Secrecy Outage Probability of Reconfigurable Intelligent Surface-Aided Cooperative Underlay Cognitive Radio Network Communications

Nhan Duc Nguyen[1], Anh-Tu Le[2] and Munyaradzi Munochiveyi[3]
[1]*Innovation Center, Van Lang University,* Ho Chi Minh City, Viet Nam
[2]*International Cooperation and Scientific Research Department, Van Lang University,* Ho Chi Minh City, Viet Nam
[3]*Department of Computer Science and Information Engineering, College of Information and Electrical Engineering, Asia University,* Taichung 41354, Taiwan
Email: nhan.nd@vlu.edu.vn, tule.iuh@gmail.com and mmunochiveyi@gmail.com

***Abstract*—With the introduction of wireless communications in a diverse range of security-sensitive scenarios such as healthcare, Smart Cities, internet-of-things (IoT) infrastructure, nuclear power plants, so forth, it has become necessary to protect the wireless network against malicious eavesdroppers via physical layer security (PLS). We analyze and study the impact of an eavesdropper located in an underlay cooperative cognitive radio network (CRN). A reconfigurable intelligent surface is used to improve the secrecy outage probability of the proposed system. CRs resolve spectrum scarcity by enabling spectrum sharing. On the other hand, RIS is a planar surface device equipped with signal enhancing reflecting elements that enhance signals at desired users and suppress signal power at undesired eavesdroppers in PLS networks. Therefore, the integration of RIS in cooperative underlay CR networks can enable secure wireless communications. To this end, we derive closed-form secrecy outage probability (SOP) expressions for a network that consists of a primary destination, secondary source, secondary user and a passive eavesdropper. The obtained equations are verified via simulation.**

***Index Terms*—Secrecy outage probability (SOP), Cognitive radio (CR).**

I. Introduction

Recent news headlines of cyberattacks that have hit key infrastructure have shifted research interest into technology that can enhance physical layer security (PLS) of these security-sensitive networks against eavesdroppers [1]. The key idea behind PLS is to take advantage of the wireless channel to ensure the intended user achieves decoding success, while disabling eavesdroppers [1]. Resulting in the secrecy of communication. In the literature, there are different performance metrics such as secrecy channel capacity, secrecy outage probability (SOP), and secrecy throughput, just to name a few [1]. In this work, we utilize secrecy outage probability (SOP) as our secrecy performance metric in order to evaluate and measure the resulting secrecy in Rayleigh fading conditions [1].

RISs have recently emerged as integral to the manifestation of beyond 5G networks [2]. Reconfigurable intelligent surface (RIS) are man-made intelligent planar surfaces composed of many low-cost passive reflecting elements linked to a smart controller, e.g. field-programmable gate array (FPGA) [3]. This enables the passive elements to smartly control the shape and amplitude and phase shift of impinging signals [3]. Since RISs are composed of passive elements, they can be manufactured into a lightweight, low profile and conformable devices that can easily be deployed on various objects such as buildings, billboards, lampposts, etc [3], [4]. In the literature, RIS is associated with other benefits such as wireless security enhancement, interference suppression, energy and spectral efficiency improvement, and multi-user enhancement [5].

On the other hand research into Cognitive radios (CRs) is influenced by the need to resolve spectrum scarcity caused by the exponential growth of internet-of-things (IoT) which rely on wireless connectivity. Consequently, the radio spectrum has become a scarce resource. CR is a promising technology designed to solve this issue, as it promises to improve spectrum efficiency via its ability to function in any bands [6]. A CR network (CRN) is comprised of three modes of operation, namely, underlay, overlay, and interweave, where all users co-exist within a cooperating shared network regardless of their licenses [6], [7]. In this paper, we focus on the underlay mode, where SUs in a secondary network are allowed to operate within a strict interference temperature constraint (ITC) [7]. The ITC keeps the transmit power of SUs within a tolerable interference limit of the PUs in the primary network.

However, CRNs suffer from security threats, such as jamming and eavesdropping at the physical layer. In this regard, it is beneficial to integrate RIS into CRNs to enhance wireless security. [8] is the only work to study RIS-assisted secure CR communication. Where the authors design an alternating optimization (AO) algorithm to optimize the secrecy channel capacity. However, the system model in [8] is based on a non-cooperating CRN and the authors do not consider SOP. Motivated by these research gaps, our contributions are:

- Analysis of CR communications secrecy when RIS is used in a cooperative underlay CRN.
- Derivation of exact SOP equations.

All expressions are validated by simulations.

The following sections are as follows. Section II, description of the system parameters. Section III, formulation of closed-

form SOP. Section IV, results and discussions presentation, followed by a summary of our findings in Section V.

II. Design of RIS-aided Cooperative underlay Network

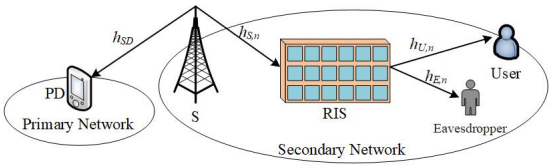

Fig. 1. Layout of RIS-CR network

We consider a cooperative underlay RIS-aided CR network which consists of a primary destination (PD), a secondary source (S), a RIS with N elements and a destination user as well as a passive eavesdropper as shown in Fig. 1. The channel gains are written as $h_i, \forall i \in [SP; S, n; U, n; E, n]$, where h_{SP} denotes the channel between S and the PD, $h_{S,n}$ the channel between S and RIS, $h_{U,n}$ and $h_{E,n}$ are the channel between the S and User and S and eavesdropper, respectively, and we assume all channel follow Rayleigh distribution. Moreover, the distances between the nodes are given as d_{SP}, d_{SR}, d_U and d_E. We assume S can interfere with PD. Further, we assume that communication from the secondary network (SN) is only allowed if there is no harmful interference transmitted to the PD by the SN. Hence, the source transmitter is restricted as [9]

$$P_S \leq \min\left(\frac{P_D d_{SP}^{\tau}}{|h_{SP}|^2}, \bar{P}_S\right) \tag{1}$$

where $\bar{P}_S$ refers to the non-interfering transmitter power, while P_D denotes the interference at the PD. The received signal at the destination and eavesdropper are respectively written as

$$r_U = \sqrt{\frac{P_S}{d_{SR}^{\tau} d_U^{\tau}}}\beta \sum_{n=1}^{N} h_{S,n} h_{U,n} e^{j\phi_n} x + n_U \tag{2}$$

and

$$r_E = \sqrt{\frac{P_S}{d_{SR}^{\tau} d_E^{\tau}}}\beta \sum_{n=1}^{N} h_{S,n} h_{E,n} e^{j\phi_n} x + n_E \tag{3}$$

where x is the information of the destination user, τ is the path-loss exponent, β is the amplitude reflection coefficient and $\beta = 1$ is the lossless reflection, ϕ_n is the nth reflecting element phase of RIS and n_U, n_E are the AWGN variables with zero mean and variance N_0. As in [10], the channel phases of h and g are perfect. Therefore, the signal-to-noise ratio (SNR) of the destination user is given by

$$\begin{aligned}\gamma_D &= \frac{P_S \left|\beta \sum_{n=1}^{N} h_{S,n} h_{U,n} e^{j\varphi_n}\right|^2}{(d_{SR} d_U)^{\tau} N_0} \\ &= \frac{\rho_S A_1^2}{(d_{SR} d_U)^{\tau}}\end{aligned} \tag{4}$$

where $\rho_S = \frac{P_S}{N_0}$ and $A_1 = \sum_{n=1}^{N} h_{S,n} h_{U,n}$. In addition, (4) maximizes the SNR at the destination when the phase shifts are optimized as in [13] as $\phi_1^{p*}, ..., \phi_N^{p*}$ in which $(\phi_1^{p*}, ..., \phi_N^{p*}) = (\arg[[h_{S,1}][h_{U,1}]]...\arg[[h_{S,N}][h_{U,N}]])$. Next, the eavesdropper SNR is

$$\begin{aligned}\gamma_E &= \frac{P_S \left|\beta \sum_{n=1}^{N} h_{S,n} h_{E,n} e^{j\varphi_n}\right|^2}{(d_{SR} d_E)^{\tau} N_0} \\ &= \frac{\rho_S A_2^2}{(d_{SR} d_E)^{\tau}}\end{aligned} \tag{5}$$

where $A_2 = \left|\sum_{n=1}^{N} h_{S,n} h_{E,n}\right|$. Similar to [11], the pdf of A_2^2 is an exponential random variable with parameter $\lambda_E = N$ written as

$$f_{A_2^2}(x) = \frac{1}{\lambda_E} e^{-\frac{x}{\lambda_E}}. \tag{6}$$

Next, $|h_{SP}|^2$ is defined as

$$f_{|h_{SP}|^2}(x) = \frac{1}{\lambda_{SP}} e^{-\frac{x}{\lambda_{SP}}}. \tag{7}$$

In addition, according to the central limit theorem (CLT), A_1 follows Gaussian random distribution with $\frac{N\pi}{4}$ denoting mean and $N\left(1 - \frac{\pi^2}{16}\right)$ based on [10], thus, the pdf of A_1^2 is given by [12]

$$f_{A_1^2}(\gamma) = \frac{1}{2\sigma^2}\left(\frac{\gamma}{\lambda}\right)^{\frac{-1}{4}} e^{-\frac{\gamma+\lambda}{2\sigma^2}} I_{-\frac{1}{2}}\left(\frac{\sqrt{\gamma\lambda}}{\sigma^2}\right) \tag{8}$$

where $\lambda = \left(\frac{N\pi}{4}\right)^2$,$\sigma^2 = N\left(1 - \frac{\pi^2}{16}\right)$. With the help of [18, Eq. 8.445], we rewrite (8) as

$$f_{A_1^2}(x) = \sum_{k=0}^{\infty} \frac{e^{-\frac{\lambda}{2\sigma^2}} \left(\lambda/2\sigma^2\right)^k}{\left(2\sigma^2\right)^{k+\frac{1}{2}} k! \Gamma\left(k + \frac{1}{2}\right)} x^{k-\frac{1}{2}} e^{-\frac{x}{2\sigma^2}}. \tag{9}$$

Based on [18, Eq. 3.351.1], the CDF of A_1^2 is obtained by

$$F_{A_1^2}(x) = \sum_{k=0}^{\infty} \frac{e^{-\frac{\lambda}{2\sigma^2}} \left(\lambda/2\sigma^2\right)^k}{k! \Gamma\left(k + \frac{1}{2}\right)} \gamma\left(k + \frac{1}{2}, \frac{x}{2\sigma^2}\right). \tag{10}$$

where $\gamma(.,.)$ is the lower incomplete gamma function [18].

Therefore, the secrecy rate is [15]

$$C_S = \max\left(\log_2\left(1 + \gamma_D\right) - \log_2\left(1 + \gamma_E\right), 0\right) \tag{11}$$

III. Secrecy Outage Probability Analysis

Here we derive the SOP for the system. The authors in [6], define secrecy outage event as C_S falling below R_S, the target secrecy rate. Therefore, the SOP is defined as [16], [17]

$$\begin{aligned}P_{OUT}^{SEC} &= \Pr\left(C_s < R_{th}\right) \\ &= \Pr\left(\log_2 \frac{1 + \gamma_D}{1 + \gamma_E} < R_S\right)\end{aligned} \tag{12}$$

Proposition 1: The exact closed-form SOP is given by

$$P_{OUT}^{SEC} = \psi_1 + \psi_2 \tag{13}$$

$$\psi_1 = \sum_{k=0}^{\infty}\sum_{n=0}^{\infty} \frac{(-1)^n e^{-\frac{\lambda}{2\sigma^2}} e^{\frac{\vartheta_S \varpi_E}{\bar{\rho}_S \gamma_S \bar{\lambda}_E}} \left(1 - e^{-\frac{\rho_D d_{SP}^{\tau}}{\bar{\rho}_S \lambda_{SP}}}\right)}{n!k!\Gamma\left(k+\frac{1}{2}\right)\left(k+n+\frac{1}{2}\right)} \left(\frac{\lambda}{2\sigma^2}\right)^k \left(\frac{\varpi_U \bar{\lambda}_E \gamma_S}{\varpi_E 2\sigma^2}\right)^{k+n+\frac{1}{2}} \Gamma\left(k+n+\frac{3}{2}, \frac{\vartheta_S \varpi_E}{\bar{\rho}_S \gamma_S \bar{\lambda}_E}\right) \tag{14}$$

$$\begin{aligned}\psi_2 = &\sum_{k=0}^{\infty}\sum_{n=0}^{\infty} \frac{(-1)^n e^{-\frac{\lambda}{2\sigma^2}}}{n!k!\Gamma\left(k+\frac{1}{2}\right)\left(k+n+\frac{1}{2}\right)\lambda_{SP}} \left(\frac{\lambda}{2\sigma^2}\right)^k \left(\frac{\varpi_U \gamma_S \bar{\lambda}_E}{2\sigma^2 \varpi_E}\right)^{k+n+\frac{1}{2}} \\ &\times \left(\Gamma\left(k+n+\frac{3}{2}\right)(\varpi \rho_D d_{SP}^{\tau}) e^{-\frac{1}{\varpi \bar{\rho}_S}} - \sum_{c=0}^{\infty} \frac{(-1)^c \Gamma\left(k+n+c+\frac{5}{2}, \frac{1}{\bar{\rho}_S \varpi}\right)(\rho_D d_{SP}^{\tau})}{c!\left(k+n+c+\frac{3}{2}\right)\varpi^{k+n+c+\frac{5}{2}}} \left(\frac{\vartheta_S \varpi_E}{\gamma_S \bar{\lambda}_E}\right)^{k+n+c+\frac{3}{2}}\right)\end{aligned} \tag{15}$$

where ψ_1 and ψ_2 are given as (14) and (15), and can be seen in the top page.

Proof: With help from (1), (4) and (5), we can rewrite (12) as

$$\begin{aligned}P_{out}^{sec} = &\underbrace{\Pr\left(\frac{1+\frac{\bar{\rho_S} A_1^2}{(d_{SR} d_U)^{\tau}}}{1+\frac{\bar{\rho_S} A_2^2}{(d_{SR} d_E)^{\tau}}} < 2^{R_S}, \bar{\rho_S} < \frac{\rho_D d_{SP}^{\tau}}{|h_{SP}|^2}\right)}_{\psi_1} \\ &+ \underbrace{\Pr\left(\frac{1+\frac{\frac{\rho_D d_{SP}^{\tau}}{|h_{SP}|^2} A_1^2}{(d_{SR} d_U)^{\tau}}}{1+\frac{\frac{\rho_D d_{SP}^{\tau}}{|h_{SP}|^2} A_2^2}{(d_{SR} d_E)^{\tau}}} < 2^{R_S}, \bar{\rho_S} > \frac{\rho_D d_{SP}^{\tau}}{|h_{SP}|^2}\right)}_{\psi_2}.\end{aligned} \tag{16}$$

The A_1 term in (16) term can be rewritten as

$$\psi_1 = \Pr\left(A_1^2 < \frac{\vartheta_s \varpi_U}{\bar{\rho}_S} + \frac{A_2^2 \gamma_s \varpi_U}{\varpi_E}, |h_{SP}|^2 < \frac{\rho_D d_{SP}^{\tau}}{\bar{\rho}_S}\right) \tag{17}$$

where $\gamma_S = 2^{R_S}$, $\vartheta_S = \gamma_S - 1$, $\varpi_U = (d_{SR} d_U)^{-\tau}$, $\varpi_E = (d_{SR} d_E)^{\tau}$. A_1^2 and $|h_{SP}|^2$ in (17) are independent from each other. Hence, ψ_1 can be further denoted as

$$\begin{aligned}\psi_1 = &\underbrace{\Pr\left(A_1^2 < \frac{\vartheta_s \varpi_U}{\bar{\rho}_S} + \frac{\varpi_U A_2^2 \gamma_s}{\varpi_E}\right)}_{\psi_{1,1}} \\ &\times \underbrace{\Pr\left(|h_{SP}|^2 < \frac{\rho_D d_{SP}^{\tau}}{\bar{\rho}_S}\right)}_{\psi_{1,2}}.\end{aligned} \tag{18}$$

With the help of (6) and (10), $\psi_{1,1}$ can be calculated by

$$\begin{aligned}\psi_{1,1} &= \Pr\left(A_1^2 < \frac{\vartheta_S \varpi_U}{\bar{\rho}_S} + \frac{\varpi_U A_2^2 \gamma_S}{\varpi_E}\right) \\ &= \int_0^0 f_{A_2^2}(x) F_{A_1^2}\left(\frac{\vartheta_S \varpi_U}{\bar{\rho}_S} + \frac{\varpi_U A_2^2 \gamma_S}{\varpi_E}\right) dx \\ &= \sum_{k=0}^{\infty} \frac{e^{-\frac{\lambda}{2\sigma^2}}}{k!\bar{\lambda}_E \Gamma\left(k+\frac{1}{2}\right)} \left(\frac{\lambda}{2\sigma^2}\right)^k \\ &\times \int_0^{\infty} \gamma\left(k+\frac{1}{2}, \frac{\varpi_U}{2\sigma^2}\left(\frac{\vartheta_S}{\bar{\rho}_S} + \frac{\gamma_S}{\varpi_E} x\right)\right) e^{-\frac{x}{\bar{\lambda}_E}} dx.\end{aligned} \tag{19}$$

Based on [18, Eq. (8.354.1)] and [18, Eq. (3.382.4)] $\psi_{1,1}$ becomes

$$\begin{aligned}\psi_{1,1} &= \sum_{k=0}^{\infty}\sum_{n=0}^{\infty} \frac{e^{-\frac{\lambda}{2\sigma^2}} (-1)^n \left(\frac{\lambda}{2\sigma^2}\right)^k}{n!k!\bar{\lambda}_E \Gamma\left(k+\frac{1}{2}\right)\left(k+n+\frac{1}{2}\right)} \\ &\times \left(\frac{\varpi_U}{2\sigma^2}\right)^{k+n+\frac{1}{2}} \int_0^{\infty} \left(\frac{\vartheta_S}{\bar{\rho}_S} + \frac{\gamma_S}{\varpi_E} x\right)^{k+n+\frac{1}{2}} e^{-\frac{x}{\bar{\lambda}_E}} dx \\ &= \sum_{k=0}^{\infty}\sum_{n=0}^{\infty} \frac{(-1)^n e^{-\frac{\lambda}{2\sigma^2}} e^{\frac{\vartheta_S \varpi_E}{\bar{\rho}_S \gamma_S \bar{\lambda}_E}} \left(\frac{\lambda}{2\sigma^2}\right)^k}{n!k!\Gamma\left(k+\frac{1}{2}\right)\left(k+n+\frac{1}{2}\right)} \\ &\times \left(\frac{\varpi_U \bar{\lambda}_E \gamma_S}{\varpi_E 2\sigma^2}\right)^{k+n+\frac{1}{2}} \Gamma\left(k+n+\frac{3}{2}, \frac{\vartheta_S \varpi_E}{\bar{\rho}_S \gamma_S \bar{\lambda}_E}\right)\end{aligned} \tag{20}$$

where $\Gamma(.,.)$ is the upper incomplete gamma function [18]. Then, the term $\psi_{1,2}$ is calculated as

$$A_{1,2} = \int_0^{\frac{\rho_D d_{SP}^{\tau}}{\bar{\rho}_S}} f_{|h_{SP}|^2}(x) dx = 1 - e^{-\frac{\rho_D d_{SP}^{\tau}}{\bar{\rho}_S \lambda_{SP}}}. \tag{21}$$

Next, we rewrite ψ_2 in (12) as follows

$$\begin{aligned}A_2 &= \Pr\left(A_1^2 < \frac{\vartheta_s |h_{SD}|^2 \varpi_U}{\rho_D d_{SP}^{\tau}} + \frac{\gamma_s A_2^2 \varpi_U}{\varpi_E}, |h_{SP}|^2 > \frac{\rho_D d_{SP}^{\tau}}{\bar{\rho}_S}\right) \\ &= \int_{\frac{\rho_D d_{SP}^{\tau}}{\bar{\rho}_S}}^{\infty} f_{|h_{SP}|^2}(x) \int_0^{\infty} f_{A_2^2}(y) F_{A_1^2}\left(\left(\frac{\vartheta_S x \varpi_U}{\rho_D d_{SP}^{\tau}} + \frac{\gamma_S y \varpi_U}{\varpi_E}\right)\right) dy dx.\end{aligned} \tag{22}$$

Similarly, ψ_2 is calculated by

$$\begin{aligned}\psi_2 = &\sum_{k=0}^{\infty} \frac{e^{-\frac{\lambda}{2\sigma^2}} \left(\frac{\lambda}{2\sigma^2}\right)^k}{k!\Gamma\left(k+\frac{1}{2}\right)\Omega_{SP}\bar{\lambda}_E} \int_{\frac{\rho_D d_{SP}^{\tau}}{\bar{\rho}_S}}^{\infty} e^{-\frac{x}{\lambda_{SP}}} dx \\ &\int_0^{\infty} e^{-\frac{y}{\bar{\lambda}_E}} \gamma\left(k+\frac{1}{2}, \frac{\varpi_U}{2\sigma^2}\left(\frac{\vartheta_S x}{\rho_D d_{SP}^{\tau}} + \frac{\gamma_S y}{\varpi_E}\right)\right) dy \\ = &\sum_{k=0}^{\infty}\sum_{n=0}^{\infty} \frac{(-1)^n e^{-\frac{\lambda}{2\sigma^2}} \left(\frac{\lambda}{2\sigma^2}\right)^k \left(\frac{\varpi_U \gamma_S \bar{\lambda}_E}{2\sigma^2 \varpi_E}\right)^{k+n+\frac{1}{2}}}{n!k!\Gamma\left(k+\frac{1}{2}\right)\lambda_{SP}\left(k+n+\frac{1}{2}\right)} \\ &\int_{\frac{\rho_D d_{SP}^{\tau}}{\bar{\rho}_S}}^{\infty} e^{-\frac{x}{\lambda_{SP}} + \frac{\vartheta_S \varpi_E}{\rho_D d_{SP}^{\tau} \gamma_S \bar{\lambda}_E} x} \Gamma\left(k+n+\frac{3}{2}, \frac{\vartheta_S \varpi_E}{\rho_D d_{SP}^{\tau} \gamma_S \bar{\lambda}_E} x\right) dx.\end{aligned} \tag{23}$$

We denote the integral of (23) as B_1. Then, B_1 can be calculated as follows

$$B_1 = \Gamma\left(k+n+\frac{3}{2}\right) \int\limits_{\frac{\rho_D d_{SP}^{\tau}}{\bar{\rho}_S}}^{\infty} e^{-\left(\frac{1}{\lambda_{SP}}+\frac{\vartheta_S \varpi_E}{\rho_D d_{SP}^{\tau} \gamma_S \bar{\lambda}_E}\right)x} - \sum_{c=0}^{\infty} \frac{(-1)^c \left(\frac{\vartheta_S \varpi_E}{\rho_D d_{SP}^{\tau} \gamma_S \bar{\lambda}_E}\right)^{k+n+c+\frac{3}{2}}}{c!\left(k+n+c+\frac{3}{2}\right)} \int\limits_{\frac{\rho_D d_{SP}^{\tau}}{\bar{\rho}_S}}^{\infty} x^{k+n+c+\frac{3}{2}} e^{-\frac{x}{\lambda_{SP}} - \frac{\vartheta_S \varpi_E}{\rho_D d_{SP}^{\tau} \gamma_S \bar{\lambda}_E} x} dx. \tag{24}$$

Based on [18, Eq. 3.351.2 Eq. 3.351.3], we can obtain B_1 by

$$B_1 = \Gamma\left(k+n+\frac{3}{2}\right)\left(\varpi \rho_D d_{SP}^{\tau}\right) e^{-\frac{1}{\varpi \bar{\rho}_S}} - \sum_{c=0}^{\infty} \frac{(-1)^c \left(\rho_D d_{SP}^{\tau}\right)\left(\frac{\vartheta_S \varpi_E}{\gamma_S \bar{\lambda}_E}\right)^{k+n+c+\frac{3}{2}}}{c!\left(k+n+c+\frac{3}{2}\right)\varpi^{k+n+c+\frac{5}{2}}} \times \Gamma\left(k+n+c+\frac{5}{2}, \frac{1}{\bar{\rho}_S \varpi}\right) \tag{25}$$

where $\varpi = \frac{\lambda_{SP}\gamma_S \bar{\lambda}_E}{\rho_D d_{SP}^{\tau} \gamma_S \bar{\lambda}_E + \lambda_{SP} \vartheta_S \varpi_E}$. Finally, putting (25) into (23), (14) and (15) are obtained.

IV. Numerical results

In this section, we set $N = 5$, $\lambda_{SP} = 1$, $d_{SR} = 10$m, $d_U = 5$m, $d_E = 5$m, $d_{SP} = 5$, $\tau = 2$, $\rho_D = 10$dB, $R_S = 0.1$ and simulate secrecy outage probability based on the derived exact closed-form expressions and use Monte-Carlo simulation to validate the results. We assume Rayleigh fading conditions.

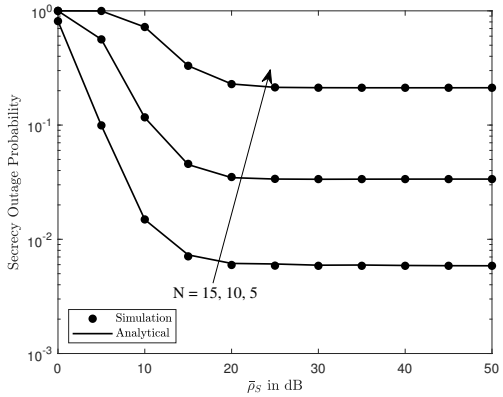

Fig. 2. Secrecy Outage probability versus $\bar{\rho}_S$ in dB varying N.

In Fig. 2, the secondary source SOP is studied when a RIS device relays signals to a user located in the vicinity of an eavesdropper. By comparing the plot of SOP versus the source SNR, with N reflecting elements increased from 5 to 15. We note the improvement of the SOP at the source. The rationale being that the more reflecting elements RIS has, the better it is at controlling the channel. However, due to the availability of an eavesdropper, the SOP always approaches a floor value. In Fig. 3, we plot a similar curve for the destination SOP versus SNR, and the results demonstrate that increasing N also contributes to better SOP at the destination despite the presence of the eavesdropper.

Finally, in Fig. 4, we see the effects of varying the target secrecy rate R_S on SOP, and the results show our proposed system can exhibit better SOP performance at high transmit SNR at the source. However, other parameters such as target secrecy rate R_S limit such performance. Therefore, we can see saturated lines of SOP when transmit SNR at the source is greater than 20 dB.

In all the curves, Fig. 2 - Fig. 4, the results obtained by proposition 1 in (13) match the simulation results.

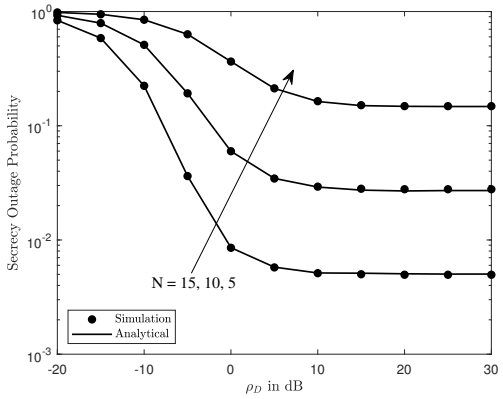

Fig. 3. Secrecy Outage probability versus ρ_D in dB varying N.

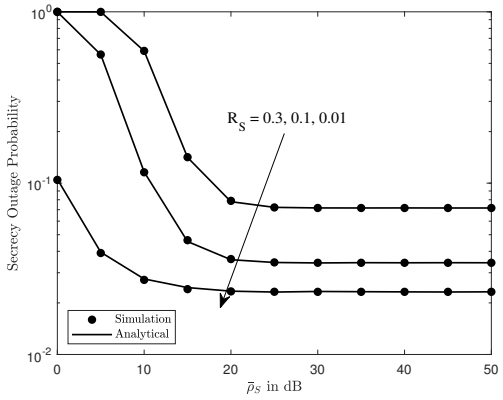

Fig. 4. Secrecy Outage probability versus $\bar{\rho}_S$ in dB varying R_S with N = 10.

V. Conclusion

In this work, we determine the impact on SOP when an eavesdropper is introduced into the RIS-aided cooperative underlay cognitive radio network (CRN). We derive exact SOP expressions and verify the results by using Monte Carlo

simulations. The obtained numerical results demonstrate that deploying RIS into a CRN can improve the secrecy performance of such networks despite the presence of eavesdroppers.

REFERENCES

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

[2] X. Yu, D. Xu and R. Schober, "Enabling Secure Wireless Communications via Intelligent Reflecting Surfaces," *2019 IEEE Global Communications Conference (GLOBECOM)*, 2019, pp. 1-6, doi: 10.1109/GLOBECOM38437.2019.9014322.

[3] R. Liu, Q. Wu, M. Di Renzo, and Y. Yuan, "A Path to Smart Radio Environments: An Industrial Viewpoint on Reconfigurable Intelligent Surfaces," *arXiv preprint* arXiv:2104.14985 (2021).

[4] M. Di Renzo et al., "Smart Radio Environments Empowered by Reconfigurable Intelligent Surfaces: How It Works, State of Research, and The Road Ahead," in *IEEE Journal on Selected Areas in Communications*, vol. 38, no. 11, pp. 2450-2525, Nov. 2020, doi: 10.1109/JSAC.2020.3007211.

[5] A. U. Makarfi, R. Kharel, K. M. Rabie, O. Kaiwartya, X. Li and D. -T. Do, "Reconfigurable Intelligent Surfaces based Cognitive Radio Networks," *2021 IEEE Wireless Communications and Networking Conference Workshops (WCNCW)*, 2021, pp. 1-6, doi:10.1109/WCNCW49093.2021.9419976.

[6] S. Yadav and D. S. Gurjar, "Secrecy Performance of SIMO Underlay Cognitive Radio Networks Over α–μ Fading Channels," *IEEE Access*, vol. 9, pp. 62616-62629, 2021, doi: 10.1109/ACCESS.2021.3074507.

[7] S. Arzykulov, T. A. Tsiftsis, G. Nauryzbayev and M. Abdallah, "Outage Performance of Cooperative Underlay CR-NOMA With Imperfect CSI," *IEEE Communications Letters*, vol. 23, no. 1, pp. 176-179, Jan. 2019, doi: 10.1109/LCOMM.2018.2878730.

[8] L. Dong, H. -M. Wang and H. Xiao, "Secure Cognitive Radio Communication via Intelligent Reflecting Surface," *IEEE Transactions on Communications*, doi: 10.1109/TCOMM.2021.3073028.

[9] S. Arzykulov, G. Nauryzbayev and T. A. Tsiftsis, "Underlay cognitive relaying system over α - μ fading channels," *IEEE Commun. Lett.,* vol. 21, no. 1, pp. 216–219, Jan. 2017.

[10] E. Basar, M. Di Renzo, J. De Rosny, M. Debbah, M. Alouini and R. Zhang, "Wireless Communications Through Reconfigurable Intelligent Surfaces," *IEEE Access,* vol. 7, pp. 116753-116773, 2019.

[11] J. D. Vega Sánchez, P. Ramírez-Espinosa and F. J. López-Martínez, "Physical Layer Security of Large Reflecting Surface Aided Communications With Phase Errors," in *IEEE Wireless Communications Letters*, vol. 10, no. 2, pp. 325-329, Feb. 2021.

[12] L. Yang, Y. Yang, M. O. Hasna, and M. Alouini, "Coverage, probability of SNR gain, and DOR analysis of RIS-aided communication systems," *IEEE Wireless Commun. Lett.,* vol. 9, no. 8, pp. 1268-1272, Aug. 2020.

[13] K. Ntontin, J. Song, M. Di Renzo, "Multi-Antenna relaying and reconfigurable intelligent surfaces: End-to-End SNR and achievable rate,"2019, arXiv:1908.07967.[online]. Available:https://arxiv.org/abs/1908.07967.

[14] L. Yang, J. Yang, W. Xie, M. O. Hasna, T. Tsiftsis and M. D. Renzo, "Secrecy Performance Analysis of RIS-Aided Wireless Communication Systems," *IEEE Trans. on Vehi. Tech.,* vol. 69, no. 10, pp. 12296-12300, 2020.

[15] M. Cui, G. Zhang and R. Zhang, "Secure Wireless Communication via Intelligent Reflecting Surface," in *IEEE Wireless Communications Letters*, vol. 8, no. 5, pp. 1410-1414, 2019.

[16] A. U. Makarfi et al., "Toward Physical-Layer Security for Internet of Vehicles: Interference-Aware Modeling," in *IEEE Internet of Things Journal*, vol. 8, no. 1, pp. 443-457, 1 Jan.1, 2021.

[17] Q. Chen, M. Li, X. Yang, R. Alturki, M. D. Alshehri and F. Khan, "Impact of Residual Hardware Impairment on the IoT Secrecy Performance of RIS-Assisted NOMA Networks," in *IEEE Access*, vol. 9, pp. 42583-42592, 2021, doi: 10.1109/ACCESS.2021.3065760.

[18] I. S. Gradshteyn and I. M. Ryzhik, "Table of Integrals, Series, and Products," 6/e. San Diego, CA: Academic Press, 2000.