017. DOI: 10.15598/aeee.v15i4.2302.

[13] Anh-Tu Le, D-H Tran, C-B Le, P.T Tin, T.N. Nguyen, Z. Ding, H. V. Poor, and M. Voznak. Power Beacon and NOMA-Assisted Cooperative IoT Networks with Co-Channel Interference: Performance Analysis and Deep Learning Evaluation. In: *IEEE Transactions on Mobile Computing*. Vol. 23, No. 6, pp. 7270-7283, 2023. DOI: 10.1109/TMC.2023.3333764.

[14] Y. Zheng, S. Bi, Y. J. Zhang, Z. Quan and H. Wang. Intelligent Reflecting Surface Enhanced User Cooperation in Wireless Powered Communication Networks. In: *IEEE Wireless Communications Letters*. vol. 9, no. 6, pp. 901-905, June 2020. DOI: 10.1109/LWC.2020.2974721.

[15] T. -H. Vu and S. Kim. Performance Evaluation of Power Beacon-Assisted Wirelessly Powered NOMA IoT-Based Systems. In: *IEEE Internet of Things Journal*. vol. 8, no. 14, pp. 11655-11665, 15 July15, 2021. DOI: 10.1109/JIOT.2021.3058680.

[16] C. Zhai, H. Chen, Z. Yu and J. Liu. Cognitive Relaying With Wireless Powered Primary User. In: *IEEE Transactions on Communications*. vol. 67, no. 3, pp. 1872-1884, March 2019. DOI: 10.1109/TCOMM.2018.2886002.

[17] T. T. Lam and M. Di Renzo. On the energy efficiency of heterogeneous cellular networks with renewable energy sources—A stochastic geometry framework.. In: *IEEE Transactions on Wireless Communications*. vol. 19, no. 10, pp. 6752-6770, Oct. 2020. DOI: 10.1109/TWC.2020.3005618.

[18] P. Ramezani and A. Jamalipour. Two-Way Dual-Hop WPCN with a Practical Energy Harvesting Model. In: *IEEE Transactions on Vehicular Technology*. vol. 69, no. 7, pp. 8013-8017, July 2020. DOI: 10.1109/TVT.2020.2993571.

[19] Phu. T T, Tran. T D and Voznak. Miroslav . Security-Reliability Analysis of Noma-Based Multi-Hop Relay Networks in Presence of an Active Eavesdropper with Imperfect Eavesdropping CSI . In: *Advances in Electrical and Electronic Engineering*. vol. 15, no. 4, pp. 591-597, 2017.. DOI: 10.15598/aeee.v15i4.2386.

[20] A. Mukherjee, S. A. A. Fakoorian, J. Huang and A. L. Swindlehurst. Principles of Physical Layer Security in Multiuser Wireless Networks: A Survey. In: *IEEE Communications Surveys & Tutorials*. vol. 16, no. 3, pp. 1550-1573, Third Quarter 2014. DOI: 10.1109/SURV.2014.012314.00178.

[21] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan and M. Di Renzo. Safeguarding 5G wireless communication networks using physical layer security. In: *IEEE Communications Magazine*. vol. 53, no. 4, pp. 20-27, April 2015. DOI: 10.1109/MCOM.2015.7081071.

[22] X. Jiang, P. Li, B. Li, Y. Zou and R. Wang. Intelligent jamming strategies for secure spectrum sharing systems. In: *IEEE Transactions on Communications*. vol. 70, no. 2, pp. 1153-1167, Feb. 2022. DOI: 10.1109/TCOMM.2021.3140082.

[23] J. M. Hamamreh, H. M. Furqan and H. Arslan. Classifications and Applications of Physical Layer Security Techniques for Confidentiality: A Comprehensive Survey. In: *IEEE Communications Surveys & Tutorials*. vol. 21, no. 2, pp. 1773-1828, Secondquarter 2019. DOI: 10.1109/COMST.2018.2878035.

[24] W. Wang, K. C. Teh and K. H. Li. Generalized Relay Selection for Improved Security in Cooperative DF Relay Networks. In: *IEEE Wireless Communications Letters*. vol. 5, no. 1, pp. 28-31, Feb. 2016. DOI: 10.1109/LWC.2015.2488660.

[25] Pandey, Anshul and Yadav, Suneel. Physical-layer security for cellular multiuser two-way relaying networks with single and multiple decode-and-forward relays. In: *Transactions on Emerging Telecommunications Technologies*. vol. 30, no. 12, pp. e3639, 2019. DOI: 10.1002/ett.3639.

[26] M. K. Shukla, A. Pandey, S. Yadav and N. Purohit. Secrecy outage analysis of full duplex cellular multiuser two-way AF relay networks. In: *2019 International Conference on Wireless Communications Signal Processing and Networking (WiSPNET)*. Chennai, India, 2019, pp. 458-463. DOI: 10.1109/WiSPNET45539.2019.9032838.

[27] Y. Liu, L. Wang, T. T. Duy, M. Elkashlan and T. Q. Duong. Relay Selection for Security Enhancement in Cognitive Relay Networks. In: *IEEE Wireless Communications Letters*. vol. 4, no. 1, pp. 46-49, Feb. 2015. DOI: 10.1109/LWC.2014.2365808.

[28] Li. Xingwang, Zhao. Mengle, Gao. Xiang-Chuan, Li. Lihua, Do. Dinh-Thuan, Rabie. Khaled M. and Kharel. Rupak. Physical Layer Security of Cooperative NOMA for IoT Networks Under I/Q Imbalance. In: *Conference Title*. vol. 8, pp. 51189-51199, 2020. DOI: 10.1109/ACCESS.2020.2980171.

[29] D. Kapetanovic, G. Zheng and F. Rusek. Physical layer security for massive MIMO: An overview on passive eavesdropping and active attacks. In: *IEEE Communications Magazine*. vol. 53, no. 6, pp. 21-27, June 2015. DOI: 10.1109/MCOM.2015.7120012.

[30] Le. S-P, Nguyen. H-N, Nguyen. N-T, Van. C H, Le. A-T and Voznak. Miroslav. Physical layer security analysis of IRS-based downlink and uplink NOMA networks. In: *EURASIP Journal on Wireless Communications and Networking*. vol. 2023, no. 1, pp. 105, 2023.. DOI: 10.1186/s13638-023-02309-5z.

[31] Nguyen, Sang Quang and Kong, Hyung Yun. Improving secrecy outage and throughput performance in two-way energy-constraint relaying networks under physical layer security. In: *Wireless Personal Communications*. Vol. 96, pp. 6425–6457, 2017. DOI: 10.1007/s11277-017-4485-8.

[32] Nguyen, Sang Quang and Kong, Hyung Yun. Combining binary jamming and network coding to improve outage performance in two-way relaying networks under physical layer security. In: *Wireless Personal Communications*. Vol. 85, pp. 2431–2446, 2015. DOI: 10.1007/s11277-015-2913-1.

[33] Nguyen, Sang Quang and Kong, Hyung Yun. Binary jamming message solutions for source-wiretapping under physical-layer security: Analysis and design. In: *Wireless Personal Communications*. Vol. 84, pp. 2493–2512, 2015. DOI: 10.1007/s11277-015-2716-4.

[34] L. Sun and Q. Du. Physical layer security with its applications in 5G networks: A review. In: *China Communications*. vol. 14, no. 12, pp. 1-14, December 2017. DOI: https://doi.org/10.1109/CC.2017.8246328.

[35] F. Jameel, Z. Hamid, F. Jabeen, S. Zeadally and M. A. Javed. A survey of Device-to-Device communications: Research issues and challenges. In: *IEEE Communications Surveys & Tutorials*. vol. 20, no. 3, pp. 2133-2168, thirdquarter 2018. DOI: 10.1109/COMST.2018.2828120.

[36] A. Asadi, Q. Wang and V. Mancuso. A survey on Device-to-Device communication in cellular networks. In: *IEEE Communications Surveys & Tutorials*. vol. 16, no. 4, pp. 1801-1819, Fourthquarter 2014. DOI: 10.1109/COMST.2014.2319555.

[37] J. Liu, N. Kato, J. Ma and N. Kadowaki. Device-to-Device Communication in LTE-Advanced Networks: A Survey. In: *IEEE Communications Surveys & Tutorials*. vol. 17, no. 4, pp. 1923-1940, Fourthquarter 2015. DOI: 10.1109/COMST.2014.2375934.

[38] J. Wang, Y. Huang, S. Jin, R. Schober, X. You and C. Zhao. Resource management for Device-to-Device communication: A physical layer security perspective. In: *IEEE Journal on Selected Areas in Communications*. vol. 36, no. 4, pp. 946-960, April 2018. DOI: 10.1109/JSAC.2018.2825484.

[39] W. Wang, K. C. Teh and K. H. Li. Enhanced physical layer security in D2D spectrum sharing networks. In: *IEEE Wireless Communications Letters*. vol. 6, no. 1, pp. 106-109, Feb. 2017. DOI: 10.1109/LWC.2016.2634559.

[40] L. Wang, J. Liu, M. Chen, G. Gui and H. Sari. Optimization-based access assignment scheme for physical-layer security in D2D communications underlaying a cellular network. In: *IEEE Transactions on Vehicular Technology*. vol. 67, no. 7, pp. 5766-5777, July 2018. DOI: 10.1109/TVT.2017.2789022.

[41] H. -M. Wang, B. -Q. Zhao and T. -X. Zheng. Adaptive Full-Duplex Jamming Receiver

for Secure D2D Links in Random Networks. In: *IEEE Transactions on Communications*. vol. 67, no. 2, pp. 1254-1267, Feb. 2019. DOI: 10.1109/TCOMM.2018.2880216.

[42] Babayo. Aliyu Aliyu, Anisi. Mohammad Hossein and Ali. Ihsan. A Review on energy management schemes in energy harvesting wireless sensor networks. In: *Renewable and Sustainable Energy Reviews*. vol. 76, pp. 1176-1184, 2017. DOI: 10.1016/j.rser.2017.03.124.

[43] Ahmed. Imran, Butt. M Majid, Psomas. Constantinos, Mohamed. Amr, Krikidis. Ioannis and Guizani. Mohsen. Survey on energy harvesting wireless communications: Challenges and opportunities for radio resource allocation. In: *Computer Networks*. vol. 88, pp. 234-248, 2015. DOI: 10.1016/j.comnet.2015.06.009.

[44] Nguyen, Long D. Resource Allocation for Energy Efficiency in 5G Wireless Networks. In: *EAI Endorsed Transactions on Industrial Networks and Intelligent Systems*. Vol. 5 No. 14 (2018). DOI: 10.4108/eai.27-6-2018.154832.

[45] Hoc. L T T, Nguyen. H-S, Ma. Q-P, Van Huynh. V, Nguyen. T-L, Phuoc. H T and Voznak. Miroslav. Outage and Bit Error Probability Analysis in Energy Harvesting Wireless Cooperative Networks. In: *Elektronika ir Elektrotechnika*. Vol. 25 No. 5, pp. 69-74, 2019. DOI: 10.5755/j01.eie.25.5.24359.

[46] L. Irio, R. Oliveira, D. B. da Costa and M. -S. Alouini. Impact of Wireless-Powered Communications in Coexisting Mobile Networks. In: *IEEE Wireless Communications Letters*. vol. 9, no. 7, pp. 1060-1064, July 2020. DOI: 10.1109/LWC.2020.2980524.

[47] X. Li, J. Li and L. Li. Performance Analysis of Impaired SWIPT NOMA Relaying Networks Over Imperfect Weibull Channels. In: *IEEE Systems Journal*. vol. 14, no. 1, pp. 669-672, March 2020. DOI: 10.1109/JSYST.2019.2919654.

[48] S. K. Nobar, J. M. Niya and B. M. Tazehkand. Performance Analysis of Cognitive Wireless Powered Communication Networks Under Unsaturated Traffic Condition. In: *IEEE Transactions on Green Communications and Networking*. vol. 4, no. 3, pp. 819-831, Sept. 2020. DOI: 10.1109/TGCN.2020.2978264.

[49] Nguyen. T N., Phuong T. Tran, and Miroslav Vozňák. Power splitting-based ˘ energy-harvesting protocol for wireless-powered communication networks with a bidirectional relay . In: *International Journal of Communication Systems* . vol. 31, no. 13, pp. e3721. 2018. DOI: 10.1002/dac.3721.

[50] Li, Xingwang, Huang. Mengyan, Li. Jingjing, Yu. Qingping, Rabie. Khaled and Cavalcante. Charles C. Secure analysis of multi-antenna cooperative networks with residual transceiver HIs and CEEs. In: *Conference Title*. Vol 13, no. 17,pp. 2649-2659, 2019. DOI: 10.1049/iet-com.2019.0011.

[51] P.T. Tin, Nguyen T.L., T.N. Nguyen, M. Tran, and T.T. Duy. Throughput Enhancement For Multi-Hop Decode-and-Forward Protocol Using Interference Cancellation With Hardware Imperfection. In: *Alexandria Engineering Journal*. vol.61, no.8, pp. 5837-5849, 2021. DOI: 10.1016/j.aej.2021.11.008.

[52] D. H. Ha, T. N. Nguyen, M. H. Q. Tran, X. Li, P. T. Tran and M. Voznak. Security and Reliability Analysis of a Two-Way Half-Duplex Wireless Relaying Network Using Partial Relay Selection and Hybrid TPSR Energy Harvesting at Relay Nodes. In: *IEEE Access*. vol. 8, pp. 187165-187181, 2020. DOI: 10.1109/ACCESS.2020.3030794.

[53] Y. Zhang, J. Ye, G. Pan and M. -S. Alouini. Secrecy Outage Analysis for Satellite-Terrestrial Downlink Transmissions. In: *IEEE Wireless Communications Letters*. vol. 9, no. 10, pp. 1643-1647, Oct. 2020. DOI: 10.1109/LWC.2020.2999555.

[54] D. Wang, P. Ren, Q. Du, L. Sun and Y. Wang. Security provisioning for MISO vehicular relay networks via cooperative jamming and signal superposition. In: *IEEE Transactions on Vehicular Technology*. vol. 66, no. 12, pp. 10732-10747, Dec. 2017. DOI: 10.1109/TVT.2017.2703780.

[55] Tran Tin P, The Hung D, Nguyen TN, Duy TT and Voznak M. Secrecy Performance Enhancement for Underlay Cognitive Radio Networks Employing Cooperative Multi-Hop Transmission with and without Presence of Hardware Impairments. In: *Entropy*. vol. 21, no. 2, pp. 217, 2019. DOI: 10.3390/e21020217.

[56] L. T. Tu and A. Bradai. On the Performance of Physical Layer Security of RIS-aided Communications. In: *IEEE Conference on Antenna Measurements & Applications (CAMA)*. Antibes Juan-les-Pins, France, 2021, pp. 570-574. DOI: 10.1109/CAMA49227.2021.9703543..

[57] Nguyen. Tan N, Tu. Lam-Thanh, Tran. Dinh-Hieu, Phan. Van-Duc, Voznak. Miroslav, Chatzinotas. Symeon and Ding. Zhiguo. Outage Performance of Satellite Terrestrial Full-Duplex Relaying Networks With co-Channel Interference. In: *IEEE Wireless Communications Letters*.

vol. 11, no. 7, pp. 1478-1482, July 2022. DOI: 10.1109/LWC.2022.3175734.

[58] Ghosh. Moloy Kumar, Kundu. Milton Kumar, Ibrahim. Md, Badrudduza. ASM, Anower. Md Shamim, Ansari. Imran Shafique, Shaikhi. Ali A and Mohandes. Mohammed A. Secrecy Outage Analysis of Energy Harvesting Relay-based Mixed UOWC-RF Network with Multiple Eavesdroppers. In: *arXiv preprint arXiv:2302.10257*. 2023. DOI: 10.48550/arXiv.2302.10257.

[59] Nguyen. Tan N, Tran. Dinh-Hieu, Chien. Trinh Van, Phan. Van-Duc, Voznak. Miroslav, Tin. Phu Tran, Chatzinotas. Symeon, Ng. Derrick Wing Kwan and Poor. H. Vincent. Security–Reliability Tradeoff Analysis for SWIPT- and AF-Based IoT Networks With Friendly Jammers. In: *IEEE Internet of Things Journal*. vol. 9, no. 21, pp. 21662-21675, 1 Nov.1, 2022. DOI: 10.1109/JIOT.2022.3182755.

[60] V T. Pham, N S. Pham, T D. Tran, Nguyen. S Q, Ngo. V Q B, V Q. Do and Koo. Insoo. Optimizing a Secure Two-Way Network with Non-Linear SWIPT, Channel Uncertainty, and a Hidden Eavesdropper. In: *Electronics*. vol. 8, no. 9, pp. 1222, 2020. DOI: 10.3390/electronics9081222.

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

[62] Sang Q.N., Tu A.L., Bao C.L., Tin P.T., and Yong-Hwa K. Exploiting User Clustering and Fixed Power Allocation for Multi-Antenna UAV-Assisted IoT Systems. *Sensors*. 23.12 (2023): 5537. DOI: 10.3390/s23125537.

[63] Nguyen. Tan N, Tran. M, Nguyen. T-L, Ha. D-H and Voznak. M. Performance analysis of a user selection protocol in cooperative networks with power splitting protocol-based energy harvesting over Nakagami-m/Rayleigh channels. In: *Electronics*. vol. 8, no. 4, pp. 448, 2019. DOI: 10.3390/electronics8040448.

[64] Nguyen. Tan N, Tran. M, Nguyen. T-L, Ha. D-H and Voznak. M. Multisource Power Splitting Energy Harvesting Relaying Network in Half-Duplex System over Block Rayleigh Fading Channel: System Performance Analysis. In: *Electronics*. vol. 8, no. 1, pp. 67, 2021. DOI: 10.3390/electronics8010067.

DOI: 10.1016/j.comnet.2020.107176.

[65] Nhat-Tien Nguyen, Hong-Nhu Nguyen, Ngoc-Long Nguyen, Anh-Tu Le, Tan N. Nguyen, and Miroslav Voznak. Performance Analysis of NOMA-based Hybrid Satellite-Terrestrial Relay System Using mmWave Technology. In: *IEEE Access*. Vol. 11, pp. 10696-10707, Jan. 2023. DOI: 10.1109/ACCESS.2023.3238335.