IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 12 June 2023, accepted 4 August 2023, date of publication 7 August 2023, date of current version 17 August 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3303369

RESEARCH ARTICLE

SWIPT-Enabled Cooperative Wireless IoT Networks With Friendly Jammer and Eavesdropper: Outage and Intercept Probability Analysis

DINH TUNG VO[1], TRINH VAN CHIEN[2], (Member, IEEE), TAN N. NGUYEN[3], (Member, IEEE), DINH-HIEU TRAN[4], (Student Member, IEEE), MIROSLAV VOZNAK[5], (Senior Member, IEEE), BYUNG SEO KIM[6], (Senior Member, IEEE), AND LAM THANH TU[3]

[1]HUTECH Institute of Engineering, HUTECH University, Ho Chi Minh City 70000, Vietnam
[2]School of Information and Communication Technology (SoICT), Hanoi University of Science and Technology (HUST), Hanoi 100000, Vietnam
[3]Communication and Signal Processing Research Group, Faculty of Electrical and Electronics Engineering, Ton Duc Thang University, Ho Chi Minh City 70000, Vietnam
[4]Nokia Bell Labs, 91620 Nozay, France
[5]Faculty of Electrical Engineering and Computer Science, VSB–Technical University of Ostrava, Poruba, 70800 Ostrava, Czech Republic
[6]Department of Software and Communications Engineering, Hongik University, Sejong 30016, South Korea

Corresponding author: Tan N. Nguyen (nguyennhattan@tdtu.edu.vn)

The research was co-funded by the European Union within the REFRESH project - Research Excellence For Region Sustainability and High-tech Industries ID No. CZ.10.03.01/00/22_003/0000048 of the European Just Transition Fund and by the Ministry of Education, Youth and Sports of the Czech Republic (MEYS CZ) through the e-INFRA CZ project (ID:90254) and also by the MEYS CZ within the project SGS ID No. SP 7/2023 conducted by VSB-Technical University of Ostrava. This research is funded by Hanoi University of Science and Technology (HUST) under project number T2022-TT-001 for Trinh Van Chien.

ABSTRACT Physical layer security (PLS) and simultaneous wireless information and power transfer (SWIPT) in cooperative relaying have gained great interest as technologies for security and energy enhancement in Internet-of-Things (IoT) networks. In this work, we investigate PLS for a SWIPT- and AF-enabled cooperative wireless IoT system, consisting of one source, multiple energy harvesting (EH) relays, and one destination, in the presence of an eavesdropper that tries to overhear the confidential information. Furthermore, an EH-friendly jammer is deployed to transmit jamming signals aimed at the eavesdropper to improve the security system. In this context, a low-complexity, sub-optimal, but efficient relay selection method is proposed. More specifically, the relay is selected to convey information such that it has the best channel to the source. Based on the proposed system model, the performance analysis of the intercept probability (IP), asymptotic IP, and non-zero secrecy probability (NZSP) is analyzed by considering the time switching (TS)-based relaying strategy. Particularly, the exact closed-form expression of IP is achieved by applying modified Bessel function expansion. Monte-Carlo simulations are employed to corroborate the correctness and efficiency of our mathematical analysis. The time splitting factor α makes variations on the IP of about $3\times$ as $\alpha \in [0.1, 0.8]$. However, a dramatic reduction of the IP up to $317\times$ is observed as α increases from 0.8 to 0.9.

INDEX TERMS Cooperative relay, eavesdropper, IoT, friendly jammer, physical layer security, SWIPT.

I. INTRODUCTION

The structure and layout of a network that links and facilitates communication among a wide variety of IoT (Internet of Things) devices utilizing radio technologies is referred to as wireless IoT network architecture. The IoT system often consists of a number of layers and equipment, each of which has a defined function.In fifth-generation (5G) and beyond networks, billions of internet of things (IoT) users are connected to the networks that provided various utilities

The associate editor coordinating the review of this manuscript and approving it for publication was Xujie Li.

to human life such as health care, smart cities, smart home, industrial automation, and agriculture [1], [2], [3]. Following Ericsson's report, the number of IoT devices is approximated to be 22 billion by 2025 [4]. Nevertheless, the massive number of IoT users (IoTU) impose challenges and become a burden for future wireless systems such as due to the limited resources, e.g., restricted in available spectrum and energy capacity. Especially, changing or recharging IoTU's batteries is generally expensive and even impossible in practice, for example, on the battlefield or inside toxic or hazardous environments. Owing to recent developments in energy harvesting (EH), which brings potential solutions to overcome the aforementioned issues.

A. RELATED WORKS

Energy can be harvested from surrounding resources such as wind [5], solar [6], vibration [7], and radio frequency (RF) [8]. Among them, RF EH has become an appealing solution due to its controllability, predictability, and it can brings both information and energy. Consequently, simultaneous wireless information and power transfer (SWIPT) has recently become one of the promising techniques for self-sustainable wireless systems [9], [10], [11], [12]. Beyond the benefits of EH for IoT networks, relay users in cooperative relaying systems help the IoTU convey information to the sink/data collector since the IoTU has inherent limitations as far-distance distribution and low power. Generally, cooperative relaying networks can be mainly divide into two type: amplify-and-forward (AF)-based relaying [13], [14] and decode-and-forward (DF)-based relaying [15], [16]. Specifically, Cao et al. [13] proposed a novel system model integrating power beacon (PB) EH, full-duplex (FD), and non-orthogonal multiple access (NOMA), whereas the source and relay can harvest energy from a PB in an AF-based system. By taking into account the hardware imperfections (HWIs) and channel estimation errors (CEEs), Shahiri et al. [14] investigated the average block error rate (BLER) for AF relaying in ultra-reliable low-latency communications (URLLC) networks. Zheng et al. [15] proposed a DF short-packet relaying system to investigate the freshness of information in IoT networks. Concretely, the authors took the age of information (AoI) as a metric for studying with the assist of a relay in FD and HD modes. Shim et al. [16] considered one-way DF-based relaying applying time switching (TS) method with rechargeable and non-rechargeable batteries. Furthermore, AF- and DF-based relay in cognitive radio networks (CRNs) was studied in [17] and [18]. Different to [13], [14], [15], [16], [17], and [18] that only considered one-way communications, recent works [19], [20], [21], [22], [23] have studied two-way relaying IoT networks. In [24] and [25], the multi-input multi-output (MIMO) system has been considered in cooperative relaying for IoT networks. In particular, the authors in [26], [27], and [28] considered an unmanned aerial vehicle (UAV) acted as a relay for aerial-terrestrial communication systems.

Besides many advantages for providing utilities in human lives, IoT communications are not without limitations. Particularly, the security requirements in IoT networks have been received significant attention from both academia and industrial perspectives. Adversarial attacks happen in real life and are not a threat. Specifically, there are more than 60000 vulnerabilities found by two researchers from Russia that can take full control of compromised systems [29]. Due to the simple in implementation compared to upper layer security methods, physical layer security (PLS) becomes a promising solution for IoT networks [30], [31], [32], [33], [34], [35], [36]. Specifically, the authors in [30] and [31] studied the PLS in Wireless powered communication networks (WPCN). Yan et al. [30] considered the secrecy outage analysis of a MIMO EH system by proposing two schemes, termed the optimal and sub-optimal antenna selection. Chu et al. [31] applied Stackelberg game for designing a secure wireless-powered multi-antenna system. In contrast to [30] and [31] that only considered single or dual-hop cooperative relaying systems, some state-of-art works [33], [34], [35], [36] have focused on multi-hop cooperative networks. Despite many fruitful results obtained from the literature to improve the PLS in IoT networks [30], [31], [32], [33], [34], [35], [36], none of these works considered jammer in their system model. Recent studies has shown that friendly jammers help enhance the system security [37], [38], [39], [40]. Cao et al. [37] proposed a novel system model in which an idle relay was selected to act as a friendly jammer to transmit artificial noise to the eavesdropper in a NOMA system. Moreover, the authors proposed two schemes, namely, random jammer selection and optimal jammer selection based on the availability of the eavesdropper's channel state information (CSI). In [38] and [39], the authors adopted jammers in secure UAV communications. Reference [38] was one of the first works that jointly optimized friendly jamming and bandwidth allocation in UAV communications. Kim et al. [39] investigated the influences of multiple UAVs jammer which are randomly distributed in the considered area and derived the secrecy transmission probability. In [40], a learning-assisted Stackelberg was applied for a friendly jammer system. Specifically, Qi et al. [40] proposed a noel system model including two adversary parties, namely the blue team and the red team. Then, the friendly jammer, blue team, and red team were modeled as Stackelberg game to find their utility maximization.

B. CONTRIBUTIONS

Despite many achievements in the literature, the study of physical layer security in SWIPT- and AF-enabled cooperative wireless IoT networks is still needed. Particularly, exact closed-from expression for the intercept probability (IP) poses challenges due to its complexity. For instance, the exact closed-form expression for the IP in [23] can not be obtained. Motivated by the above discussions, we propose a SWIPT relaying network consisting of one source, multiple relays,

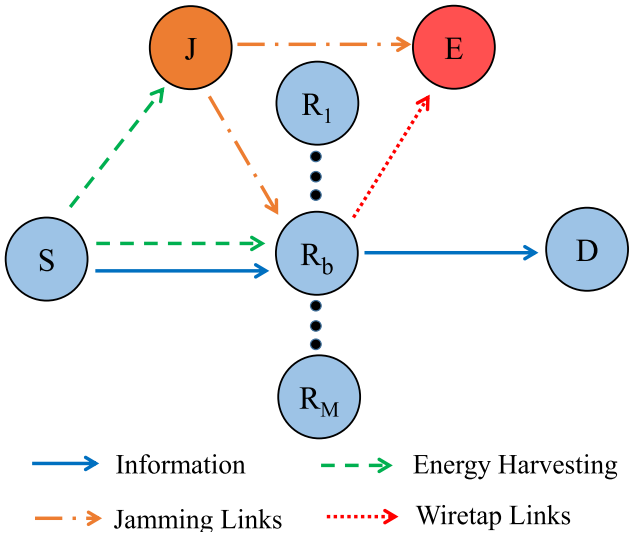


FIGURE 1. The considered system model.

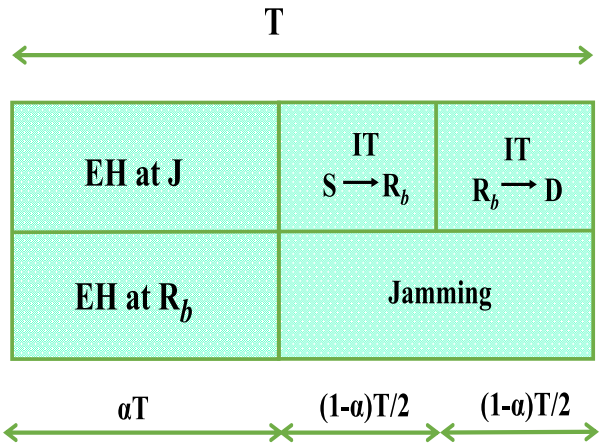


FIGURE 2. Schematic illustration of EH and information transmission processes at the friendly jammer and the selected relay.

one destination, in the presence of one eavesdropper and one friendly jammer. The contributions of this work can be summarized as follows:

- Due to the high cost of seeking the optimal relay selection, we propose a simple yet efficient method, termed the partial relay selection (PRS), to select the best relay with the highest channel gain to the source to transfer information to the destination. In the proposed system model, we apply the harvest-then-transmit scheme. Specifically, the selected relay and friendly jammer can harvest energy from the source's RF signal and then use it for transferring and jamming signals.
- To the best of our knowledge, this is the first work that obtains exact closed-form expression in terms of IP for the proposed system model adopting modified Bessel function expansion. Furthers, the asymptotic IP and the non-zero secrecy probability (NZSP) expressions are also derived. This is highly challenging because the analysis involves many random variables.
- Finally, the numerical results are performed to corroborate the exactness of the mathematical analysis. The simulation results show the influences of different parameters on the system performance and how to select these parameters appropriately to eliminate the eavesdropper's impacts.

II. SYSTEM MODEL

As shown in Fig. 1, we propose a SWIPT-enabled HD relaying network in the presence of a friendly jammer (J) and an eavesdropper (E). Transmitter (S) can communicate with a receiver (D) through multi-relay nodes (R) since the direct link is missing due to severe fading or obstacles [41]. The friendly jammer can transmit the jamming signals to eliminate overheard information from the eavesdropper. Moreover, relay users can harvest energy from S signals using the time switching (TW) method as illustrated in Fig. 1. Specifically, the total operation time T can be divided into three time slots. In the first time slot αT, where α is the TS factor and satisfying $0 \leq \alpha \leq 1$, transmitter S supplies power to the jammer and relay. In the last two time slots, transmitter S transmits information to the selected relay during the $(1-\alpha)$T/2 time period, and the selected relay will convey information to the receiver in the third time period, i.e., $(1-\alpha)$T/2.

A. ENERGY HARVESTING PHASE

In the first time slot, the received signal at relay b−th and the jammer can be respectively given by

$$y_{R_b} = h_{SR_b} x_s + n_{R_b}, \tag{1}$$

$$y_J = h_{SJ} x_s + n_J, \tag{2}$$

where x_s is the information transmitted from S; h_{SR_b} and h_{SJ} are channel gains from $S \to R_b$ and $S \to j$, respectively; n_{R_b} and n_J denote additive White Gaussian noise (AWGN) at R_b and S, respectively.

Without loss of generality, we assume that relay R_b and jammer J use all harvested energy for data transmission and jamming. Consequently, the transmit power of R_b and J are respectively calculated as

$$P_{R_b} = \frac{E_{R_b}}{(1-\alpha)T/2} = \frac{\alpha T P_s |h_{SR_b}|^2}{(1-\alpha)T/2} = \kappa P_s |h_{SR_b}|^2, \tag{3}$$

$$P_J = \frac{E_J}{(1-\alpha)T/2} = \frac{\alpha T P_s |h_{SJ}|^2}{(1-\alpha)T/2} = \kappa P_s |h_{SJ}|^2, \tag{4}$$

where $0 \leq \eta \leq 1$ denotes the energy harvesting conversion coefficient, $0 \leq \alpha \leq 1$ is the TS factor, and $\kappa \triangleq \frac{2\alpha\eta}{1-\alpha}$.

B. INFORMATION AND JAMMING TRANSMISSION PHASE

In the second time slot, the received signal at relay b-th can be expressed as

$$y_{R_b} = h_{SR_b} x_s + h_{JR_b} x_J + n_{R_b}, \tag{5}$$

where h_{JR_b} is the channel gain between $J \rightarrow R_b$ and $E\{|x_J|^2\} = P_J$.

Notably, we assume that the jamming signal x_J is known in advance at relay R_b. Therefore, the jamming signal can be perfectly canceled at R_b. Consequently, y_{R_b} can be rewritten as

$$y_{R_b} = h_{SR_b}x_s + n_{R_b}, \tag{6}$$

In the system model, we consider amplify-and-forward (AF) protocol. Therefore, the amplified factor χ at R_b can be given as

$$\chi = \frac{x_{R_b}}{y_{R_b}} = \sqrt{\frac{P_{R_b}}{\left|h_{SR_b}\right|^2 P_s + N_0}}. \tag{7}$$

In the third time slot, the signals received at the destination can be expressed as

$$y_D = h_{R_bD}x_{R_b} + n_D, \tag{8}$$

where h_{R_bD} is the channel gain between $R_b \rightarrow D$ and n_D is the AWGN at destination D with variance N_0.

By substituting (6) and (7) into (8), we have

$$\begin{aligned} y_D &= h_{R_bD}\chi y_{R_b} + n_D = h_{R_bD}\chi\left(h_{SR_b}x_s + n_{R_b}\right) + n_D \\ &= \underbrace{h_{R_bD}\chi h_{SR_b}x_s}_{\text{signal}} + \underbrace{h_{R_bD}\chi n_{R_b} + n_D}_{\text{noise}}. \end{aligned} \tag{9}$$

Then, the end-to-end signal-to-noise (SNR) ratio at the destination can be given by

$$\gamma_D = \frac{E\left\{|\text{signal}|^2\right\}}{E\{|\text{noise}|^2\}} = \frac{\left|h_{SR_b}\right|^2\left|h_{R_bD}\right|^2\chi^2 P_s}{\left|h_{R_bD}\right|^2\chi^2 N_0 + N_0}. \tag{10}$$

Based on $N_0 << P_{R_b}$ and by substituting (3) and (4) into (10), it yields

$$\gamma_D = \frac{\kappa\left|h_{SR_b}\right|^2\left|h_{R_bD}\right|^2\Psi}{\kappa\left|h_{R_bD}\right|^2 + 1} = \frac{\kappa\varphi_1\varphi_2\Psi}{\kappa\varphi_2 + 1}, \tag{11}$$

where $\varphi_1 = \left|h_{SR_b}\right|^2, \varphi_2 = \left|h_{R_bD}\right|^2$ and $\Psi = \frac{P_s}{N_0}$. Next, we analyze the secrecy of the proposed system since an eavesdropper can overhear confidential information from relay R_b in the presence of jamming signals from a friendly jammer. Specifically, the signals received at the eavesdropper can be given as

$$y_E = h_{R_bE}\chi\left(h_{SR_b}x_s + n_{R_b}\right) + h_{JE}x_J + n_E, \tag{12}$$

where h_{JE} is the channel gain between $J \rightarrow E$ and n_E is the AWGN at the eavesdropper with variance N_0.

From (12), the SNR at the eavesdropper can be given by

$$\begin{aligned} \gamma_E &= \frac{\left|h_{SR_b}\right|^2\left|h_{R_bE}\right|^2\chi^2 P_s}{\left|h_{R_bE}\right|^2\chi^2 N_0 + P_J\left|h_{JE}\right|^2 + N_0} \\ &\approx \frac{\left|h_{SR_b}\right|^2\left|h_{R_bE}\right|^2 P_s}{\left|h_{R_bE}\right|^2 N_0 + \frac{P_J\left|h_{JE}\right|^2}{\kappa} + \frac{N_0}{\kappa}}. \end{aligned} \tag{13}$$

By substituting (3) and (4) into (13), we have

$$\begin{aligned} \gamma_E &= \frac{\kappa\left|h_{SR_b}\right|^2\left|h_{R_bE}\right|^2\Psi}{\kappa\left|h_{R_bE}\right|^2 + \kappa\Psi\left|h_{SJ}\right|^2\left|h_{JE}\right|^2 + 1} \\ &= \frac{\kappa\varphi_1\varphi_3\Psi}{\kappa\varphi_3 + \kappa\Psi\varphi_4\varphi_5 + 1}, \end{aligned} \tag{14}$$

where $\varphi_3 = \left|h_{R_bE}\right|^2, \varphi_4 = \left|h_{SJ}\right|^2$, and $\varphi_5 = \left|h_{JE}\right|^2$.

Remark 1: We assume that all channels are Rayleigh fading appearing in rich scattering environments where scatterers are located around the receivers' side. Consequently, the channel gains follow exponential random variable (RV). Cumulative distribution function (CDF) and probability density function (PDF) can be respectively given by

$$F_{\varphi_a}(x) = 1 - \exp(-\lambda_a x), \tag{15}$$

$$f_{\varphi_a}(x) = \lambda_a \exp(-\lambda_a x), \tag{16}$$

where $a \in (1, 2, \ldots, 5)$, $\lambda_a = (d_a)^\beta$, where β is the path loss exponent and d_a denotes the distance between users.

Remark 2: Due to the high computational complexity of finding the global optimum to the relay selection problem, in this paper, we consider partial relay selection (PRS) method, whereas the best relay can be selected as follows:

$$R_b : \varphi_1 = \left|h_{SR_b}\right|^2 = \max_{m=1,2,\ldots,M}\left(\left|h_{SR_m}\right|^2\right). \tag{17}$$

Equation (17) means that relay R_b providing the highest channel to the source is selected as the best relay for the cooperation between $S \rightarrow R_b$. In practice, the CSIs between S and relays can be estimated through local control message, and thus the best candidate can be easy determined as in (16). Moreover, we assume in this paper that $d_{SR_j} > d_{R_jD}$, thus the relay selection should be performed at the first hop to enhance the quality of the channel between $S \rightarrow R_b$.

From (17), the CDF of φ_1 can be given by [42]

$$\begin{aligned} F_{\varphi_1}(x) &= \sum_{j=0}^{M}(-1)^j C_M^j \times \exp(-j\lambda_1 x) \\ &= 1 + \sum_{j=1}^{M}(-1)^j C_M^j \times \exp(-j\lambda_1 x), \end{aligned} \tag{18}$$

$$f_{\varphi_1}(x) = \lambda_1 \sum_{j=0}^{M-1}(-1)^j C_{M-1}^j M \times \exp\left[-(j+1)x\lambda_1\right], \tag{19}$$

where $C_M^j = \frac{M!}{j!(M-j)!}$. The data rate at destination D and eavesdropper E can be respectively given by

$$C_D = \frac{(1-\alpha)T}{2} \times \log_2\left(1 + \gamma_D\right), \tag{20}$$

$$C_E = \frac{(1-\alpha)T}{2} \times \log_2\left(1 + \gamma_E\right). \tag{21}$$

III. PERFORMANCE ANALYSIS

A. INTERCEPT PROBABILITY (IP)

Relay R_b can be intercepted if eavesdropper E can successfully decode the signal, i.e., $C_E \geq C_{th}$. Thus, intercept

probability can be defined as [43] and [44]

$$IP = \Pr\left(C_E \geq C_{th}\right) = \Pr\left(\gamma_E \geq \gamma_{th}\right) = \Pr\left(\frac{\kappa\varphi_1\varphi_3\Psi}{\kappa\varphi_3 + \kappa\Psi\varphi_4\varphi_5 + 1} \geq \gamma_{th}\right), \quad (22)$$

where $\gamma_{th} = 2^{\frac{2C_{th}}{(1-\alpha)T}} - 1$ and C_{th} is the predetermined threshold value. In order to obtain the closed-form expression of IP, we introduce following lemmas

Lemma 1: In order to obtain the closed-form expression for the PDF of SNR in amplify-and-forward system, a new series expansion of the modified Bessel function for K_v is mathematically represented as [45]

$$K_v(x) = \exp[-x] \times \sum_{l=0}^{\infty}\sum_{m=0}^{l}(x)^{m-v}\Lambda(v,l,m), \quad (23)$$

where $\Lambda(v,l,m) = \frac{(-1)^m\sqrt{\pi}\Gamma(2v)\Gamma(l-v+1/2)L(l,m)}{\Gamma(1/2-v)\Gamma(1/2+l+v)m!}$ and $L(l,m)$ is Lah number, which is defined as $L(l,m) = \binom{l-1}{m-1}\frac{l!}{m!}$.

Lemma 2: The function $\exp(x)$ is transformed by applying the Taylor series [46, Eq. (1.211.1)] as follows:

$$\exp(x) = \sum_{i=0}^{\infty}\frac{x^i}{i!}. \quad (24)$$

1) EXACT ANALYSIS

Based on (22), IP can be recalculated as

$$IP = \int_0^{\infty}\Pr\left(\frac{\kappa\varphi_1\varphi_3\Psi}{\kappa\varphi_3 + \kappa\Psi x + 1} \geq \gamma_{th}\right) \times f_X(x)dx, \quad (25)$$

where $X = \varphi_4\varphi_5$.

The first term in (25) can be calculated as

$$\begin{aligned} P_1 &= \Pr\left(\frac{\kappa\varphi_1\varphi_3\Psi}{\kappa\varphi_3 + \kappa\Psi x + 1} \geq \gamma_{th}\right) \\ &= 1 - \Pr\left[\varphi_1 < \frac{\gamma_{th}(\kappa\varphi_3 + \kappa\Psi x + 1)}{\kappa\varphi_3\Psi}\right] \\ &= 1 - \int_0^{\infty} F_{\varphi_1}\left[\frac{\gamma_{th}(\kappa\varphi_3 + \kappa\Psi x + 1)}{\kappa\varphi_3\Psi}|\varphi_3 = \varphi\right] f_{\varphi_3}(\varphi)d\varphi. \end{aligned} \quad (26)$$

By applying (15) and (18), P_1 can be re-written as

$$\begin{aligned} P_1 &= \sum_{j=1}^{M}(-1)^{j+1}C_M^j\lambda_3 \\ &\quad \times \int_0^{\infty}\exp\left[\frac{-j\lambda_1\gamma_{th}(\kappa\varphi + \kappa\Psi x + 1)}{\kappa\varphi\Psi}\right]\exp(-\lambda_3\varphi)\,d\varphi \\ &= \sum_{j=1}^{M}(-1)^{j+1}C_M^j \times \lambda_3\exp\left(-\frac{j\lambda_1\gamma_{th}}{\Psi}\right) \\ &\quad \times \int_0^{\infty}\exp\left[\frac{-j\lambda_1\gamma_{th}(\kappa\Psi x + 1)}{\kappa\varphi\Psi}\right] \times \exp(-\lambda_3\varphi)\,d\varphi. \end{aligned} \quad (27)$$

By applying [46, Eq. (3.324.1)], P_1 can be obtained as

$$\begin{aligned} P_1 &= \sum_{j=1}^{M}(-1)^{j+1}C_M^j \times \exp\left(-\frac{j\lambda_1\gamma_{th}}{\Psi}\right) \\ &\quad \times \sqrt{\frac{4j\lambda_1\lambda_3\gamma_{th}(\kappa\Psi x + 1)}{\kappa\Psi}} \\ &\quad \times K_1\left(2\sqrt{\frac{j\lambda_1\lambda_3\gamma_{th}(\kappa\Psi x + 1)}{\kappa\Psi}}\right), \end{aligned} \quad (28)$$

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

Next, we need to calculate the pdf of $f_X(x)$ in (25). First, we can obtain the CDF function as [32]

$$F_X(x) = 1 - 2\sqrt{\lambda_4\lambda_5 x} \times K_1\left(2\sqrt{\lambda_4\lambda_5 x}\right). \quad (29)$$

Then, by applying $\frac{\partial}{\partial x}\left(x^vK_v(x)\right) = -x^vK_{v-1}(x)$, the PDF of X is formulated as

$$f_X(x) = 2\lambda_4\lambda_5 \times K_0\left(2\sqrt{\lambda_4\lambda_5 x}\right). \quad (30)$$

By substituting (28) and (30) into (25), IP can be claimed as

$$\begin{aligned} IP &= 4\sum_{j=1}^{M}(-1)^{j+1}C_M^j\lambda_4\lambda_5\exp\left(-\frac{j\lambda_1\gamma_{th}}{\Psi}\right)\sqrt{\frac{j\lambda_1\lambda_3\gamma_{th}}{\kappa\Psi}} \\ &\quad \times \int_0^{\infty}\sqrt{(\kappa\Psi x + 1)}K_1\left(2\sqrt{\frac{j\lambda_1\lambda_3\gamma_{th}(\kappa\Psi x + 1)}{\kappa\Psi}}\right) \\ &\quad \times K_0\left(2\sqrt{\lambda_4\lambda_5 x}\right)dx. \end{aligned} \quad (31)$$

Remark 3: From (31), it is challenging to obtain the closed-form expression of IP. Therefore, we apply Lemmas 1 and 2 to solve this problem.

By applying Lemma 1, we have

$$\begin{aligned} &K_v\left(2\sqrt{\frac{j\lambda_1\lambda_3\gamma_{th}(\kappa\Psi x + 1)}{\kappa\Psi}}\right) \\ &= \exp\left[-2\sqrt{\frac{j\lambda_1\lambda_3\gamma_{th}(\kappa\Psi x + 1)}{\kappa\Psi}}\right] \times \\ &\quad \times \sum_{l=0}^{\infty}\sum_{m=0}^{l}\left(\frac{j\lambda_1\lambda_3\gamma_{th}}{\kappa\Psi}\right)^{\frac{m-v}{2}}\frac{(2)^{2m-2v}}{m!l!}\Lambda(v,l,m) \\ &\quad \times (\kappa\Psi x + 1)^{\frac{m-v}{2}}. \end{aligned} \quad (32)$$

Next, we apply Lemma 2, which yields

$$\exp\left[-2\sqrt{\frac{j\lambda_1\lambda_3\gamma_{th}(\kappa\Psi x + 1)}{\kappa\Psi}}\right]$$

$$= \sum_{i=0}^{\infty} \frac{\left(-2\sqrt{\frac{j\lambda_1\lambda_3\gamma_{th}(\kappa\Psi x+1)}{\kappa\Psi}}\right)^i}{i!} = \sum_{i=0}^{\infty} \left(\frac{j\lambda_1\lambda_3\gamma_{th}}{\kappa\Psi}\right)^{i/2} \frac{(-1)^i(2)^i(\kappa\Psi x+1)^{i/2}}{i!}. \quad (33)$$

By replacing (33) into (32) and applying $K_1(\cdot)$, we have

$$K_1\left(2\sqrt{\frac{j\lambda_1\lambda_3\gamma_{th}(\kappa\Psi x+1)}{\kappa\Psi}}\right) = \sum_{i=0}^{\infty}\sum_{l=0}^{\infty}\sum_{m=0}^{l}\left(\frac{j\lambda_1\lambda_3\gamma_{th}}{\kappa\Psi}\right)^{\frac{m-1+i}{2}} \times \frac{(-1)^i(2)^{2m-2+i}}{m!l!i!}\Lambda(1,l,m)\times(\kappa\Psi x+1)^{\frac{m-1+i}{2}}. \quad (34)$$

By substituting (34) into (31), we have

$$IP = \sum_{i=0}^{\infty}\sum_{l=0}^{\infty}\sum_{m=0}^{l}\sum_{j=0}^{M}\frac{(-1)^{i+j}(2)^{2m+i}\Lambda(1,l,m)\,C_M^j\times\lambda_4\lambda_5}{m!l!i!} \times\left(\frac{j\lambda_1\lambda_3\gamma_{th}}{\kappa\Psi}\right)^{\frac{m+i}{2}}\times\exp\left(-\frac{j\lambda_1\gamma_{th}}{\Psi}\right) \times\int_0^{\infty}(\kappa\Psi x+1)^{\frac{m+i}{2}}\times K_0\left(2\sqrt{\lambda_4\lambda_5 x}\right)dx. \quad (35)$$

Then, by applying

$$(x+y)^m = \sum_{n=0}^{m}\binom{m}{n}x^{m-n}y^n$$

and denoting $y=\sqrt{x}$, the IP can be expressed as in (36) in the top of next page.

$$IP = \widetilde{\sum}\binom{t}{n}\frac{(-1)^{i+j}(2)^{t_1}\Lambda(1,l,m)\,C_M^j\lambda_4\lambda_5(j\lambda_1\lambda_3\gamma_{th})^t}{m!l!i!(\kappa\Psi)^{n+t}} \times\exp\left(-\frac{j\lambda_1\gamma_{th}}{\Psi}\right)\int_0^{\infty}y^{2n+1}K_0\left(2y\sqrt{\lambda_4\lambda_5}\right)dx, \quad (36)$$

where $\widetilde{\sum} = \sum_{i=0}^{\infty}\sum_{l=0}^{\infty}\sum_{m=0}^{l}\sum_{n=0}^{t}\sum_{j=0}^{M}$, $t \triangleq \frac{m+i}{2}$, $t_1 \triangleq 2m+i+1$.

Finally, by applying [46, Eq. (6.561.16)], the IP can be represented as the following theorem.

Theorem 1: In the HD SWIPT-enabled wireless system with a friendly jammer and an eavesdropper, the closed-form expression of the IP can be presented as

$$\mathrm{IP} = \widetilde{\sum}\binom{t}{n}\frac{(-1)^{i+j}(2)^{2m+i-1}\Lambda(1,l,m)\,C_M^j(j\lambda_1\lambda_3\gamma_{th})^t}{m!l!i!(\kappa\Psi)^{n+t}(\lambda_4\lambda_5)^n} \times\exp\left(-\frac{j\lambda_1\gamma_{th}}{\Psi}\right)\times[\Gamma(1+n)]^2, \quad (37)$$

where $\Gamma(z)=\int_0^{\infty}e^{-t}t^{z-1}dt$ is the complete gamma function.

2) ASYMPTOTIC ANALYSIS

At high SNR regime, γ_E in (14) can be expressed as

$$\gamma_E^{\infty} \approx \frac{\varphi_1\varphi_3}{\varphi_4\varphi_5}. \quad (38)$$

Then, the IP can be calculated as

$$IP^{\infty} = \Pr\left(\frac{\varphi_1\varphi_3}{\varphi_4\varphi_5}\geq\gamma_{th}\right) = 1-\int_0^{\infty}F_Y(x\gamma_{th})\times f_X(x)dx, \quad (39)$$

where $Y=\varphi_1\varphi_3$.

Lemma 3: The CDF of Y can be given as

$$F_Y(y) = 1+2\sum_{j=1}^{M}(-1)^jC_M^j\sqrt{j\lambda_1\lambda_3 y}K_1\left(2\sqrt{j\lambda_1\lambda_3 y}\right). \quad (40)$$

Proof: The CDF of Y can be calculated as

$$F_Y(y) = \Pr(Y<y) = \Pr\left(\varphi_1<\frac{y}{\varphi_3}\right) = \int_0^{\infty}F_{\varphi_1}\left(\frac{y}{\varphi}\right)\times f_{\varphi_3}(\varphi)d\varphi. \quad (41)$$

By applying (18), we have

$$F_Y(y) = 1+\sum_{j=1}^{M}(-1)^jC_M^j\lambda_3 \times\int_0^{\infty}\exp\left(-\frac{j\lambda_1 y}{\varphi}\right)\exp(-\lambda_3\varphi)\,d\varphi. \quad (42)$$

By applying [46, Eq. (3.324.1)], the CDF of Y can be obtained as in Lemma 3. ■

By substituting (30) and (42) into (39), the IP can be given as

$$IP^{\infty} = 4\sum_{j=1}^{M}(-1)^{j+1}C_M^j\times\sqrt{j\lambda_1\lambda_3\gamma_{th}}\times\lambda_4\lambda_5 \times\int_0^{\infty}\sqrt{x}\times K_1\left(2\sqrt{j\lambda_1\lambda_3\gamma_{th}x}\right)\times K_0\left(2\sqrt{\lambda_4\lambda_5 x}\right)dx. \quad (43)$$

Let us denote $t=\sqrt{x}$, (43) can be rewritten as

$$IP^{\infty} = 8\sum_{j=1}^{M}(-1)^{j+1}C_M^j\sqrt{j\lambda_1\lambda_3\gamma_{th}}\lambda_4\lambda_5 \times\int_0^{\infty}t^2K_1\left(2t\sqrt{j\lambda_1\lambda_3\gamma_{th}}\right)K_0\left(2t\sqrt{\lambda_4\lambda_5}\right)dt. \quad (44)$$

By applying [46, Eq. (6.576. 4)], the IP can be represented as the following theorem.

Theorem 2: In the HD SWIPT-enabled wireless system with a friendly jammer and an eavesdropper, the closed-form expression of the IP in high SNR regime can be represented as

$$\mathrm{IP}^{\infty} = \sum_{j=1}^{M} \frac{(-1)^{j+1} C_M^j \times \lambda_4 \lambda_5}{2j\lambda_1 \lambda_3 \gamma_{th}} \times F\left(2, 1; 2; 1 - \frac{\lambda_4 \lambda_5}{j\lambda_1 \lambda_3 \gamma_{th}}\right), \quad (45)$$

where $F(\alpha, \beta; \gamma; z)$ is the Gauss Hypergeometric function.

B. NON ZERO-SECRECY PROBABILITY (NZSP)

Non-zero secrecy capacity (NZSC) can be defined as the end-to-end secrecy capacity is higher than zero [47]

$$NZSP = \Pr(C_D - C_E > 0) = \Pr(\gamma_D > \gamma_E). \quad (46)$$

By substituting (9) and (12) into (46), we have

$$NZSP = \Pr\left(\frac{\varphi_2}{\kappa\varphi_2 + 1} > \frac{\varphi_3}{\kappa\varphi_3 + \kappa\Psi\varphi_4\varphi_5 + 1}\right) = \int_0^{\infty} F_{\tilde{\gamma}_E}\left(\frac{x}{\kappa x + 1} | \varphi_2 = x\right) \times f_{\varphi_2}(x) dx, \quad (47)$$

where $\tilde{\gamma}_E = \frac{\varphi_3}{\kappa\varphi_3 + \kappa\Psi\varphi_4\varphi_5 + 1}$.

Lemma 4: The closed-form expression of CDF of $\tilde{\gamma}_E$ can be given as

$$F_{\tilde{\gamma}_E}\left(\frac{x}{\kappa x + 1}\right) = 1 - \sqrt{\lambda_4\lambda_5} \times \frac{\exp\left(\frac{\lambda_4\lambda_5}{2\lambda_3\kappa\Psi x} - \lambda_3 x\right)}{\sqrt{\lambda_3\kappa\Psi x}} \times W_{-\frac{1}{2},0}\left(\frac{\lambda_4\lambda_5}{\lambda_3\kappa\Psi x}\right), \quad (48)$$

where $W(\bullet)$ is the Whittaker function.

Proof: The CDF of $\tilde{\gamma}_E$ can be calculated as

$$\begin{aligned} F_{\tilde{\gamma}_E}(a) &= \Pr\left(\frac{\varphi_3}{\kappa\varphi_3 + \kappa\Psi\varphi_4\varphi_5 + 1} < a\right) \\ &= \Pr\left[\varphi_3(1 - \kappa a) < \kappa\Psi a\varphi_4\varphi_5 + a\right] \\ &= \begin{cases} \Pr\left(\varphi_3 < \dfrac{\kappa\Psi a\varphi_4\varphi_5 + a}{1 - \kappa a}\right), & a \le \dfrac{1}{\kappa} \\ 1, & a > \dfrac{1}{\kappa} \end{cases} \\ &= \int_0^{\infty} F_{\varphi_3}\left[\frac{\kappa\Psi a y + a}{1 - \kappa a}\right] \times f_X(y) dy, \; a \le \frac{1}{\kappa}. \end{aligned} \quad (49)$$

By applying (30), $F_{\tilde{\gamma}_E}(a)$ with $a \le 1/\kappa$ is calculated as

$$\begin{aligned} F_{\tilde{\gamma}_E}(a) &= 1 - 2\lambda_4\lambda_5 \int_0^{\infty} \exp\left[-\frac{\lambda_3(\kappa\Psi a y + a)}{1 - \kappa a}\right] \times K_0\left(2\sqrt{\lambda_4\lambda_5 y}\right) dy \\ &= 1 - 2\lambda_4\lambda_5 \times \exp\left(-\frac{\lambda_3 a}{1 - \kappa a}\right) \int_0^{\infty} \exp\left(-\frac{\lambda_3\kappa\Psi a y}{1 - \kappa a}\right) \times K_0\left(2\sqrt{\lambda_4\lambda_5 y}\right) dy. \end{aligned} \quad (50)$$

By setting $a = \frac{x}{\kappa x + 1}$, it yields

$$F_{\tilde{\gamma}_E}\left(\frac{x}{\kappa x + 1}\right) = 1 - 2\lambda_4\lambda_5 \times \exp(-\lambda_3 x) \times \int_0^{\infty} \exp(-\lambda_3\kappa\Psi x y) K_0\left(2\sqrt{\lambda_4\lambda_5 y}\right) dy. \quad (51)$$

Then, by applying [46, Eq. (6.614.4)], (48) is obtained. Thus, the proof is complete. ■

By substituting (48) into (47), the NZSP can be expressed as

$$NZSP = 1 - \lambda_2 \int_0^{\infty} \sqrt{\lambda_4\lambda_5} \frac{\exp\left(\frac{\lambda_4\lambda_5}{2\lambda_3\kappa\Psi x} - \lambda_3 x - \lambda_2 x\right)}{\sqrt{\lambda_3\kappa\Psi x}} \times W_{-\frac{1}{2},0}\left(\frac{\lambda_4\lambda_5}{\lambda_3\kappa\Psi x}\right) dx. \quad (52)$$

By applying [46, Eq. (7.629.1)], the NZSP can be expressed as the following theorem.

Theorem 3: In the HD SWIPT-enabled wireless system with a friendly jammer and an eavesdropper, the closed-form expression of the NZSP can be represented as

$$NZSP = 1 - \frac{4\lambda_2\lambda_4\lambda_5(\lambda_2 + \lambda_3)}{\lambda_3\kappa\Psi} \times S_{-1,0}\left(2\sqrt{\frac{\lambda_4\lambda_5(\lambda_2 + \lambda_3)}{\lambda_3\kappa\Psi}}\right), \quad (53)$$

where $S(\bullet)$ is the Lommel functions.

IV. SIMULATION RESULTS

In this section, we present the intercept probability and non zero-secrecy probability for theoretical analytical evaluation. For Monte-Carlo simulations, we perform 10^6 independent random channels, and they are Rayleigh fading for each realization. The obtained results are averaged to remove the randomness and compare with the analytical results. Unless otherwise stated, the simulation parameters are listed in Table 1.

Fig. 3 shows the intercept probability as a function of Ψ (in dB), where $C_{th} = 0.25$ bps/Hz, $\eta = 0.8$, and $\alpha = 0.5$. It can be seen from the figure that IP increases with a higher value of Ψ. This is due to the fact that Ψ can be defined as the fractional between the source transmit power and the white noise. Therefore, the higher the Ψ is, the more power at source S is transmitted. Consequently, the higher data transmission rate can be obtained at eavesdropper E, which improves the intercept probability. More specifically, when the number of relays $M = 1$, the IP value is 0.0616 and 0.2393, corresponding to Ψ equals 5 dB and 10 dB, respectively. We also observe from Fig. 3 that intercept performance is enhanced as the number of relays increases. This can be

TABLE 1. Simulation parameters.

Symbol	Parameter name	Fixed value	Varying range
C_{th}	Rate requirement	0.25; 0.05 bps/Hz	none
η	EH factor	0.8	none
α	time switching ratio	0.5	0.05 to 0.95 [32]
Ψ	Power-to-noise-ratio	5 dB	0 to 25 (dB)
d_{SR_b}	distance from $\mathrm{S} \to \mathrm{R}_b$	2	none
$d_{\mathrm{R}_b\mathrm{D}}$	distance from $\mathrm{R}_b \to D$	1	none
$d_{\mathrm{R}_b\mathrm{E}}$	distance from $\mathrm{R}_b \to E$	1	0.2 to 2
d_{SJ}	distance from $\mathrm{S} \to J$	2	none
d_{JE}	distance from $\mathrm{J} \to E$	1	none
λ_{SR_b}	Mean of $\lvert h_{\mathrm{SR}_b}\rvert^2$	4	none
$\lambda_{\mathrm{R}_b\mathrm{D}}$	Mean of $\lvert h_{\mathrm{R}_b\mathrm{D}}\rvert^2$	1	none
$\lambda_{\mathrm{R}_b\mathrm{E}}$	Mean of $\lvert h_{\mathrm{R}_b\mathrm{E}}\rvert^2$	1	none
λ_{JE}	Mean of $\lvert h_{\mathrm{JE}}\rvert^2$	1	none
λ_{SJ}	Mean of $\lvert h_{\mathrm{SJ}}\rvert^2$	4	none

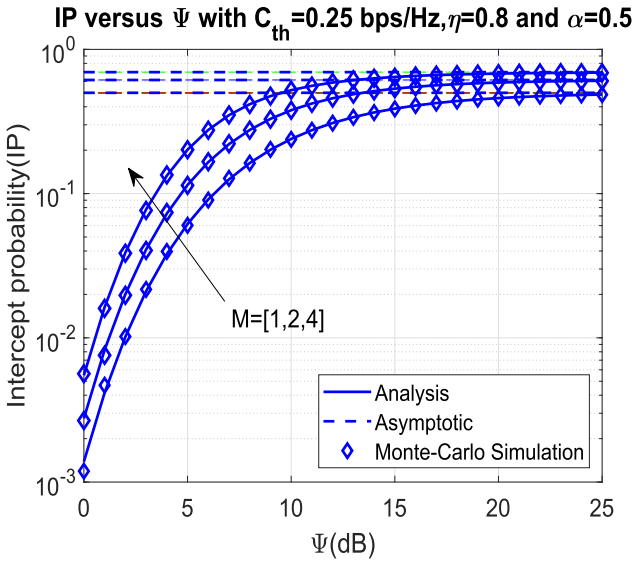


FIGURE 3. IP versus Ψ, with $C_{th} = 0.5$ bps/Hz, $\eta = 0.8$, $M = 2$.

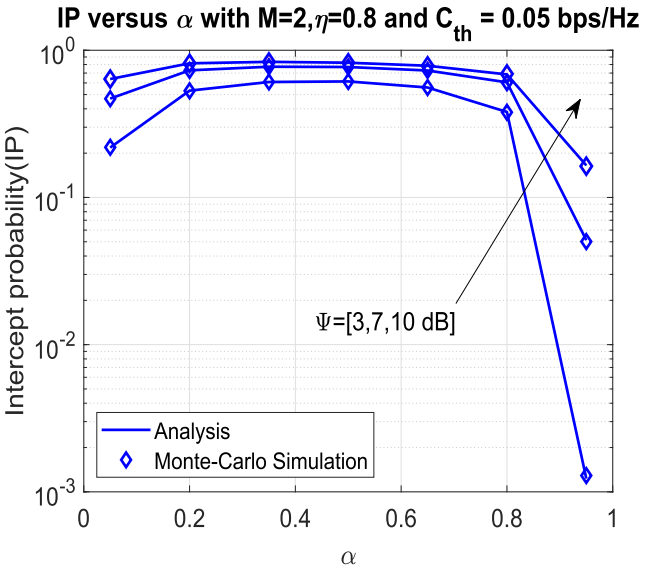


FIGURE 4. IP vs. α, with $C_{th} = 0.5$ bps/Hz, $M = 2$, $K = 1$, $\Phi = 1$ dB.

explained based on equation (13) since the signal-to-noise-ratio at the eavesdropper, i.e., γ_E, is linearly proportional to the channel gain between $S \to R_b$, i.e., $|h_{SR_b}|^2$. Therefore, the higher the number of relays is, the better channel to eavesdropper can be obtained. For instance, when $\Psi = 5$ dB, the IP is 0.0616, 0.1148, and 0.2016, corresponding to the number of relays is 4, 2, 1, respectively. Fig. 3 also validates the correctness of the exact and asymptotic analysis compared to the Monte-Carlo simulation.

Fig. 4 illustrates the intercept probability versus time switching factor, where the number of relays $M = 2$, $\eta = 0.8$, and $C_{th} = 0.05$ bps/Hz. The time switching factor plays a crucial role since it influences the time used for energy harvesting and the allocation time for data transmission. Therefore, it significantly impacts the network performance. First, it is observed that the intercept performance is improved to an optimal point when the time switching ratio α increases to the optimal value, then IP decreases when α continues increasing. Specifically, when $\Psi = 3$ dB, the IP achieves maximum value 0.6141 at α equals 0.5, then it decreases to 0.0012 at α equals 0.9. Second, it is also observed that the intercept performance is improved as a higher Ψ value. For instance, the IP is 0.6087, 0.7729, and 0.833 when Ψ equals 3, 7, 10 dB, respectively.

Fig. 5 further characterizes the intercept probability versus number of relays M, where $\Psi = 5$ dB, $\eta = 0.8$. It is observed from this figure that the IP is greatly improved with a higher number of relays. This phenomenon has been explained in Fig. 3. Moreover, the intercept performance also increases as α value decreases from 0.5 to 0.25, and $C_{th} = 0.25$ bps/Hz. For instance, the IP is 0.0052, 0.0226, and 0.2016 corresponding to three cases $\alpha = 0.5$, $C_{th} = 0.5$ bps/Hz, $\alpha = 0.25$, $C_{th} = 0.5$ bps/Hz, and $\alpha = 0.5$, $C_{th} = 0.25$ bps/Hz, respectively. Further observation reveals that the lower the threshold rate is, the higher IP can be obtained. It can be explained based on equation (22). Specifically, the lower the C_{th} is, the higher the IP can be obtained.

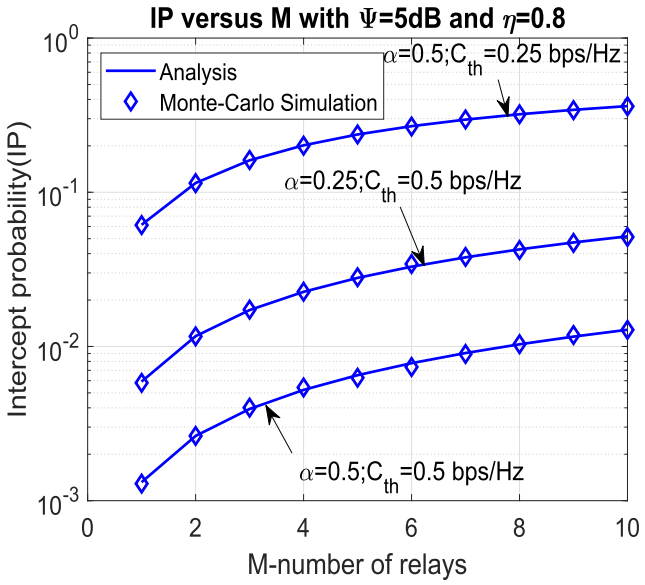


FIGURE 5. IP versus number of relays M, with $\Psi = 5$ dB, $\eta = 0.8$.

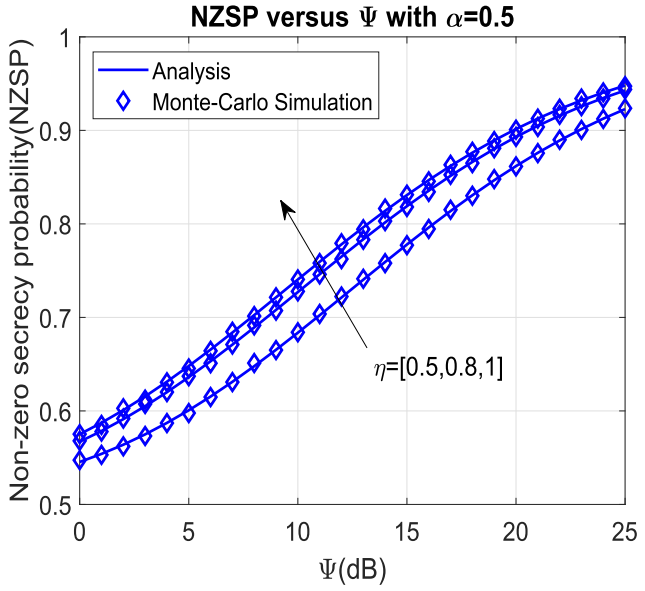


FIGURE 6. IP versus Ψ, with $\alpha = 0.5$.

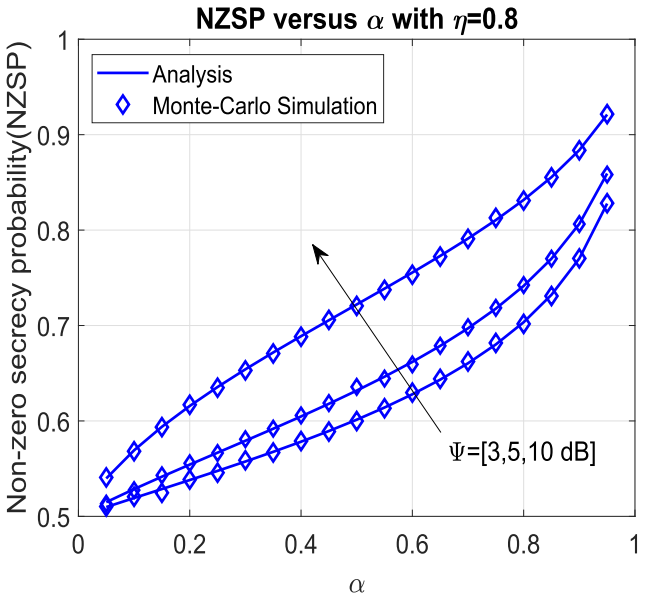


FIGURE 7. NZSP versus α, with $\eta = 0.8$.

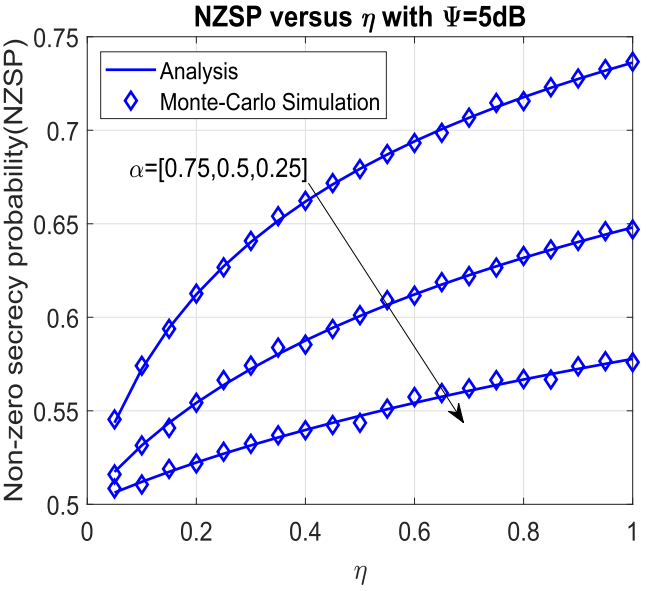


FIGURE 8. NZSP versus η, with $\Psi = 5$ dB.

In Fig. 6, we investigate non-zero secrecy probability as a function of Ψ (in dB), where $\alpha = 0.5$. From Fig. 6, it can be shown that the non-zero secrecy probability is greatly improved as Ψ increases from 0 to 25 dB. It means that the data transmission rate received at destination D is higher than that at eavesdropper E. More specifically, when $\eta = 0.5$, the NZSP is 0.6007, 0.6836, 0.7779 corresponding to Ψ equals 5, 10, and 15, respectively. Furthermore, it also be shown that the NZSP is enhanced as the η value increases. For instance, when $\Psi = 10$ dB, the NZSP is 0.6836, 0.7271, 0.7405 corresponding to η equals 0.5, 0.8, and 1, respectively.

In Fig. 7, we study non-zero secrecy probability depending on time switching factor α, with $\eta = 0.8$. from Fig. 7, it can be seen that the NZSP is enhanced as time switching ratio increases from 0.1 to 0.9. It shows the superiority of transmission rate at the destination D compared to that at the eavesdropper when increasing time switching factor α. For instance, when $\Psi = 3$ dB, the NZSP imposes 0.6279, 0.6604, and 0.7035 corresponding to α equals 0.6, 0.7, and 0.8, respectively. It is also observed that the NZSP is improved with a higher value of Ψ. For instance, at $\alpha = 0.4$, the NZSP is 0.5782, 0.6047, and 0.6888 corresponding to Ψ equals 3, 5, and 10 dB, respectively. It explains the fact that the increase of source's power has more effects on the transmission rate at the destination D than the transmission rate at eavesdropper E.

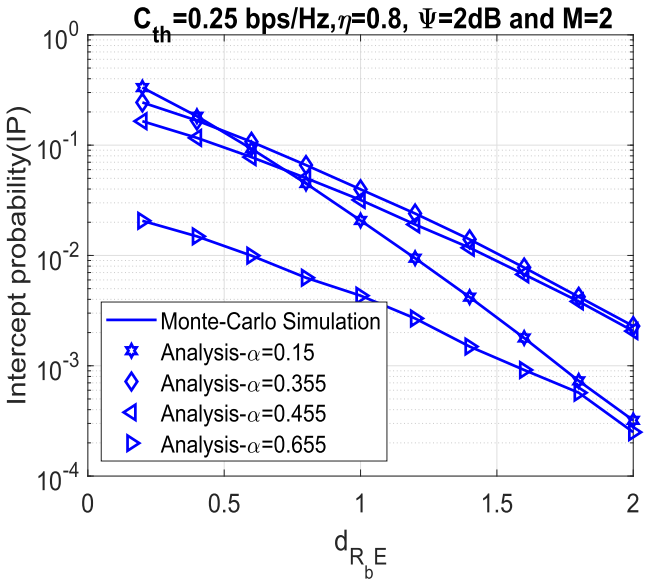


FIGURE 9. IP versus d_{R_bE}, with $C_{th} = 0.25$ bps/Hz, $\eta = 0.8$, $\Psi = 2$ dB, and $M = 2$.

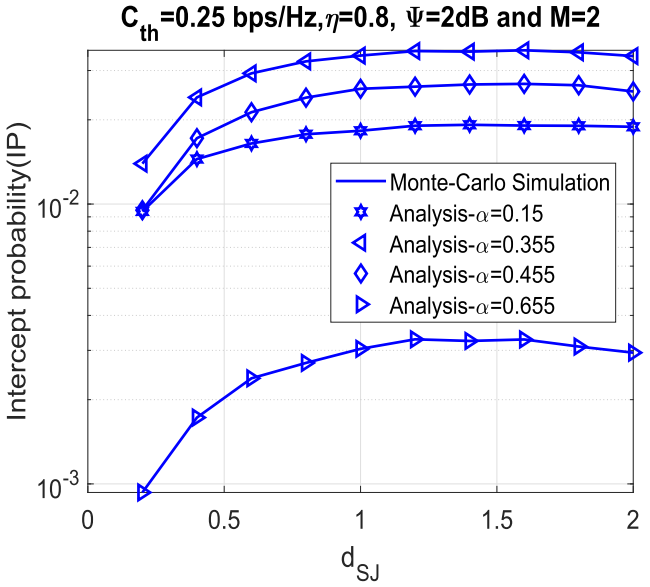


FIGURE 10. IP versus d_{SJ}, with $C_{th} = 0.25$ bps/Hz, $\eta = 0.8$, $\Psi = 2$ dB, and $M = 2$.

In Fig. 8, we show the result corresponding to non-zero secrecy probability versus energy harvesting coefficient η, with $\Psi = 5$ dB. From Fig. 8, it is clear to see that the higher the energy harvesting coefficient is, the more NZSP can be achieved. This phenomenon can be explained based on equation (3), whereas the amount of harvested energy at the relay R_b is linearly proportional with the energy harvesting coefficient η. More specifically, the NZSP imposes 0.5315, 0.5542, and 0. 5724 when η is 0.1, 0.2, and 0.3, respectively.

The simulation results in Fig. 9 show the influences of different eavesdropper locations on the intercept performance, where $C_{th} = 0.25$ bps/Hz, $\eta = 0.8$, $\Psi = 2$ dB, and $M = 2$. In practice, it is difficult to know exactly the eavesdropper position to prevent them from wire-tapping information. Therefore, Fig. 9 investigates the influences of different eavesdropper locations on the network performance, i.e., intercept probability. First, it can be seen from Fig. 9 that the higher the distance from $E \rightarrow R_b$ is, the worse intercept probability can be obtained. This is expected since by increasing distance d_{R_bE}, we make the channel gain between $E \rightarrow R_b$ deteriorate, which reduces the intercept performance. Specifically, the IP is 0.0206, 0.01, and 0.0043 when d_{R_bE} equals 0.2, 0.6, and 1, respectively. Besides, we also study the effects of different time switching factor α with the variances of d_{R_bE}. We observe that when d_{R_bE} is less than 0.5, the IP of scheme with $\alpha = 0.15$ obtains the best performance compared to other cases with α equals 0.55, 0.455, and 0.655, respectively. Nevertheless, hen d_{R_bE} is larger than 0.5, the IP of the scheme is the best one. While the IP of scheme with $\alpha = 0.15$ is significantly decreased with $d_{R_bE} > 0.5$.

In Fig. 10, we investigate the effects of different jammer locations on the intercept performance, where $C_{th} = 0.25$ bps/Hz, $\eta = 0.8$, $\Psi = 2$ dB, and $M = 2$. Fig. 10 aims to find the best position of a friendly jammer to reduce the influences of eavesdropper. It can be seen that the intercept performance can obtain the best performance at an optimal value of d_{SJ}, then it reduces later on. Specifically, when $\alpha = 0.655$, the IP achieves the best performance at d_{SJ} equals 1.4. There also exists the optimum α value corresponding to difference d_{SJ} ranging from 0.2 to 2. Indeed, the intercept performance of the scheme with $\alpha = 0.355$ obtains the best results compared to others, i.e., α is 0.15, 0.455, and 0.655, respectively. For example, when $d_{SJ} = 1$, the IP is 0.003, 0.0183, 0.0258, and 0.339 corresponding to α equals 0.355, 0.15, 0. 455, and 0.15, respectively.

V. CONCLUSION AND FUTURE DIRECTIONS

In this paper, we investigated the intercept and non-zero secrecy probability of an AF- and SWIPT-based IoT network, including one source, multiple relays, one destination in the presence of one jammer, and one eavesdropper. By applying the time switching method, the selected relay can harvest energy from the source's RF signals, and then it uses its energy for conveying information to the destination. Especially, the exact closed-form expressions of IP, asymptotic IP, and NZSP were derived. Moreover, these mathematical analyses have been validated throughput simulation results, which showed the correctness of the analysis and Monte-Carlo simulations. Based on the simulation results, we recommend suitable system parameters for designing in practice. Specifically, the values of time switching factor α, source transmit power Ψ, the number of relays, and position of jammer can be selected appropriately to reduces the effects of the eavesdropper. The IP fluctuates less than $3\times$ as $\alpha \in [0.1, 0.8]$, while the fluctuation of the IP is in a wide range as $\alpha > 0.8$. Multiple sources and destinations should be of interest for future work investigating cooperative networks or mutual interference management. Moreover, multiple-input multiple-output systems also have the potential to improve system performance.

REFERENCES

[1] P. X. Nguyen, D.-H. Tran, O. Onireti, P. T. Tin, S. Q. Nguyen, S. Chatzinotas, and H. V. Poor, "Backscatter-assisted data offloading in OFDMA-based wireless-powered mobile edge computing for IoT networks," *IEEE Internet Things J.*, vol. 8, no. 11, pp. 9233–9243, Jun. 2021.

[2] N. Wang, P. Wang, A. Alipour-Fanid, L. Jiao, and K. Zeng, "Physical-layer security of 5G wireless networks for IoT: Challenges and opportunities," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8169–8181, Oct. 2019.

[3] T. N. Nguyen, D.-H. Tran, T. V. Chien, V.-D. Phan, M. Voznak, P. T. Tin, S. Chatzinotas, D. W. K. Ng, and H. V. Poor, "Security-reliability tradeoff analysis for SWIPT- and AF-based IoT networks with friendly jammers," *IEEE Internet Things J.*, vol. 9, no. 21, pp. 21662–21675, Nov. 2022.

[4] *Ericsson Mobility Report*, Ericsson, Stockholm, Sweden, Nov. 2019.

[5] Y. K. Tan and S. K. Panda, "Self-autonomous wireless sensor nodes with wind energy harvesting for remote sensing of wind-driven wildfire spread," *IEEE Trans. instrum. Meas.*, vol. 60, no. 4, pp. 1367–1377, Apr. 2011.

[6] A. Shekhar, V. K. Kumaravel, S. Klerks, S. de Wit, P. Venugopal, N. Narayan, P. Bauer, O. Isabella, and M. Zeman, "Harvesting roadway solar energy—performance of the installed infrastructure integrated PV bike path," *IEEE J. Photovolt.*, vol. 8, no. 4, pp. 1066–1073, Jul. 2018.

[7] Y. Sun, N. H. Hieu, C.-J. Jeong, and S.-G. Lee, "An integrated high-performance active rectifier for piezoelectric vibration energy harvesting systems," *IEEE Trans. Power Electron.*, vol. 27, no. 2, pp. 623–627, Feb. 2012.

[8] T. N. Nguyen, T. H. Quang Minh, P. T. Tran, M. Voznak, T. T. Duy, T.-L. Nguyen, and P. T. Tin, "Performance enhancement for energy harvesting based two-way relay protocols in wireless ad-hoc networks with partial and full relay selection methods," *Ad Hoc Netw.*, vol. 84, pp. 178–187, Mar. 2019.

[9] P. T. Tin, T. N. Nguyen, D.-H. Tran, M. Voznak, V.-D. Phan, and S. Chatzinotas, "Performance enhancement for full-duplex relaying with time-switching-based SWIPT in wireless sensors networks," *Sensors*, vol. 21, no. 11, p. 3847, Jun. 2021.

[10] X. Zhang, J. Wang, and H. V. Poor, "Statistical delay and error-rate bounded QoS provisioning for SWIPT over CF M-MIMO 6G mobile wireless networks using FBC," *IEEE J Sel. Topics Signal Process.*, vol. 15, no. 5, pp. 1272–1287, Aug. 2021.

[11] T. N. Nguyen, D.-H. Tran, T. Van Chien, V.-D. Phan, M. Voznak, and S. Chatzinotas, "Security and reliability analysis of satellite-terrestrial multirelay networks with imperfect CSI," *IEEE Syst. J.*, vol. 17, no. 2, pp. 2824–2835, Jun. 2022.

[12] M. Hayajneh and T. A. Gulliver, "Physical layer security in two-way SWIPT relay networks with imperfect CSI and a friendly jammer," *Entropy*, vol. 25, no. 1, p. 122, Jan. 2023.

[13] B. C. Nguyen, T. M. Hoang, P. T. Tran, and T. N. Nguyen, "Outage probability of NOMA system with wireless power transfer at source and full-duplex relay," *AEU Int. J. Electron. Commun.*, vol. 116, Mar. 2020, Art. no. 152957.

[14] V. Shahiri, A. Kuhestani, and L. Hanzo, "Short-packet amplify-and-forward relaying for the internet-of-things in the face of imperfect channel estimation and hardware impairments," *IEEE Trans. Green Commun. Netw.*, vol. 6, no. 1, pp. 20–36, Mar. 2022.

[15] D. Zheng, Y. Yang, L. Wei, and B. Jiao, "Decode-and-forward short-packet relaying in the Internet of Things: Timely status updates," *IEEE Trans. Wireless Commun.*, vol. 20, no. 12, pp. 8423–8437, Dec. 2021.

[16] Y. Shim, H. Park, and W. Shin, "Joint time allocation for wireless energy harvesting decode-and-forward relay-based IoT networks with rechargeable and nonrechargeable batteries," *IEEE Internet Things J.*, vol. 8, no. 4, pp. 2792–2801, Feb. 2021.

[17] V. Aswathi and A. V. Babu, "Performance analysis of NOMA-based underlay cognitive radio networks with partial relay selection," *IEEE Trans. Veh. Technol.*, vol. 70, no. 5, pp. 4615–4630, May 2021.

[18] T. He, K.-W. Chin, S. Soh, and Z. Zhang, "A novel distributed resource allocation scheme for wireless-powered cognitive radio Internet of Things networks," *IEEE Internet Things J.*, vol. 8, no. 20, pp. 15486–15499, Oct. 2021.

[19] T. N. Nguyen, P. T. Tran, and M. Voznak, "Wireless energy harvesting meets receiver diversity: A successful approach for two-way half-duplex relay networks over block Rayleigh fading channel," *Comput. Netw.*, vol. 172, May 2020, Art. no. 107176.

[20] Z. Fang, S. Shen, J. Liu, W. Ni, and A. Jamalipour, "New NOMA-based two-way relay networks," *IEEE Trans. Veh. Technol.*, vol. 69, no. 12, pp. 15314–15324, Dec. 2020.

[21] N. Hoang An, M. Tran, T. N. Nguyen, and D.-H. Ha, "Physical layer security in a hybrid TPSR two-way half-duplex relaying network over a Rayleigh fading channel: Outage and intercept probability analysis," *Electronics*, vol. 9, no. 3, p. 428, Mar. 2020.

[22] Z. Wang, W. Shi, W. Liu, Y. Zhao, and K. Kang, "Performance analysis of two-way full-duplex relay mixed RF/FSO system with self-interference," *IEEE Commun. Lett.*, vol. 25, no. 1, pp. 209–213, Jan. 2021.

[23] 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," *IEEE Access*, vol. 8, pp. 187165–187181, 2020.

[24] Z. Peng, X. Chen, W. Xu, C. Pan, L.-C. Wang, and L. Hanzo, "Analysis and optimization of massive access to the IoT relying on multi-pair two-way massive MIMO relay systems," *IEEE Trans. Commun.*, vol. 69, no. 7, pp. 4585–4598, Jul. 2021.

[25] T. Lv, Z. Lin, P. Huang, and J. Zeng, "Optimization of the energy-efficient relay-based massive IoT network," *IEEE Internet Things J.*, vol. 5, no. 4, pp. 3043–3058, Aug. 2018.

[26] D.-H. Tran, S. Chatzinotas, and B. Ottersten, "Satellite- and cache-assisted UAV: A joint cache placement, resource allocation, and trajectory optimization for 6G aerial networks," 2021, *arXiv:2106.05016*.

[27] W. Feng, J. Wang, Y. Chen, X. Wang, N. Ge, and J. Lu, "UAV-aided MIMO communications for 5G Internet of Things," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 1731–1740, Apr. 2019.

[28] M. Liu, J. Yang, and G. Gui, "DSF-NOMA: UAV-assisted emergency communication technology in a heterogeneous Internet of Things," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 5508–5519, Jun. 2019.

[29] D. Storm, "Hackers exploit SCADA holes to take full control of critical infrastructure," *Computerworld*, vol. 15, 2014.

[30] P. Yan, J. Yang, M. Liu, J. Sun, and G. Gui, "Secrecy outage analysis of transmit antenna selection assisted with wireless power beacon," *IEEE Trans. Veh. Technol.*, vol. 69, no. 7, pp. 7473–7482, Jul. 2020.

[31] Z. Chu, H. X. Nguyen, and G. Caire, "Game theory-based resource allocation for secure WPCN multiantenna multicasting systems," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 4, pp. 926–939, Apr. 2018.

[32] P. T. Tin, B. H. Dinh, T. N. Nguyen, D. H. Ha, and T. T. Trang, "Power beacon-assisted energy harvesting wireless physical layer cooperative relaying networks: Performance analysis," *Symmetry*, vol. 12, no. 1, p. 106, Jan. 2020.

[33] H.-M. Wang, Y. Zhang, X. Zhang, and Z. Li, "Secrecy and covert communications against UAV surveillance via multi-hop networks," *IEEE Trans. Commun.*, vol. 68, no. 1, pp. 389–401, Jan. 2020.

[34] T. D. Hieu, T. T. Duy, and S. G. Choi, "Performance enhancement for harvest-to-transmit cognitive multi-hop networks with best path selection method under presence of eavesdropper," in *Proc. 20th Int. Conf. Adv. Commun. Technol. (ICACT)*, Feb. 2018, pp. 323–328.

[35] P. T. Tin, D. T. Hung, T. Nguyen, T. Duy, and M. Voznak, "Secrecy performance enhancement for underlay cognitive radio networks employing cooperative multi-hop transmission with and without presence of hardware impairments," *Entropy*, vol. 21, no. 2, p. 217, Feb. 2019.

[36] T. D. Hieu, T. T. Duy, and B.-S. Kim, "Performance enhancement for multihop harvest-to-transmit WSNs with path-selection methods in presence of eavesdroppers and hardware noises," *IEEE Sensors J.*, vol. 18, no. 12, pp. 5173–5186, Jun. 2018.

[37] K. Cao, B. Wang, H. Ding, L. Lv, J. Tian, and F. Gong, "On the security enhancement of uplink NOMA systems with jammer selection," *IEEE Trans. Commun.*, vol. 68, no. 9, pp. 5747–5763, Sep. 2020.

[38] H. Zhang, X. He, and H. Dai, "Secure UAV communication networks via friendly jamming and bandwidth allocation," in *Proc. IEEE Conf. Comput. Commun. Workshops (INFOCOM WKSHPS)*, Jul. 2020, pp. 894–899.

[39] M. Kim, S. Kim, and J. Lee, "Securing communications with friendly unmanned aerial vehicle jammers," *IEEE Trans. Veh. Technol.*, vol. 70, no. 2, pp. 1972–1977, Feb. 2021.

[40] N. Qi, W. Wang, M. Xiao, L. Jia, S. Jin, Q. Zhu, and T. A. Tsiftsis, "A learning-based spectrum access Stackelberg game: Friendly jammer-assisted communication confrontation," *IEEE Trans. Veh. Technol.*, vol. 70, no. 1, pp. 700–713, Jan. 2021.
[41] T. A. Le, T. Van Chien, and M. D. Renzo, "Robust probabilistic-constrained optimization for IRS-aided MISO communication systems," *IEEE Wireless Commun. Lett.*, vol. 10, no. 1, pp. 1–5, Jan. 2021.
[42] V.-D. Phan, T. N. Nguyen, A. V. Le, and M. Voznak, "A study of physical layer security in SWIPT-based decode-and-forward relay networks with dynamic power splitting," *Sensors*, vol. 21, no. 17, p. 5692, Aug. 2021.
[43] X. Li, M. Zhao, Y. Liu, L. Li, Z. Ding, and A. Nallanathan, "Secrecy analysis of ambient backscatter NOMA systems under I/Q imbalance," *IEEE Trans. Veh. Technol.*, vol. 69, no. 10, pp. 12286–12290, Oct. 2020.
[44] X. Li, M. Huang, C. Zhang, D. Deng, K. M. Rabie, Y. Ding, and J. Du, "Security and reliability performance analysis of cooperative multi-relay systems with nonlinear energy harvesters and hardware impairments," *IEEE Access*, vol. 7, pp. 102644–102661, 2019.
[45] D. J. Maširević and T. K. Pogány, "On series representations for modified Bessel function of second kind of integer order," *Integral Transforms Special Functions*, vol. 30, no. 3, pp. 181–189, Mar. 2019.
[46] A. Jeffrey and D. Zwillinger, *Table of Integrals, Series, and Products*, 7th ed. Amsterdam, The Netherlands: Elsevier, 2007.
[47] H. D. Tran, D. T. Tran, and S. G. Choi, "Secrecy performance of a generalized partial relay selection protocol in underlay cognitive networks," *Int. J. Commun. Syst.*, vol. 31, no. 17, p. e3806, Nov. 2018.

DINH TUNG VO received the Engineering degree in electrical electronic engineering from the HCMC University of Technology and Education University, HCM city, Vietnam, in 1998, the master's degree in control and automation engineering from the Ho Chi Minh City University of Transport, HCM city, in 2008, and the Ph.D. degree in system analysis, control system, and data transfer from the Experimental Institute of Automotive Electronics and Electric Equipment, Ministry of Industry and Energy of the Russian Federation, Moscow, Russian Federation.

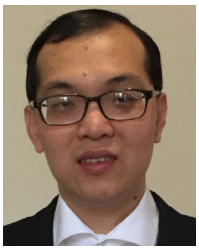
TRINH VAN CHIEN (Member, IEEE) received the B.S. degree in electronics and telecommunications from the Hanoi University of Science and Technology (HUST), Vietnam, in 2012, the M.S. degree in electrical and computer engineering from Sungkyunkwan University (SKKU), South Korea, in 2014, and the Ph.D. degree in communication systems from Linköping University (LiU), Sweden, in 2020. He was a Research Associate with the University of Luxembourg. He is currently with the School of Information and Communication Technology (SoICT), HUST. His research interests include convex optimization problems and machine learning applications for wireless communications and image and video processing. He received the Award of Scientific Excellence in the first year of the 5G Wireless Project funded by the European Union Horizon's 2020. He was the IEEE Wireless Communications Letters Exemplary Reviewer, in 2016, 2017, and 2021.

TAN N. NGUYEN (Member, IEEE) was born in Nha Trang, Vietnam, in 1986. He received the B.S. degree in electronics and telecommunications engineering from the Ho Chi Minh University of Natural Sciences, in 2008, the M.S. degree in electronics and telecommunications engineering from Vietnam National University, Ho Chi Minh City, Vietnam, in 2012, and the first Ph.D. degree in computer science, communication technology, and applied mathematics from the VSB Technical University of Ostrava, Czech Republic, in 2019, where he is currently pursuing the second Ph.D. degree in electrical engineering. He is a member of Vietnam National University. In 2013, he joined the Faculty of Electrical and Electronics Engineering, Ton Duc Thang University, Vietnam, where he has been a Lecturer. His major interests include cooperative communications, cognitive radio, and physical layer security.

DINH-HIEU TRAN (Student Member, IEEE) was born in Gia Lai, Vietnam, in 1989. He received the B.E. degree from the Electronics and Telecommunication Engineering Department, Ho Chi Minh City University of Technology, Vietnam, in 2012, the M.Sc. degree in electronics and computer engineering from Hongik University, South Korea, in 2017, and the Ph.D. degree in telecommunications engineering from the Interdiscipline Reliability and Trust (SnT) Research Center, University of Luxembourg, December 2021, under the supervision of Prof. Symeon Chatzinotas and Prof. Brn Ottersten. His major interests include UAV, satellite, the IoT, mobile edge computing, caching, and B5G for wireless communication networks. In 2016, he received the Hongik Rector Award for his excellence during the master's study. He was a co-recipient of the IS3C 2016 Best Paper Award. In 2021, he was nominated for the Best Ph.D. Thesis Award at the University of Luxembourg.

MIROSLAV VOZNAK (Senior Member, IEEE) received the Ph.D. degree in telecommunications from the Faculty of Electrical Engineering and Computer Science, VSB—Technical University of Ostrava, in 2002, and the Habilitation degree, in 2009. He was a Full Professor of electronics and communications technologies, in 2017. He has authored or coauthored over 100 articles indexed in SCI/SCIE journals. According to the Stanford University study released in 2020, he is one of the researchers who belong to Top 2 % of scientists in networking and telecommunications and information and communications technologies. He has 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. His research interests include ICT, especially on quality of service and experience, network security, wireless networks, and big data analytics. He served as the General Chair for 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.

BYUNG SEO KIM (Senior Member, IEEE) received the B.S. degree in electrical engineering from Inha University, Incheon, South Korea, in 1998, and the M.S. and Ph.D. degrees in electrical and computer engineering from the University of Florida, in 2001 and 2004, respectively. His Ph.D. study was supervised by Dr. Yuguang Fang. From 1997 to 1999, he was with Motorola Korea Ltd., Paju, South Korea, as a Computer Integrated Manufacturing (CIM) Engineer in advanced technology research and development (ATR&D). From January 2005 to August 2007, he was with Motorola Inc., Schaumburg Illinois, as a Senior Software Engineer in networks and enterprises, where his research focuses in designing protocol and network architecture of wireless broadband mission critical communications. From 2012 to 2014, he was the Chairperson with the Department of Software and Communications Engineering, Hongik University, South Korea, where he is currently a Professor. His work has appeared in around 167 publications and 22 patents. His research interests include the design and development of efficient wireless/wired networks, including linkadaptable/cross-layer-based protocols, multi-protocol structures, wireless CCNs/NDNs, mobile edge computing, physical layer design for broadband PLC, and resource allocation algorithms for wireless networks. He was served as a member for the Sejong Construction Review Committee and the Ansan Design Advisory Board. He served as the General Chair for third IWWCN 2017; and a TPC Member for the IEEE VTC 2014-Spring, the EAI FUTURE2016, and ICGHIC 2016 2019 Conferences. He served as the Guest Editor for special issues of *International Journal of Distributed Sensor Networks* (SAGE), IEEE Access, and *Journal of the Institute of Electrics and Information Engineers*. He is an Associative Editor of IEEE Access.



LAM THANH TU was born in Ho Chi Minh City, Vietnam. He received the B.Sc. degree in electronics and telecommunications engineering from the Ho Chi Minh City University of Technology, Vietnam, in 2009, the M.Sc. degree in telecommunications engineering from the Posts and Telecommunications Institute of Technology, Vietnam, in 2014, and the Ph.D. degree from the Laboratory of Signals and Systems, Paris-Saclay University, Paris, France, in 2018. He is currently a Research Fellow with the Xlim Research Institute, University of Poitiers, Poitiers, France. From 2015 to 2018, he was with the French National Center for Scientific Research (CNRS), Paris, as an Early Stage Researcher of the European-Funded Project H2020 ETN-5Gwireless. He was an Assistant Project Manager of the H2020 MCSA 5Gwireless and 5Gaura projects. His research interests include stochastic geometry, LoRa networks, physical layer security, energy harvesting, and machine learning applications for wireless communications. He was a recipient of the 2017 IEEE SigTelCom Best Paper Award. He was the IEEE Transactions on Communications Exemplary Reviewer, in 2016.