Security–Reliability Tradeoff Analysis for SWIPT- and AF-Based IoT Networks With Friendly Jammers

Tan N. Nguyen, *Member, IEEE*, Dinh-Hieu Tran, *Graduate Student Member, IEEE*, Trinh Van Chien, *Member, IEEE*, Van-Duc Phan, Miroslav Voznak, *Senior Member, IEEE*, Phu Tran Tin, Symeon Chatzinotas, *Senior Member, IEEE*, Derrick Wing Kwan Ng, *Fellow, IEEE*, and H. Vincent Poor, *Life Fellow, IEEE*

***Abstract*—Radio-frequency (RF) energy harvesting (EH) in wireless relaying networks has attracted considerable recent interest, especially for supplying energy to relay nodes in the Internet of Things (IoT) systems to assist the information exchange between a source and a destination. Moreover, limited hardware, computational resources, and energy availability of IoT devices have raised various security challenges. To this end, physical-layer security (PLS) has been proposed as an effective alternative to cryptographic methods for providing information security. In this study, we propose a PLS approach for simultaneous wireless information and power transfer (SWIPT)-based half-duplex (HD) amplify-and-forward (AF) relaying systems in the presence of an eavesdropper. Furthermore, we take into account both static power splitting relaying (SPSR) and dynamic power splitting relaying (DPSR) to thoroughly investigate the benefits of each one. To further enhance secure communication, we consider multiple friendly jammers to help prevent wiretapping attacks from the eavesdropper. More specifically, we provide a reliability and security analysis by deriving closed-form expressions of outage probability (OP) and intercept probability (IP), respectively, for both the SPSR and DPSR schemes. Then, simulations are also performed to validate our analysis and the effectiveness of the proposed schemes. Specifically, numerical results illustrate the nontrivial tradeoff between reliability and security of the proposed system. In addition, we conclude from the simulation results that the proposed DPSR scheme outperforms the SPSR-based scheme in terms of OP and IP under the influences of different parameters on system performance.**

***Index Terms*—Amplify and forward (AF), dynamic power splitting (PS), intercept probability (IP), outage probability (OP), source selection, simultaneous wireless information and power transfer (SWIPT).**

Manuscript received 26 January 2022; revised 26 April 2022; accepted 6 June 2022. Date of publication 14 June 2022; date of current version 24 October 2022. This work was supported in part by Van Lang University, Vietnam; in part by the Industrial University of Ho Chi Minh City (IUH) under Grant 131/HD-DHCN; in part by the Australian Research Council's Discovery Project under Grant DP210102169; and in part by the Ministry of Education, Youth and Sports of the Czech Republic under Grant SP2021/25 and Grant e-INFRA CZ (ID:90140). *(Corresponding author: Van-Duc Phan.)*

Tan N. Nguyen is with the Communication and Signal Processing Research Group, Faculty of Electrical and Electronics Engineering, Ton Duc Thang University, Ho Chi Minh City 70000, Vietnam (e-mail: nguyennhattan@tdtu.edu.vn).

Dinh-Hieu Tran and Symeon Chatzinotas are with the Interdisciplinary Centre for Security, Reliability and Trust, The University of Luxembourg, 1855 Luxembourg city, Luxembourg (e-mail: hieu.tran-dinh@uni.lu; symeon.chatzinotas@uni.lu).

Trinh Van Chien is with the School of Information and Communication Technology, Hanoi University of Science and Technology, Hanoi 100000, Vietnam (e-mail: chientv@soict.hust.edu.vn).

Van-Duc Phan is with the Faculty of Automotive Engineering and the School of Engineering and Technology, Van Lang University, Ho Chi Minh City 700000, Vietnam (e-mail: duc.pv@vlu.edu.vn).

Miroslav Voznak is with the Department of Telecommunications, VSB—Technical University of Ostrava, Ostrava 70800, Czech Republic (e-mail: miroslav.voznak@vsb.cz).

Phu Tran Tin is with the Faculty of Electronics Technology, Industrial University of Ho Chi Minh City, Ho Chi Minh City 727000, Vietnam (e-mail: phutrantin@iuh.edu.vn).

Derrick Wing Kwan Ng is with the School of Electrical Engineering and Telecommunications, University of New South Wales, Sydney, NSW 2052, Australia (e-mail: w.k.ng@unsw.edu.au).

H. Vincent Poor is with the Department of Electrical and Computer Engineering, Princeton University, Princeton, NJ 08544 USA (e-mail: poor@princeton.edu).

I. Introduction

THE Internet of Things (IoT) has played a pivotal role in fifth generation (5G) and beyond networks, seen as a novel solution to enable a smarter and safer life via autonomous monitoring and control in fields, such as healthcare, manufacturing, and agriculture as demonstrated in [1]–[7] and the reference therein. Nevertheless, the enormous number of potential IoT devices also impose technical challenges in wireless communication due to limited resources comprising, for example, available bandwidth and energy supply. In particular, replacing or recharging batteries for IoT devices is generally costly, inconvenient, and even impossible in many scenarios, such as hazardous or toxic environments or inside the human body. Smart ways of using and harvesting energy in IoT devices have attracted particular interest.

A. Related Works

To address these issues, energy harvesting (EH) communication networks are considered as alternative solutions. Energy can be harvested from sources such solar [8], wind [9], [10], vibration [11], [12], and radio-frequency (RF) signals, among which RF-based EH is an attractive solution because of its controllability and predictability. More importantly, it can carry both energy and information. Based on the above discussion, simultaneous wireless information and power transfer (SWIPT) is a promising future direction for realizing sustainable wireless communication [13]. There are two kinds of EH

receivers used in SWIPT networks: 1) time switching (TS) and 2) power splitting (PS) techniques. For the TS technique, the receiving node switches between information transfer (IT) and EH in different time slots, whereas, in the PS method, it splits the received power into factors for IT and EH [14], [15].

Beyond the benefits of EH, relay nodes in cooperative communication networks can help a source node transfer information to a destination, which can extend the coverage of IoT devices with inherent limitations, such as low power and remote location [16]–[19]. Therefore, cooperative relay networks with EH have received significant attention from researchers in recent years [20]–[27]. For example, amplify-and-forward (AF)-based wireless cooperative or sensor networks with TS and PS protocols were considered [20]. Also, Chen *et al.* [21] proposed and investigated a novel multihop AF relaying network in terms of co-channel interference (CCI) and Nakagami-*m* fading, whereas each user could harvest energy from the CCI. In contrast to [20], [21] and [28] which considered only SISO systems, a multiple-input–multiple-output (MIMO) system for maximizing the efficiency of SWIPT was investigated in [22]. Furthermore, the system performance of cognitive radio networks (CRNs) was studied in [23] and [24], and the system performance of bidirectional relay networks was considered in [25]. Besides, Tin *et al.* [26] proposed a new EH-based two-way (TW) half-duplex (HD) relay sensor network in the presence of a direct link between a transmitter and a receiver. Specifically, they derived the exact and asymptotic ergodic capacity and performed an exact analysis of the symbol error rate. Furthermore, Nguyen *et al.* [27] also proposed and investigated a new system model for SWIPT-based TW relaying systems. Therein, they derived closed-form expressions for the outage probability (OP) of three relaying schemes, termed decode-and-forward (DF), AF, and hybrid-DF (HDAF). In addition, An *et al.* [29] considered hybrid time–PS (HTPS) TW HD cooperative relaying in the presence of an eavesdropper. In this context, they derived closed-form expressions for OP and intercept probability (IP) using the maximal ratio combining (MRC) and the selection combining (SC). Tin *et al.* [30] investigated physical-layer security (PLS) in a power beacon-assisted full-duplex (FD) EH relaying system using delay-tolerant (DT) and delay-limited (DL) methods. It was shown that the OP can be significantly improved by applying a dynamic PS scheme in [31] and an adaptive PS scheme as in [32] and [33]. Ye *et al.* [31] considered a novel dynamic asymmetric PS scheme based on asymmetric instantaneous channel gains between relay and destinations to improve the OP. Ashraf *et al.* [32] proposed an adaptive PS protocol to enhance OP performance and average achievable capacity. Moreover, Singh and Ochiai [33] took into account the combination of the TS protocol and the dynamic PS to demonstrate the superiority of their proposed scheme in terms of OP and data transmission rate over the TS and PS schemes.

Due to the broadcast nature of the wireless medium, information in IoT networks can be easily overheard, thus, the problem of enhancing security in IoT communications is an important issue. In comparison with conventional upper layer security methods, PLS has many advantages, such as: 1) uncomplicated secret key distribution and management due to independence in encryption/decryption operations; 2) simple signal processing operations that involve minor additional overhead; and 3) adaptive signal design and resource allocation with flexible security levels. Based on these advantages, PLS represents a promising solution for IoT networks [34]–[39]. In [40], secrecy outage performance (SOP) using transmit antenna selection (TAS)/SC of multihop cognitive wireless sensor networks was investigated, and secure performance in a dual-hop MIMO relay system with outdated channel state information (CSI) was evaluated in [41]. Also, Tran *et al.* [42] proposed and analyzed a generalized partial relay selection (PRS) protocol to improve security for CRNs with both cases of perfect or imperfect CSI. Moreover, Hieu *et al.* [43] also considered a novel system model for an EH-based PLS multihop multipath cooperative wireless network. They then proposed three relay protocols, termed the shortest path, the random path, and the best path selection schemes to enhance PLS performance. A power allocation scheme to improve the PLS of the relay network was presented in [44], and Shukla *et al.* [45] proposed user selection along with an antenna selection (AS) scheme to maximize the end-to-end signal-to-noise ratios (SNRs) of a cellular multiuser TW AF relay network. In addition, a novel wireless caching scheme to enhance the PLS of video streaming in cellular networks was proposed in [46] and [47]; and the influence of an eavesdropper and CCI on IP was considered in [48].

Despite the fruitful research in the literature, the aforementioned works in [34]–[48] did not take into account jammers or artificial noises (ANs) to improve system security. Recently, intensive works have brought ANs and jammers into consideration [49]–[55]. To prevent the eavesdropper from intercepting transmitted signals, Oggier and Hassibi [49] studied the employment of multiple transmit antennas for generating AN to interfere with the eavesdropper without disturbing the legitimate receiver. It was shown in [49] that wireless secrecy can be guaranteed with the aid of AN if the transmitter has more antennas than the eavesdropper. Wang *et al.* [50] investigated secure communication of a MIMO system, in which the source, destination, and eavesdropper are each equipped with a random number of antennas. In [51]–[53], distributed beamforming or friendly jammers were deployed in the relay networks to prevent the eavesdropper from overhearing confidential information. Zou *et al.* [54], [55] studied multiuser scheduling as a method to enhance the system PLS.

B. Motivation and Contributions

Despite previous achievements in the above-mentioned works, the investigation of SWIPT and PLS in cooperative IoT networks still has room for research in terms of the closed-form expressions for the OP and IP, which are independent of small-scale fading coefficients and can work for a long period of time. Moreover, to the best of our knowledge, there is no such related work on designing the optimal dynamic PS scheme for a SWIPT- and AF-based relay network consisting of multiple sources, multiple friendly jammers, an EH relay, and a destination in the presence of an eavesdropper.

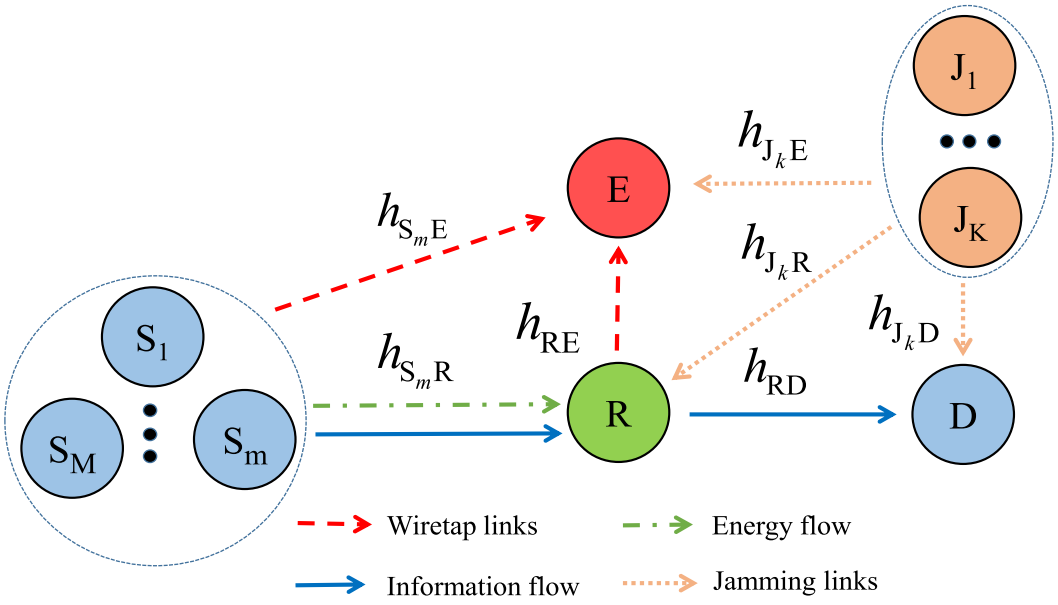


Fig. 1. SWIPT-based relay system with friendly jammers against attack from an eavesdropper.

Motivated by the above discussions, this article provides a thorough analysis of the reliability and security tradeoff using PS-based relay protocol. The best source approach is proposed to enhance performance with the effect of an eavesdropper and the presence of friendly jammers to prevent this eavesdropper. The main contributions of this research can be summarized as follows.

1) We derive closed-form expressions for the OP of the legitimate communications and an exact integral form for the IP of the eavesdropper's channel under the assistance from multiple friendly jammers.
2) This work also provides an in-depth analysis of the influence of various system parameters on security and reliability performance. For the SWIPT technique, both dynamic PS-based relaying (DPSR) and static PS-based relaying (SPSR) are considered in our work to give a full picture of the advantages of each method for OP and IP cases.
3) Mathematical analysis is given to obtain an exact closed-form expression for the optimal PS ratio, i.e., $\rho^{\star}$, to maximize the total achievable rate at the destination.
4) The correctness of our analysis is confirmed through numerical simulations. From the simulation results, we provide recommendations on selecting the configurations to obtain reliable and secure transmission without paying too much for the complexity of the system.

The remainder of this article is organized as follows. The system model is given in Section II. The performance is presented in Section III. Numerical results are depicted in Sections IV and V concludes this article.

II. System Model

As described in Fig. 1, the system model includes multi-source (M source nodes) transfer information to the destination (D) via one relay (R) with the presence of multi friendly jammers ($J_1, \ldots, J_K$) and an eavesdropper (E). Friendly jammers are legitimate users in the system and emit AN using a pseudorandom sequence, which is known to other legitimate users (i.e., source, relay, and destination) and remains unknown to eavesdropper E [56]. It should be noted that these pseudorandom sequences are known among legitimate users but not to the illegitimate user. Moreover, similar to conventional cryptography, pseudorandom sequences do not have to be preshared, they can be acquired by legitimate users through physical-layer key agreement and generation that supports channel estimation, as intensively studied in the information-theoretic PLS literature [57], [58]. Particularly, the wireless system is assumed to change the pseudorandom sequence frequently, which significantly reduces the possibility that an eavesdropper can know all of these sequences and enhances system security.

We assume that the direct connection between the M sources and the destination nodes is too weak due to severe fading or long distances, hence, the only available communication path as well as power transfer path is through relay R. We also assume that E is located far away from M sources and cannot overhear the messages transmitted from these sources. All nodes in this model are single-antenna devices and operate on the HD mode. The EH and information transmission processes for the model system are shown in Fig. 2. In Fig. 2, we exploit the first phase to supply the required power to the relay from the best source S to help the relay forward the exchange data afterward. Specifically, the relay R utilizes a power splitter to divide the received signal into two parts, whereas the first part is used for collecting energy and storing it in the battery, while the second part is used for transferring received data. We define ρ as a PS ratio, i.e., the ratio of the power received at the relay node used for the EH. Next, the IT process from R to D is conducted in the remaining time period [59]–[61].

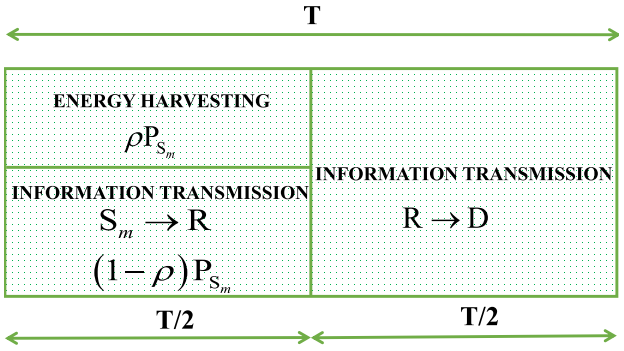


Fig. 2. EH and IT processes with PS relaying protocol.

Assuming the channel coefficient between any two nodes follows Rayleigh fading in which the channel is unchanged within a transmission block and to vary independently on different blocks. Let h_{XY} with $\mathrm{XY} \in \{S_m R, \mathrm{RE}, \mathrm{RD}, \mathrm{JE}, \mathrm{JR}, \mathrm{JD}\}$ denote the channel from $X \rightarrow Y$, then the corresponding channel gains can be defined as follows:

$$\gamma_{\mathrm{XY}} = |h_{\mathrm{XY}}|^2, \mathrm{XY} \in \{S_m R, \mathrm{RE}, \mathrm{RD}, \mathrm{JE}, \mathrm{JR}, \mathrm{JD}\}. \quad (1)$$

Notice that the channel gains are assumed to be exponential random variables in which probability density function (PDF) and cumulative distribution function (CDF) are, respectively, represented as follows:

$$F_X(x) = 1 - \exp(-\lambda x) \quad (2)$$

$$f_X(x) = \frac{\partial F_{\mathrm{X}}(x)}{\partial x} = \lambda \exp(-\lambda x) \quad (3)$$

where λ is the rate parameter of the exponential random variable X. To take path-loss into account, we can model the parameters as follows:

$$\lambda_{\mathrm{XY}} = (d_{\mathrm{XY}})^{\chi} \quad (4)$$

where χ is the pathloss exponent and d_{XY} is distance between nodes X and Y.

Now, we discuss the adopted system model. As mention above, supposing source S_m is chosen to send its information and energy. During the first transmission phase, the received signal at the relay can be given by

$$y_R = \sqrt{1-\rho} h_{S_m R} x_{S_m} + \sum_{k=1}^{K} x_k h_{J_k R} + n_R \quad (5)$$

where x_{S_m} is the message transmitted with $\mathbb{E}\{|x_{S_m}|^2\} = P_S$; x_k is the AN transmitted by the jammer J_k, which satisfies $\mathbb{E}\{|x_k|^2\} = P_J$, $\mathbb{E}\{\cdot\}$ denotes the expectation operation; and n_R is the zero mean additive white Gaussian noise (AWGN) with variance N_0. Our proposed model only considers the multifriendly jammers, which are just against the eavesdropper. Hence, relay R and destination D will know the jamming signals and cancel them in their received signals. So, the received signal at R can be rewritten as follows:

$$y_R = \sqrt{1-\rho} h_{S_m R} x_{S_m} + n_R. \quad (6)$$

Following the same methodology as in [62], the EH in relay can be computed as:

$$P_R = \frac{E_R}{T/2} = \eta \rho P_{S_m} \gamma_{S_m R} \quad (7)$$

where $0 < \eta \leq 1$ is energy conversion efficiency (which takes into account the energy loss by harvesting circuits and also by decoding and processing circuits); and P_{S_m} and P_R are the transmit powers of S_n and R, respectively. E_R is the amount of the harvested energy at the relay and it can be calculated as $E_R \triangleq \eta \rho P_{S_m} \gamma_{S_m R} T/2$. The channel gain $\gamma_{S_m R}$ is defined as $\gamma_{S_m R} = |h_{S_m R}|^2$, which is a special case of (1). Besides, $\rho \in [0, 1]$ is the PS factor, where ρ equals zero (or one) signifies that total received RF signals used for EH (or information transmission).

As mentioned above, the received signal at the destination can be given as follows:

$$y_D = h_{\mathrm{RD}} x_R + n_D \quad (8)$$

where n_D is the zero mean AWGN with variance N_0.

In this article, we consider the AF relaying protocol. Therefore, the signal transmitted by the relay is an amplified version of y_R, which is denoted by a factor β as follows:

$$\beta = \frac{x_R}{y_R} = \sqrt{\frac{P_R}{(1-\rho) P_{S_m} |h_{S_m R}|^2 + N_0}} \approx \sqrt{\frac{\eta \rho}{1-\rho}}. \quad (9)$$

From (6) and (9), the received signal at D can be rewritten by

$$\begin{aligned} y_D &= h_{\mathrm{RD}} x_R + n_D = h_{\mathrm{RD}} \beta y_R + n_D \\ &= h_{\mathrm{RD}} \beta \left[\sqrt{1-\rho} h_{S_m R} x_{S_m} + n_R \right] + n_D \\ &= \underbrace{\sqrt{1-\rho} h_{\mathrm{RD}} h_{S_m R} \beta x_{S_m}}_{\text{signal}} + \underbrace{h_{\mathrm{RD}} \beta n_R + n_D}_{\text{noise}}. \end{aligned} \quad (10)$$

Hence, the SNR at D in this phase can be obtained by

$$\gamma_D = \frac{E\{|\text{signal}|^2\}}{E\{|\text{noise}|^2\}} = \frac{(1-\rho) P_{S_m} \gamma_{S_m R} \gamma_{\mathrm{RD}} \beta^2}{\gamma_{\mathrm{RD}} \beta^2 N_0 + N_0}. \quad (11)$$

After some algebraic manipulations, we have

$$\gamma_D = \frac{\eta \rho (1-\rho) \Psi \gamma_{S_m R} \gamma_{\mathrm{RD}}}{\eta \rho \gamma_{\mathrm{RD}} + (1-\rho)} \quad (12)$$

where $\Psi = (P_S/N_0)$. The achievable rate of system can be claimed by

$$C_{\mathrm{AF}} = \frac{1}{2} \log_2(1 + \gamma_D). \quad (13)$$

Taking into account the impact of eavesdropper E, at the first time slot the chosen source S_m will broadcast its signal to relay and E can overhear this information. To prevent E from eavesdropping legitimate information, jammers will send the jamming signals to E, so the received signal at E can be expressed by

$$y_E^1 = h_{S_m E} x_{S_m} + h_{\mathrm{RE}} x_R + \sum_{k=1}^{K} x_k h_{J_k E} + n_E \quad (14)$$

where n_E[1] is the zero mean AWGN with variance N_0. Based on (14), the SNR at the E during first time slot is given as follows:

$$\gamma_E^1 = \frac{P_{S_m}\gamma_{S_mE}}{P_J\sum_{k=1}^{K}\gamma_{J_kE}+N_0} = \frac{\Psi\gamma_{S_mE}}{\Phi\Xi+1} \approx \frac{\Psi\gamma_{S_mE}}{\Phi\Xi} \quad (15)$$

where $\Phi = (P_J/N_0)$ and $\Xi = \sum_{k=1}^{K}\gamma_{J_kE}$. Here, please note that after received the information from chosen source S_m, R will amplify this information to D, and also to E with the same amplification factor β. Therefore, the received signal at E can be reexpressed by

$$\begin{aligned} y_E^2 &= h_{\mathrm{RE}}\beta\left[\sqrt{1-\rho}h_{S_mR}x_{S_m}+n_R\right]+\sum_{k=1}^{K}x_kh_{J_kR}+n_E^2 \\ &= \underbrace{\sqrt{1-\rho}h_{S_mR}h_{\mathrm{RE}}\beta x_{S_m}}_{\text{signal}} + \underbrace{h_{\mathrm{RE}}\beta n_R+\sum_{k=1}^{K}x_kh_{J_kE}+n_E^2}_{\text{noise}} \end{aligned} \quad (16)$$

where n_E^2 is the zero mean AWGN with variance N_0. Hence, the received SNR at E during second time slot can be obtained as follows:

$$\begin{aligned} \gamma_E^2 &= \frac{(1-\rho)\gamma_{S_mR}\gamma_{\mathrm{RE}}\beta^2P_{S_m}}{\gamma_{\mathrm{RE}}\beta^2N_0+P_J\sum_{k=1}^{K}\gamma_{J_kE}+N_0} \\ &= \frac{\eta\rho(1-\rho)\gamma_{S_mR}\gamma_{\mathrm{RE}}\Psi}{\eta\rho\gamma_{\mathrm{RE}}+(1-\rho)\Phi\Xi+(1-\rho)}. \end{aligned} \quad (17)$$

Finally, the eavesdropper can apply SC technique, thus, the achievable rate at E can be given by

$$C_E = \frac{1}{2}\log_2(1+\gamma_E) \quad (18)$$

where $\gamma_E = \max\left(\gamma_E^1, \gamma_E^2\right)$.

Remark 1: The best source $\mathrm{S_m}$ would be selected for the purpose of enhancing the transmission performance. Mathematically speaking, we can write as followings:

$$\begin{aligned} n &\triangleq \arg \max_{m=1,2,\ldots,M} \{\gamma_{S_mR}\} \\ \Leftrightarrow \gamma_{S_mR} &\triangleq \max_{m=1,2,\ldots,M} \{\gamma_{S_mR}\}. \end{aligned} \quad (19)$$

Assume that the links from M sources to the relay R are identical independent distribution (i.i.d), and hence CDF and PDF of γ_{S_mR} can be formulated as, respectively

$$\begin{aligned} F_{\gamma_{S_mR}}(x) &= \Pr(\gamma_{S_mR} < x) \\ &= \Pr(\gamma_{S_mR} < x, \forall m = 1,2,\ldots,M) \\ &= \prod_{m=1}^{M} F_{\gamma_{S_mR}}(x) = \left[1-e^{-\lambda_{S_mR}x}\right]^M \\ &= 1+\sum_{b=1}^{M}(-1)^bC_M^b\exp(-b\lambda_{\mathrm{SR}}x), \end{aligned} \quad (20)$$

$$f_{\gamma_{S_mR}}(x) = \lambda_{\mathrm{SR}}\sum_{b=1}^{M-1}(-1)^bC_{M-1}^b\exp(-(b+1)\lambda_{\mathrm{SR}}x) \quad (21)$$

where $C_M^b = (M!/b!(M-b)!)$.

Remark 2: Because Ξ is a summation of K i.i.d. exponential random variables, its PDF can be given by [63]

$$f_\Xi(x) = \frac{(\lambda_{\mathrm{JE}})^K}{(K-1)!}x^{K-1}\exp(-\lambda_{\mathrm{JE}}x). \quad (22)$$

III. Performance Analysis

This section provides the mathematical analysis of the OP and IP to provide further insight into the two-hop data transmission for SWIPT-based HD AF relay networks in two cases, i.e., DPSR and SPSR.

A. SPSR Case

1) Outage Probability Analysis: In this section, the OP of the SWIPT-aided HD AF relaying system over Rayleigh fading channels is derived. Specifically, it can be calculated as follows:

$$\mathrm{OP} = \Pr(C_{AF} < C_{th}) = \Pr(\gamma_D < \gamma_{th}) \quad (23)$$

where $\gamma_{th} = 2^{2C_{th}} - 1$ is the SNR threshold of system and C_{th} is the target rate. The closed-form expression for the OP in (23) is given as follows.

Theorem 1: In static PS-based relaying, the closed-form expression of the OP can be given as follows:

$$\begin{aligned} \mathrm{OP}_{\mathrm{SPSR}} &= 1+2\sum_{b=1}^{M}(-1)^bC_M^b\exp\left(-\frac{b\lambda_{\mathrm{SR}}\lambda_{th}}{(1-\rho)\Psi}\right) \\ &\times \sqrt{\frac{b\lambda_{\mathrm{SR}}\lambda_{\mathrm{RD}}\gamma_{th}}{\eta\rho\Psi}}K_1\left(2\sqrt{\frac{b\lambda_{\mathrm{SR}}\lambda_{\mathrm{RD}}\gamma_{th}}{\eta\rho\Psi}}\right) \end{aligned} \quad (24)$$

where $K_v(\cdot)$ is the modified Bessel function of the second kind and the fifth order.

Proof: The detailed proof is available in Appendix A. ■

2) Intercept Probability Analysis: Destination D will be intercepted if E can successfully wiretap signal, i.e., $C_E \geq C_{th}$. Therefore, the IP can be defined as [64]

$$\mathrm{IP} = \Pr(C_E \geq C_{th}) = \Pr(\gamma_E \geq \gamma_{th}). \quad (25)$$

Theorem 2: The closed-form expression of the IP in this case can be derived by

$$\begin{aligned} \mathrm{IP}_{\mathrm{SPSR}} &= \left(\frac{\lambda_{\mathrm{JE}}}{\tilde{\lambda}_{\mathrm{JE}}}\right)^K + \sum_{t=0}^{\infty}\sum_{b=1}^{M}\frac{(-1)^{b+t}C_M^b\Gamma(t+K)}{t!\Phi^{t+K}} \\ &\times \exp\left(-\frac{b\lambda_{\mathrm{SR}}\gamma_{th}}{\rho_1\Psi}\right) \\ &\times \frac{(\lambda_{\mathrm{JE}})^K}{(K-1)!}\times G_{1,3}^{3,0}\left(\frac{b\lambda_{\mathrm{SR}}\lambda_{\mathrm{RE}}\gamma_{th}}{\eta\rho\Psi}\middle|\begin{matrix}0\\-t-K,1,0\end{matrix}\right) \\ &\times \left[\left(\tilde{\lambda}_{\mathrm{JE}}\right)^t-(\lambda_{\mathrm{JE}})^t\right] \end{aligned} \quad (26)$$

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

Proof: The detailed proof is available in Appendix B. ■

TABLE I
SIMULATION PARAMETERS

Symbol	Parameter name	Fixed value	Varying range
C_{th}	Source rate	0.25; 0.5 bps/Hz	none
η	Energy harvesting efficiency	0.8	none
ρ	Power splitting factor	0.225; 0.325; 0.5; 0.875; 0.915	0 to 1
$\lambda_{\mathrm{S_m R}}$	Rate parameter of $\lvert h_{\mathrm{S}_m\mathrm{R}}\rvert^2$	0.1768	none
λ_{RD}	Rate parameter of $\lvert h_{\mathrm{RD}}\rvert^2$	0.1768	none
λ_{RE}	Rate parameter of $\lvert h_{\mathrm{RE}}\rvert^2$	2.7557 (S1); 1.3216 (S2)	none
λ_{JE}	Rate parameter of $\lvert h_{\mathrm{JE}}\rvert^2$	0.1768 (S1); 1 (S2)	none
λ_{SE}	Rate parameter of $\lvert h_{\mathrm{SE}}\rvert^2$	3.1434 (S1); 1 (S2)	none
Ψ	Transmit-power-to-noise-ratio of source	2 dB	-5 to 15 (dB)
Φ	Transmit-power-to-noise-ratio of jammer	-1;1 dB	none
M	Number of source node(s)	2; 3	1 to 10
K	Number of jammer(s)	1	1 to 10

B. DPSR Case

In this section, we would like to find the optimal PS factor, i.e., $\rho^\star$ to maximize the achievable rate C_{AF}. By observing (13), we have $\max(C_{\mathrm{AF}}) \Leftrightarrow \max(\gamma_D)$. It is easy to prove that $(\partial^2\gamma_D/\partial^2\rho)$ is negative for all $0 < \rho < 1$. Hence, we conclude that γ_D is a concave function of ρ. We can find the value of ρ to maximize γ_D by differentiating γ_D concerning ρ and then equate it to zero. After doing some algebraic calculations, $\rho^\star$ can be given as $\rho^* = (1/[1+|h_{\mathrm{RD}}|\sqrt{\eta}])$ or $\rho^* = (1/[1-|h_{\mathrm{RD}}|\sqrt{\eta}])$. Because of $\rho^* = (1/[1-|h_{\mathrm{RD}}|\sqrt{\eta}])$ results in the value of $\rho^* > 1$ or $\rho^* < 0$. Therefore, $\rho^* = (1/[1+|h_{\mathrm{RD}}|\sqrt{\eta}])$ is selected as the optimal solution.

Theorem 3: The closed-form expression of the OP in this case can be derived by

$$\begin{aligned}\mathrm{OP}_{\mathrm{DPSR}} = 1 + \sum_{t=0}^{\infty}\sum_{b=1}^{M}\frac{(-1)^{t+b}C_M^b 2^{t+1}}{t!} \\ \times \left(\frac{\lambda_{\mathrm{RD}}}{\eta}\right)^{t/4+1/2}\left(\frac{b\lambda_{\mathrm{SR}}\gamma_{th}}{\Psi}\right)^{3t/4+1/2} \\ \times \exp\left(-\frac{b\lambda_{\mathrm{SR}}\gamma_{th}}{\Psi}\right) \times K_{-t/2+1}\left(2\sqrt{\frac{b\lambda_{\mathrm{SR}}\lambda_{\mathrm{RD}}\gamma_{th}}{\eta\Psi}}\right)\end{aligned} \tag{27}$$

where $K_v(\cdot)$ is the modified Bessel function of the second kind and v^{th} order.

Proof: The detailed proof is available in Appendix C. ■

1) IP Analysis:

Theorem 4: In dynamic PS-based relaying, the exact integral-form expression of the IP is derived as follows:

$$\begin{aligned}\mathrm{IP}_{\mathrm{DPSR}} = \left(\frac{\lambda_{\mathrm{JE}}}{\tilde{\lambda}_{\mathrm{JE}}}\right)^K + 2\sum_{b=1}^{M}\frac{(-1)^b C_M^b(\lambda_{\mathrm{JE}})^K}{(K-1)!} \\ \times \exp\left(-\frac{b\lambda_{\mathrm{SR}}\gamma_{th}}{\Psi}\right) \times \sqrt{\frac{b\lambda_{\mathrm{SR}}\lambda_{\mathrm{RE}}\gamma_{th}}{\eta\Psi}} \\ \times \left[\int_0^\infty x^{K-1}\exp\left(-\tilde{\lambda}_{\mathrm{JE}}x\right)\Delta(\omega)\sqrt{(\Phi x+1)}dx\right. \\ \left. - \int_0^\infty x^{K-1}\exp(-\lambda_{\mathrm{JE}}x)\Delta(\omega)\sqrt{(\Phi x+1)}dx\right].\end{aligned} \tag{28}$$

We have obtained the analytical results in Theorems 1–4, which are independent of small-scale fading coefficients and only based on the statistical CSI. The obtained analyses work for a long period of time and reduce the computational complexity in evaluating the OP and IP of the network.

Remark 3: This article considers scenarios where the jammers are closer to the eavesdropper than the relay. Hence, the RF transmission from friendly jammers was neglected for the sake of simplicity. Once the information of jammers is carefully exploited, both eavesdropper (E) and destination (D) will get benefits to enhance the system performance. A framework using the RF transmission from friendly jammers shares a similar analytical methodology as initially established in this article but with more complicated in detail. This interesting extension is left for future work.

IV. SIMULATION RESULTS

In this section, Monte Carlo simulations are provided to validate the theoretical expressions and the impacts of various parameters on the system performance. To claim the OP and IP for the proposed schemes, we perform 5×10^6 independent trials, and the channel coefficients are randomly generated as Rayleigh fading in each trial. The settings of simulation parameters are detailed in Table I. In particular, we provide two scenarios in other to investigate the system performance corresponding to different node deployments. In the first scenario (S1), sources are located around $(0, 0)$, the relay is located at $(0.5, 0)$, the destination is located at $(1, 0)$, and the eavesdropper is located closer to the relay at $(0.5, 1.5)$. In the second scenario (S2), sources, relay, and destination are kept the same locations, while the eavesdropper is located closer to the sources at $(0, 1)$. The average channel gains, $\mathbb{E}\{\gamma_{\mathrm{XY}}\}$ are computed by utilizing (1), where the propagation distances are obtained from the above setting. Furthermore, the rate parameters λ_{S_mR}, λ_{RD}, λ_{JE}, λ_{RE}, and λ_{SE} are given in Table I. The system performance metrics comprising the OP and IP are evaluated as a function of different parameters.

In Figs. 3 and 4, we show the impact of Ψ on OP and IP, where $\eta = 0.8$, $C_{th} = 0.5$ bps/Hz, and $M = 2$. In Fig. 3, we compare DPSR with SPSR in OP analysis, whereas the SPSR is considered in two modes with ρ equals 0.225 and 0.875, respectively. First, it is easy to observe that DPSR obtains

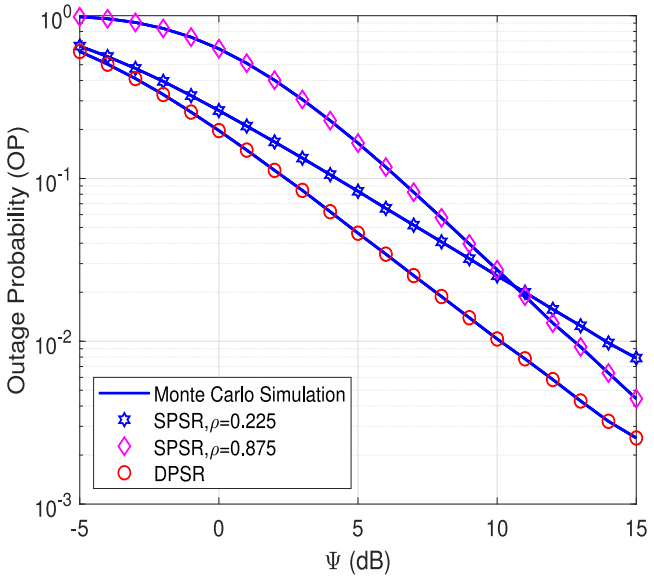


Fig. 3. OP versus Ψ with $C_{th} = 0.5$ bps/Hz, $\eta = 0.8$, and $M = 2$.

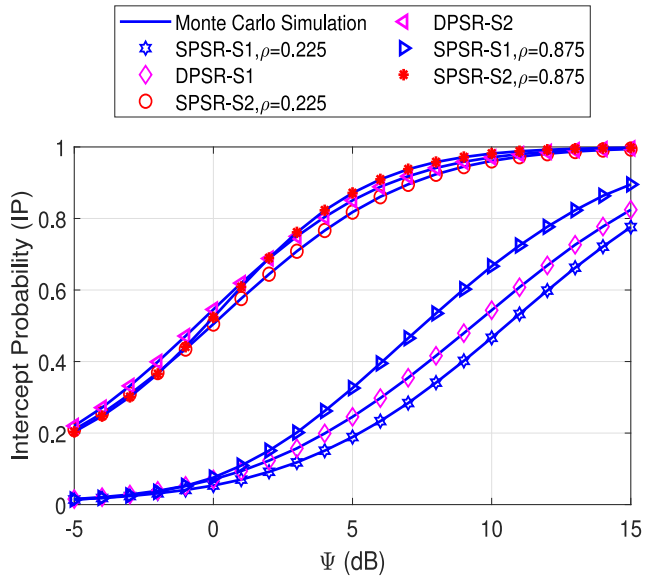


Fig. 4. IP versus Ψ with $C_{th} = 0.5$ bps/Hz, $\eta = 0.8$, $M = 2$, $K = 1$, and $\Phi = 1$ dB.

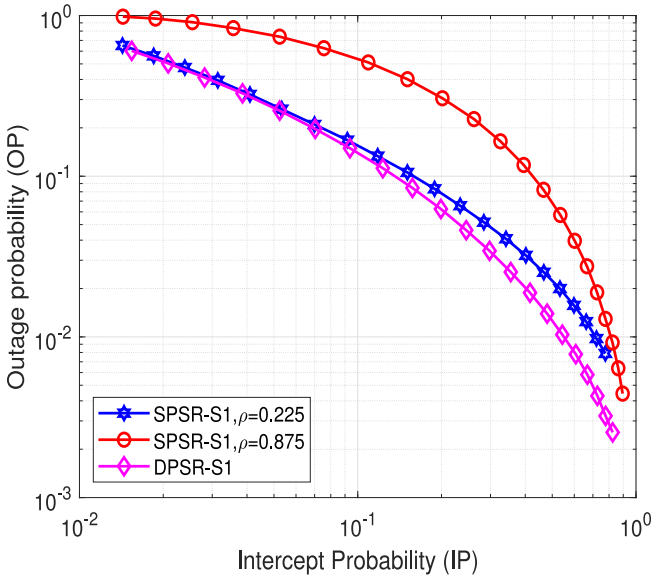


Fig. 5. OP versus IP in scenario 1 with $C_{th} = 0.5$ bps/Hz, $\eta = 0.8$, $M = 2$, $K = 1$, $\Phi = 1$ dB, and $\Psi \in [-5, 15\, dB]$.

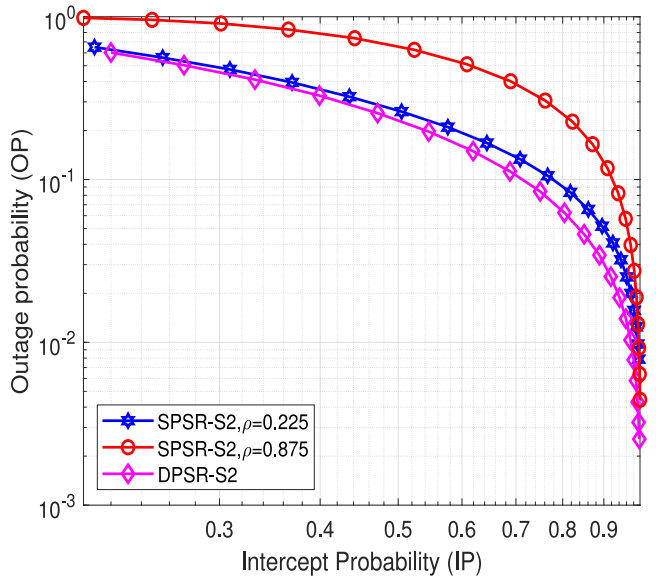


Fig. 6. OP versus IP in scenario 2 with $C_{th} = 0.5$ bps/Hz, $\eta = 0.8$, $M = 2$, $K = 1$, $\Phi = 1$ dB, and $\Psi \in [-5, 15\, dB]$.

better OP results than SPSR methods. Specifically, when $\Psi = 15$ dB, the OP of DPSR approximately reach to $10^{-2.7}$, while the SPSBR with $\rho = 0.225$ and $\rho = 0.875$ impose 0.0025 and 0.0079, respectively. This is because the DPSR scheme aims to maximize the system capacity, thus it can improve the outage performance while the SPSR scheme always selects a fixed value of PS factor ρ. Second, the higher the Ψ value is, the better the OP can be obtained. It can be explained by the fact that the higher Ψ value means transmit power of source S is assigned more, which is defined in (24). In Fig. 4, the IP in both the DPSR and SPSR cases is studied, where $\eta = 0.8$, $C_{th} = 0.5$ bps/Hz, $M = 2$, $K = 1$, and $\Phi = 1$ dB. It can be seen that the intercept performance increases with a higher value of Ψ. It is anticipated because the eavesdropper has more ability to overhear the message with a higher source transmit power S_m. When the value of Ψ is large enough, the IP in all schemes can converge to 1. An interesting thing in Fig. 4 is that the SPSR in S2 obtains better IP performance as compared to the case in the first scenario. When $-5 \leq \Psi \leq 1$, the IP value of SPSR with $\rho = 0.875$ is better than that of the SPSR with $\rho = 0.225$. Otherwise, when $\Psi > -1$ dB, the IP value of the SPSR with $\rho = 0.875$ is higher than that of SPSR with $\rho = 0.225$. As $-5 \leq \Psi \leq 0$ dB, the DPSR does not play a significant role compared with the other benchmarks since the PS factor ρ is only optimized for the received signal strength of a specific legitimate user. For the eavesdropper, the IP gets higher as the PS factor ρ gets larger, which is a consequence of the high transmit power of relay R. This observation is applied for all the considered benchmarks. In Figs. 3 and 4, simulations agree with the analytical values, which confirms our mathematical derivations' correctness.

In Figs. 5 and 6, we investigate security–reliability trade-off for S1 and S2 with the same parameter as in Figs. 3

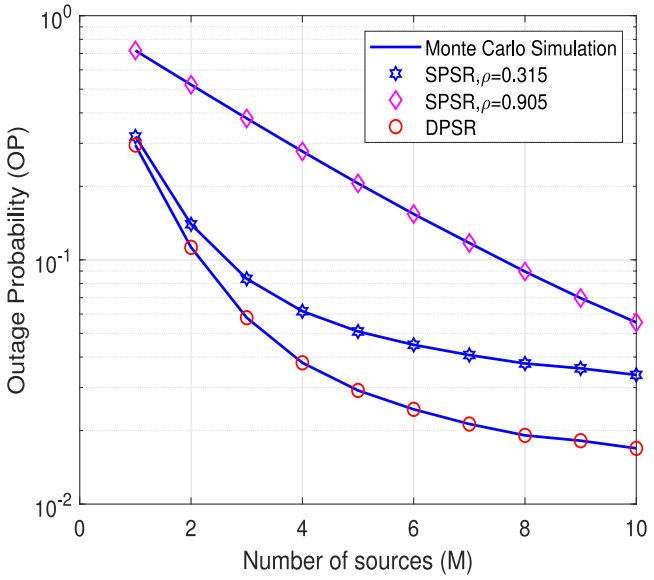


Fig. 7. OP versus number of sources (M) with $C_{th} = 0.5$ bps/Hz, $\eta = 0.8$, and $\Psi = 2$ dB.

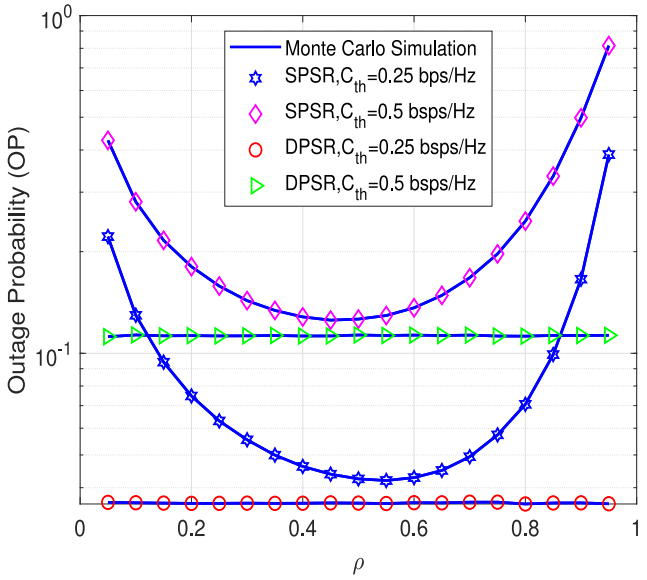


Fig. 9. OP versus ρ with $\eta = 0.8$, $M = 2$, $\Psi = 2$ dB, $\Phi = 1$ dB, and $K = 1$.

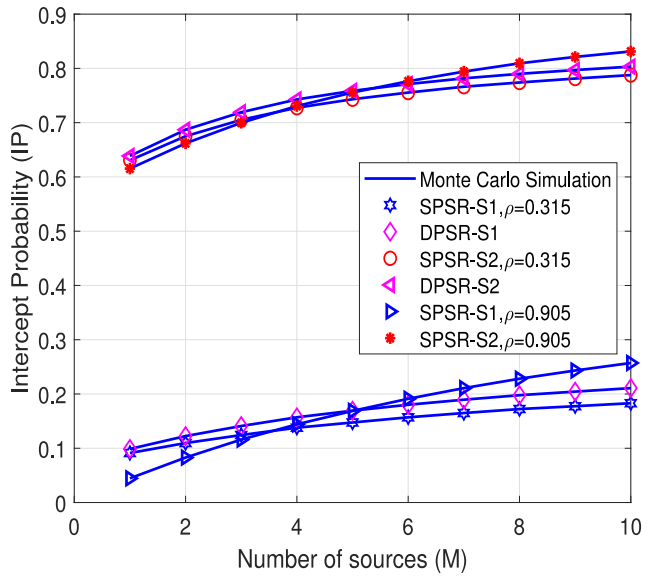


Fig. 8. IP versus number of sources (M) with $C_{th} = 0.5$ bps/Hz, $\eta = 0.8$, $K = 1$, $\Phi = 1$ dB, and $\Psi = 2$ dB.

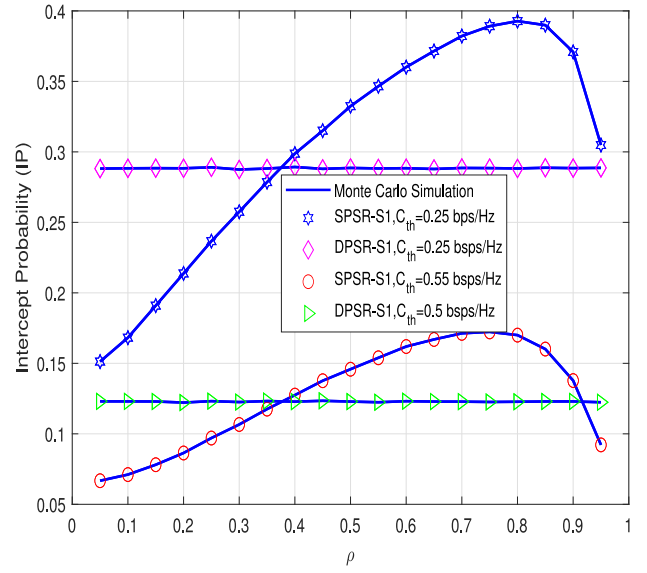


Fig. 10. IP versus ρ with $\eta = 0.8$, $M = 2$, and $\Psi = 2$ dB.

and 4. Nonetheless, these results demonstrate the benefits of our theoretical analysis. As observed in these figures, with increasing IP, the OP decrease and vice versa, indicating a tradeoff between security and reliability. Figs. 5 and 6 also shows that the DPSR method can provide the best IP and OP value. However, this requires us to tradeoff the choice that if we want the system obtains a better outage performance, it will be easier for the eavesdropper to steal information, on the contrary, if we want to restrict eavesdropping, we also reduce the outage performance.

Figs. 7 and 8 study the impact of the number of sources M on the OP and IP, respectively. Herein, simulation parameters are set as $C_{th} = 0.5$ bps/Hz, $\eta = 0.8$, $\Psi = 2$ dB, $K = 1$, and $\Phi = 1$ dB. Fig. 7 shows a better OP as the number of sources increases, i.e., M varies from 1 to 10. It is because, by increasing M, we will have more options to transmit information to the destination and choose the best source S_m. Moreover, the OP of DPSR is still better than that of other SPSR cases. However, as shown in Fig. 8, the IP will also increase by using a larger number of sources. Once again, this shows the tradeoff between security and reliability.

In Figs. 9 and 10, we study OP and IP depending on different PS factor ρ, where $\eta = 0.8$, $M = 2$, $\Psi = 2$ dB, $\Phi = 1$ dB, and $K = 1$. The ρ value plays an important role since it influences not only the amount of harvested energy at the relay but also the data transmission from $R \to D$. Therefore, there exists an optimal value of PS factor ρ to maximize OP. Particularly, the OP of DPSR obtain the best performance compared to the two SPSR schemes since this method always optimizes the ρ value during the system design. It also explains for the fact that why the DPSR curses are straight lines because DPSR does not depend on ρ value. Besides, the DPSR scheme always obtains the best OP performance and that does not

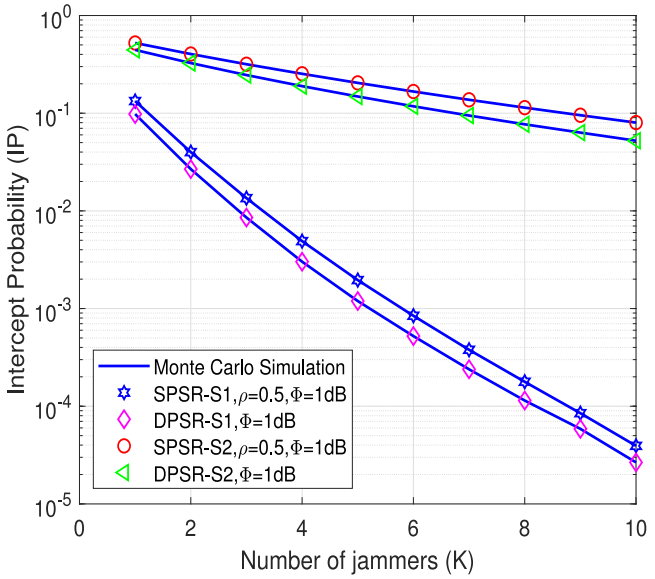


Fig. 11. IP versus number of jammers (K) with $\eta = 0.8$, $\rho = 0.5$, $M = 3$, and $\Psi = 2$ dB.

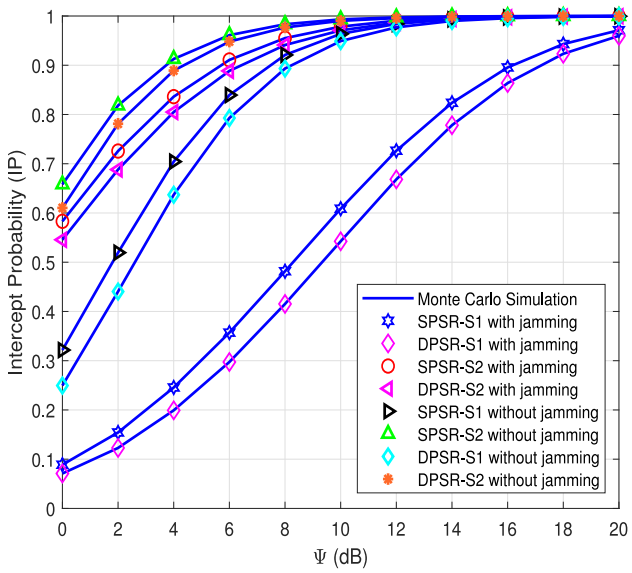


Fig. 12. IP versus Ψ with and without jamming cases.

mean it will have the worst IP performance, which is verified in Fig. 10. This result is consistent with the result in Fig. 4. For instance, when $0.35 < \rho < 0.9$, the DPSR scheme has a better IP value than the SPSR scheme. In order to provide an explicit explanation, we first observe that the IP is directly proportional to the PS factor as $0.35 < \rho < 0.9$. In contrast, the DPSR yields the performance independent of the variation of ρ since this benchmark exploits the optimal value ρ^* as shown in Section III-B. Furthermore, it holds that $\rho^* < \rho$ on average and, therefore, the strength of the received signal by the DPSR is better than the SPSR. Consequently, the DPSR provides lower IP than the SPSR. Here again, the reliability-security tradeoff phenomenon also happens in both figures.

To reduce the IP as well as the eavesdropping ability of E, we will consider the effect of the number of jammers as shown in Fig. 11. In this figure, we can see that this will be consistent with reality because increasing K will cause more jamming signals to be sent to E and reduce its SNR ratio and its ability to overhear from the relay. Furthermore, in this figure, we compared DPSR with SPSR in IP analysis, while SPSR is considered in two cases with Φ equals -1 and 1 dB, respectively. It is easy to see that if the jammers' transmit power Φ is reduced, the jamming signal will be weaker and it is difficult to suppress the effect of the eavesdropping devices.

In Fig. 12, we investigate the IP as a fuction of Ψ (dB) for the case with and without jamming, where $\eta = 0.8$, $C_{\text{th}} = 0.5$ bps/Hz, $M = 2$, $K = 1$, $\rho = 0.55$, and $\Phi = 1$ dB. First, it can be observed from Fig. 12 that the intercept performance of the SPSR schemes is much better than that as compared to the DPSR ones, which has been explained in other figures. Furthermore, the intercept performance of the SPSR and DPSR with jamming is lower than that compared to without jamming scenarios. This is expected since the eavesdropper gains higher SNR in the case of no jamming signals. Thus, it has a higher probability to successfully decode the received signals from the source and relay. Specifically, when Ψ equals 2 and 4 dB, the IP of SPSR-S1 (or DPSR-S1) with jamming is 0.1542 (or 0.1228) and 0.2456 (or 0.1992), respectively. Meanwhile, the IP of the SPSR-S1 (or DPSR-S1) without jamming imposes 0.5194 (or 0.4404) and 0.7043 (or 0.6370), respectively. Moreover, the intercept performance of the S2 is better than that as compared to the S1. This is because the eavesdropper is located closer to sources in S2, thus it has a further distance to the jammer than the S1 case. Consequently, the jammer has less effect on the eavesdropper in S2 than S1 schemes.

V. Conclusion and Future Directions

In this article, we have studied PLS for an AF-based SWIPT relay network consisting of multiple sources, multiple friendly jammers, an EH relay, and a destination in the presence of an eavesdropper. We have investigated the reliability-security tradeoff performance of DPSR and SPSR schemes in terms of the IP and OP. Furthermore, the impact of system parameters on network performance, and the correctness of the analytical expressions have been verified and investigated by using Monte Carlo simulations. Based on plots of the OP versus IP, we can recommend suitable system parameters to meet the predefined requirements on IP and OP. Particularly, a sufficient number of friendly jammers can significantly enhance system security by reducing the SNR at the eavesdropper. The results of this article can provide guidance for securing IoT networks in which the confidentiality in information transmission is important. An interesting topic for further exploration in this area is the extension to cases in which source and eavesdropping nodes have multiple antennas.

The outcome of this work will motivate a more general model that considers a direct link between source and destination, which imposes new challenges and complexities but might enhance network performance.

Appendix A
Proof of Theorem 1

Based on the definition of the OP in (23) with the SNR in (12), $\mathrm{OP}_{\mathrm{SPSR}}$ can be expressed as follows:

$$\begin{aligned}\mathrm{OP}_{\mathrm{SPSR}} &= \Pr\left(\frac{\eta\rho(1-\rho)\Psi\gamma_{S_mR}\gamma_{\mathrm{RD}}}{\eta\rho\gamma_{\mathrm{RD}}+(1-\rho)} < \gamma_{th}\right)\\ &= \Pr\left(\gamma_{S_mR} < \frac{\gamma_{th}(\eta\rho\gamma_{\mathrm{RD}}+(1-\rho))}{\eta\rho(1-\rho)\Psi\gamma_{\mathrm{RD}}}\right)\\ &= \int_0^\infty F_{\gamma_{S_mR}}\left\{\frac{\gamma_{th}(\eta\rho x+(1-\rho))}{\eta\rho(1-\rho)\Psi x}\right\} f_{\gamma_{\mathrm{RD}}}(x)dx \quad (29)\end{aligned}$$

where the CDF of γ_{S_mR} is given in (20) and the PDF of $f_{\gamma_{\mathrm{RD}}}(x)$ is given in (3). By utilizing (20), we obtain the following expression:

$$\begin{aligned}&F_{\gamma_{S_mR}}\left\{\frac{\gamma_{th}(\eta\rho x+(1-\rho))}{\eta\rho(1-\rho)\Psi x}\right\}\\ &= 1+\sum_{b=1}^{M}(-1)^b C_M^b \exp\left(-\frac{b\lambda_{\mathrm{SR}}\gamma_{th}}{\eta\rho\Psi x}-\frac{b\lambda_{\mathrm{SR}}\gamma_{th}}{(1-\rho)\Psi}\right). \quad (30)\end{aligned}$$

After that, by plugging (3) and (30) into (29), $\mathrm{OP}_{\mathrm{SPSR}}$ can be represented as follows:

$$\begin{aligned}\mathrm{OP}_{\mathrm{SPSR}} &= 1+\sum_{b=1}^{M}(-1)^b C_M^b \exp\left(-\frac{b\lambda_{\mathrm{SR}}\lambda_{th}}{(1-\rho)\Psi}\right)\\ &\quad\times\ \lambda_{\mathrm{RD}}\int_0^\infty \exp\left(-\frac{b\lambda_{\mathrm{SR}}\gamma_{th}}{\eta\rho\Psi x}-\lambda_{\mathrm{RD}}x\right)dx. \quad (31)\end{aligned}$$

With the help of [65, 3.324.1] and some algebraic manipulations, we obtain (24), which completes the proof.

Appendix B
Proof of Theorem 2

Based on (15), (17), (18), and (25), the $\mathrm{IP}_{\mathrm{SPSR}}$ can be rewritten by

$$\begin{aligned}\mathrm{IP}_{\mathrm{SPSR}} &= 1-\Pr(\alpha<\gamma_{th})\\ &= 1-\int_0^\infty \Pr(\max(\vartheta_1,\vartheta_2)<\gamma_{th})f_{\Xi}(x)dx\\ &= 1-\int_0^\infty Q(x)f_{\Xi}(x)dx \quad (32)\end{aligned}$$

where $\alpha = \max([\Psi\gamma_{S_mE}]/[\Phi\Xi], [\eta\rho(1-\rho)\Psi\gamma_{S_mR}\gamma_{\mathrm{RE}}]/[\eta\rho\gamma_{\mathrm{RE}}+(1-\rho)\Phi\Xi+(1-\rho)])$ and the following definitions hold:

$$\vartheta_1 \triangleq \frac{\Psi\gamma_{S_mE}}{\Phi x} \quad (33)$$

$$\vartheta_2 \triangleq \frac{\eta\rho(1-\rho)\gamma_{S_mR}\gamma_{\mathrm{RE}}\Psi}{\eta\rho\gamma_{\mathrm{RE}}+(1-\rho)\Phi x+(1-\rho)} \quad (34)$$

$$\begin{aligned}Q(x) &\triangleq \Pr(\max(\vartheta_1,\vartheta_2)<\gamma_{th})\\ &= \underbrace{\Pr(\vartheta_1<\gamma_{th})}_{Q_1(x)}\times\underbrace{\Pr(\vartheta_2<\gamma_{th})}_{Q_2(x)}. \quad (35)\end{aligned}$$

From (35), $Q_1(x)$ and $Q_2(x)$ can be calculated by

$$\begin{aligned}Q_1(x) &= \Pr\left(\frac{\Psi\gamma_{S_mE}}{\Phi x}<\gamma_{th}\right)=\Pr\left(\gamma_{S_mE}<\frac{\gamma_{th}\Phi x}{\Psi}\right)\\ &= 1-\exp\left(-\frac{\gamma_{th}\lambda_{\mathrm{SE}}\Phi x}{\Psi}\right) \quad (36)\end{aligned}$$

$$\begin{aligned}Q_2(x) &= \Pr\left(\frac{\eta\rho\rho_1\Psi\gamma_{S_mR}\gamma_{\mathrm{RE}}}{\eta\rho\gamma_{\mathrm{RE}}+\rho_1\Phi x+\rho_1}<\gamma_{th}\right)\\ &= \Pr\left\{\gamma_{S_mR}<\frac{\gamma_{th}(\eta\rho\gamma_{\mathrm{RE}}+\rho_1\Phi x+\rho_1)}{\eta\rho\rho_1\gamma_{\mathrm{RE}}\Psi}\right\}\\ &= \int_0^\infty F_{\gamma_{S_mR}}\left\{\frac{\gamma_{th}(\eta\rho y+\rho_1\Phi x+\rho_1)}{\eta\rho\rho_1 y\Psi}\right\}f_{\gamma_{\mathrm{RE}}}(y)dy \quad (37)\end{aligned}$$

where $\rho_1 \triangleq (1-\rho)$. By using the same approach as what has done in (30) to the last equation of (37), we obtain the closed-form expression of $Q_2(x)$

$$\begin{aligned}Q_2(x) &= 1+2\sum_{b=1}^{M}(-1)^b C_M^b \exp\left(-\frac{b\lambda_{\mathrm{SR}}\gamma_{th}}{\rho_1\Psi}\right)\\ &\quad\times\sqrt{\frac{b\lambda_{\mathrm{SR}}\lambda_{\mathrm{RE}}\gamma_{th}(\Phi x+1)}{\eta\rho\Psi}}K_1\left(2\sqrt{\frac{b\lambda_{\mathrm{SR}}\lambda_{\mathrm{RE}}\gamma_{th}(\Phi x+1)}{\eta\rho\Psi}}\right). \quad (38)\end{aligned}$$

Following the same methodology as done to obtain the result in (24), we obtain the closed-form expression of $Q_2(x)$ as:

$$\begin{aligned}Q_2(x) &= 1+2\sum_{b=1}^{M}(-1)^b C_M^b \exp\left(-\frac{b\lambda_{\mathrm{SR}}\gamma_{th}}{\rho_1\Psi}\right)\\ &\quad\times\sqrt{\frac{b\lambda_{\mathrm{SR}}\gamma_{\mathrm{RE}}\gamma_{th}(\Phi x+1)}{\eta\rho\Psi}}\times K_1\left(2\sqrt{\frac{b\lambda_{\mathrm{SR}}\gamma_{\mathrm{RE}}\gamma_{th}(\Phi x+1)}{\eta\rho\Psi}}\right). \quad (39)\end{aligned}$$

Based on (22), (36), and (39), the $\mathrm{IP}_{\mathrm{SPSR}}$ in (32) can be reformulated as in (40), shown at the bottom of the next page, where $\tilde{\lambda}_{\mathrm{JE}} = ([\gamma_{th}\lambda_{\mathrm{SE}}\Phi]/\Psi)+\lambda_{\mathrm{JE}}$. Thanks to [65, 3.381.4], Υ_1 in (40) can be calculated as follows:

$$\Upsilon_1 = \left(\frac{\lambda_{\mathrm{JE}}}{\tilde{\lambda}_{\mathrm{JE}}}\right)^K. \quad (41)$$

By applying Taylor series for $\exp(-\lambda_{\mathrm{JE}}x) = \sum_{t=0}^{\infty}([(-\tilde{\lambda}_{\mathrm{JE}}x)^t]/t!) = \sum_{t=0}^{\infty}([(-1)^t(\tilde{\lambda}_{\mathrm{JE}})^t]/t!)x^t$ and by changing the variable $y=\Phi x+1$, Υ_2 can be rewritten as follows:

$$\begin{aligned}\Upsilon_2 &= \sum_{t=0}^{\infty}\frac{(-1)^t\left(\tilde{\lambda}_{\mathrm{JE}}\right)^t}{t!\Phi^{t+K}}\int_1^\infty y^{1/2}(y-1)^{t+K-1}\\ &\quad\times\ K_1\left(2\sqrt{\frac{b\lambda_{\mathrm{SR}}\lambda_{\mathrm{RE}}\gamma_{th}y}{\eta\rho\Psi}}\right)dy. \quad (42)\end{aligned}$$

Next, by using [65, 6.592.4], the above equation can be reformulated by

$$\begin{aligned}\Upsilon_2 &= \sum_{t=0}^{\infty}\frac{(-1)^t\left(\tilde{\lambda}_{\mathrm{JE}}\right)^t\Gamma(t+K)}{t!\Phi^{t+K}}\times\left(2\sqrt{\frac{b\lambda_{\mathrm{SR}}\lambda_{\mathrm{RE}}\gamma_{th}}{\eta\rho\Psi}}\right)^{-1}\\ &\quad\times\ G_{1,3}^{3,0}\left(\frac{b\lambda_{\mathrm{SR}}\lambda_{\mathrm{RE}}\gamma_{th}}{\eta\rho\Psi}\middle|\begin{matrix}0\\-t-K,1,0\end{matrix}\right) \quad (43)\end{aligned}$$

where $\Gamma(\cdot)$ is the Gamma function and $G_{p,q}^{m,n}\left(z\middle|\begin{matrix}a_1,\ldots,a_p\\b_1,\ldots,b_q\end{matrix}\right)$ is the Meijer G-function. By applying the same approach for (43), Υ_3 can be formulated as follows:

$$\Upsilon_3 = \sum_{t=0}^{\infty}\frac{(-1)^t(\lambda_{\mathrm{JE}})^t\Gamma(t+K)}{t!\Phi^{t+K}}\times\left(2\sqrt{\frac{b\lambda_{\mathrm{SR}}\lambda_{\mathrm{RE}}\gamma_{th}}{\eta\rho\Psi}}\right)^{-1}$$

$$\times\ G_{1,3}^{3,0}\left(\frac{b\lambda_{\mathrm{SR}}\lambda_{\mathrm{RE}}\gamma_{th}}{\eta\rho\Psi}\Big|\begin{matrix}0\\-t-K,1,0\end{matrix}\right). \tag{44}$$

Finally, by substituting (41), (43), and (44), the $\mathrm{IP}_{\mathrm{SPSR}}$, we obtain (26). This is the end of the proof.

Appendix C
Proof of Theorem 3

Substituting the optimal $\rho^* = (1/[1+|h_{\mathrm{RD}}|\sqrt{\eta}])$ into (29), the $\mathrm{OP}_{\mathrm{DPSR}}$ is expressed as follows:

$$\begin{aligned}
&\mathrm{OP}_{\mathrm{DPSR}}\\
&= \Pr\left(\frac{\eta\Psi\gamma_{S_mR}\gamma_{\mathrm{RD}}}{\left(1+\sqrt{\eta\gamma_{\mathrm{RD}}}\right)^2} < \gamma_{th}\right)\\
&= \Pr\left(\gamma_{S_mR} < \frac{\gamma_{th}\left(1+2\sqrt{\eta\gamma_{\mathrm{RD}}}+\eta\gamma_{\mathrm{RD}}\right)}{\eta\Psi\gamma_{\mathrm{RD}}}\right)\\
&= \int_0^{\infty} F_{\gamma_{S_mR}}\left(\frac{\gamma_{th}\left(1+2\sqrt{\eta x}+\eta x\right)}{\eta\Psi x}\right)\times f_{\gamma_{\mathrm{RD}}}(x)dx\\
&= 1+\sum_{b=1}^{M}(-1)^b C_M^b \exp\left(-\frac{b\lambda_{\mathrm{SR}}\gamma_{th}}{\Psi}\right)\\
&\int_0^{\infty}\lambda_{\mathrm{RD}}\exp\left(-\frac{2b\lambda_{\mathrm{SR}}\gamma_{th}}{\Psi\sqrt{\eta x}}\right)\exp\left(-\frac{b\lambda_{\mathrm{SR}}\gamma_{th}}{\eta\Psi x}-\lambda_{\mathrm{RD}}x\right)dx.
\end{aligned} \tag{45}$$

By adopting Taylor series for $\exp(-([2b\lambda_{\mathrm{SR}}\gamma_{th}]/\Psi\sqrt{\eta x})) = \sum_{t=0}^{\infty}([(-1)^t 2^t]/t!)([b\lambda_{\mathrm{SR}}\gamma_{th}]/[\Psi\sqrt{\eta}])^t x^{-t/2}$, (45) can be rewritten as follows:

$$\begin{aligned}
&\mathrm{OP}_{\mathrm{DPSR}}\\
&= 1+\sum_{t=0}^{\infty}\sum_{b=1}^{M}\frac{(-1)^{t+b}C_M^b 2^t\lambda_{\mathrm{RD}}}{t!}\left(\frac{b\lambda_{\mathrm{SR}}\gamma_{th}}{\Psi\sqrt{\eta}}\right)^t\\
&\exp\left(-\frac{b\lambda_{\mathrm{SR}}\gamma_{th}}{\Psi}\right)\int_0^{\infty}x^{-t/2}\exp\left(-\frac{b\lambda_{\mathrm{SR}}\gamma_{th}}{\eta\Psi x}-\lambda_{\mathrm{RD}}x\right)dx.
\end{aligned} \tag{46}$$

Finally, by applying [65, 3.471.9], we obtain (27), which finishes the proof.

Appendix D
Proof of Theorem 4

By substituting $\rho^* = (1/[1+|h_{\mathrm{RD}}|\sqrt{\eta}])$ into (32), Q_2^* can be calculated as follows:

$$\begin{aligned}
Q_2^*(w) &= \Pr\left(\frac{\eta\gamma_{S_mR}\gamma_{\mathrm{RE}}\Psi}{\eta\Phi_1\gamma_{\mathrm{RE}}+\Phi_2\Phi x+\Phi_2} < \gamma_{th}\right)\\
&= \int_0^{\infty}\underbrace{\Pr\left(\frac{\eta\gamma_{S_mR}\gamma_{\mathrm{RE}}\Psi}{\eta\Phi_3\gamma_{\mathrm{RE}}+\Phi_4\Phi x+\Phi_4} < \gamma_{th}\right)}_{\Theta} f_{\gamma_{\mathrm{RD}}}(\omega)d\omega
\end{aligned} \tag{47}$$

where $\Phi_1 \triangleq ([1+\sqrt{\gamma_{\mathrm{RD}}\eta}]/[\sqrt{\gamma_{\mathrm{RD}}\eta}])$, $\Phi_2 \triangleq 1+\sqrt{\gamma_{\mathrm{RD}}\eta}$, $\Phi_3 \triangleq ([1+\sqrt{\eta w}]/[\sqrt{\eta w}])$, and $\Phi_4 \triangleq 1+\sqrt{w\eta}$. Based on (21) and then with the help of [65, 3.324.1], Θ can be computed as follows:

$$\begin{aligned}
\Theta(x) &= \Pr\left(\frac{\eta\gamma_{S_mR}\gamma_{\mathrm{RE}}\Psi}{\eta\Phi_3\gamma_{\mathrm{RE}}+\Phi_4\Phi x+\Phi_4} < \gamma_{th}\right)\\
&= \int_0^{\infty}\Pr\left(\gamma_{S_mR} < \frac{\gamma_{th}(\eta\Phi_3 z+\Phi_4\Phi x+\Phi_4)}{\eta z\Psi}\right)f_{\gamma_{\mathrm{RE}}}(z)dz\\
&= 1+\sum_{b=1}^{M}(-1)^b C_M^b\exp\left(-\frac{b\lambda_{\mathrm{SR}}\gamma_{th}\Phi_3}{\Psi}\right)\\
&= 1+\sum_{b=1}^{M}(-1)^b C_M^b\exp\left(-\frac{b\lambda_{\mathrm{SR}}\gamma_{th}\Phi_3}{\Psi}\right)\\
&\quad\times\int_0^{\infty}\lambda_{\mathrm{RE}}\exp\left(-\frac{b\lambda_{\mathrm{SR}}\gamma_{th}(\Phi x+1)\Phi_4}{\eta z\Psi}-\lambda_{\mathrm{RE}}z\right)dz\\
&= 1+2\sum_{b=1}^{M}(-1)^b C_M^b\exp\left(-\frac{b\lambda_{\mathrm{SR}}\gamma_{th}\Phi_3}{\Psi}\right)\\
&\quad\times\sqrt{\frac{b\lambda_{\mathrm{SR}}\lambda_{\mathrm{RE}}\gamma_{th}(\Phi x+1)\Phi_4}{\eta\Psi}}\\
&\quad\times K_1\left(2\sqrt{\frac{b\lambda_{\mathrm{SR}}\lambda_{\mathrm{RE}}\gamma_{th}(\Phi x+1)\Phi_4}{\eta\Psi}}\right).
\end{aligned} \tag{48}$$

$$\begin{aligned}
\mathrm{IP}_{\mathrm{SPSR}} &= 1-\int_0^{\infty}\left\{1-\exp\left(-\frac{\gamma_{th}\lambda_{\mathrm{SE}}\Phi x}{\Psi}\right)\right\}\left\{\begin{matrix}1+2\sum_{b=1}^{M}(-1)^b C_M^b\exp\left(-\frac{b\lambda_{\mathrm{SR}}\gamma_{th}}{\rho_1\Psi}\right)\\ \times\sqrt{\frac{b\lambda_{\mathrm{SR}}\lambda_{\mathrm{RE}}\gamma_{th}(\Phi x+1)}{\eta\rho\Psi}}\\ \times K_1\left(2\sqrt{\frac{b\lambda_{\mathrm{SR}}\lambda_{\mathrm{RE}}\gamma_{th}(\Phi x+1)}{\eta\rho\Psi}}\right)\end{matrix}\right\}\frac{(\lambda_{\mathrm{JE}})^K}{(K-1)!}x^{K-1}\exp(-\lambda_{\mathrm{JE}}x)dx\\
&= \underbrace{\frac{(\lambda_{\mathrm{JE}})^K}{(K-1)!}\int_0^{\infty}x^{K-1}\exp\left(-x\tilde{\lambda}_{\mathrm{JE}}\right)dx}_{\Upsilon_1}+2\sum_{b=1}^{M}(-1)^b C_M^b\exp\left(-\frac{b\lambda_{\mathrm{SR}}\gamma_{th}}{\rho_1\Psi}\right)\\
&\quad\times\frac{(\lambda_{\mathrm{JE}})^K}{(K-1)!}\sqrt{\frac{b\lambda_{\mathrm{SR}}\lambda_{\mathrm{RE}}\gamma_{th}}{\eta\rho\Psi}}\left\{\begin{matrix}\underbrace{\int_0^{\infty}x^{K-1}\exp\left(-x\tilde{\lambda}_{\mathrm{JE}}\right)\times\sqrt{(\Phi x+1)}\times K_1\left(2\sqrt{\frac{b\lambda_{\mathrm{SR}}\lambda_{\mathrm{RE}}\gamma_{th}(\Phi x+1)}{\eta\rho\Psi}}\right)dx}_{\Upsilon_2}\\ -\underbrace{\int_0^{\infty}x^{K-1}\exp(-\lambda_{\mathrm{JE}}x)\sqrt{(\Phi x+1)}\times K_1\left(2\sqrt{\frac{b\lambda_{\mathrm{SR}}\lambda_{\mathrm{RE}}\gamma_{th}(\Phi x+1)}{\eta\rho\Psi}}\right)dx}_{\Upsilon_3}\end{matrix}\right\}
\end{aligned} \tag{40}$$

By substituting (48) into (22), the term Q_2^* can be reformulated as follows:

$$Q_2^*(w) = 1 + 2\sum_{b=1}^{M}(-1)^b C_M^b \exp\left(-\frac{b\lambda_{\rm SR}\gamma_{th}}{\Psi}\right) \times \sqrt{\frac{b\lambda_{\rm SR}\lambda_{\rm RE}\gamma_{th}(\Phi x+1)}{\eta\Psi}} \times \lambda_{\rm RD}\int_0^{\infty} \frac{\sqrt{1+\sqrt{\eta\omega}}\exp\left(-\frac{b\lambda_{\rm SR}\gamma_{th}}{\Psi\sqrt{\eta\omega}} - \lambda_{\rm RD}\omega\right)}{K_1\left(2\sqrt{\frac{b\lambda_{\rm SR}\lambda_{\rm RE}\gamma_{th}(\Phi x+1)(1+\sqrt{\eta\omega})}{\eta\Psi}}\right)} d\omega \tag{50}$$

$$= 1 + 2\sum_{b=1}^{M}(-1)^b C_M^b \exp\left(-\frac{b\lambda_{\rm SR}\gamma_{th}}{\Psi}\right) \times \sqrt{\frac{b\lambda_{\rm SR}\lambda_{\rm RE}\gamma_{th}(\Phi x+1)}{\eta\Psi}} \times \Delta(\omega) \tag{51}$$

where the following definition holds:

$$\Delta(\omega) \triangleq \lambda_{\rm RD}\int_0^{\infty} \sqrt{1+\sqrt{\eta\omega}}\exp\left(-\frac{b\lambda_{\rm SR}\gamma_{th}}{\Psi\sqrt{\eta\omega}} - \lambda_{\rm RD}\omega\right) \times K_1\left(2\sqrt{\frac{b\lambda_{\rm SR}\lambda_{\rm RE}\gamma_{th}(\Phi x+1)(1+\sqrt{\eta\omega})}{\eta\Psi}}\right) d\omega. \tag{52}$$

Finally, based on (32), (36), and (50), we claim (28), which completes the proof.

REFERENCES

[1] 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.

[2] X. Ge, R. Zhou, and Q. Li, "5G NFV-based tactile Internet for mission-critical IoT services," *IEEE Internet Things J.*, vol. 7, no. 7, pp. 6150–6163, Jul. 2020.

[3] Y. Liu, M. Peng, G. Shou, Y. Chen, and S. Chen, "Toward edge intelligence: Multiaccess edge computing for 5G and Internet of Things," *IEEE Internet Things J.*, vol. 7, no. 8, pp. 6722–6747, Aug. 2020.

[4] P. X. Nguyen *et al.*, "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.

[5] R. Cong, Z. Zhao, G. Min, C. Feng, and Y. Jiang, "EdgeGO: A mobile resource-sharing framework for 6G edge computing in massive IoT systems," *IEEE Internet Things J.*, early access, Mar. 11, 2021, doi: 10.1109/JIOT.2021.3065357.

[6] X. Fang, W. Feng, T. Wei, Y. Chen, N. Ge, and C.-X. Wang, "5G embraces satellites for 6G ubiquitous IoT: Basic models for integrated satellite terrestrial networks," *IEEE Internet Things J.*, vol. 8, no. 18, pp. 14399–14417, Sep. 2021.

[7] D.-H. Tran, V.-D. Nguyen, C. Symeon, T X. Vu, and B. Ottersten, "UAV relay-assisted emergency communications in IoT networks: Resource allocation and trajectory optimization," *IEEE Trans. Wireless Commun.*, vol. 21, no. 3, pp. 1621–1637, Mar. 2022.

[8] T. D. Hieu, L. T. Dung, and B.-S. Kim, "Stability-aware geographic routing in energy harvesting wireless sensor networks," *Sensors*, vol. 16, no. 5, p. 696, 2016.

[9] H.-J. Jung, J. Park, and I.-H. Kim, "Investigation of applicability of electromagnetic energy harvesting system to inclined stay cable under wind load," *IEEE Trans. Magn.*, vol. 48, no. 11, pp. 3478–3481, Nov. 2012.

[10] 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.

[11] Y. Sang, X. Huang, H. Liu, and P. Jin, "A vibration-based hybrid energy harvester for wireless sensor systems," *IEEE Trans. Magn.*, vol. 48, no. 11, pp. 4495–4498, Nov. 2012.

[12] J. Qiu, X. Liu, H. Chen, X. Xu, Y. Wen, and P. Li, "A low-frequency resonant electromagnetic vibration energy harvester employing the Halbach arrays for intelligent wireless sensor networks," *IEEE Trans. Magn.*, vol. 51, no. 11, pp. 1–4, Nov. 2015.

[13] H. Tran-Dinh, S. Chatzinotas, and B. Ottersten, "Throughput maximization for backscatter- and cache-assisted wireless powered UAV technology," *IEEE Trans. Veh. Technol.*, vol. 71, no. 5, pp. 5187–5202, May 2022.

[14] D. S. Gurjar, U. Singh, and P. K. Upadhyay, "Energy harvesting in hybrid two-way relaying with direct link under Nakagami-m fading," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, 2018, pp. 1–6.

[15] T. D. Hieu, T. T. Duy, S. G. Choi, and T. H. Dung, "Performance evaluation of relay selection schemes in beacon-assisted dual-hop cognitive radio wireless sensor networks under impact of hardware noises," *Sensors*, vol. 18, no. 6, p. 1843, 2018.

[16] V. Petrov *et al.*, "Vehicle-based relay assistance for opportunistic crowdsensing over narrowband IoT (NB-IoT)," *IEEE Internet Things J.*, vol. 5, no. 5, pp. 3710–3723, Oct. 2018.

[17] T.-T. Nguyen, T.-V. Nguyen, T.-H. Vu, D. B. D. Costa, and C. D. Ho, "IoT-based coordinated direct and relay transmission with non-orthogonal multiple access," *IEEE Wireless Commun. Lett.*, vol. 10, no. 3, pp. 503–507, Mar. 2021.

[18] T. Van Chien *et al.*, "Controlling smart propagation environments: Long-term versus short-term phase shift optimization," in *Proc. IEEE Int. Conf. Acoust. Speech Signal Process. (ICASSP)*, 2022, pp. 5348–5352.

[19] 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," *IEEE Open J. Veh. Technol.*, vol. 3, pp. 40–54, 2022.

[20] A. A. Nasir, X. Zhou, S. Durrani, and R. A. Kennedy, "Relaying protocols for wireless energy harvesting and information processing," *IEEE Trans. Wireless Commun.*, vol. 12, no. 7, pp. 3622–3636, Jul. 2013.

[21] E. Chen, M. Xia, D. B. da Costa, and S. Aïssa, "Multi-hop cooperative relaying with energy harvesting from cochannel interferences," *IEEE Commun. Lett.*, vol. 21, no. 5, pp. 1199–1202, May 2017.

[22] R. Zhang and C. K. Ho, "MIMO broadcasting for simultaneous wireless information and power transfer," *IEEE Trans. Wireless Commun.*, vol. 12, no. 5, pp. 1989–2001, May 2013.

[23] C. Xu, M. Zheng, W. Liang, H. Yu, and Y.-C. Liang, "Outage performance of underlay multihop cognitive relay networks with energy harvesting," *IEEE Commun. Lett.*, vol. 20, no. 6, pp. 1148–1151, Jun. 2016.

[24] F. Zeng, J. Xu, Y. Li, K. Li, and L. Jiao, "Performance analysis of underlay two-way relay cooperation in cognitive radio networks with energy harvesting," *Comput. Netw.*, vol. 142, pp. 13–23, Sep. 2018.

[25] T. N. Nguyen, P. T. Tran, and M. Vozňák, "Power splitting–based energy-harvesting protocol for wireless-powered communication networks with a bidirectional relay," *Int. J. Commun. Syst.*, vol. 31, no. 13, p. e3721, 2018.

[26] P. T. Tin, T. N. Nguyen, M. Tran, T. T. Trang, and L. Sevcik, "Exploiting direct link in two-way half-duplex sensor network over block Rayleigh fading channel: Upper bound ergodic capacity and exact SER analysis," *Sensors*, vol. 20, no. 4, p. 1165, 2020.

[27] 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.

[28] T. Van Chien, L. T. Tu, S. Chatzinotas, and B. Ottersten, "Coverage probability and ergodic capacity of intelligent reflecting surface-enhanced communication systems," *IEEE Commun. Lett.*, vol. 25, no. 1, pp. 69–73, Jan. 2021.

[29] N. H. 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, 2020.

[30] 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, 2020.

[31] Y. Ye, Y. Li, Z. Wang, X. Chu, and H. Zhang, "Dynamic asymmetric power splitting scheme for SWIPT-based two-way multiplicative AF relaying," *IEEE Signal Process. Lett.*, vol. 25, no. 7, pp. 1014–1018, Jul. 2018.

[32] M. Ashraf, J.-W. Jang, J.-K. Han, and K. G. Lee, "Capacity Maximizing adaptive power splitting protocol for cooperative energy harvesting communication systems," *IEEE Commun. Lett.*, vol. 22, no. 5, pp. 902–905, May 2018.

[33] V. Singh and H. Ochiai, "An efficient time switching protocol with adaptive power splitting for wireless energy harvesting relay networks," in *Proc. IEEE 85th Veh. Technol. Conf. (VTC Spring)*, 2017, pp. 1–5.

[34] L. Sun and Q. Du, "A review of physical layer security techniques for Internet of Things: Challenges and solutions," *Entropy*, vol. 20, no. 10, p. 730, 2018.

[35] J. Zhang, T. Q. Duong, R. Woods, and A. Marshall, "Securing wireless communications of the Internet of Things from the physical layer, an overview," *Entropy*, vol. 19, no. 8, p. 420, 2017.

[36] T. Zhang, Y. Cai, Y. Huang, T. Q. Duong, and W. Yang, "Secure transmission in cognitive MIMO relaying networks with outdated channel state information," *IEEE Access*, vol. 4, pp. 8212–8224, 2016.

[37] Y. Huang, J. Wang, C. Zhong, T. Q. Duong, and G. K. Karagiannidis, "Secure transmission in cooperative relaying networks with multiple antennas," *IEEE Trans. Wireless Commun.*, vol. 15, no. 10, pp. 6843–6856, Oct. 2016.

[38] M. Yang, D. Guo, Y. Huang, T. Q. Duong, and B. Zhang, "Secure multiuser scheduling in downlink dual-hop regenerative relay networks over Nakagami- *m* fading channels," *IEEE Trans. Wireless Commun.*, vol. 15, no. 12, pp. 8009–8024, Dec. 2016.

[39] R. Zhao, H. Lin, Y.-C. He, D.-H. Chen, Y. Huang, and L. Yang, "Secrecy performance of transmit antenna selection for MIMO relay systems with outdated CSI," *IEEE Trans. Commun.*, vol. 66, no. 2, pp. 546–559, Feb. 2018.

[40] P. T. Tin, P. M. Nam, T. T. Duy, P. T. Tran, and M. Voznak, "Secrecy performance of TAS/SC-based multi-hop harvest-to-transmit cognitive WSNs under joint constraint of interference and hardware imperfection," *Sensors*, vol. 19, no. 5, p. 1160, 2019.

[41] J. Mo, M. Tao, and Y. Liu, "Relay placement for physical layer security: A secure connection perspective," *IEEE Commun. Lett.*, vol. 16, no. 6, pp. 878–881, Jun. 2012.

[42] 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, 2018.

[43] 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.

[44] Z. Ma, N. Wang, Y. Lu, and D. Zhang, "Relay power allocation for security enhancement in three-phase AF two-way relaying systems," in *Proc. 9th Int. Conf. Wireless Commun. Signal Process. (WCSP)*, 2017, pp. 1–6.

[45] M. K. Shukla, S. Yadav, and N. Purohit, "Secure transmission in cellular multiuser two-way amplify-and-forward relay networks," *IEEE Trans. Veh. Technol.*, vol. 67, no. 12, pp. 11886–11899, Dec. 2018.

[46] L. Xiang, D. W. K. Ng, R. Schober, and V. W. S. Wong, "Cache-enabled physical-layer security for video streaming in wireless networks with limited backhaul," in *Proc. IEEE Globecom Workshops (GC Wkshps)*, 2016, pp. 1–7.

[47] L. Xiang, D. W. K. Ng, R. Schober, and V. W. S. Wong, "Secure video streaming in heterogeneous small cell networks with untrusted cache helpers," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, 2017, pp. 1–7.

[48] J. M. Moualeu, W. Hamouda, and F. Takawira, "Intercept probability analysis of wireless networks in the presence of eavesdropping attack with co-channel interference," *IEEE Access*, vol. 6, pp. 41490–41503, 2018.

[49] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," in *Proc. IEEE Int. Symp. Inf. Theory*, 2008, pp. 524–528.

[50] H.-M. Wang, Q. Yin, and X.-G. Xia, "Distributed beamforming for physical-layer security of two-way relay networks," *IEEE Trans. Signal Process.*, vol. 60, no. 7, pp. 3532–3545, Jul. 2012.

[51] J. Huang and A. L. Swindlehurst, "Cooperative jamming for secure communications in MIMO relay networks," *IEEE Trans. Signal Process.*, vol. 59, no. 10, pp. 4871–4884, Oct. 2011.

[52] Y. Zou, J. Zhu, X. Wang, and V. C. M. Leung, "Improving physical-layer security in wireless communications using diversity techniques," *IEEE Netw.*, vol. 29, no. 1, pp. 42–48, Jan./Feb. 2015.

[53] W. Liu, X. Zhou, S. Durrani, and P. Popovski, "Secure communication with a wireless-powered friendly jammer," *IEEE Trans. Wireless Commun.*, vol. 15, no. 1, pp. 401–415, Jan. 2016.

[54] Y. Zou, X. Wang, and W. Shen, "Physical-layer security with multiuser scheduling in cognitive radio networks," *IEEE Trans. Commun.*, vol. 61, no. 12, pp. 5103–5113, Dec. 2013.

[55] Y. Zou, X. Li, and Y.-C. Liang, "Secrecy outage and diversity analysis of cognitive radio systems," *IEEE J. Sel. Areas Commun.*, vol. 32, no. 11, pp. 2222–2236, Nov. 2014.

[56] Y. Zou, "Physical-layer security for spectrum sharing systems," *IEEE Trans. Wireless Commun.*, vol. 16, no. 2, pp. 1319–1329, Feb. 2017.

[57] C. Ye, S. Mathur, A. Reznik, Y. Shah, W. Trappe, and N. B. Mandayam, "Information-theoretically secret key generation for fading wireless channels," *IEEE Trans. Inf. Forensics Security*, vol. 5, pp. 240–254, 2010.

[58] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge, U.K.: Cambridge Univ. Press, 2011.

[59] D.-H. Ha, S. T. C. Dong, T. N. Nguyen, T. T. Trang, and M. Voznak, "Half-duplex energy harvesting relay network over different fading environment: System performance with effect of hardware impairment," *Appl. Sci.*, vol. 9, no. 11, p. 2283, 2019.

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

[61] T. N. Nguyen, M. Tran, T.-L. Nguyen, D.-H. Ha, and M. Voznak, "Multisource power splitting energy harvesting relaying network in half-duplex system over block Rayleigh fading channel: System performance analysis," *Electronics*, vol. 8, no. 1, p. 67, 2019.

[62] 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, 2021.

[63] T. T. Duy, T. Q. Duong, T. L. Thanh, and V. N. Q. Bao, "Secrecy performance analysis with relay selection methods under impact of co-channel interference," *IET Commun.*, vol. 9, no. 11, pp. 1427–1435, 2015.

[64] 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 Tran. Veh. Technol.*, vol. 69, no. 10, pp. 12286–12290, Oct. 2020.

[65] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*. San Diego, CA, USA: Academic, 2014.

Tan N. Nguyen (Member, IEEE) was born at Nha Trang, Vietnam, in 1986. He received the B.S. and M.S. degrees in electronics and telecommunications engineering from Ho Chi Minh University of Natural Sciences, a member of Vietnam National University, Ho Chi Minh City, Vietnam, in 2008 and 2012, respectively, and the Ph.D. degree in computer science, communication technology and applied mathematics from the VSB Technical University of Ostrava, Ostrava, Czechia, in 2019, where he is currently pursuing the Ph.D. degree in electrical engineering.

He joined the Faculty of Electrical and Electronics Engineering, Ton Duc Thang University, Ho Chi Minh City, in 2013, where has been working as a Lecturer since then. His major interests are cooperative communications, cognitive radio, and physical-layer security.

Dinh-Hieu Tran (Graduate Student Member, IEEE) was born and grew up in Gia Lai, Vietnam, in 1989. He received the B.E. degree with the Electronics and Telecommunication Engineering Department, Ho Chi Minh City University of Technology, Ho Chi Minh City, Vietnam, in 2012, the M.Sc. degree in electronics and computer engineering from Hongik University, Seoul, South Korea, in 2017, and the Ph.D. degree in telecommunications engineering from the Interdiscipline Reliability and Trust (SnT) Research Center, University of Luxembourg, Luxembourg, Luxembourg, in December 2021, under the supervision of Prof. S. Chatzinotas and Prof. B. Ottersten.

His major interests include UAV, satellite, IoT, mobile-edge computing, caching, and B5G for wireless communication networks.

Dr. Tran received the Hongik Rector Award for his excellence during his master's study at Hongik University, in 2016. 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.

Trinh Van Chien (Member, IEEE) received the B.S. degree in electronics and telecommunications from Hanoi University of Science and Technology (HUST), Hanoi, Vietnam, in 2012, the M.S. degree in electrical and computer engineering from Sungkyunkwan University, Seoul, South Korea, in 2014, and the Ph.D. degree in communication systems from Linköping University, Linköping, Sweden, in 2020.

He was a Research Associate with the University of Luxembourg, Luxembourg, Luxembourg. He is currently with the School of Information and Communication Technology, HUST. His interest lies in convex optimization problems and machine-learning applications for wireless communications and image and video processing.

Dr. Chien also received the Award of Scientific Excellence in the first year of the 5G wireless project funded by European Union Horizon's 2020. He was an IEEE WIRELESS COMMUNICATIONS LETTERS Exemplary Reviewer for 2016, 2017, and 2021.

Van-Duc Phan was born in Long An, Vietnam, in 1975. He received the M.S. degree with the Department of Electric, Electrical and Telecommunication Engineering from Ho Chi Minh City University of Transport, Ho Chi Minh City, Vietnam, and the Ph.D. degree from the Department of Mechanical and Automation Engineering, Da-Yeh University, Changhua, Taiwan, in 2016.

His current research interests are in sliding-mode control, nonlinear systems or active magnetic bearing, flywheel store energy systems, power system optimization, optimization algorithms, renewable energies, energy harvesting-enabled cooperative networks, improving the optical properties, lighting performance of white LEDs, energy efficiency LED driver integrated circuits, novel radio access technologies, and physical security in communication network.

Miroslav Voznak (Senior Member, IEEE) was born in 1971. He received the Ph.D. degree in telecommunications from the VSB, Technical University of Ostrava, Ostrava, Czechia, in 2002.

He is currently a Professor of electronics and communication technologies with the Department of Telecommunications, VSB, Technical University of Ostrava and a Foreign Professor with Ton Duc Thang University, Ho Chi Minh City, Vietnam. He has coauthored more than one hundred articles in journals indexed in the SCIE database. His research interests include IP telephony, wireless networks, network security, and big data analytics.

Phu Tran Tin was born in Khanh Hoa, Vietnam, in 1979. He received the bachelor's and master's degrees from Ho Chi Minh City University of Science, Ho Chi Minh City, Vietnam, in 2002 and 2008, respectively, and the Ph.D. degree in faculty of electrical engineering and computer science, VSB—Technical University of Ostrava, Ostrava, Czechia, in 2019.

He is currently a Lecturer with the Faculty of Electronics Technology, Industrial University of Ho Chi Minh City, Ho Chi Minh City. His major research interests are wireless communication in 5G, energy harvesting, performance of cognitive radio, physical-layer security, and NOMA.

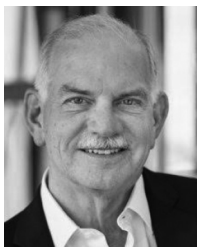
Symeon Chatzinotas (Senior Member, IEEE) is currently a Full Professor/Chief Scientist I and the Head of the SIGCOM Research Group, SnT, University of Luxembourg, Luxembourg, Luxembourg. He is coordinating the research activities on communications and networking, acting as a PI for more than 20 projects and main representative for 3GPP, ETSI, DVB. In the past, he was a Visiting Professor with the University of Parma, Parma, Italy, lecturing on "5G Wireless Networks." He was involved in numerous Research and Development projects for NCSR Demokritos, Athens, Greece; CERTH Hellas, Thessaloniki, Greece; and CCSR, University of Surrey, Guildford, U.K. He has (co-)authored more than 450 technical papers in refereed international journals, conferences, and scientific books.

Prof. Chatzinotas was the co-recipient of the 2014 IEEE Distinguished Contributions to Satellite Communications Award and Best Paper Awards at EURASIP JWCN, CROWNCOM, and ICSSC. He is currently in the editorial board of the IEEE TRANSACTIONS ON COMMUNICATIONS, IEEE OPEN JOURNAL OF VEHICULAR TECHNOLOGY, and the *International Journal of Satellite Communications and Networking*.

Derrick Wing Kwan Ng (Fellow, IEEE) received the bachelor's degree (First-Class Hons.) and the Master of Philosophy degree in electronic engineering from Hong Kong University of Science and Technology, Hong Kong, in 2006 and 2008, respectively, and the Ph.D. degree from The University of British Columbia, Vancouver, BC, Canada, in November 2012.

He was a Senior Postdoctoral Fellow with the Institute for Digital Communications, Friedrich-Alexander-University Erlangen-Nürnberg, Erlangen, Germany. He is currently working as a Scientia Associate Professor, University of New South Wales, Sydney, NSW, Australia. His research interests include convex and nonconvex optimization, physical-layer security, IRS-assisted communication, UAV-assisted communication, wireless information and power transfer, and green (energy efficient) wireless communications.

Dr. Ng received the Australian Research Council Discovery Early Career Researcher Award 2017, the IEEE Communications Society Stephen O. Rice Prize 2022, the Best Paper Awards at the WCSP in 2020 and 2021, the IEEE TCGCC Best Journal Paper Award 2018, INISCOM 2018, IEEE International Conference on Communications in 2018 and 2021, IEEE International Conference on Computing, Networking and Communications 2016, IEEE Wireless Communications and Networking Conference 2012, the IEEE Global Telecommunication Conference in 2011 and 2021, and the IEEE Third International Conference on Communications and Networking in China 2008. He has been listed as a Highly Cited Researcher by Clarivate Analytics (Web of Science) since 2018. He has been serving as an Editorial Assistant to the Editor-in-Chief of the IEEE TRANSACTIONS ON COMMUNICATIONS from January 2012 to December 2019. He is currently serving as an editor for the IEEE TRANSACTIONS ON COMMUNICATIONS and the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, and an Area Editor for the IEEE Open Journal of the Communications Society.



H. Vincent Poor (Life Fellow, IEEE) received the Ph.D. degree in EECS from Princeton University, Princeton, NJ, USA, in 1977.

From 1977 to 1990, he was on the faculty of the University of Illinois at Urbana–Champaign. Since 1990, he has been on the faculty at Princeton, where he is currently the Michael Henry Strater University Professor. He has also held visiting appointments at several other universities, including most recently at Berkeley and Cambridge. From 2006 to 2016, he also served as Dean of Princeton's School of Engineering and Applied Science. His research interests are in the areas of information theory, machine learning and network science, and their applications in wireless networks, energy systems, and related fields. Among his publications in these areas is the forthcoming book *Machine Learning and Wireless Communications* (Cambridge University Press).

Dr. Poor is a member of the National Academy of Engineering and the National Academy of Sciences, and is a foreign member of the Chinese Academy of Sciences, the Royal Society, and other national and international academies. He received the IEEE Alexander Graham Bell Medal in 2017.