Self-Energy Recycling in DF Full-Duplex Relay Network: Security-Reliability Analysis

Bui Vu MINH[1], *Anh-Vu LE*[2], *Van-Duc PHAN*[3], *Thu-Ha Thi PHAM*[4]

[1]Faculty of Engineering and Technology, Nguyen Tat Thanh University,
300A - Nguyen Tat Thanh, Ward 13, District 4, Ho Chi Minh City 754000, Vietnam
[2]Communication and Signal Processing Research Group, Faculty of Electrical and Electronics Engineering,
Ton Duc Thang University, Ho Chi Minh City, Vietnam
[3]Faculty of Automotive Engineering, School of Technology, Van Lang University,
Ho Chi Minh City 70000, Vietnam
[4]Faculty of Electrical and Electronics Engineering, Ton Duc Thang University,
Ho Chi Minh City 70000, Vietnam

bvminh@ntt.edu.vn,leanhvu@tdtu.edu.vn,duc.pv@vlu.edu.vn, 42101299@student.tdtu.edu.vn

DOI: 10.15598/aeee.v22i1.5528

Article history: Received Oct 30, 2023; Revised Dec 20, 2023; Accepted Feb 03, 2024; Published Mar 31, 2024.

Abstract. *This paper studied the physical layer security (PLS) reliability of concurrent wireless communications. A decode and forward (DF) full-duplex (FD) network with the impact of an eavesdropper was proposed to evaluate the security and reliability. Essentially, the DF-FD relay adopted the power-splitting (PS) protocol to gather energy from the source and simultaneously utilized the self-energy recycling (S-ER) technique by manipulating the loopback interference to increase the harvested energy. By constructing closed-form expressions for outage probability (OP) and intercept probability (IP), we offer the trade-off analysis between them. Monte Carlo simulation was conducted to verify the analytical formulations. Furthermore, the key parameters were also examined to play an important role in selecting the suitable trade-off for the proposed system.*

Keywords

Full-duplex, Self-energy recycling, Outage probability, Intercept probability, Decode-and-forward

1. Introduction

5G wireless networks can provide not only traditional audio and data information but also many new industrial applications, multiple devices, and apps to connect to a wider society. It is believed that 5G wireless telecommunications systems can increase mobile bandwidth with large services and IoT. The term "Internet-of-Things" (IoT) is applied to describe how all physical objects are connected to the Internet through information sensing devices for the exchange of information, i.e., how physical objects communicate with one another for the purpose of intelligent identification and administration. Next-generation telecommunications networks are required to be highly secure, unlike previous cellular networks. Due to the natural broadcast and bandwidth limitations of wireless communications, tt leads to security that is possible but will be difficult to provide security features such as authentication, integrity, and privacy. The service direction for 5G will pay particular attention to the problems mentioned above. [1–4]

In general, the new characteristics of 5G networks have presented many complex situations in dealing with eavesdropping, and since then wireless physical layer security (PLS) has recently received significant research attention. The advantages of using PLS algorithms for wireless networks in the context of 5G and beyond are double those of conventional cryptography methods. Compared PLS to cryptography at higher layers, PLS is first independent of computing complexity [5]. Accordingly, safe and trustworthy communications can be ensured even when eavesdroppers have extremely powerful computational capabilities. The second is the remarkable scalability of PLS techniques [6]. It is significant to note that PLS can be used as an additional layer of security on top of the existing security measures. To provide secure and private communication data in wireless networks beyond 5G, PLS can be coupled with other security technologies [7], [8]. Numerous methods have been developed to reduce the quality of the wiretapped signals at the eavesdropper, including cooperative beamforming [9], artificial noise [10], and multi-antenna beamforming [11]. Multiple investigations have advanced our understanding of the physics layer's fundamental potential to sustain secure communications and revealed its subsequent limits. [12–15]. It has been demonstrated, in particular, that the two fundamental characteristics of radio transmission—diffusion and superposition—can be used to provide data confidentiality through a number of mechanisms that limit the information that potential listeners can learn about private messages. These methods make advantage of fading, interference, and path diversity (by employing numerous antennas), all of which can potentially lead to strategies that can be used in real-world wireless systems. Moreover, because an intermediate relay node is more susceptible to eavesdropping than any other endpoint, PLS techniques are crucial in relay networks. Relaying of signals has also been extensively employed to improve cellular networks' service quality. Numerous benefits of relaying techniques include increased data rate and wider coverage. Numerous studies have been conducted to determine the advantages of cooperative relaying systems in the context of PLS [16–21]. In [16], power allocation strategies for both legal and jamming signals were developed as part of an investigation into the PLS for the cooperative non-orthogonal multiple access (NOMA) system. In [17], the security vs. dependability trade-off for wireless communications was explored. An opportunistic relay selection strategy was then presented to boost the cellular network's capacity for secrecy. To ensure a safe transmission for the cellular network, the relay selection of a cooperative scenario was examined in [18] in this regard. In order to prevent eavesdropping attempts on wireless broadcasts, the relay selection strategy was devised. The PLS of energy harvesting for cognitive radio networks utilizing the cooperative relaying technique was investigated by the authors in [19]. For IoT networks, the PLS of cooperative dual-hop NOMA was examined in [20]. In [21], the PLS of underlay multihop D2D relaying was examined. Besides, in wireless ad-hoc networks, energy harvesting (EH) has become a promising method for extending the lifespan of IoT devices. Solar, wind, and water are examples of potential ambient energy sources. Particularly, researchers have paid close attention to radio frequency (RF) energy harvesting (EH) because it is independent of the environment's randomness and intermittency, i.e., wind and solar. The effect of RF EH on cognitive radio networks was studied in [22, 23]. In particular, the energy from the primary transmitters (PTs) could be harvested by the secondary transmitters (STs), which are then stored in their rechargeable batteries. When the PTs were far away, the STs utilized this energy to transmit data. In another aspect of EH, the authors in [24] put forth a single-input multiple-output system concept in which a two-antenna Full-Duplex (FD) relay node can harvest energy from RF signals coming from a single antenna source and utilize that energy for transmitting information to a multi-antenna destination. To decode the received information, the destination can adopt selection combining (SC) or maximal ratio combing (MRC) techniques. Tan et al. in [25] analyzed the system performance of a multisource power splitting EH relaying network operating in half-duplex (HD) mode over a block Rayleigh-fading channel in both delay-limited transmission and delay-tolerant transmission modes. The energy-harvesting approach based on PS was applied by the authors in [26] to improve the transmission between a wireless access point and a mobile user via a helpful relay. In which, the energy is provided by the access point and then forwarded by the relay, the mobile user transmits its own data back to the access point with the help of the relay again. In addition [27] constituted one of the few research investigations that focused on user selection and EH protocols employing different Nakagami-m/Rayleigh channels. Specifically, the authors examined the performance of user selection protocol cooperative networks using PS protocol-based EH.

Although Full-duplex (FD) communication improves spectral efficiency for relay deployment, it is hampered by the high communication signal coupling to the sensitive receive chain that causes inherent self-interference. The author in [28] presented a self-energy recycling (S-ER) protocol for FD multi-relay networks, in which self-interference energy is captured and used again at the relay. To increase the reliability of the suggested systems, two amplify-and-forward (AF) relay selection algorithms—partial relay selection and full relay selection are presented by using the power splitting (PS) protocol. In an AF relaying cooperative network, where the relay node harvests the energy from the RF transmission, Hu et al. [29] examined the problem of beamforming optimization. The authors researched the beamforming optimization problem using the S-ER relay technique. The goal of the formulated problem is to maximize the rate that can be achieved given the transmitting power that is available at the relay node. An energy-constrained relay node helps the information transfer from the source to the destination utilizing the energy captured from the source, according to research done in [30]. The relays operated in FD mode with simultaneous energy harvesting and information transmission, and they suggested a novel two-phase protocol for efficient energy transfer and information transmission. The proposed design has two main benefits: it ensures uninterrupted information transmission because no time switching (TS) or PS is required at the relay for EH, and it enables what is known as "S-ER," which allows for the harvesting and reusing of some of the energy (referred to as "loop energy"). This harvested energy is also used to decode the received information and then transfer it to the destination.

The PLS in the cooperative relaying network has been extensively researched in recent literature. By adopting the source jamming strategy, the authors in [31] investigated the issue of security in the untrusted FD relaying using the AF protocol system. However, the authors did not think that EH would lengthen the device's lifetime. In addition, S-ER was not stated, even though a different protocol decode-and-forward (DF) FD relay networks' PLS has been provided in [32]. Moreover, the security-reliability of AF FD relay network and using S-ER has been studied in [33]. The security performance of the AF relaying FD system in the presence of a passive eavesdropper was examined in [34]. The dependability and security of the AF relaying system in the presence of an eavesdropper were investigated in [35, 36].

Different from some above-related works, in this paper, we studied the security-reliability analysis for DF FD relay network by adopting the EH PS scheme at the relay. In particular, the relay can apply the S-ER technique to increase its harvested energy. The main contributions and novelties are listed as follows:

- We propose a model for relaying information from sources (S) to users and devices (D) via an FD Relay (R) with the appearance of Eavesdropper (E). PLS is taken into account in the DF-FD Relay network to assess the security and reliability trade-offs in our suggested model. In particular, the relay can employ the PS protocol to achieve a battery-free system by harvesting energy from the source and reusing the self-interference channel in order to enhance the EH.

- The approximation expressions of OP and IP are derived by using the Gaussian-Chebyshev quadrature to analyze the security-reliability trade-off of the proposed system.

- Finally, the Monte Carlo simulation is adopted to verify the accuracy of the mathematical analysis. Moreover, the key parameters are examined to give more physical meaning insights.

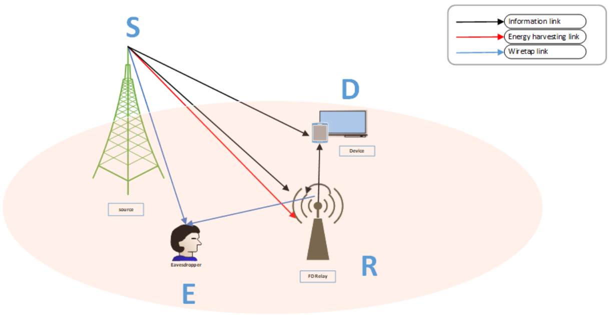
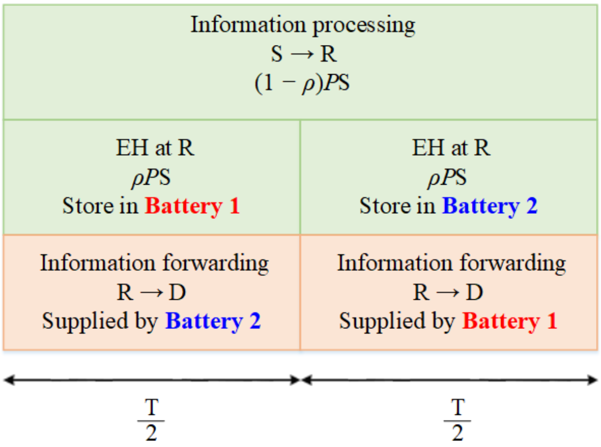


Fig. 1: System Model



Information processing
$S \to R$
$(1-\rho)PS$

EH at R
ρPS
Store in Battery 1

EH at R
ρPS
Store in Battery 2

Information forwarding
$R \to D$
Supplied by Battery 2

Information forwarding
$R \to D$
Supplied by Battery 1

Fig. 2: Virtual harvest-use protocol for S-ER

2. System Model

According to the suggested wireless communication system model as illustrated in Fig. 1, one source node S and one destination node D connect with the aid of one FD relay node R while an eavesdropper node E attempts to steal the data from both R and S. We made the assumption that S could send its signal both directly to D and through the relay R, which would improve performance at D. Due to the energy shortage, R must first harvest wireless energy from S by adopting PS protocol and then harvest the energy from loop-back interference called S-ER technique implemented as shown in Fig.2. Specifically, each transmission block is split up into two-time slots of the same length, and the duration of each slot lasts $\frac{T}{2}$. After every time slot, two batteries alternate between two different functions: one battery is used for storing the harvested energy, and the other is to supply the power to the activated relay. It should be mentioned that the original assumption is that every battery has enough redundant energy [28]. Finally, the R will employ the whole amount of harvested energy to decode the information from S and then forward to D.

Let's refer to the links among these nodes as the given channel coefficients h_{SD}, h_{SR}, h_{SE}, h_{RD}, and

h_{RE} as well as the links $\mathrm{S} \rightarrow \mathrm{D}, \mathrm{S} \rightarrow \mathrm{R}, \mathrm{S} \rightarrow \mathrm{E}, \mathrm{R} \rightarrow \mathrm{D}, \mathrm{R} \rightarrow \mathrm{E}$, respectively. The self-interference coefficient between the transmit and receive antennas of relay node R is also denoted by the letter h_{RR}. Assume that h_{X} ($\mathrm{X} \in \{\mathrm{SD}, \mathrm{SR}, \mathrm{SE}, \mathrm{RD}, \mathrm{RE}\}$) are Rayleigh fading channels, the channel gains $\gamma_{\mathrm{X}} = |h_{\mathrm{X}}|^2$ are exponential random variables (RVs) whose cumulative distribution function (CDF) are given as:

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

To take into account the simple path loss model, we have:

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

where ω is the path-loss exponent and d_{X} is the distance between two respectively nodes.

$\gamma_{\mathrm{RR}} = |h_{\mathrm{RR}}|^2$ is also an exponential RV. Hence, its CDF can be thus expressed by:

$$F_{\gamma_{\mathrm{RR}}}(x) = 1 - \exp\left(-\frac{x}{\lambda_{\mathrm{RR}}}\right). \tag{3}$$

Then, probability density function (PDF) of γ_{Y} is given by:

$$f_{\gamma_{\mathrm{X}}}(x) = \frac{1}{\xi}\exp\left(\frac{-x}{\xi}\right). \tag{4}$$

where $\xi \in \{\lambda_{\mathrm{SR}}, \lambda_{\mathrm{SD}}, \lambda_{\mathrm{RD}}, \lambda_{\mathrm{SE}}, \lambda_{\mathrm{RE}}, \lambda_{\mathrm{RR}}\}$.

In the energy harvesting phase, firstly R will harvest the energy from S and then simultaneously perform S-ER. Therefore, the total captured energy at the R can be expressed as [28]

$$\mathrm{E}_{\mathrm{R}} = \eta\rho\frac{\mathrm{T}}{2}\left(P_{\mathrm{S}}\gamma_{\mathrm{SR}} + P_{\mathrm{R}}\gamma_{\mathrm{RR}}\right). \tag{5}$$

The transmit power of R can then be computed as:

$$P_{\mathrm{R}} = \frac{\mathrm{E}_{\mathrm{R}}}{\frac{\mathrm{T}}{2}} = \frac{\eta\rho P_{\mathrm{S}}\gamma_{\mathrm{SR}}}{1 - \eta\rho\gamma_{\mathrm{RR}}}. \tag{6}$$

It is important to know from (6) that $P_{\mathrm{R}} = 0$ when

$$\gamma_{\mathrm{RR}} < \frac{1}{\eta\rho}. \tag{7}$$

Because passive interference cancellation (IC), such as antenna isolation, causes γ_{RR} to be significantly less than 1 in actuality, the denominator in equation (6) is positive [28].

The received signal at R during the information transmission phase is described as follows:

$$y_{\mathrm{R}} = \sqrt{1-\rho}\,h_{\mathrm{SR}}x_{\mathrm{S}} + \sqrt{1-\rho}\,h_{\mathrm{RR}}x_{\mathrm{R}} + n_{\mathrm{R}}. \tag{8}$$

The received signal-to-interference-plus-noise ratio (SINR) at R to decode the message from S in this phase can be found by:

$$\gamma_R = \frac{\mathbb{E}\left\{|signal|^2\right\}}{\mathbb{E}\left\{|noise|^2\right\}} = \frac{(1-\rho)\gamma_{\mathrm{SR}}P_{\mathrm{S}}}{(1-\rho)\gamma_{\mathrm{RR}}P_R + N_0}. \tag{9}$$

Using the fact that $N_0 << P_S$, then by doing some algebra, and finally by substituting (6) into (9) , we have:

$$\gamma_{\mathrm{R}} \approx \frac{1 - \eta\rho\gamma_{\mathrm{RR}}}{\eta\rho\gamma_{\mathrm{RR}}}. \tag{10}$$

In this model, we applied the DF protocol. Therefore, after receiving the information from S, R will decode this information and forward to both D and E in the broadcast phase. The received signal was illustrated at E and D as follows:

$$y_{\mathrm{D}}^1 = h_{\mathrm{RD}}x_{\mathrm{R}} + n_{\mathrm{D}}^1. \tag{11}$$

$$y_{\mathrm{E}}^1 = h_{\mathrm{RE}}x_{\mathrm{R}} + n_{\mathrm{E}}^1. \tag{12}$$

The received SINR at D and E in the first phase can be thus calculated by, respectively.

$$\gamma_{\mathrm{D}}^1 = \frac{\mathbb{E}\left\{|signal|^2\right\}}{\mathbb{E}\left\{|noise|^2\right\}} = \frac{\gamma_{\mathrm{RD}}P_{\mathrm{R}}}{N_0}. \tag{13}$$

$$\gamma_{\mathrm{E}}^1 = \frac{\mathbb{E}\left\{|signal|^2\right\}}{\mathbb{E}\left\{|noise|^2\right\}} = \frac{\gamma_{\mathrm{RE}}P_{\mathrm{R}}}{N_0}. \tag{14}$$

By substituting (6) into (13) and (14), then by doing some algebra, the SINR at D and E can be rewritten as:

$$\gamma_{\mathrm{D}}^1 = \frac{\gamma_{\mathrm{SR}}\gamma_{\mathrm{RD}}\eta\rho\Psi}{1 - \eta\rho\gamma_{\mathrm{RR}}}, \tag{15}$$

$$\gamma_{\mathrm{E}}^1 = \frac{\gamma_{\mathrm{SR}}\gamma_{\mathrm{RE}}\eta\rho\Psi}{1 - \eta\rho\gamma_{\mathrm{RR}}}, \tag{16}$$

where $\Psi = \frac{P_{\mathrm{S}}}{N_0}$ denotes the average transmit signal-to-noise ratio (SNR).

Finally, the overall SINR of the system in DF mode of both signaling paths: $\mathrm{S} \rightarrow \mathrm{R} \rightarrow \mathrm{D}$ and $\mathrm{S} \rightarrow \mathrm{R} \rightarrow \mathrm{E}$ can be confirmed as follows, respectively.

$$\begin{aligned}\gamma_{\mathrm{SRD}} &= \min(\gamma_{\mathrm{R}}, \gamma_{\mathrm{D}}^1)\\ &= \min\left(\frac{1 - \eta\rho\gamma_{\mathrm{RR}}}{\eta\rho\gamma_{\mathrm{RR}}}, \frac{\gamma_{\mathrm{SR}}\gamma_{\mathrm{RD}}\eta\rho\Psi}{1 - \eta\rho\gamma_{\mathrm{RR}}}\right).\end{aligned} \tag{17}$$

$$\begin{aligned}\gamma_{\mathrm{SRE}} &= \min(\gamma_{\mathrm{R}}, \gamma_{\mathrm{E}}^1)\\ &= \min\left(\frac{1 - \eta\rho\gamma_{\mathrm{RR}}}{\eta\rho\gamma_{\mathrm{RR}}}, \frac{\gamma_{\mathrm{SR}}\gamma_{\mathrm{RE}}\eta\rho\Psi}{1 - \eta\rho\gamma_{\mathrm{RR}}}\right).\end{aligned} \tag{18}$$

Our suggested model takes into account the direct link. As a result, when S broadcasts to R and D during the broadcast phase, D can receive the direct signal from S, and E can overhear this signal. Consequently, the received signal at D and E can be thus expressed by

$$y_{\mathrm{D}}^2 = h_{\mathrm{SD}} x_{\mathrm{S}} + n_{\mathrm{D}}^2. \tag{19}$$

$$y_{\mathrm{E}}^2 = h_{\mathrm{SE}} x_{\mathrm{S}} + n_{\mathrm{E}}^2. \tag{20}$$

The SNR at D and E in this phase can be computed by, respectively.

$$\gamma_{\mathrm{D}}^2 = \Psi\gamma_{\mathrm{SD}}, \tag{21}$$

$$\gamma_{\mathrm{E}}^2 = \Psi\gamma_{\mathrm{SE}}. \tag{22}$$

Finally, the end-to-end SNR at D and E can be claimed as, respectively, by using the selection combining (SC) technique at the receiver.

$$\gamma_{\mathrm{D}} = \max\left(\gamma_{\mathrm{SRD}}, \gamma_{\mathrm{D}}^2\right). \tag{23}$$

$$\gamma_{\mathrm{E}} = \max\left(\gamma_{\mathrm{SRE}}, \gamma_{\mathrm{E}}^2\right). \tag{24}$$

3. Performance Analysis

In this section, the performances of the proposed system were analyzed. In particular, the closed-form of OP and IP were derived.

3.1. Outage Probability Analysis

The OP of the system can be thus defined by:

$$\mathrm{OP} = \Pr\left(\gamma_{\mathrm{SRD}} \leqslant \gamma_{\mathrm{th}}\right), \tag{25}$$

where $\gamma_{\mathrm{th}} = 2^{\mathrm{R_{th}}} - 1$ is the threshold of the system and $\mathrm{R_{th}}$ is the target rate.

From (23) and (25), the OP can be reformulated as

$$\begin{aligned}\mathrm{OP} &= \Pr\left[\max\left(\min(\gamma_{\mathrm{R}}, \gamma_{\mathrm{D}}^1), \gamma_{\mathrm{D}}^2\right) \leqslant \gamma_{\mathrm{th}}\right] \\ &= \underbrace{\Pr(\gamma_{\mathrm{D}}^2 \leqslant \gamma_{\mathrm{th}})}_{Y_1} \underbrace{\Pr\left(\min(\gamma_{\mathrm{R}}, \gamma_{\mathrm{D}}^1) \leqslant \gamma_{\mathrm{th}}\right)}_{Y_2}.\end{aligned} \tag{26}$$

Based on (26), Y_1 can be figured out as

$$\begin{aligned}Y_1 &= \Pr(\gamma_{\mathrm{D}}^2 \leqslant \gamma_{\mathrm{th}}) = \Pr\left(\Psi\gamma_{\mathrm{SD}} \leqslant \gamma_{\mathrm{th}}\right) \\ &= \Pr\left(\gamma_{\mathrm{SD}} \leqslant \frac{\gamma_{\mathrm{th}}}{\Psi}\right) = 1 - \exp\left(-\frac{\gamma_{\mathrm{th}}}{\lambda_{\mathrm{SD}}\Psi}\right).\end{aligned} \tag{27}$$

Next, Y_2 can be thus computed by

$$\begin{aligned}Y_2 &= \Pr\left(\min(\gamma_{\mathrm{R}}, \gamma_{\mathrm{D}}^1) \leqslant \gamma_{\mathrm{th}}\right) \\ &= \Pr\left[\min\left(\frac{1-\eta\rho\gamma_{\mathrm{RR}}}{\eta\rho\gamma_{\mathrm{RR}}}, \frac{\gamma_{\mathrm{SR}}\gamma_{\mathrm{RD}}\eta\rho\Psi}{1-\eta\rho\gamma_{\mathrm{RR}}}\right) \leqslant \gamma_{\mathrm{th}}\right] \\ &= 1 - \Pr\left[\min\left(\frac{1-\eta\rho\gamma_{\mathrm{RR}}}{\eta\rho\gamma_{\mathrm{RR}}}, \frac{\gamma_{\mathrm{SR}}\gamma_{\mathrm{RD}}\eta\rho\Psi}{1-\eta\rho\gamma_{\mathrm{RR}}}\right) \geqslant \gamma_{\mathrm{th}}\right] \\ &= 1 - \Pr\left[\left(\frac{\gamma_{\mathrm{SR}}\gamma_{\mathrm{RD}}\eta\rho\Psi}{1-\eta\rho\gamma_{\mathrm{RR}}}\right) \geqslant \gamma_{\mathrm{th}}, \gamma_{\mathrm{RR}} \leqslant \frac{1}{\eta\rho(1+\gamma_{\mathrm{th}})}\right].\end{aligned} \tag{28}$$

Combined with (7) and (28), we will have the constraint condition of γ_{RR} as

$$\gamma_{\mathrm{RR}} < \min\left(\frac{1}{\eta\rho(1+\gamma_{\mathrm{th}})}, \frac{1}{\eta\rho}\right) \Leftrightarrow \gamma_{\mathrm{RR}} < \frac{1}{\eta\rho(1+\gamma_{\mathrm{th}})}. \tag{29}$$

So (28) is calculated where $\gamma_{\mathrm{SRD}} = \gamma_{\mathrm{SR}}\gamma_{\mathrm{RD}}$ as follows:

$$\begin{aligned}Y_2 &= 1 - \int_0^{\frac{1}{\eta\rho(1+\gamma_{\mathrm{th}})}} \Pr\left(\frac{\gamma_{\mathrm{SRD}}\eta\rho\Psi}{1-\eta\rho x} \geqslant \gamma_{\mathrm{th}}\right) f_{\gamma_{\mathrm{RR}}}(x)dx \\ &= 1 - \int_0^{\frac{1}{\eta\rho(1+\gamma_{\mathrm{th}})}} f_{\gamma_{\mathrm{RR}}}(x)\left[1 - F_{\gamma_{\mathrm{SRD}}}\left(\frac{(1-\eta\rho x)\gamma_{\mathrm{th}}}{\eta\rho\Psi}\right)\right] dx \\ &= 1 - \frac{1}{\lambda_{\mathrm{RD}}\lambda_{\mathrm{RR}}} \int_0^{\frac{1}{\eta\rho(1+\gamma_{\mathrm{th}})}} \exp\left(\frac{-x}{\lambda_{\mathrm{RR}}}\right)dx \\ &\times \int_0^{\infty} \exp\left(-\frac{\left(\frac{(1-\eta\rho x)\gamma_{\mathrm{th}}}{\eta\rho\Psi}\right)}{y\lambda_{\mathrm{SR}}} - \frac{y}{\lambda_{\mathrm{RD}}}\right) dy.\end{aligned} \tag{30}$$

With the help of [37, Eq. 3.324.1], we claim:

$$\begin{aligned}Y_2 &= 1 - \frac{1}{\lambda_{\mathrm{RR}}} \int_0^{\frac{1}{\eta\rho(1+\gamma_{\mathrm{th}})}} \exp\left(\frac{-x}{\lambda_{\mathrm{RR}}}\right) \\ &\times \sqrt{\frac{4(1-\eta\rho x)\gamma_{\mathrm{th}}}{\eta\rho\Psi\lambda_{\mathrm{SR}}\lambda_{\mathrm{RD}}}} K_1\left(\sqrt{\frac{4(1-\eta\rho x)\gamma_{\mathrm{th}}}{\eta\rho\Psi\lambda_{\mathrm{SR}}\lambda_{\mathrm{RD}}}}\right) dx.\end{aligned} \tag{31}$$

Unfortunately, the integral in Y_2 is a tough task to find a closed-form expression. Hence, by applying the Gaussian-Chebyshev quadrature in [38], Y_2 can be approximated as in (32) and shown on the top next page with $\phi_n = \cos\left(\frac{2n-1}{2N}\pi\right)$.

Finally, by substituting (27) and (32) into (26), the OP can be obtained as in (33) and shown on the top next page.

3.2. Intercept Probability analysis

The considered system will be wiretapped if E can successfully decode received signals from the source and

$$\begin{aligned} Y_2 \approx 1 - \frac{1}{2\lambda_{\mathrm{RR}}\eta\rho(\gamma_{\mathrm{th}}+1)} \Bigg[\frac{\pi}{N}\sum_{n=1}^{N}\sqrt{1-\varphi_n^2}\exp\left(\frac{-\varphi_n-1}{2\eta\rho(\gamma_{\mathrm{th}}+1)\lambda_{\mathrm{RR}}}\right) \\ \times \sqrt{\frac{2\gamma_{\mathrm{th}}(2\gamma_{\mathrm{th}}-2\varphi_n+1)}{\eta\rho\Psi\lambda_{\mathrm{SR}}\lambda_{\mathrm{RD}}(\gamma_{\mathrm{th}}+1)}} K_1\left(\sqrt{\frac{2\gamma_{\mathrm{th}}(2\gamma_{\mathrm{th}}-2\varphi_n+1)}{\eta\rho\Psi\lambda_{\mathrm{SR}}\lambda_{\mathrm{RD}}(\gamma_{\mathrm{th}}+1)}}\right)\Bigg]. \end{aligned} \tag{32}$$

$$\begin{aligned} \mathrm{OP} \approx \left[1-\exp\left(-\frac{\gamma_{\mathrm{th}}}{\lambda_{\mathrm{SD}}\Psi}\right)\right]\Bigg[1 - \frac{1}{2\lambda_{\mathrm{RR}}\eta\rho(\gamma_{\mathrm{th}}+1)}\Bigg[\frac{\pi}{N}\sum_{n=1}^{N}\sqrt{1-\varphi_n^2} \\ \times \exp\left(\frac{-\varphi_n-1}{2\eta\rho(\gamma_{\mathrm{th}}+1)\lambda_{\mathrm{RR}}}\right)\sqrt{\frac{2\gamma_{\mathrm{th}}(2\gamma_{\mathrm{th}}-2\varphi_n+1)}{\eta\rho\Psi\lambda_{\mathrm{SR}}\lambda_{\mathrm{RD}}(\gamma_{\mathrm{th}}+1)}}K_1\left(\sqrt{\frac{2\gamma_{\mathrm{th}}(2\gamma_{\mathrm{th}}-2\varphi_n+1)}{\eta\rho\Psi\lambda_{\mathrm{SR}}\lambda_{\mathrm{RD}}(\gamma_{\mathrm{th}}+1)}}\right)\Bigg]\Bigg]. \end{aligned} \tag{33}$$

relay [36]. Therefore, the IP is given by

$$\begin{aligned} \mathrm{IP} &= 1 - \Pr\left[\max\left(\min(\gamma_{\mathrm{R}},\gamma_{\mathrm{E}}^1),\gamma_{\mathrm{E}}^2\right) < \gamma_{th}\right] \\ &= 1 - \Pr(\gamma_{\mathrm{E}}^2 < \gamma_{\mathrm{th}})\Pr\left(\min(\gamma_{\mathrm{R}},\gamma_{\mathrm{E}}^1) < \gamma_{\mathrm{th}}\right). \end{aligned} \tag{34}$$

By the same proof for OP, the IP can be obtained as (35) and shown on the top next page.

4. Numerical results

In this section, we provide numerical results to not only verify the accuracy of the proposed mathematical frameworks but also discuss the behaviors of the considered systems under the impact of various important parameters by using the Monte Carlo approach [39–43]. The simulation parameters are listed in Table 1.

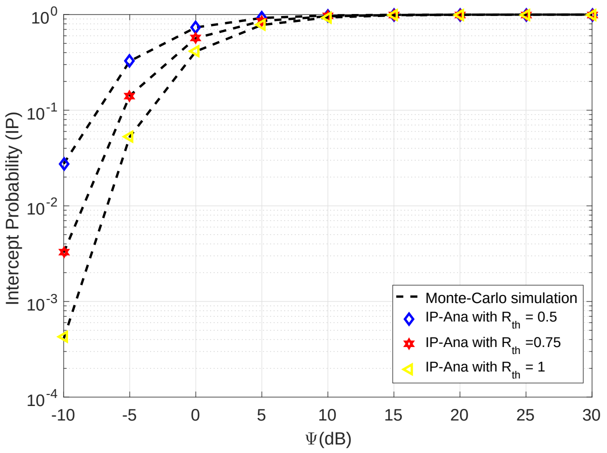


Fig. 4: The IP versus Ψ(dB) with varying R_{th} and $\eta = 0.8$, $\lambda_{\mathrm{RR}} = 2$, $\rho = 0.5$.

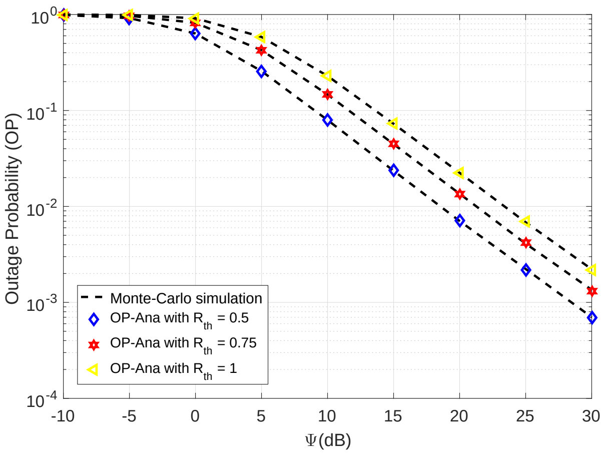


Fig. 3: The OP versus Ψ(dB) with varying R_{th} and $\eta = 0.8$, $\lambda_{\mathrm{RR}} = 2$, $\rho = 0.5$.

With varying R_{th}, the fix values $\eta = 0.8$, $\lambda_{\mathrm{RR}} = 2$, and $\rho = 0.5$, Fig. 3 and 4 displayed the OP and IP versus Ψ(dB). The curves of OP and IP match the Monte Carlo simulation findings exactly, as can be seen. By observing in Fig. 3, an increase in Ψ will result in a drop in OP performance. Because the higher Ψ is applied, the higher harvested energy at the relay will be obtained and it leads to the received SINR will be greatly improved when Ψ is large. Contrary, Fig. 4 showed that the IP performance will likewise increase. This was expected because an eavesdropper is more likely to overhear the message with higher transmission power at S. In both figures, when R_{th} is decreased, the better OP performance will be claimed and reversed with the IP case. It can be explained that the higher R_{th} leads to the higher system threshold. In addition, based on the definition of OP and IP as in equations (25) and (34), the ability to successfully decode data at D will be decreased but will be increased at E. This phenomenon can be concluded as the trade-off between OP and IP.

In Fig. 5 and 6, We presented the OP and IP versus λ_{RR} with varying η with fixed parameters $\rho = 0.5$,

$$\mathrm{IP} \approx 1 - \left[1 - \exp\left(-\frac{\gamma_{\mathrm{th}}}{\lambda_{\mathrm{SE}}\Psi}\right)\right]\left[1 - \frac{1}{2\lambda_{\mathrm{RR}}\eta\rho(\gamma_{\mathrm{th}}+1)}\left[\frac{\pi}{N}\sum_{n=1}^{N}\sqrt{1-\varphi_n^2}\right.\right.$$
$$\left.\left.\times\ \exp\left(\frac{-\varphi_n - 1}{2\eta\rho(\gamma_{\mathrm{th}}+1)\lambda_{\mathrm{RR}}}\right)\sqrt{\frac{2\gamma_{\mathrm{th}}(2\gamma_{\mathrm{th}}-2\varphi_n+1)}{\eta\rho\Psi\lambda_{\mathrm{SR}}\lambda_{\mathrm{RE}}(\gamma_{\mathrm{th}}+1)}}K_1\left(\sqrt{\frac{2\gamma_{\mathrm{th}}(2\gamma_{\mathrm{th}}-2\varphi_n+1)}{\eta\rho\Psi\lambda_{\mathrm{SR}}\lambda_{\mathrm{RE}}(\gamma_{\mathrm{th}}+1)}}\right)\right]\right]. \qquad (35)$$

Tab. 1: Simulation parameters.

Symbol	Parameter name	Value
R_{th}	Target rate	0.5; 0.75 1(bps/Hz)
η	EH efficiency	0.5;0.8;1
ρ	Power splitting ratio	0.5
d_{SR}	Distance between S and R	1m
d_{RD}	Distance between R and D	1m
d_{SD}	Distance between S and D	2m
d_{RE}	Distance between R and E	1m
d_{SE}	Distance between S and E	1m
λ_{RR}	Mean of $\lvert h_{\mathrm{RR}}\rvert^2$	2
β	Path-loss exponent	2.2
Ψ	Transmit power to noise ratio at source	-10 to 30 (dB)

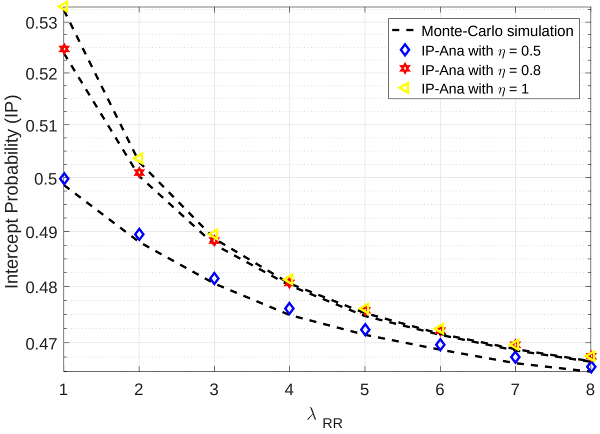


Fig. 6: The IP versus λ_{RR} with varying η and $\Psi(\mathrm{dB}) = 1$, $\rho = 0.5$, $R_{\mathrm{th}} = 1$.

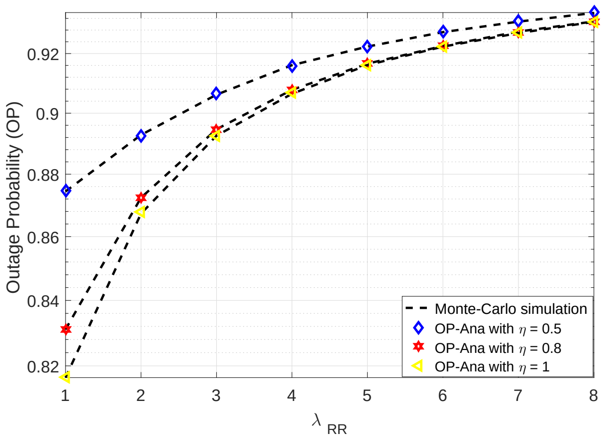


Fig. 5: The OP versus λ_{RR} with varying η and $\Psi(\mathrm{dB}) = 1$, $\rho = 0.5$, $R_{\mathrm{th}} = 1$.

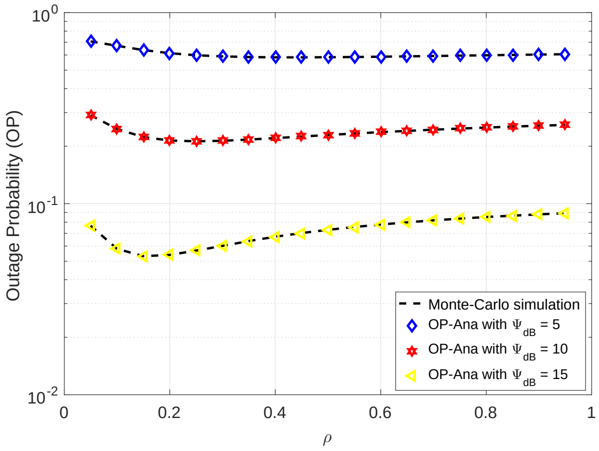


Fig. 7: The OP versus ρ varying $\Psi(\mathrm{dB})$ with $\eta = 0.8$, λ_{RR} and $R_{\mathrm{th}} = 0.5$.

$\Psi(\mathrm{dB}) = 1$, $R_{\mathrm{th}} = 1$ (bps/hz). In Fig. 5, the higher λ_{RR} will increase the OP. The reason is that increasing λ_{RR} will make (31) to converge 1, so OP in (33) will get worse. However, when the energy efficiency η is increased, the average transmit power of R will be higher and will therefore lead to an improvement in OP. Contrary, when λ_{RR} is large, it will reduce E's eavesdropping ability, but if we increase η, E's eavesdropping ability also increases significantly. Thus, the possibility of E can overhear information from S and R is also very high.

Finally, Fig. 7 and 8 displayed the OP and IP versus ρ, with varying $\Psi(\mathrm{dB})$, the fix values $\eta = 0.8$, $\lambda_{\mathrm{RR}} = 2$, and $R_{\mathrm{th}} = 0.5$. The curves of OP and IP match the Monte Carlo simulation findings exactly. The power splitting factor ρ plays an important role because it affects the portion of the used energy for energy collection and data transmission. As a result, the higher the value of ρ, the more likely it is to successfully decode the signal at R. However, the received data at the relay will decrease and vice versa. Thus, OP will be resulted in a concave function, hence, OP can obtain

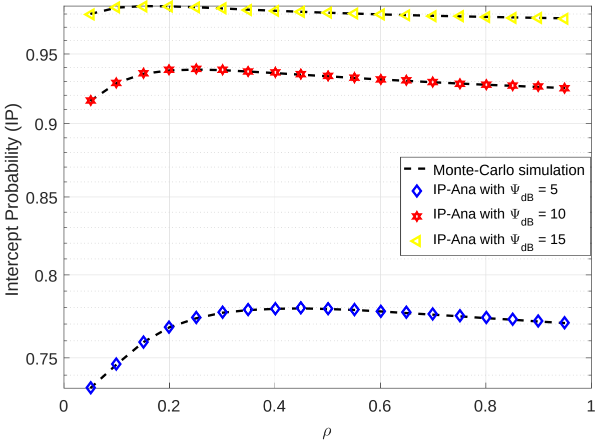


Fig. 8: The IP versus ρ varying $\Psi(dB)$ with $\eta = 0.8$, $\lambda_{\mathrm{RR}} = 2$ and $R_{\mathrm{th}} = 0.5$.

the best value at the optimal point of ρ, and after that the performance deteriorates. By observing in Fig. 7, OP with $\Psi(\mathrm{dB}) = 15$ can obtain the best values respectively at point $\rho = 0.15$. So, when the value of ρ is small, the eavesdropper has a low probability of intercepting the information. When ρ is higher than the optimal value, the outage performance and system security are worse. Furthermore, the increasing $\Psi(\mathrm{dB})$ also improved OP but also led to increase eavesdropping as similar discussion in Fig. 3 and 4. Once again, when considering the trade-off between OP and IP, selecting suitable parameters plays an important role to enhance the reliability or prevent the wiretap channel. Therefore, in order for the system to work well, we must accept high levels of eavesdropping information and vice versa.

5. Conclusion

In this study, we examined the security and reliability of a DF-FD relay network with the existence of an eavesdropper by using S-ER to improve the EH at the relay. With respect to the OP and IP, we also assessed how well the security-reliability trade-offs performed. Specifically, in Figure 7 OP with $\Psi(\mathrm{dB}) = 15$ can obtain the best values respectively at point $\rho = 0.15$. But for the same $\Psi(\mathrm{dB})$ and ρ value, in Figure8 IP has a significantly high value. So it can be said that when OP improves, IP also increases significantly. Thus, for the system to operate optimally, we used the trade-off method, which means we will calculate the probability of stopping the user's OP and the probability of intercepting the IP when eavesdropped by eavesdropper. Based on that, we will trade off between OP and IP to have both guaranteed OP and guaranteed IP. Moreover, the accuracy of the analytical formulations and the impact of system settings on network performance were confirmed and investigated through the use of Monte Carlo simulation. Especially, compared to other works as in [24], [25] and [41]. The authors only investigated full-duplex or half-duplex relay networks with the source, relay, and destination. They did not consider the existence of eavesdropper in their proposed systems. But, the model which we examine has the appearance of an eavesdropper and at the same time, we also demonstrate the interception probability of the eavesdropper and then set the optimal settings for the system. In the future, we will apply the findings of this work to scenarios including many devices, models with several relays, and the presence of interfering devices. In addition, other transmission channels, including the Rician and Nakagami-m channels, will also be taken into consideration in order to assess system performance in a more realistic manner.

Author Contributions

Both B.V.Minh and Thu-Ha Thi Pham performed the analytic calculations and performed numerical simulations. Van-Duc Phan and Anh-Vu Le wrote the whole paper.

References

[1] Huawei.5G Security: Forward Thinking. *Huawei White Paper.* 2015.

[2] Panwar, Nisha, Sharma, Shantanu, Singh and Awadhesh Kumar. A survey on 5G: The next generation of mobile communication. *Physical Communication.* vol.18, no. 2, pp. 64-84, 2016. DOI: 10.1016/j.phycom.2015.10.006.

[3] Fang, Dongfeng, Qian, Yi, Hu and Rose Qingyang. Security for 5G mobile wireless networks. *IEEE Access.* vol.6, no. 2, pp. 4850-4874, 2018. DOI: 10.1109/ACCESS.2017.2779146.

[4] Chettri, Lalit, Bera and Rabindranath. A Comprehensive Survey on Internet of Things (IoT) Toward 5G Wireless Systems. *IEEE Internet of Things Journal.* vol. 7, no. 1, pp. 16-32, Jan. 2020. DOI: 10.1109/JIOT.2019.2948888.

[5] Mukherjee, Amitav, Fakoorian, S Ali A, Huang, Jing, Swindlehurst, and A. Lee. Principles of physical layer security in multiuser wireless networks: A survey. *IEEE Communications Surveys & Tutorials.* 16.3 (2014): 1550-1573. DOI: 10.1109/SURV.2014.012314.00178.

[6] Yang N., Wang L., Geraci G., Elkashlan M., Yuan J., and Di Renzo M. Safeguarding 5G

wireless communication networks using physical layer security. *IEEE Communications Magazine*. vol. 53, no. 4, pp. 20-27, April 2015. DOI: 10.1109/MCOM.2015.7081071.

[7] Makarfi A.U., Rabie K.M., Kaiwartya O., Adhikari K., Nauryzbayev G., Li X., and Kharel R. Toward Physical-Layer Security for Internet of Vehicles: Interference-Aware Modeling. *IEEE Internet of Things Journal*. 8.1 (2020): 443-457. DOI: 10.1109/JIOT.2020.3006527.

[8] Jiang X., Li P., Li B., Zou Y., and Wang R. Intelligent jamming strategies for secure spectrum sharing systems. *IEEE Transactions on Communications*. 70.2 (2022): 1153-1167. DOI: 10.1109/TCOMM.2021.3140082.

[9] Jeong C., Kim I., Kim D.I. Joint Secure Beamforming Design at the Source and the Relay for an Amplify-and-Forward MIMO Untrusted Relay System. *IEEE Transactions on Signal Processing*. vol. 60, no. 1, pp. 310-325, Jan. 2012. DOI: 10.1109/TSP.2011.2172433.

[10] Wang H.M., Wang C., and Derrick W.K.N. Artificial Noise Assisted Secure Transmission Under Training and Feedback. *IEEE Transactions on Signal Processing*. vol. 63, no. 23, pp. 6285-6298, Dec.1, 2015. DOI: 10.1109/TSP.2015.2465301.

[11] A. Mukherjee and A. L. Swindlehurst. Robust beamforming for security in MIMO wiretap channels with imperfect CSI. *IEEE Transactions on Signal Processing*. vol. 59, no. 1, pp. 351-361, Jan. 2011. DOI: 10.1109/TSP.2010.2078810.

[12] Liang Y., Poor H.V., Shamai S., and others. Information theoretic security. *Foundations and Trends® in Communications and Information Theory*. 5.4–5 (2009): 355-580. DOI: 10.1561/0100000036.

[13] Bloch M. and Barro J. *Physical-layer security: from information theory to security engineering*. City: publisher, 2015. ISBN 978-0-521-51650-1.

[14] Poor H.V. and Schaefer Rafael F. Wireless physical layer security. *Proceedings of the National Academy of Sciences*. 114.1 (2017): 19-26. DOI: 10.1073/pnas.1618130114.

[15] Sun L. and Du Qinghe. Physical layer security with its applications in 5G networks: A review. *China communications*. 14.12 (2017): 1-14. DOI: 10.1109/CC.2017.8246328.

[16] Cao Y., Wang S., Jin M., Zhao N., Xing C., Chen Y., and Ding Z. Power Optimization for Enhancing Secrecy of Cooperative User Relaying NOMA Networks. *IEEE Transactions on Vehicular Technology*. vol. 69, no. 7, pp. 8008-8012, Jul. 2020. DOI: 10.1109/TVT.2020.2992765.

[17] Zou Y., Wang X., Shen W., and Hanzo L. Security Versus Reliability Analysis of Opportunistic Relaying. *IEEE Transactions on Vehicular Technology*. vol. 63, no. 6, pp. 2653-2661, Jul. 2014. DOI: 10.1109/TVT.2013.2292903.

[18] Zhu J., Zou Y., Champagne B., Zhu W.P., and Hanzo L. Security–Reliability Tradeoff Analysis of Multirelay-Aided Decode-and-Forward Cooperation Systems. *IEEE Transactions on Vehicular Technology*. vol. 65, no. 7, pp. 5825-5831, Jul. 2016. DOI: 10.1109/TVT.2015.2453364.

[19] Khoshafa M.H., Moualeu J.M., Ngatched T.M.N., and Ahmed M.H. On the Performance of Secure Underlay Cognitive Radio Networks With Energy Harvesting and Dual-Antenna Selection. *IEEE Communications Letters*. vol. 25, no. 6, pp. 1815-1819, Jun. 2021. DOI: 10.1109/LCOMM.2021.3063673.

[20] Li X., Zhao M., Gao X.C., Li L., Do D.T., Rabie K.M., and Kharel R. Physical Layer Security of Cooperative NOMA for IoT Networks Under I/Q Imbalance. *IEEE Access*. vol. 8, pp. 51189-51199, 2020. DOI: 10.1109/ACCESS.2020.2980171.

[21] Khoshafa M.H., Ngatched T.M.N., and Ahmed M.H. On the Physical Layer Security of Underlay Multihop Device-to-Device Relaying. *2019 IEEE Wireless Communications and Networking Conference (WCNC)*. Marrakesh, Morocco, 2019, pp. 1-6. DOI: 10.1109/WCNC.2019.8886089.

[22] Yan P., Zou Y., Ding X., and Zhu J. Energy-Aware Relay Selection Improves Security-Reliability Tradeoff in Energy Harvesting Cooperative Cognitive Radio Systems. *IEEE Transactions on Vehicular Technology*. vol. 69, no. 5, pp. 5115-5128, May 2020. DOI: 10.1109/TVT.2020.2979267.

[23] Lee S., Zhang R., and Huang K. Opportunistic Wireless Energy Harvesting in Cognitive Radio Networks. *IEEE Transactions on Wireless Communications*. vol. 12, no. 9, pp. 4788-4799, September 2013. DOI: 10.1109/TWC.2013.072613.130323.

[24] Tin P.T., Nguyen T.N., Tran D.H., Voznak M., Phan V.D., and Chatzinotas S. Performance Enhancement for Full-Duplex Relaying with Time-Switching-Based SWIPT in Wireless Sensors Networks. *Sensors*. 2021, 21, 3847. DOI: 10.3390/s21113847.

[25] Nguyen T.N., Tran M., Nguyen T.L., Ha D.H., and Voznak M. Multisource Power Splitting Energy Harvesting Relaying Network in Half-Duplex System over Block Rayleigh Fading Channel: System Performance Analysis. *Electronics*. 2019, 8, 67. DOI: 10.3390/electronics8010067.

[26] Nguyen T.N, Tran P.T., and Vozňák M. Power splitting–based energy-harvesting protocol for wireless-powered communication networks with a bidirectional relay. *International Journal of Communication Systems*. 31.13 (2018): e3721. DOI: 10.1002/dac.3721.

[27] Nguyen T.N., Tran M., Nguyen T.L., Ha D.H., and Voznak M. Performance analysis of a user selection protocol in cooperative networks with power splitting protocol-based energy harvesting over Nakagami-m/Rayleigh channels. *Electronics*. 8.4 (2019): 448. DOI: 10.3390/electronics8040448.

[28] Nguyen T.N., Duy T.T., Phuong T.T, Voznak M., Li X., and Poor H.V. Partial and full relay selection algorithms for AF multi-relay full-duplex networks with self-energy recycling in non-identically distributed fading channels. *IEEE Transactions on Vehicular Technology*. 71.6 (2022): 6173-6188. DOI: 10.1109/TVT.2022.3158340.

[29] Hu S., Ding Z., and Ni Q. Beamforming optimization in energy harvesting cooperative full-duplex networks with self-energy recycling protocol. *IET Communications*. 10.7 (2016): 848-853. DOI: 10.1049/iet-com.2015.0476.

[30] Zeng Y. and Zhang R. Full-duplex wireless-powered relay with self-energy recycling. *IEEE Wireless Communications Letters*. 4.2 (2015): 201-204. DOI: 10.1109/LWC.2015.2396516.

[31] Atapattu S., Ross N., Jing Y., and Premaratne M. Source-based jamming for physical-layer security on untrusted full-duplex relay. *IEEE Communications Letters*. 23.5 (2019): 842-846. DOI: 10.1109/LCOMM.2019.2907627.

[32] Phan V.D., Nguyen T.N., A.V. Le, and Voznak M. A study of physical layer security in SWIPT-based decode-and-forward relay networks with dynamic power splitting. *Sensors*. 21.17 (2021): 5692. DOI: 10.3390/s21175692.

[33] Nguyen T.N., Minh B.V., Tran D.H., Le T.L., Le, A.T., Q.S. Nguyen, and Lee B. M. Security–Reliability Analysis of AF Full-Duplex Relay Networks Using Self-Energy Recycling and Deep Neural Networks. *Sensors*. 23.17 (2023): 7618. DOI: 10.3390/s23177618.

[34] Pandey A. and Yadav S. Physical layer security in cooperative amplify-and-forward relay networks over mixed Nakagami-m and double Nakagami-m fading channels: performance evaluation and optimization. *IET Communications*. 14.1 (2020): 95-104. DOI: 10.1049/iet-com.2019.0584.

[35] Nguyen T.N., Tran D.H., Chien T.V., Phan V.D., Voznak M., Tin P.T., Chatzinotas S., D.W Kwan Ng, and Poor H.V. Security–Reliability Tradeoff Analysis for SWIPT- and AF-Based IoT Networks With Friendly Jammers. *IEEE Internet of Things Journal*. vol. 9, no. 21, pp. 21662-21675, 1 Nov.1, 2022. DOI: 10.1109/JIOT.2022.3182755.

[36] Nguyen T.N., Tran D.H., Chien T.V., Phan V.D., N.Tien Nguyen, Voznak M., Chatzinotas S., Ottersten B., and Poor H.V. Physical Layer Security in AF-Based Cooperative SWIPT Sensor Networks. *IEEE Sensors Journal*. Vol. 23, No. 1, pp. 689-705, Nov. 2022. DOI: 10.1109/JSEN.2022.3224128.

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

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

[39] Nguyen B.C., Tran M.H., and Phuong T.T. Improving the performance of spatial modulation full-duplex relaying system with hardware impairment using transmit antenna selection. *IEEE Access*. vol. 8, pp. 20191-20202, Jan. 2020. DOI: 10.1109/ACCESS.2020.2968571.

[40] Tran M.H., Nguyen B.C., and Phuong T.T. Outage Analysis of RF Energy Harvesting Cooperative Communication Systems Over Nakagami- Fading Channels With Integer and Non-Integer m. *IEEE Trans. on Vehicu. Techno.*. vol. 69, no. 3, pp. 2785-2801, Jan. 2020. DOI: 10.1109/TVT.2020.2964809.

[41] Nguyen T.N., Phuong T.T., and Voznal M. Wireless energy harvesting meets receiver diversity: A successful approach for two-way half-duplex relay networks over block Rayleigh fading channel. *Computer Networks*. vol. 172, p. 107176, May. 2020. DOI: 10.1016/j.comnet.2020.107176.

[42] Hung Nguyen, Tan N. Nguyen, Bui Vu Minh, Thu-Ha Thi Pham, Anh-Tu Le, and Miroslav Voznak. Security-Reliability Analysis in CR-NOMA IoT Network Under I/Q Imbalance. *IEEE Access*. Vol. 11, pp. 119045-119056, Nov. 2023. DOI: 10.1109/ACCESS.2023.3327789.

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

About Authors

Bui Vu MINH was born on March 02, 1991, in Dong Nai, Vietnam. He graduated in Electrical and Electronic Engineering in 2015 from Nguyen Tat Thanh University, Ho Chi Minh City, Vietnam. End of 2014, he joined the Faculty of Engineering and Technology of Nguyen Tat Thanh University as a laboratory practice management, and then he became a lecturer in 2017. In 2019, he received a Master's degree in Electrical Engineering from Ho Chi Minh City University of Technology and Education, Ho Chi Minh City, Vietnam. His major research interests are Wireless Networks, Robot, Artificial Neural Networks, and Power Electronics.

Anh-Vu LE (corresponding author) is at Communication and Signal Processing Research Group, Faculty of Electrical and Electronics Engineering, Ton Duc Thang University, Ho Chi Minh City, Vietnam. He has been worked as a Postdoc Research Fellow in ROAR Laboratory at Singapore University of Technology and Design. He received his BS in Electronics and Telecommunications from Ha Noi University of Technology, Vietnam and Ph.D. in Electronics and Electrical from the Dongguk University, Korea in 2007 and 2015, respectively. His current research interests include Robotics vision, Robot navigation, Human detection, Action recognition, Feature matching, 3D video processing, Signal processing.

Van-Duc PHAN was born in 1975 in Long An province, Vietnam. He received his M.S. degree in Department of Electric, Electrical and Telecommunication Engineering from Ho Chi Minh City University of Transport, Ho Chi Minh, Vietnam and Ph.D. degree in Department of Mechanical and Automation Engineering, Da-Yeh University, Taiwan in 2016. Currently, his research interests are in sliding mode control, non-linear systems or active magnetic bearing, flywheel store energy systems, power system optimization, optimization algorithms, renewable energies, Energy harvesting (EH) enabled cooperative networks, Improving the optical properties, lighting performance of white LEDs, Energy efficiency LED driver integrated circuits, Novel radio access technologies, Physical security in the communication network.

Thu-Ha Thi PHAM was born in 2003 in Ha Tinh City, Vietnam. She is currently pursuing the B.Sc. degree in electronics and telecommunications engineering at Ton Duc Thang University, Viet Nam. Her current research interests include non-orthogonal multiple-access (NOMA), energy harvesting, full-duplex networks, physical layer security, and reconfigurable intelligent surface (RIS).