Proceedings of the Seventh International Conference on Research in Intelligent and Computing in Engineering pp. 165–170 ISSN 2300-5963 ACSIS, Vol. 33
DOI: 10.15439/2022R21

Outage Probability and Intercept Probability Of Cognitive IoTs Networks With Relay Selection, Passive Eavesdropper and Hardware Noises

Pham Xuan Minh, Nguyen Van Hien,
Pham Quoc Hop, Tran Trung Duy, Le Quang Phu
Posts and Telecommunications Institute of Technology
HoChiMinh city campus, Viet Nam
{minhpx, nvhien, pqhop, trantrungduy, phulq}
@ptithcm.edu.vn

Nguyen Trung Hieu
Department of Electrical Engineering
Posts and Telecommunications
Institute of Technology
Ha Noi, Viet Nam
hieunt@ptit.edu.vn

***Abstract*—This paper measures outage probability (OP) and intercept probability (IP) of a secondary secure network in a relaying underlay spectrum-sharing cognitive radio (USS-CR) system. In this scheme, one of successful secondary relays is chosen to obtain the highest signal-to-noise ratio (SNR) at a secondary destination. This paper considers the case where channel state information (CSI) of the eavesdropping links is not available. The OP and IP performance of the considered scheme is calculated via analysis and simulations, under impact of hardware noises, over Rayleigh fading channels**

***Index Terms*—Underlay spectrum-sharing cognitive radio, physical-layer security, outage probability, intercept probability, hardware impairments.**

I. Introduction

Recently, physical-layer security (PLS) has been reported in many literature (i.e., [1]-[4]) as an efficient approach to obtain security for wireless communication systems. For the secure communication in PLS over fading channels, the data links should be better than the eavesdropping ones. In [5]-[8], diversity-based transmitting/ receiving techniques in multi-input multi-output (MIMO) networks were proposed to increase SNR of the data channels. In [9]-[11], various cooperative jamming approaches were proposed to reduce SNR of the eavesdropping channels. However, implementation of the approaches in [9]-[11] is a difficult work because they require a high synchronization and a perfect interference cancellation. When wireless devices, e.g., sensors, are only equipped with a single antenna, cooperative relaying [12]-[15] can be efficiently applied into the PLS networks. Moreover, relay selection algorithms such as partial and full relay selection were employed to increase the e2e SNR of the data links, which also improved the secrecy performance such as secrecy outage probability (SOP) and IP/OP trade-off. Published works [15]-[16] proposed joint relay selection and cooperative jamming strategies for secured communication cooperative relaying scenarios. In [17]-[18], the authors introduced intelligent reflecting surface (IRS)-based PLS schemes, where the source-destination communication was assisted by IRS, instead of the cooperative relays.

In the USS-CR networks [19]-[20], secondary users must optimally change their transmit power to protect quality of service of a primary network. Particularly, CSI of the secondary transmitter -the primary receiver links are used to calculate the instantaneous transmit power. Different from [19]-[20], published work [21] introduced a new transmit power adaptation method, where average transmit power of the secondary devices was appropriately adjusted so that the OP performance of the primary network did not exceed a pre-designed value. Published works [22]-[26] concerned with PLS in the USS-CR networks. In particular, the authors in [22]-[23] evaluated the IP-OP trade-off of the PLS USS-CR networks. The authors [24] measured SOP and average secrecy capacity (ASC) for USS-CR over Nakagamim channels. Reference [25] proposed a new PLS Internet of Things (IoTs) model using NOMA and short packet communication. The authors in [26] derived secrecy outage probability of unmanned aerial vehicle-aided USS-CR networks adopting non-orthogonal multiple access (NOMA).

Recently, topic of evaluating performance of the PLS schemes under impact of hardware imperfection has gained much attention. In [27], the authors calculated probability of positive secrecy capacity for multi-hop PLS schemes with hardware noises. In [28], the authors proposed a secure amplify-and-forward (AF) scheme, with a multi-antenna eavesdropper and hardware impairments. The authors in [29] studied the OP-IP trade-off for NOMA-aided PLS models, under effect of IQI (in-phase and quadrature-phase imbalance). Reference [30] investigated joint impact of co-channel interference and hardware imperfection on the IP and OP performance of sensor networks. The authors of [31]-[32] studied performance of hybrid satellite-terrestrial relaying PLS schemes with hardware impairments.

This paper evaluates OP and IP of the secure USS-CR networks, under effect of hardware impairments. Particularly, we focus on the cooperative phase in the secondary network, where successful relays transmit the data to a destination. Follows operation principle of USS-CR [19]-[20], these relays must change their transmit power to satisfy the interference constraint. With presence of a passive eavesdropper, one of the successful relays is selected to provide the highest instantaneous SNR for the relay-destination communication. We then derive exact formulas of OP and IP for the proposed PLS USS-CR scheme, and realize computer simulations to validate them.

A. *Related Works*

At first, different with [27]-[30], this paper considers the PLS USS-CR networks. Next, although the related works [22]-[26] and [33]-[37] also study the IP/OP trade-off performance for the PLS USS-CR networks, the main difference can be listed as follows:

- Published work [22] considered full-duplex jamming with assistance of IRS in device-to-device communication networks; the authors in [23] applied radio-frequency energy harvesting technique into the PLS USS-CR networks; and reference [24] evaluated secrecy outage performance. However, the works [22]-[24] did not consider impact of hardware noises on the secrecy performance.

- Reference [25] applied NOMA and short packet communication for the PLS USS-CR networks, while published work [26] studied UAV-aided NOMA MIMO systems. However, the techniques adopted in [25]-[26] are out of scope of this paper.

- Although the authors in [33] also studied PLS in the cooperative phase, the main difference is that [33] adopted jammer and relay selection strategies for maximizing instantaneous secrecy capacity. Next, effect of hardware noises was not studied in [33]. Finally, this paper considers the PLS scheme with presence of the passive eavesdropper, i.e., CSI of the eavesdropping link is not available at the legitimate transmitters and receivers.

- Different with relay selection methods studied in [34], the relay selection method in this paper is performed to maximize SNR obtained at the secondary destination.

- Different with this paper, reference [35] concerns with SOP evaluation of the multi-hop PLS scheme in the USS-CR with hardware imperfection. In addition, this paper does not study radio frequency energy harvesting as in [35].

- Main difference between this work and [36] can be listed as: i) the secondary transmitters in [36] must change transmit power, follows a joint constraint of minimum OP value of the primary network and maximum IP value at the secondary eavesdropper; ii) this paper does not consider presence of the interference from the primary network.

- Different with published work [37], this paper does not consider Fountain codes and the cooperative jamming technique.

Finally, we note that different with the previous works, this paper uses mathematical tools to derive new OP and IP formulas for the proposed scheme over Rayleigh fading channel. Moreover, this paper also analyzes impact of hardware noises and number of relay nodes on the IP-OP trade-off.

The remainder of this paper is given as follows. Operation principle and performance of the considered scheme are shown in Section II and III, respectively. Both the computer simulations and the theoretical results are given in Section IV. Finally, final discussion and recommendation are given in Section V.

II. System Model

Figure 1 presents the cooperative transmission in the considered USS-CR IoTs scheme, where in the secondary network, M successful relays (SR) want to send the source data to the destination (SD) with presence of the eavesdropper (SE). For ease of presentation, the broadcast phase, the transmission between the secondary source and the secondary relays, is not illustrated in this paper (see [33]). Then, one of these relays is selected to forward the source data to SD. Moreover, the selected relay must change transmit power to satisfy the interference threshold $\left(I_{\text{th}}\right)$ given by the primary receiver (PR). All the SR, SD, SE and PR nodes are assumed to have only one antenna.

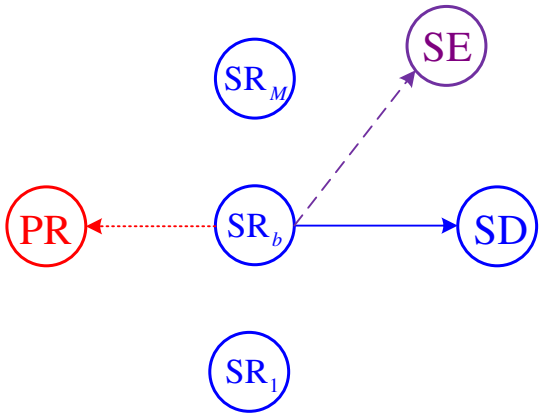

Fig. 1. The considered USS-CR IoTs scheme.

Considering the $\text{A}\to\text{B}$ Rayleigh fading channel between the transmitter A $\left(\text{A}\in\{\text{SR}_m\}\right)$ and the receiver B $\left(\text{B}\in\{\text{PR},\text{SD},\text{SE}\}\right)$, with $m\in\{1,2,...,M\}$. Let $g_{\text{A,B}}$ denote channel gain between A and B. Therefore, cumulative distribution function (CDF) and probability density function (PDF) of $g_{\text{A,B}}$ are expressed, respectively as

$$\begin{aligned} F_{g_{\text{A,B}}}(x) &= 1-\exp\left(-\lambda_{\text{A,B}}x\right), \\ f_{g_{\text{A,B}}}(x) &= \lambda_{\text{A,B}}\exp\left(-\lambda_{\text{A,B}}x\right). \end{aligned} \tag{1}$$

We assume that the random variables $g_{\text{SR}_m,\text{B}}$ are idependent and identical, i.e., $\lambda_{\text{SR}_m,\text{B}}=\lambda_{\text{SR,B}}$ for all m and B. Similar to [35]-[36], the transmit power of SR_m can be obtained as

$$P_{\text{SR}_m}=\frac{I_{\text{th}}}{\left(1+\kappa_{\text{P}}^2\right)g_{\text{SR}_m,\text{PR}}}=\frac{Q_{\text{th}}}{g_{\text{SR}_m,\text{PR}}}, \tag{2}$$

where κ_{P}^2 is hardware-noise level of the $\text{SR}_m\to\text{PR}$ link (see [35]-[36]), for all m, and $Q_{\text{th}}=I_{\text{th}}\Big/\left(1+\kappa_{\text{P}}^2\right)$.

From (2), we can write SNR of the $\text{SR}_m\to\text{SD}$ link as

$$\gamma_{\text{SR}_m,\text{SD}}=\frac{P_{\text{SR}_m}g_{\text{SR}_m,\text{SD}}}{\kappa_{\text{D}}^2P_{\text{SR}_m}g_{\text{SR}_m,\text{SD}}+N_0}, \tag{3}$$

where κ_{D}^2 is hardware-noise level of the $\text{SR}_m\to\text{SD}$ links, for all m, and N_0 is variance of additive noise at SD.

Substituting (2) into (3), which yields

$$\gamma_{\mathrm{SR}_m,\mathrm{SD}}=\frac{\frac{Q_{\mathrm{th}}}{g_{\mathrm{SR}_m,\mathrm{PR}}}g_{\mathrm{SR}_m,\mathrm{SD}}}{\kappa_{\mathrm{D}}^2\frac{Q_{\mathrm{th}}}{g_{\mathrm{SR}_m,\mathrm{PR}}}g_{\mathrm{SR}_m,\mathrm{SD}}+N_0}. \tag{4}$$

From (4), the best relay is selected as follows:

$$\begin{aligned}\mathrm{SR}_b:\gamma_{\mathrm{SR}_b,\mathrm{SD}}&=\max_{m=1,2,\ldots,M}\left(\gamma_{\mathrm{SR}_m,\mathrm{SD}}\right)\\ \leftrightarrow\frac{g_{\mathrm{SR}_b,\mathrm{SD}}}{g_{\mathrm{SR}_b,\mathrm{PR}}}&=\max_{m=1,2,\ldots,M}\left(\frac{g_{\mathrm{SR}_m,\mathrm{SD}}}{g_{\mathrm{SR}_m,\mathrm{PR}}}\right),\end{aligned} \tag{5}$$

where $b\in\{1,2,...,M\}$. Equation (5) implies that SR_b provides the highest SNR obtained at SD (or the ratio $g_{\mathrm{SR}_b,\mathrm{SD}}/g_{\mathrm{SR}_b,\mathrm{PR}}$ is highest).

Then, the instantaneous SNR obtained at SE can be obtained as

$$\begin{aligned}\gamma_{\mathrm{SR}_b,\mathrm{SE}}&=\frac{P_{\mathrm{SR}_b}g_{\mathrm{SR}_b,\mathrm{SE}}}{\kappa_{\mathrm{E}}^2P_{\mathrm{SR}_b}g_{\mathrm{SR}_b,\mathrm{SE}}+N_0},\\ &=\frac{\frac{Q_{\mathrm{th}}}{g_{\mathrm{SR}_b,\mathrm{PR}}}g_{\mathrm{SR}_b,\mathrm{SE}}}{\kappa_{\mathrm{E}}^2\frac{Q_{\mathrm{th}}}{g_{\mathrm{SR}_b,\mathrm{PR}}}g_{\mathrm{SR}_b,\mathrm{SE}}+N_0},\end{aligned} \tag{6}$$

where κ_{E}^2 is hardware-noise level of the eavesdropping links, for all m, and N_0 also denotes variance of the noise at SE.

Next, OP at SD and IP at SE are defined, respectively as

$$\begin{aligned}\mathrm{OP}&=\Pr\left(\gamma_{\mathrm{SR}_b,\mathrm{SD}}<\gamma_{\mathrm{th}}\right),\\ \mathrm{IP}&=\Pr\left(\gamma_{\mathrm{SR}_b,\mathrm{SE}}\geq\gamma_{\mathrm{th}}\right),\end{aligned} \tag{7}$$

where γ_{th} is a pre-determined value.

III. Performance Analysis

Combining (4) and (7), we rewrite OP as follows:

$$\mathrm{OP}=\Pr\left(\left(1-\kappa_{\mathrm{D}}^2\gamma_{\mathrm{th}}\right)X_b<\frac{N_0\gamma_{\mathrm{th}}}{Q_{\mathrm{th}}}\right), \tag{8}$$

where $X_m=g_{\mathrm{SR}_m,\mathrm{SD}}/g_{\mathrm{SR}_m,\mathrm{PR}}\ (\forall m)$. We observe that if $1-\kappa_{\mathrm{D}}^2\gamma_{\mathrm{th}}\leq 0$ then $\mathrm{OP}=1$. Considering the case of $1-\kappa_{\mathrm{D}}^2\gamma_{\mathrm{th}}>0$, we can rewrite (8) as

$$\mathrm{OP}=\Pr\left(X_b<\theta_{\mathrm{D,th}}\right)=F_{X_b}\left(\theta_{\mathrm{D,th}}\right), \tag{9}$$

where

$$\theta_{\mathrm{D,th}}=\frac{N_0\gamma_{\mathrm{th}}}{\left(1-\kappa_{\mathrm{D}}^2\gamma_{\mathrm{th}}\right)Q_{\mathrm{th}}}. \tag{10}$$

To find CDF $F_{X_b}(x)$, we first find CDF $F_{X_m}(x)$ which can be formulated as

$$\begin{aligned}F_{X_m}(x)&=\Pr\left(g_{\mathrm{SR}_m,\mathrm{SD}}<xg_{\mathrm{SR}_m,\mathrm{PR}}\right)\\ &=\int_0^{+\infty}F_{g_{\mathrm{SR}_m,\mathrm{SD}}}(xy)f_{g_{\mathrm{SR}_m,\mathrm{PR}}}(y)dy.\end{aligned} \tag{11}$$

Substituting (1) into (11), after calculating the integral, we obtain (12) as

$$F_{X_m}(x)=\frac{\lambda_{\mathrm{SR,SD}}x}{\lambda_{\mathrm{SR,PR}}+\lambda_{\mathrm{SR,SD}}x}=\frac{x}{x+\Omega_{\mathrm{D}}}, \tag{12}$$

where $\Omega_{\mathrm{D}}=\lambda_{\mathrm{SR,PR}}/\lambda_{\mathrm{SR,SD}}$. Then, PDF of X_m is obtained as

$$f_{X_m}(x)=\frac{\Omega_{\mathrm{D}}}{\left(x+\Omega_{\mathrm{D}}\right)^2}. \tag{13}$$

Therefore, the distribution functions of X_b are given as

$$F_{X_b}(x)=\left[F_{X_m}(x)\right]^M=\left(\frac{x}{x+\Omega_{\mathrm{D}}}\right)^M, \tag{14}$$

$$f_{X_b}(x)=\frac{M\Omega_{\mathrm{D}}x^{M-1}}{\left(x+\Omega_{\mathrm{D}}\right)^{M+1}}. \tag{15}$$

Substituting (14) into (9), we obtain OP as given in (16) below:

$$\mathrm{OP}=\left(\frac{\theta_{\mathrm{D,th}}}{\theta_{\mathrm{D,th}}+\Omega_{\mathrm{D}}}\right)^M. \tag{16}$$

For the IP performance; combining (6) and (7), we can obtain (17) as

$$\begin{aligned}\mathrm{IP}&=\Pr\left(\frac{g_{\mathrm{SR}_b,\mathrm{SE}}}{g_{\mathrm{SR}_b,\mathrm{PR}}}\geq\theta_{\mathrm{E,th}}\right)\\ &=\int_0^{+\infty}F_{g_{\mathrm{SR}_b,\mathrm{PR}}}\left(\frac{x}{\theta_{\mathrm{E,th}}}\right)f_{g_{\mathrm{SR}_b,\mathrm{SE}}}(x)dx.\end{aligned} \tag{17}$$

where

$$\theta_{\mathrm{E,th}}=\frac{N_0\gamma_{\mathrm{th}}}{\left(1-\kappa_{\mathrm{E}}^2\gamma_{\mathrm{th}}\right)Q_{\mathrm{th}}}. \tag{18}$$

It is noted from (17)-(18) that we only consider the case where $1-\kappa_{\mathrm{E}}^2\gamma_{\mathrm{th}}>0$. Indeed, if $1-\kappa_{\mathrm{E}}^2\gamma_{\mathrm{th}}\leq 0$, IP always equals to zero.

Moreover, to calculate IP in (17), our next objective is to find CDF of $g_{\mathrm{SR}_b,\mathrm{PR}}$. Using derivation methods used in [38]-[40], we can formulate $F_{g_{\mathrm{SR}_b,\mathrm{PR}}}(x)$ as

$$\begin{aligned}&F_{g_{\mathrm{SR}_b,\mathrm{PR}}}(x)=\\ &\int_0^{+\infty}\frac{\partial\Pr\left(g_{\mathrm{SR}_m,\mathrm{PR}}<x,X_m<z\right)}{\partial z}\frac{f_{X_b}(z)}{f_{X_m}(z)}dz.\end{aligned} \tag{19}$$

As marked in (19), the probability $\Pr\left(g_{\mathrm{SR}_m,\mathrm{PR}}<x,X_m<z\right)$ is computed as

$$\begin{aligned}
&\Pr\left(g_{\mathrm{SR}_m,\mathrm{PR}} < x, X_m < z\right) \\
&= \Pr\left(g_{\mathrm{SR}_m,\mathrm{PR}} < x, g_{\mathrm{SR}_m,\mathrm{SD}} < g_{\mathrm{SR}_m,\mathrm{PR}} z\right) \\
&= \int_0^x f_{g_{\mathrm{SR}_m,\mathrm{PR}}}(u)\left[\int_0^{uz} f_{g_{\mathrm{SR}_m,\mathrm{SD}}}(v)dv\right]du \qquad (20) \\
&= \frac{z}{z+\Omega} - \exp\left(-\lambda_{\mathrm{SR,PR}} x\right) \\
&+ \frac{\Omega}{z+\Omega}\exp\left(-\lambda_{\mathrm{SR,PR}} x\right)\exp\left(-\lambda_{\mathrm{SR,SD}} xz\right).
\end{aligned}$$

Plugging (13), (15), (19) and (20) together, after some careful calculation, we obtain

$$\begin{aligned}
F_{g_{\mathrm{SR}_b,\mathrm{PR}}}(x) &= 1 - \sum_{n=0}^{M-1}(-1)^n C_{M-1}^n M \\
&\times \left\{ \begin{array}{l} (-1)^n \dfrac{n}{(n+1)!}\left(\lambda_{\mathrm{SR,PR}}\right)^{n+1} x^{n+1} E_1\left(\lambda_{\mathrm{SR,PR}} x\right) + \\ \exp\left(-\lambda_{\mathrm{SR,PR}} x\right)\left[\begin{array}{l} \displaystyle\sum_{k=0}^{n}(-1)^{k+2}\frac{\left(\lambda_{\mathrm{SR,PR}}\right)^k}{(n+1)n\ldots(n+1-k)}x^k \\ + \displaystyle\sum_{k=0}^{n-1}(-1)^{k+2}\frac{\left(\lambda_{\mathrm{SR,PR}}\right)^{k+1}}{n(n-1)\ldots(n-k)}x^{k+1} \end{array}\right] \end{array}\right\}, \qquad (21)
\end{aligned}$$

where $E_1(.)$ is exponential integral function [41].

Substituting (21) and $f_{g_{\mathrm{SR}_b,\mathrm{SE}}}(x) = \lambda_{\mathrm{SR,SE}}\exp\left(-\lambda_{\mathrm{SR,SE}} x\right)$ into (17); using [41, eq. (6.228.2)] and $E_1(x) = -\mathrm{E}i(-z)$, we finally obtain an exact formula of IP as follows:

$$\begin{aligned}
\mathrm{IP} &= 1 - \sum_{n=0}^{M-1}(-1)^n C_{M-1}^n M \\
&\times \left\{ \begin{array}{l} (-1)^n \dfrac{n\left(\Omega_{\mathrm{E}}\right)^{n+1}\theta_{\mathrm{E,th}}}{(n+2)\left(\theta_{\mathrm{E,th}}+\Omega_{\mathrm{E}}\right)^{n+2}} \\ \times {}_2F_1\left(1, n+2; n+3, \dfrac{\theta_{\mathrm{E,th}}}{\Omega_{\mathrm{E}}+\theta_{\mathrm{E,th}}}\right) \\ + \displaystyle\sum_{k=0}^{n}\frac{(-1)^{k+2}\,k!}{(n+1)n\ldots(n+1-k)}\frac{\left(\Omega_{\mathrm{E}}\right)^k\theta_{\mathrm{E,th}}}{\left(\theta_{\mathrm{E,th}}+\Omega_{\mathrm{E}}\right)^{k+1}} \\ + \displaystyle\sum_{k=0}^{n-1}\frac{(-1)^{k+2}(k+1)!}{n(n-1)\ldots(n-k)}\frac{\left(\Omega_{\mathrm{E}}\right)^{k+1}\theta_{\mathrm{E,th}}}{\left(\theta_{\mathrm{E,th}}+\Omega_{\mathrm{E}}\right)^{k+2}} \end{array}\right\}, \qquad (22)
\end{aligned}$$

where $\Omega_{\mathrm{E}} = \lambda_{\mathrm{SR,PR}}/\lambda_{\mathrm{SR,SE}}$, and ${}_2F_1(.)$ is Gaussian hypergeometric function [41].

IV. Simulation and Theoretical Results

This section presents both simulation and theoretical results of OP and IP, which are in an excellent agreement in all figures below. To focus on evaluating impact of the number of relays (M) and hardware noises, we fix the other parameters as follows: $\kappa_{\mathrm{P}}^2 = 0$, $\lambda_{\mathrm{SR,SD}} = 1$, $\lambda_{\mathrm{SR,SE}} = 50$, $\lambda_{\mathrm{SR,PR}} = 5$, and $\gamma_{\mathrm{th}} = 5$.

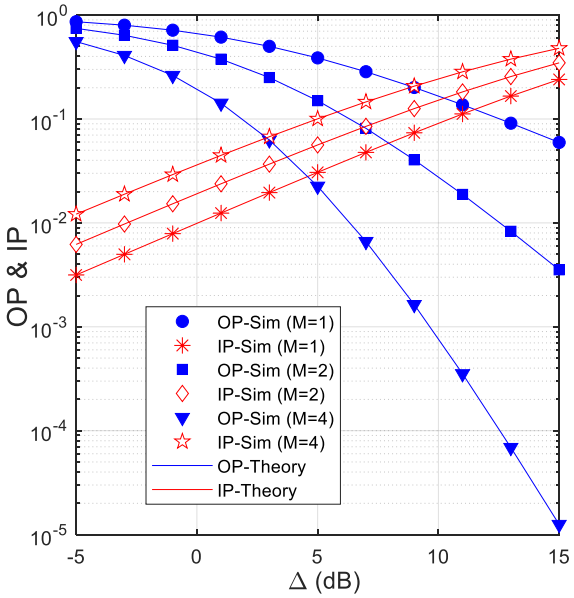

Fig. 2. OP and IP as a function of Δ (dB) when $\kappa_{\mathrm{D}}^2 = \kappa_{\mathrm{E}}^2 = 0.1$.

Fig. 2 presents the considered performance metrics IP and OP, follows $\Delta\left(\Delta = Q_{\mathrm{th}}/N_0\right)$ in dB, where $\kappa_{\mathrm{D}}^2 = \kappa_{\mathrm{E}}^2 = 0.1$ and the number of secondary relays (M) changes from 1 to 4. As we can see, the OP value decreases as increasing Δ because increasing Δ (or Q_{th}) also increases transmit power of the secondary relays. However, with higher value of Δ, IP at SE also increases. Therefore, Fig. 2 shows the OP-IP trade-off with the changing of Δ. It is also seen that OP significantly decreases as increasing M. However, with higher value of M, transmit power of the selected relay also increases, which leads to the increasing of IP. Hence, the value of M also impacts on the IP-OP trade-off.

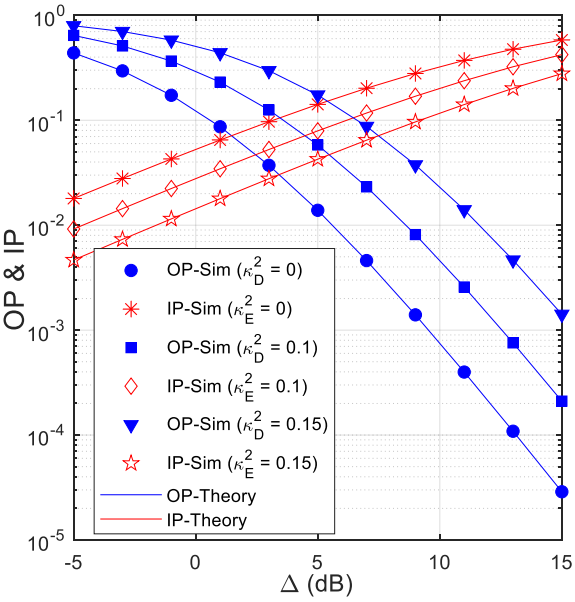

Fig. 3. OP and IP as a function of Δ (dB) with $M = 3$.

Figure 3 shows negative effect of hardware-impairment level on the OP and IP performance. In Fig. 3, the number

of secondary relays is fixed by 3, while values of κ_D^2 and κ_E^2 are assigned by 0, 0.1 and 0.15. It is worth noting that $\kappa_D^2 = 0$ (or κ_E^2=0) means that the transceiver hardware of SR and SD (or SR and SE) is perfect. As expected, OP (IP) increases as increasing (decreasing) $\kappa_D^2\left(\kappa_E^2\right)$. As a result, if the SD and SE nodes have the same transceiver hardware, i.e., $\kappa_D^2 = \kappa_E^2$, there also exists the OP-IP trade-off. Particularly, the outage performance can be improved when SR and SD are equipped with better transceiver hardware (i.e., κ_D^2 and κ_E^2 are lower), but the IP performance is worse.

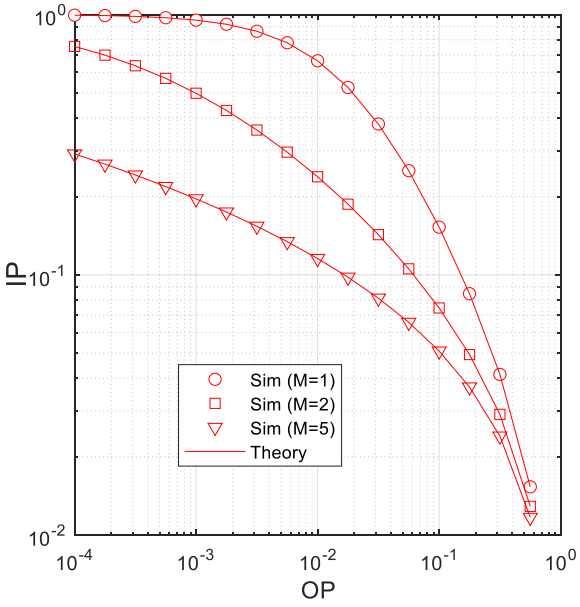

Fig. 4. IP versus OP when $\kappa_D^2 = \kappa_E^2 = 0.05$.

Fig. 4 illustrates the IP/OP trade-off, where we first fix OP by pre-determined values (denoted by ε_{OP}). Then, by solving $OP = \varepsilon_{OP}$, we find values of Δ, by using (16), as

$$\Delta = \frac{\gamma_{th}\left(\left(\varepsilon_{OP}\right)^{-\frac{1}{M}} - 1\right)}{\Omega_D\left(1 - \kappa_D^2\gamma_{th}\right)}. \quad (23)$$

Next, substituting Δ into (22), we obtain the corresponding values of IP. As we can see from Fig. 4, to obtain lower OP value, the considered scheme gets higher IP one, and vice verse. Moreover, with the same OP; IP decreases as increasing M. Therefore, increasing the number of relays also enhances the OP-IP trade-off.

V. Conclusion

This paper derived new formulas of OP and IP for the proposed PLS USS-CR networks with the opportunistic relay selection and under impact of hardware imperfection. The results showed the OP-IP trade-off, which could be significantly enhanced by increasing the number of secondary relays.

In future, we will develop our scheme to the multi-eavesdropper ones as well as evaluate the OP-IP trade-off of the proposed schemes over Nakagami-*m* or Rician fading channels.

References

[1] N. Nguyen, et al, "Secure Massive MIMO With the Artificial Noise-Aided Downlink Training," IEEE Journal on Selected Areas in Communications, vol. 36, no. 4, pp. 802–816, Apr. 2018.

[2] B. M. ElHalawany, A. A. A. El-Banna and K. Wu, "Physical-Layer Security and Privacy for Vehicle-to-Everything," IEEE Communications Magazine, vol. 57, no. 10, pp. 84-90, Oct. 2019.

[3] K. N. Le and V. W. Y. Tam, "Wireless Secrecy Under Multivariate Correlated Nakagami-m Fading," IEEE Access, vol. 8, pp. 33223-33236, Jan. 2020.

[4] Z. Wei, et al, "Energy- and Cost-Efficient Physical Layer Security in the Era of IoT: The Role of Interference," IEEE Communications Magazine, vol. 58, no. 4, pp. 81-87, April 2020.

[5] N. Yang, et al, "Transmit Antenna Selection for Security Enhancement in MIMO Wiretap Channels," IEEE Transactions on Communications, vol. 61, no. 1, pp. 144-154, Jan. 2013.

[6] N. Yang, H. A. Suraweera, I. B. Collings and C. Yuen, "Physical Layer Security of TAS/MRC With Antenna Correlation," IEEE Transactions on Information Forensics and Security, vol. 8, no. 1, pp. 254-259, Jan. 2013.

[7] L. Yang, M. O. Hasna and I. S. Ansari, "Physical Layer Security for TAS/MRC Systems With and Without Co-Channel Interference Over $\eta - \mu$ Fading Channels," EEE Transactions on Vehicular Technology, vol. 67, no. 12, pp. 12421-12426, Dec. 2018.

[8] D. T. Hung, et al, "Performance Comparison between Fountain Codes-Based Secure MIMO Protocols with and without Using Non-Orthogonal Multiple Access," Entropy, vol. 21, no. 10, pp. 1-23, Oct. 2019.

[9] T. M. Hoang, T. Q. Duong, N. -S. Vo and C. Kundu, "Physical Layer Security in Cooperative Energy Harvesting Networks With a Friendly Jammer," IEEE Wireless Communications Letters, vol. 6, no. 2, pp. 174-177, April 2017.

[10] H. D. Hung, T. T. Duy and M. Voznak, "Secrecy Outage Performance of Multi-hop LEACH Networks using Power Beacon Aided Cooperative Jamming with Jammer Selection Methods," AEU-International Journal of Electronics and Communications, vol. 124, ID 153357, pp. 1-25, Sept. 2020.

[11] P. M. Nam, H. D. Hung, T. T. Duy and L. T. Thuong, "Security-Reliability Tradeoff of MIMO TAS/SC Networks using Harvest-to-Jam Cooperative Jamming Methods With Random Jammer Location," ICT Express, 2022. Doi: 10.1016/j.icte.2021.11.003

[12] P. N. Son and H. Y. Kong, "Exact Outage Probability of Two-Way Decode-and-Forward Scheme with Opportunistic Relay Selection Under Physical Layer Security," Wireless Personal Communications, vol. 77, no. 4, pp. 2889-2917, Aug. 2014.

[13] P. T. Tin and T. T. Duy, "Power Allocation Strategies For Dual-Hop Relay Protocols With Best Relay Selection Under Constraint Of Intercept Probability," ICT Express, vol. 5, no. 1, pp. 52-55, Mar. 2019.

[14] H. Li, et al, "Secrecy Outage Probability of Relay Selection Based Cooperative NOMA for IoT Networks," IEEE Access, vol. 9, pp. 1655-1665, Dec. 2020.

[15] D. -H. Ha, et al, "Security-Reliability Trade-Off Analysis for Rateless Codes-Based Relaying Protocols Using NOMA, Cooperative Jamming and Partial Relay Selection," IEEE Access, vol. 9, pp. 131087-131108, Sept. 2021.

[16] X. Ding, et al, "Security-Reliability Tradeoff Analysis of Artificial Noise Aided Two-Way Opportunistic Relay Selection," IEEE Transactions on Vehicular Technology, vol. 66, no. 5, pp. 3930-3941, May 2017.

[17] W. Khalid, et al, "RIS-Aided Physical Layer Security With Full-Duplex Jamming in Underlay D2D Networks," IEEE Access, vol. 9, pp. 99667-99679, Jul. 2021.

[18] L. -T. Tu and A. Bradai, "On the Performance of Physical Layer Security of RIS-aided Communications," in Proc. of 2021 IEEE Conference on Antenna Measurements & Applications (CAMA), 2021, pp. 570-574.

[19] T. D. Hieu, T. T. Duy and S. G. Choi, "Performance Enhancement for Harvest-to-Transmit Cognitive Multi-hop Networks With Best Path

Selection Method Under Presence Of Eavesdropper," in Proc. of ICACT 2018, Feb. 2018, pp. 323-328

[20] P. T, Tin, et al, "Outage Analysis of the Power Splitting Based Underlay Cooperative Cognitive Radio Networks," Sensors, vol. 21, no. 22, 7653, Nov. 2021.

[21] T. L. Thanh, et al, "Broadcasting in Cognitive Radio Networks: A Fountain Codes Approach," IEEE Transactions on Vehicular Technology, 2022. Doi: 10.1109/TVT.2022.3188969

[22] W. Khalid, et al, "RIS-Aided Physical Layer Security With Full-Duplex Jamming in Underlay D2D Networks," IEEE Access, vol. 9, pp. 99667-99679, Jul. 2021.

[23] P. Yan, Y. Zou, X. Ding and J. Zhu, "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.

[24] P. Chakraborty and S. Prakriya, "Secrecy Outage Performance of a Cooperative Cognitive Relay Network," IEEE Communications Letters, vol. 21, no. 2, pp. 326-329, Feb. 2017.

[25] Z. Xiang, et al, "NOMA-Assisted Secure Short-Packet Communications in IoT," IEEE Wireless Communications, vol. 27, no. 4, pp. 8-15, Aug. 2020.

[26] X. Zheng, J. Zhang and G. Pan, "On Secrecy Analysis of Underlay Cognitive UAV-Aided NOMA Systems with TAS/MRC," IEEE Internet of Things Journal, (2022). Doi: 10.1109/JIOT.2022.3181826.

[27] P. T. Tin, D. T. Hung, T. T. Duy and M. Voznak, "Analysis of Probability of Non-zero Secrecy Capacity for Multi-hop Networks in Presence of Hardware Impairments over Nakagami-m Fading Channels," RadioEngineering, vol. 25, no. 4, pp. 774-782, Dec. 2016.

[28] M. Li, et al., "Effects of Residual Hardware Impairments on Secure NOMA-Based Cooperative Systems," IEEE Access, vol. 8, pp. 2524-2536, Nov. 2020.

[29] X. Li, et al, "Secrecy Analysis of Ambient Backscatter NOMA Systems Under I/Q Imbalance," IEEE Transactions on Vehicular Technology, vol. 69, no. 10, pp. 12286-12290, Oct. 2020.

[30] B. Li, Y. Zou, J. Zhu and W. Cao, "Impact of Hardware Impairment and Co-Channel Interference on Security-Reliability Trade-Off for Wireless Sensor Networks," IEEE Transactions on Wireless Communications, vol. 20, no. 11, pp. 7011-7025, Nov. 2021.

[31] K. Guo, et al, "On the Secrecy Performance of NOMA-Based Integrated Satellite Multiple-Terrestrial Relay Networks With Hardware Impairments," IEEE Transactions on Vehicular Technology, vol. 70, no. 4, pp. 3661-3676, April 2021.

[32] K. Guo, C. Dong and K. An, "NOMA-Based Cognitive Satellite Terrestrial Relay Network: Secrecy Performance Under Channel Estimation Errors and Hardware Impairments," IEEE Internet of Things Journal, vol. 9, no. 18, pp. 17334-17347, Sept. 2022.

[33] Y. Liu, et al, "Relay Selection for Security Enhancement in Cognitive Relay Networks," IEEE Wireless Communications Letters, vol. 4, no. 1, pp. 46-49, Feb. 2015.

[34] Y. Zou, B. Champagne, W. -P. Zhu and L. Hanzo, "Relay-Selection Improves the Security-Reliability Trade-Off in Cognitive Radio Systems," IEEE Transactions on Communications, vol. 63, no. 1, pp. 215-228, Jan. 2015.

[35] P. T. Tin, et al, "Secrecy Performance of TAS/SC-based Multi-hop Harvest-to-Transmit Cognitive WSNs under Joint Constraint of Interference and Hardware Imperfection," Sensors MDPI, vol. 19, no. 5, (1160), March 2019.

[36] P. T. D. Ngoc, T. T. Duy and H. V. Khuong, "Outage Performance of Cooperative Cognitive Radio Networks under Joint Constraints of Co-Channel Interference, Intercept Probability and Hardware Imperfection," EAI Transactions on Industrial Networks and Intelligent Systems, vol. 6, no. 19, pp. 1-8, Jun. 2019.

[37] T. T. Duy, L. C. Khan, N. T. Binh and N. L. Nhat, "Intercept Probability Analysis of Cooperative Cognitive Networks Using Fountain Codes and Cooperative Jamming," EAI Transactions on Industrial Networks and Intelligent Systems, vol. 8, no. 26, pp. 1-9, Apr. 2021.

[38] K. Tourki, H. -C. Yang and M. -S. Alouini, "Accurate Outage Analysis of Incremental Decode-and-Forward Opportunistic Relaying," IEEE Transactions on Wireless Communications, vol. 10, no. 4, pp. 1021-1025, Apr. 2011.

[39] K. Tourki, K. A. Qaraqe and M. -S. Alouini, "Outage Analysis for Underlay Cognitive Networks Using Incremental Regenerative Relaying," IEEE Transactions on Vehicular Technology, vol. 62, no. 2, pp. 721-734, Feb. 2013.

[40] K. Tourki, F. A. Khan, K. A. Qaraqe, H. -C. Yang and M. -S. Alouini, "Exact Performance Analysis of MIMO Cognitive Radio Systems Using Transmit Antenna Selection," IEEE Journal on Selected Areas in Communications, vol. 32, no. 3, pp. 425-438, Mar. 2014.

[41] I. S. Gradshteyn and I. M. Ryzhik. *Table of Integrals, Series, and Products*. Academic Press, 2014.