RIS-Aided Physical Layer Security Improvement in Underlay Cognitive Radio Networks

Majid H. Khoshafa, *Member, IEEE,* Telex M. N. Ngatchede, *Senior Member, IEEE,* and Mohamed H. Ahmed, *Senior Member, IEEE,*

arXiv:2209.12389v1 [eess.SP] 26 Sep 2022

***Abstract*—In this paper, a reconfigurable intelligent surface (RIS)-aided underlay cognitive radio network is investigated. An RIS is utilized to improve the secondary network (SN) reliability and robustness while simultaneously increasing the physical layer security of the primary network (PN). Toward this end, closed-form expressions for the SN outage probability, PN secrecy outage probability, and PN probability of non-zero secrecy capacity are derived. To increase the eavesdropping signals of the PN, the eavesdropper uses two combining techniques, namely maximal ratio combining and selection combining. Furthermore, the advantages of the proposed system model are verified through numerical and simulation results.**

***Index Terms*—Reconfigurable intelligent surfaces, cognitive radio network, physical layer security.**

I. Introduction

RECONFIGURABLE Intelligent Surfaces (RISs) are attracting much consideration as a leading technology to achieve intelligent wireless channels environment for the next generation networks [1]. RISs are planar surfaces of electromagnetic (EM) material comprising a large number of cheap passive reflecting elements. A microcontroller controls each element to alter the amplitude and phase of the reflected signal. The RIS technology has many advantages, including the ability to change transmission environments into intelligent ones, enhancing the quality of the received signals at the destination, reducing the power consumption compared with other technologies, increasing the physical layer security (PLS), and alleviating the undesired interference [2]–[5]. Passive RISs prototypes were assembled in [6]–[8] to acquire more practical and precise results regarding the actual performance of RISs-aided systems by taking experimental measurements.

With the envision new technologies and utilizing higher frequency bands, secure communications are significant in the sixth generation (6G) wireless networks, where new security challenges arise [9]. Present research contributions have established RISs as cutting-edge technology, with promising research directions toward the 6G. To take things further, integrating RISs with emerging communication technologies results in higher performance gains that can be achieved [10]. The PLS, initially investigated by Wyner [11], has evolved as an attractive technique for improving the cellular network's secrecy performance against signal leakage. In this respect, PLS utilizes the natural properties and characteristics of wireless communication channels and noise to secure data transmission by limiting the amount of data that can be leaked at the bit level by eavesdroppers. Thanks to their distinctive characteristics, which enable them to control the transmission environment, RISs can be utilized to eliminate interference and improve the received signal without using active elements. In this respect, the RIS technology has been recently utilized to improve the PLS of wireless communication system [4], [12], [13]. To guarantee a secure transmission, the RIS was deployed near the eavesdropper to cancel out the eavesdropping signal received by the eavesdropper [14], which can actually decrease the information leakage to enhance the PLS of the wireless network.

On the other hand, mobile wireless communication has experienced rapid development in data traffic due to the dramatic growth of smart devices. According to Cisco, the average number of mobiles per capita will be 3.6 by 2023 [15], leading to an enormous demand for radio spectrum resources, including bandwidth and energy. Consequently, spectral and energy efficiency are two crucial principles for designing future wireless networks. Cognitive radio (CR) has been introduced as an efficient technique to improve spectral efficiency. In CR networks, the spectrum can be shared by two different networks, the primary network (PN) and the secondary network (SN), provided that the interference produced by the SN to the PN is controlled by interference constraint. The authors in [16] studied the PLS of energy harvesting for CR networks using the cooperative relaying technique. A common technique is to employ beamforming to improve the performance of the SN while guaranteeing that the interference power received by the PN users is below the predefined interference limit. Nevertheless, the beamforming gain is restricted when the link between the SN transmitter and SN receiver is weak due to severe attenuation. To address such a problem, an RIS can be deployed to improve the performance of the SN while enhancing the secrecy rate of the PN [17]. In [18], the RIS technology has been employed to aid data transmission in CR networks. The authors in [19] proposed an RIS-assisted CR network to enhance the SN's achievable rate. In this work, we propose a secure RISs-aided underlay CR network. To the best of our knowledge, there is no previous work studying the advantage of the RIS technology to secure CR network. Furthermore, the influence of the

M. H. Khoshafa is with the Department of Electrical and Computer Engineering, Queen's University, Kingston, Canada (e-mail: mhk5@queensu.ca)
T. M. N. Ngatched is with the Department of Electrical and Computer Engineering, Memorial University of Newfoundland, St. John's, Canada (e-mail: tngatched@grenfell.mun.ca)
M. H. Ahmed is with the School of Electrical Engineering and Computer Science, University of Ottawa, Ottawa, Canada (e-mail: mahme3@uottawa.ca)

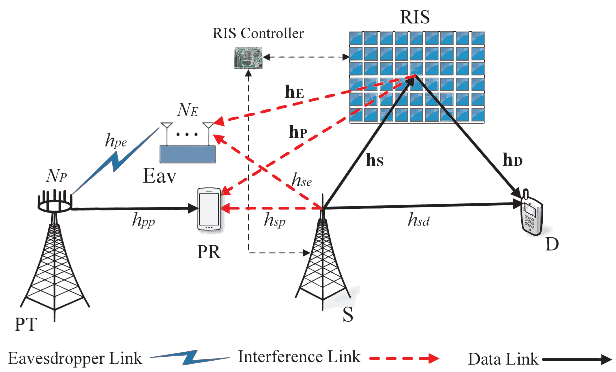

Fig. 1. System Model.

RIS technology on the PN secrecy capacity is investigated. The main contributions of this paper can be summarized as follows:

- The RIS technology is introduced to improve the reliability of the SN, while concurrently increasing the physical layer security of the PN.
- To compensate for the spectrum sharing, the RIS technology is utilized as a friendly jammer to ensure a high-secrecy performance for the PN, consequently enabling a win-win situation between the two networks, i.e., security provisioning for the PN and high reliability and robustness for the SN.
- The SN outage probability is studied, and a novel analytical expression is derived. Besides, closed-form expressions for the secrecy outage probability (SOP) of the PN are also derived, considering two combining techniques, namely maximal ratio combining (MRC) and selection combining (SC), which are employed by an eavesdropper.
- Asymptotic analysis is provided for the SOP of the PN. Moreover, the benefits of the proposed system model are confirmed through numerical and simulation results.

II. System Model

A proposed RISs-aided underlay CR system, including a license-holding PN and an unlicensed SN, is considered as shown in Fig. 1. Specifically, the SN comprises a secondary transmitter (S) and a secondary receiver (D), each equipped with a single antenna, while the PN comprises a primary transmitter (PT) and a single-antenna primary receiver (PR). The PT is equipped with $N_P \geq 1$ antennas. In addition, an eavesdropper (Eav), equipped with $N_E \geq 1$ antennas, intends to overhear the PN's data streams. Therefore, an RIS, made of N reflecting elements, is utilized to enhance the achievable secrecy rate of the PN by interfering with the eavesdropping signals at Eav while improving the transmission conditions of the SN. It is worth mentioning that a field-programmable gate array (FPGA) can be utilized as a controller to achieve adjustable control of the RIS in practice, which often communicates and coordinates with other network elements (e.g., BS and users) via dedicated connections [20]. It is assumed that the channel state information (CSI) of all channels employed

TABLE I
Table of Symbols

Symbol	Description
S	Secondary transmitter
D	Secondary receiver
PT	Primary transmitter
PR	Primary receiver
Eav	Eavesdropper
N_P	Number of antennas at PT
N_E	Number of antennas at Eav
N	Number of reflecting elements at RIS
h_{ab}	Channel coefficient of ab link
d_{ab}	Euclidean distance between ab
n_a	AWGN node at a
σ_a^2	AWGN variance at node a
y_a	Received signal at node a
x_s	SN transmitted signal
x_p	PN transmitted signal
P_{S}	SN transmitted power
P_{P}	PN transmitted power
d_o	Reference distance
ϕ_i	Phase coefficient of the i^{th} element of the RIS
θ_i	Residual phase errors affecting the PR
ψ_i	Residual phase errors affecting the Eav
γ_a	SINR at node a
$\bar{\gamma}_a$	Average SNR at node a
η	Path loss exponent
$f_X(\cdot)$	PDF of random variable X
$F_X(\cdot)$	CDF of random variable X
$F_X^{\infty}(\cdot)$	Asymptotic CDF of random variable X
$\mathcal{Q}$	Threshold of interference temperature
$\mathcal{C}_{\text{S}}$	PN secrecy capacity
$\mathcal{C}_{\text{P}}$	PN capacity
$\mathcal{C}_{\text{E}}$	Eav capacity
$\mathcal{R}_d$	SN achievable data rate
$\mathcal{R}_s$	PN target secrecy rate
$\Pr(\cdot)$	Probability of an event
SOP	Secrecy outage probability
P_{out}	SN outage probability
SOP^{∞}	Asymptotic SOP
$\mathcal{G}_a$	Secrecy diversity order
$\mathcal{G}_d$	Secrecy array gain
$\mathcal{O}(\cdot)$	Higher order term
β	$2^{\mathcal{R}_s}$
α	$\beta - 1$

in the system is known[1]. As we consider a passive Eav, its CSI is unknown at both the RIS and the PT.

The channel coefficients for the PT $\to$ PR, PT $\to$ Eav, RIS $\to$ Eav, RIS $\to$ PR, S $\to$ Eav, S $\to$ PR, S $\to$ D, S $\to$ RIS, and RIS $\to$ D links are expressed as h_{pp}, h_{pe}, $\mathbf{h_E}$[2], $\mathbf{h_P}$, h_{se}, h_{sp}, h_{sd}, $\mathbf{h_S}$, and $\mathbf{h_D}$, respectively. The above channel coefficients are assumed to undergo Rayleigh fading[3]. To elaborate, $\mathbf{h_S} \in \mathbb{C}^{N\times 1}$, $\mathbf{h_D} \in \mathbb{C}^{1\times N}$, $\mathbf{h_E} \in \mathbb{C}^{1\times N}$, and $\mathbf{h_P} \in \mathbb{C}^{1\times N}$ denote the channel vector between the SN transmitter and RIS, RIS and SN receiver, RIS and eavesdropper, and RIS and PN receiver, respectively. Moreover, the Euclidean distances between S $\to$ RIS, RIS $\to$ D, S $\to$ D, PT $\to$ PR, PT $\to$ Eav, RIS $\to$ Eav, RIS $\to$ PR, S $\to$ Eav, and S $\to$ PR links are denoted as d_{sr}, d_{rd}, d_{sd}, d_{pp}, d_{pe}, d_{re}, d_{rp}, d_{se}, and d_{sp}, respectively. In addition, n_{ϱ} is the additive white

[1]The traditional pilot signaling techniques can be utilized to estimate the CSI of the legitimate transmission links [1], [13], [18], [21], [22]

[2]The bold font is used to indicate vectors.

[3]Since the transmission links experience blockages and the RIS's location cannot be optimized to guarantee reliable line-of-sight links, similar to [13], [21], [22], Rayleigh fading environment is assumed in this work.

Gaussian noise (AWGN) at D, PR, and E, respectively, where $\varrho \in \{d, p, e\}$, with zero mean and variance σ_ϱ^2. Consequently, the received signal at D can be written as

$$y_{\text{D}} = \sqrt{P_{\text{S}}}\, x_s \left[\left(\frac{d_{sr}\, d_{rd}}{d_o^2} \right)^{-\frac{\eta}{2}} \sum_{i=1}^{N} h_{s_i}\, h_{d_i}\, e^{j\phi_i} + h_{sd} \left(\frac{d_{sd}}{d_o} \right)^{-\frac{\eta}{2}} \right] + n_d, \tag{1}$$

where x_s is the SN transmitted signal, P_{S} denotes the SN transmitted power, d_o is a reference distance, and η is the path loss exponent. In addition, h_{s_i} and h_{d_i} are complex Gaussian random variables (RV) with a zero mean and unit variance, and ϕ_i is the alterable phase coefficient of the i^{th} element of the RIS. Moreover, it is assumed that the PT position is distant from the RIS and D and, therefore, does not impose any real interference. Consequently, the interference at the RIS and D from PT is negligible; this is a well-known assumption that is widely used in the literature [23], [24]. Furthermore, the phases of the channels h_{s_i} and h_{d_i} are assumed to be perfectly known at the RIS. Hence, the optimal phase shift is selected to maximize the instantaneous signal-to-noise ratio (SNR) at D [1], [25]. Besides, the reflected gain of the i^{th} reflecting element is assumed to equal to one [1], [13]. Thus, the received signal at the PR can be written as

$$y_{\text{P}} = \sqrt{P_{\text{P}}} \left(\frac{d_{pp}}{d_o} \right)^{-\frac{\eta}{2}} h_{pp}\, x_p + \sqrt{P_{\text{S}}}\; x_s \left[\left(\frac{d_{sr}\, d_{rp}}{d_o^2} \right)^{-\frac{\eta}{2}} \times \sum_{i=1}^{N} h_{s_i}\, h_{p_i}\, e^{j\theta_i} + h_{sp} \left(\frac{d_{sp}}{d_o} \right)^{-\frac{\eta}{2}} \right] + n_p, \tag{2}$$

where x_p is the PN transmitted signal, P_{P} denotes the PN transmitted power, and θ_i is the residual phase errors affecting the PR. In a similar way, the wiretapped signal at Eav can be written as

$$y_{\text{E}} = \sqrt{P_{\text{P}}} \left(\frac{d_{pe}}{d_o} \right)^{-\frac{\eta}{2}} h_{pe}\, x_p + \sqrt{P_{\text{S}}}\, x_s \left[\left(\frac{d_{sr}\, d_{re}}{d_o^2} \right)^{-\frac{\eta}{2}} \times \sum_{i=1}^{N} h_{s_i}\, h_{e_i}\, e^{j\psi_i} + h_{se} \left(\frac{d_{se}}{d_o} \right)^{-\frac{\eta}{2}} \right] + n_e, \tag{3}$$

where h_{e_i} is the channel coefficient between Eav and the i^{th} reflecting element of the RIS and ψ_i is the residual phase errors affecting the Eav. The instantaneous SNR at D, γ_D, is given by

$$\gamma_{\text{D}} = \frac{P_{\text{S}}}{\sigma_d^2} \left| \left(\frac{d_{sr} d_{re}}{d_o^2} \right)^{-\frac{\eta}{2}} \sum_{i=1}^{N} h_{s_i} h_{d_i} e^{j\phi_i} + h_{sd} \left(\frac{d_{sd}}{d_o} \right)^{-\frac{\eta}{2}} \right|^2. \tag{4}$$

Moreover, the instantaneous signal-to-interference-and-noise ratio (SINR) at PR and Eav, denoted as γ_P and γ_E, respectively, are given by

$$\gamma_{\text{P}} = \frac{P_{\text{P}} \left(\frac{d_{pp}}{d_o^2} \right)^{-\eta} |h_{pp}|^2}{P_{\text{S}} \left| \left(\frac{d_{sr} d_{rp}}{d_o^2} \right)^{-\frac{\eta}{2}} \sum_{i=1}^{N} h_{s_i} h_{p_i} e^{j\theta_i} + \left(\frac{d_{sp}}{d_o} \right)^{-\frac{\eta}{2}} h_{sp} \right|^2 + \sigma_p^2}, \tag{5}$$

and

$$\gamma_{\text{E}} = \frac{P_{\text{P}} \left(\frac{d_{sd}}{d_o} \right)^{-\eta} |h_{pe}|^2}{P_{\text{S}} \left| \left(\frac{d_{sr} d_{re}}{d_o^2} \right)^{-\frac{\eta}{2}} \sum_{i=1}^{N} h_{s_i} h_{e_i} e^{j\psi_i} + \left(\frac{d_{se}}{d_o} \right)^{-\frac{\eta}{2}} h_{se} \right|^2 + \sigma_e^2}, \tag{6}$$

which can be rewritten as

$$\gamma_{\text{E}} = \frac{\Psi_{\text{PE}}}{\Psi_{\text{E}} + 1}, \tag{7}$$

where

$$\Psi_{\text{E}} = \left| \Lambda_1 \sum_{i=1}^{N} h_{s_i}\, h_{e_i}\, e^{j\psi_i} + \Lambda_2\, h_{se} \right|^2,$$

$\Lambda_1 = \sqrt{\bar{\gamma}_{se}} \left(\frac{d_{sr}\, d_{re}}{d_o^2} \right)^{-\frac{\eta}{2}}$, $\Lambda_2 = \sqrt{\bar{\gamma}_{se}} \left(\frac{d_{se}}{d_o^2} \right)^{-\frac{\eta}{2}}$, $\bar{\gamma}_{se} = \frac{P_{\text{S}}}{\sigma_e^2}$, $\Psi_{\text{PE}} = \omega_e\, |h_{pe}|^2$, $\omega_e = \bar{\gamma}_e \left(\frac{d_{sd}}{d_o} \right)^{-\eta}$, and $\bar{\gamma}_e = \frac{P_{\text{P}}}{\sigma_e^2}$. As the phase shifts of the RIS elements are designed based on the legitimate SN link, the resulting phase distributions for each RIS→E link ψ_i are i.i.d. and uniformly distributed RVs by virtue of [21]. Thus, Ψ_{E} can be approximated by an exponential RV according to [26, Corollary 2] with a parameter $\Lambda_E = N\,\Lambda_1^2 + \Lambda_2^2$. Therefore, the PDF of Ψ_{E} is given by

$$f_{\Psi_{\text{E}}}(\gamma) = \frac{1}{\Lambda_E} \exp\left(-\frac{\gamma}{\Lambda_E} \right). \tag{8}$$

It is worth mentioning that the SN transmitted power, P_{S}, must be under a certain level to limit the interference. Consequently, the interference signal power towards the PR should be constrained as $P_{\text{S}}\, \Psi_{\text{P}} \leq \mathcal{Q}$, where Ψ_{P} is the summation of the channel power gains from the RIS and S, and $\mathcal{Q}$ is the threshold of interference temperature. Precisely, Ψ_{P} consists of the reflected link RIS → PR and the S → PR link, while $\mathcal{Q}$ expresses the maximum tolerant interference imposed on the PR. From (5), Ψ_{P} can be expressed as

$$\Psi_{\text{P}} = \left| \left(\frac{d_{sr} d_{rp}}{d_o^2} \right)^{-\frac{\eta}{2}} \sum_{i=1}^{N} h_{s_i} h_{p_i} e^{j\theta_i} + \left(\frac{d_{sp}}{d_o} \right)^{-\frac{\eta}{2}} h_{sp} \right|^2. \tag{9}$$

Similar to Ψ_{E}, Ψ_{P} also can be approximated as an exponential RV with a parameter $\lambda_{\text{P}} = \left(\frac{d_{sr} d_{rp}}{d_o^2} \right)^{-\eta} N + \left(\frac{d_{sp}}{d_o} \right)^{-\eta}$, where the PDF of Ψ_{P} is given by

$$f_{\Psi_{\text{P}}}(\gamma) = \frac{1}{\lambda_P} \exp\left(-\frac{\gamma}{\lambda_P} \right). \tag{10}$$

III. Performance Analysis

A. PN Secrecy Outage Probability

In this subsection, the SOP of the PN is investigated. The SOP can be expressed as

$$\mathrm{SOP} = \Pr\left(\mathcal{C}_{\mathrm{S}} < \mathcal{R}_s\right), \tag{11}$$

where $\mathcal{C}_{\mathrm{S}}$ is the PN secrecy capacity and $\mathcal{R}_s$ is the PN target secrecy rate. In this regard, $\mathcal{C}_{\mathrm{S}}$ can be obtained by

$$\mathcal{C}_{\mathrm{S}} = \left[\mathcal{C}_{\mathrm{P}} - \mathcal{C}_{\mathrm{E}}, 0\right]^{+}, \tag{12}$$

where $\mathcal{C}_{\mathrm{P}}$ and $\mathcal{C}_{\mathrm{E}}$ are the PN and the Eav capacities, respectively, and $[x,0]^{+} = \max(x,0)$. Accordingly, $\mathcal{C}_{\mathrm{P}}$ is given by

$$\mathcal{C}_{\mathrm{P}} = \log_2\Big(1+\gamma_{\mathrm{P}}\Big), \tag{13}$$

where γ_{P} is given by

$$\gamma_{\mathrm{P}} = \frac{P_{\mathrm{P}}\left(\frac{d_{pp}}{d_o^2}\right)^{-\eta}|h_{pp}|^2}{P_{\mathrm{S}}\Psi_{\mathrm{P}}+\sigma_p^2} = \frac{P_{\mathrm{P}}\left(\frac{d_{pp}}{d_o^2}\right)^{-\eta}|h_{pp}|^2}{\mathcal{Q}+\sigma_p^2} = \Phi\,|h_{pp}|^2, \tag{14}$$

where $\mathcal{Q} = P_{\mathrm{S}}\,\Psi_{\mathrm{P}}$, $\Phi = \omega_p\,\vartheta$, $\omega_p = \frac{P_{\mathrm{P}}}{\sigma_p^2}\left(\frac{d_{pp}}{d_o^2}\right)^{-\eta}$, and $\vartheta = \left(\frac{\mathcal{Q}}{\sigma_p^2}+1\right)^{-1}$. Antenna selection approach is employed at the PT to avoid the high hardware complexity while maintaining the diversity and reliability advantages of multiple antennas. More specifically, the importance of using the antenna selection approach lies in the fact that the power consumption and the complexity of signal processing overhead are low as compared with other techniques such as beamforming techniques. Antenna selection strategy is applied at the PT to maintain multiple antennas' diversity and reliability benefits, while avoiding high hardware complexity. Therefore, the best antenna at PT is selected according to the following criterion

$$|h_{pp}|^2 = \max_{n\in\{1,\ldots,N_P\}} |h_{p_n p}|^2. \tag{15}$$

The CDF of γ_{P} is given by

$$F_{\gamma_{\mathrm{P}}}(\gamma) = \sum_{n=0}^{N_P-1}\frac{N_P\binom{N_P-1}{n}}{(-1)^{-n}(n+1)}\left(1-\exp\left(\frac{-\gamma\,(n+1)}{\Phi}\right)\right). \tag{16}$$

Moreover, $\mathcal{C}_{\mathrm{E}}$ is given by $\mathcal{C}_{\mathrm{E}} = \log_2(1+\gamma_{\mathrm{E}})$, where γ_{E} is given in (6). Now, the SOP can be derived as

$$\mathrm{SOP}_{\varsigma} = \int_0^{\infty} F_{\gamma_P}(\beta\gamma+\alpha) f_{\gamma_E}^{\varsigma}(\gamma)\,d\gamma, \tag{17}$$

where $\alpha = \beta - 1$, $\beta = 2^{\mathcal{R}_s}$, and $\varsigma \in \{\mathrm{SC},\mathrm{MRC}\}$. For the SC technique, the PDF of γ_E, $f_{\gamma_E}^{\mathrm{SC}}(\gamma)$, is given by [27, eq. (31)]

$$f_{\gamma_{\mathrm{E}}}^{\mathrm{SC}}(\gamma) = \sum_{k=0}^{N_E-1}\frac{N_E(-1)^k\binom{N_E-1}{k}}{\omega_e\Lambda_E}\exp\left(-\frac{\gamma(k+1)}{\omega_e}\right) \times\left(\frac{1+\frac{\gamma(k+1)}{\omega_e}+\frac{1}{\Lambda_E}}{\left(\frac{\gamma(k+1)}{\omega_e}+\frac{1}{\Lambda_E}\right)^2}\right). \tag{18}$$

By plugging (16) and (18) into (17), and after simple algebraic manipulations, then with the help of [28, eq. (3.383.9)], the SOP for SC, $\mathrm{SOP}_{\mathrm{SC}}$, can be derived as

$$\begin{aligned}\mathrm{SOP}_{\mathrm{SC}} =& N_P\sum_{n=0}^{N_P-1}\frac{(-1)^n\binom{N_P-1}{n}}{(n+1)}\Bigg[1-\frac{N_E}{\omega_e\,\Lambda_E}\\ &\times\sum_{k=0}^{N_E-1}\frac{(-1)^k\binom{N_E-1}{k}}{\mathcal{H}_1\exp\left(-\left(\mathcal{H}_3-\mathcal{H}_2\right)\right)}\\ &\left(\frac{\Lambda_E}{\exp\left(-\mathcal{H}_3\right)}+\frac{(\mathcal{H}_4-\mathcal{H}_1)}{\mathcal{H}_1}\Gamma\left(0,\mathcal{H}_3\right)\right)\Bigg],\end{aligned} \tag{19}$$

where $\mathcal{H}_1 = \frac{(k+1)}{\omega_e}$, $\mathcal{H}_2 = \frac{\alpha\,(n+1)}{\Phi}$, $\mathcal{H}_3 = \frac{\mathcal{H}_4}{\Lambda_E\,\mathcal{H}_1}$, $\mathcal{H}_4 = \frac{\beta(n+1)}{\Phi}+\frac{(k+1)}{\omega_e}$, and $\Gamma(\cdot,\cdot)$ denotes the upper incomplete gamma function [28, eq. (8.350.2)]. For the MRC technique, the PDF of γ_E, $f_{\gamma_E}^{\mathrm{MRC}}(\gamma)$, is given by [27, eq. (37)]

$$f_{\gamma_{\mathrm{E}}}^{\mathrm{MRC}}(\gamma) = \frac{\gamma^{N_E-1}\exp\left(\frac{-\gamma}{\omega_e}\right)}{\Gamma(N_E)\,\omega_e^{N_E}\Lambda_E}\sum_{k=0}^{N_E}\frac{\binom{N_E}{k}\Gamma(k+1)}{\left(\frac{\gamma}{\omega_e}+\frac{1}{\Lambda_E}\right)^{k+1}}. \tag{20}$$

By plugging (16) and (20) into (17), and after simple algebraic manipulations, then with the help of [28, eq. (3.383.4)], the SOP for MRC, $\mathrm{SOP}_{\mathrm{MRC}}$, can be derived as

$$\begin{aligned}\mathrm{SOP}_{\mathrm{MRC}} =& \sum_{n=0}^{N_P-1}\frac{N_P\binom{N_P-1}{n}}{(-1)^{-n}(n+1)}\Bigg[1-\sum_{k=0}^{N_E}\frac{\binom{N_E}{k}\Gamma(k+1)}{\Lambda_E^{N_E-k}}\\ &\frac{\mathcal{H}_5^{-\left(\frac{N_E-k}{2}\right)}W_{\frac{-N_E-k}{2},\frac{-N_E+k+1}{2}}\left(\mathcal{H}_5\right)}{\exp\big(-\left(0.5\,\mathcal{H}_5-\mathcal{H}_2\right)\big)}\Bigg],\end{aligned} \tag{21}$$

where $\mathcal{H}_5 = \left(\frac{\Phi+\beta\,\omega_e\,(n+1)}{\Phi\,\Lambda_E}\right)$, and $W_{a,b}(\cdot)$ denotes the Whittaker function [28, eq. (9.220.4)].

B. Asymptotic SOP Analysis

The PN asymptotic SOP, SOP^{∞}, is studied when $\omega_p \to \infty$. In this scenario, we consider that $\omega_p >> \omega_e$. SOP^{∞} is given by

$$\mathrm{SOP}^{\infty} = (\mathcal{G}_a\overline{\gamma}_d)^{-\mathcal{G}_d} + \mathcal{O}(\overline{\gamma}_d^{-\mathcal{G}_d}), \tag{22}$$

where $\mathcal{G}_d$ is the secrecy diversity order, $\mathcal{G}_a$ is the secrecy array gain, and $\mathcal{O}(.)$ is the higher order terms. In this respect, the SOP^{∞} can be derived by first obtaining the asymptotic CDF, $F_{\gamma_{\mathrm{P}}}^{\infty}(\gamma)$, [29, eq. (42)]. Then, by plugging $F_{\gamma_{\mathrm{P}}}^{\infty}(\gamma)$ into (17), and using [28, eq. (3.382.4)] the SOP^{∞} can be derived. For the SC technique, $\mathcal{G}_d^{\mathrm{SC}} = N_P$ and $\mathcal{G}_a^{\mathrm{SC}}$ is given by

$$\begin{aligned}\mathcal{G}_a^{\mathrm{SC}} =& \left[\sum_{k=0}^{N_E-1}\sum_{n=0}^{N_P}\frac{\binom{N_E-1}{k}\binom{N_P}{n}\mathcal{Z}_1}{(-1)^{-k}(k+1)^n}\left(W_{\frac{-n-1}{2},\frac{-n}{2}}\left(\frac{1}{\Lambda_E}\right)\right.\right.\\ &\left.\left.\times\frac{1}{\sqrt{\Lambda_E}}+W_{\frac{-n-2}{2},\frac{-i+1}{2}}\left(\frac{1}{\Lambda_E}\right)\right)\right]^{\frac{-1}{N_P}},\end{aligned} \tag{23}$$

where $\mathcal{Z}_1 = \frac{N_E\, \beta^n\, \alpha^{N_P-n} \Gamma(n+1)\, \omega_e^n}{\vartheta^{N_P} \exp\left(\frac{-1}{2\omega_e}\right)}$. For the MRC technique, $\mathcal{G}_d^{\mathrm{MRC}} = N_P$ and $\mathcal{G}_a^{\mathrm{MRC}}$ is given by

$$\mathcal{G}_a^{\mathrm{MRC}} = \Bigg[\sum_{k=0}^{N_E} \sum_{n=0}^{N_P} \binom{N_E}{k} \binom{N_P}{n} \mathcal{Z}_2 \times W_{\frac{-N_E-k-n}{2}, \frac{-N_E+k-n+1}{2}} \left(\frac{1}{\omega_e}\right)\Bigg]^{\frac{-1}{N_P}}, \tag{24}$$

where $\mathcal{Z}_2 = \frac{\beta^n\, \alpha^{N_P-n} \Gamma(N_E+n) \Gamma(k+1)\, \omega_e^n}{\Gamma(N_E) \vartheta^{N_P} \exp\left(\frac{-1}{2\omega_e}\right) \Lambda_E^{\frac{N_E+n-k}{2}}}$.

C. Probability of Non-zero Secrecy Capacity

In this subsection, the requirement for the presence of non-zero secrecy capacity is investigated. It is worth noting that the non-zero secrecy capacity is achieved when $\gamma_C > \gamma_E$. From (11), the PNSC is given by

$$\begin{aligned}\mathrm{PNSC}_\varsigma = \Pr(\mathcal{C}_\mathrm{S} > 0) &= \Pr\left(\frac{1+\gamma_\mathrm{P}}{1+\gamma_\mathrm{E}} > 1\right) \\ &= 1 - \int_0^\infty F_{\gamma_\mathrm{P}}(\gamma) f_{\gamma_\mathrm{E}}^\varsigma(\gamma)\, d\gamma.\end{aligned} \tag{25}$$

1) Eavesdropper's Channel with SC: By plugging (16) and (18) into (25), and after simple algebraic manipulations, then with the help of [28, eq. (3.383.9)], the PNSC for SC, $\mathrm{PNSC}_{\mathrm{SC}}$, can be derived as

$$\begin{aligned}\mathrm{PNSC}_{\mathrm{SC}} =& 1 - N_P \sum_{n=0}^{N_P-1} \frac{(-1)^n \binom{N_P-1}{n}}{(n+1)} \Bigg[1 - \frac{N_E}{\omega_e\, \Lambda_E} \\ &\times \sum_{k=0}^{N_E-1} \frac{(-1)^k \binom{N_E-1}{k}}{\mathcal{H}_1 \exp\left(-\mathcal{H}_6\right)} \\ &\times \left(\frac{\Lambda_E}{\exp\left(-\mathcal{H}_6\right)} + \frac{(\mathcal{H}_7 - \mathcal{H}_1)}{\mathcal{H}_1} \Gamma\left(0, \mathcal{H}_6\right)\right)\Bigg],\end{aligned} \tag{26}$$

where $\mathcal{H}_6 = \frac{\mathcal{H}_7}{\Lambda_E\, \mathcal{H}_1}$, $\mathcal{H}_7 = \frac{(n+1)}{\Phi} + \frac{(k+1)}{\omega_e}$.

2) Eavesdropper's Channel with MRC: By plugging (16) and (20) into (25), and after simple algebraic manipulations, then with the help of [28, eq. (3.383.4)], the PNSC for MRC, $\mathrm{PNSC}_{\mathrm{MRC}}$, can be derived as

$$\begin{aligned}\mathrm{PNSC}_{\mathrm{MRC}} =& 1 - \sum_{n=0}^{N_P-1} \frac{N_P \binom{N_P-1}{n}}{(-1)^{-n} (n+1)} \Bigg[1 - \sum_{k=0}^{N_E} \frac{\binom{N_E}{k}}{\Lambda_E^{N_E-k}} \\ &\times \frac{\Gamma(k+1) \mathcal{H}_8^{-\left(\frac{N_E-k}{2}\right)} W_{\frac{-N_E-k}{2}, \frac{-N_E+k+1}{2}} \left(\mathcal{H}_8\right)}{\exp\left(-0.5\, \mathcal{H}_8\right)}\Bigg],\end{aligned} \tag{27}$$

where $\mathcal{H}_8 = \left(\frac{\Phi + \omega_e\, (n+1)}{\Phi\, \Lambda_E}\right)$, and $W_{a,b}(\cdot)$ denotes the Whittaker function [28, eq. (9.220.4)].

D. SN Outage Probability

For the SN, the outage probability, P_{out}, can be expressed by

$$P_{out} = \Pr\left(\gamma_\mathrm{D} \le 2^{\mathcal{R}_d} - 1\right) = F_{\gamma_\mathrm{D}}(2^{\mathcal{R}_d} - 1), \tag{28}$$

where $\mathcal{R}_d$ is the SN achievable data rate, and γ_D is the instantaneous SNR of the CR link. Now, by replacing P_S with $\frac{\mathcal{Q}}{\Psi_\mathrm{P}}$ in (4), γ_D can be written as

$$\gamma_\mathrm{D} = \frac{\mathcal{Q}}{\Psi_\mathrm{P}\, \sigma_d^2} \left| \left(\frac{d_{sr} d_{rd}}{d_o^2}\right)^{-\frac{\eta}{2}} \sum_{i=1}^N h_{s_i} h_{d_i} e^{j\phi_i} + h_{sd} \left(\frac{d_{sd}}{d_o}\right)^{-\frac{\eta}{2}} \right|^2, \tag{29}$$

which can be rewritten as $\gamma_\mathrm{D} = \frac{\Psi_\mathrm{D}}{\Psi_\mathrm{P}}$, where $\Psi_\mathrm{D} = \left(\Omega_1 \sum_{i=1}^N |h_{s_i}|\, |h_{d_i}| + \Omega_2 |h_{sd}|\right)^2$, $\Omega_1 = \frac{\sqrt{\mathcal{Q}}}{\sigma_d} \left(\frac{d_{sr}\, d_{rd}}{d_o^2}\right)^{-\frac{\eta}{2}}$, $\Omega_2 = \frac{\sqrt{\mathcal{Q}}}{\sigma_d} \left(\frac{d_{sd}}{d_o^2}\right)^{-\frac{\eta}{2}}$. According to the central limit theorem, $\chi_1 = \sum_{i=1}^N |h_{s_i}|\, |h_{d_i}|$ can be approximated as a Gaussian RV with a mean value $\varepsilon = \frac{N\pi}{4}$ and variance $\sigma^2 = N\left(1 - \frac{\pi}{16}\right)$ [1]. Moreover, $\chi_2 = |h_{sd}|$ is a Rayleigh-distributed RV with a parameter δ. Thus, the pdfs of χ_1 and χ_2 are given by

$$f_{\chi_1}(\gamma) = \frac{1}{\sqrt{2\pi\sigma^2}} \exp\left(\frac{-\left(\gamma - \mu\right)^2}{2\sigma^2}\right), \tag{30}$$

and

$$f_{\chi_2}(\gamma) = \frac{\gamma}{\delta} \exp\left(-\frac{\gamma^2}{2\delta}\right), \tag{31}$$

respectively. Thus, Ψ_D can be expressed as $\Psi_\mathrm{D} = \Big(\Omega_1 \chi_1 + \Omega_2\, \chi_2\Big)^2$, leading to the cumulative distribution function (CDF) given by [30]

$$\begin{aligned}F_{\Psi_\mathrm{D}}(\gamma) =& 0.5 \left[\mathrm{erf}\left(\frac{(\varphi_1/\varphi_2)\sqrt{\gamma} - \varepsilon}{\sqrt{2\sigma^2}}\right) + \mathrm{erf}\left(\frac{\varepsilon}{\sqrt{2\sigma^2}}\right)\right] \\ &- \frac{\sqrt{\delta}}{2\xi_1} \exp\left(\frac{-\left(\varphi_1\sqrt{\gamma} - \varphi_2\varepsilon\right)^2}{2\xi_1^2}\right) \mathrm{erf}\left(\frac{\xi_4\sqrt{\gamma} - \xi_5}{\xi_1\xi_2}\right) \\ &- \frac{\sqrt{\delta}}{2\xi_1} \exp\left(\frac{-\left(\varphi_1\sqrt{\gamma} - \varphi_2\varepsilon\right)^2}{2\xi_1^2}\right) \mathrm{erf}\left(\frac{\xi_3\sqrt{\gamma} + \xi_5}{\xi_1\xi_2}\right),\end{aligned} \tag{32}$$

where δ is a Rayleigh-distributed RV parameter, $\varepsilon = \frac{N\pi}{4}$, $\sigma^2 = N\left(1 - \frac{\pi}{16}\right)$, $\varphi_1 = \frac{1}{\Omega_2}$, $\varphi_2 = \frac{\Omega_1}{\Omega_2}$, $\xi_1 = \sqrt{\sigma^2\varphi_2 + \delta}$, $\xi_2 = \sqrt{2\sigma^2\delta}$, $\xi_3 = \sigma^2\varphi_1\varphi_2$, $\xi_4 = \frac{\delta\varphi_1}{\varphi_2}$, $\xi_5 = \delta\,\varepsilon$, and $\mathrm{erf}(\cdot)$ is the error function [28, eq. (8.250.1)]. P_{out} can be further written mathematically as [31]

$$P_{out} = \int_0^\infty F_{\Psi_\mathrm{D}}(\gamma\, x)\, f_{\Psi_\mathrm{P}}(x)\, dx. \tag{33}$$

However, utilizing (32) to derive P_{out} is not mathematically tractable. Therefore, the below approximation of the $\mathrm{erf}(\cdot)$ function is utilized [32]

$$\mathrm{erf}\,(x) \approx \begin{cases} 1 - \sum_{m=1}^4 \Upsilon_m \exp\left(-\Theta_m\, x^2\right) & x \ge 0 \\ -1 + \sum_{m=1}^4 \Upsilon_m \exp\left(-\Theta_m\, x^2\right) & x < 0, \end{cases} \tag{34}$$

where $\Theta = [1, 2, 20/3, 20/17]$, and $\Upsilon = [1/8, 1/4, 1/4, 1/4]$.

$$\mathcal{A}_1 = \exp\left(\frac{-b_2^2}{b_1^2\lambda_P}\right) + \frac{1}{2}\left(\operatorname{erf}\left(\frac{\varepsilon}{\sqrt{2\sigma^2}}\right) - 1\right) + \sum_{m=1}^{4}\frac{\Upsilon_m \exp\left(-\frac{a_2}{2}\right)}{4b_1^2\sqrt{(a_2/2)^3}\lambda_P}\left[2\sqrt{a_1}\left(\exp\left(b_2\left(a_2 - a_1 b_2\right)\right) - 2\right) + \exp\left(\frac{a_2^2}{4a_1}\right)\right.$$
$$\left.\sqrt{\pi}\left(a_2 - 2a_1 b_2\right)\left(\operatorname{erfc}\left(\frac{a_2}{2\sqrt{a_1}}\right) - \operatorname{erf}\left(\frac{a_2}{2\sqrt{a_1}}\right) + \operatorname{erf}\left(\frac{a_2 - 2a_1 b_2}{2\sqrt{a_1}}\right)\right)\right], \tag{35}$$

$$\begin{aligned}\mathcal{A}_2 =& \frac{\exp\left(-c_3\right)\Xi_1}{4}\left[\frac{1}{\sqrt{c_1^3}}\left(2\sqrt{c_1}\left(2 - \exp\left(\left(\frac{\xi_5}{\xi_1\xi_2}\right)\left(c_2 - c_1\left(\frac{\xi_5}{\xi_1\xi_2}\right)\right)\right)\right) - \Xi_2\sqrt{\pi}\exp\left(\frac{c_2^2}{4c_1}\right)\left(\operatorname{erf}\left(\frac{\Xi_2}{2\sqrt{c_1}}\right)\right.\right.\right.\\ &\left.\left.-\operatorname{erf}\left(\frac{c_2}{2\sqrt{c_1}}\right) + \operatorname{erfc}\left(\frac{c_2}{2\sqrt{c_1}}\right)\right)\right) + \sum_{m=1}^{4}\frac{\Upsilon_m}{\sqrt{c_4^3}}\left(2\sqrt{c_4}\left(\exp\left(\left(\frac{\xi_5}{\xi_1\xi_2}\right)\left(c_2 - c_4\left(\frac{\xi_5}{\xi_1\xi_2}\right)\right)\right) - 2\right)\right.\\ &\left.\left.+\Xi_3\sqrt{\pi}\exp\left(\frac{c_2^2}{4c_4}\right)\left(\operatorname{erf}\left(\frac{\Xi_3}{2\sqrt{c_4}}\right) - \operatorname{erf}\left(\frac{c_2}{2\sqrt{c_4}}\right) + \operatorname{erfc}\left(\frac{c_2}{2\sqrt{c_4}}\right)\right)\right)\right],\end{aligned} \tag{36}$$

$$\begin{aligned}\mathcal{A}_3 =& \frac{\Xi_4}{4}\exp\left(-\left(\upsilon_3 - \left(\frac{\xi_5}{\xi_1\xi_2}\right)\upsilon_2\right)\right)\left[\upsilon_1^{-\frac{3}{2}}\exp\left(-\left(\frac{\xi_5}{\xi_1\xi_2}\right)^2\upsilon_1\right)\left(2\sqrt{\upsilon_1} - \Xi_5\sqrt{\pi}\,\exp\left(\frac{\Xi_5^2}{4\upsilon_1}\right)\operatorname{erf}\left(\frac{\Xi_5}{2\sqrt{\upsilon_1}}\right)\right)\right.\\ &\left.+\sum_{m=1}^{4}\frac{\Upsilon_m}{\sqrt{\upsilon_4^3}}\exp\left(-\left(\frac{\xi_5}{\xi_1\xi_2}\right)^2\upsilon_4\right)\left(-2\sqrt{\upsilon_4} + \Xi_6\sqrt{\pi}\,\exp\left(\frac{\Xi_6^2}{4\upsilon_4}\right)\operatorname{erf}\left(\frac{\Xi_6}{2\sqrt{\upsilon_4}}\right)\right)\right],\end{aligned} \tag{37}$$

where

$$b_1 = \frac{\varphi_1\sqrt{\gamma}}{\sqrt{2\sigma^2}},\ b_2 = \frac{\varepsilon}{\sqrt{2\sigma^2}},\ a_1 = \frac{1}{\lambda_p\, b_1^2} + \Theta_m,\ a_2 = \frac{2b_2}{\lambda_p\, b_1^2},\ \Xi_1 = \frac{\xi_1\xi_2^2\sqrt{\delta}}{\lambda_P\xi_4^2},\ \Xi_2 = c_2 - 2c_1\left(\frac{\xi_5}{\xi_1\xi_2}\right),\ \Xi_3 = c_2 - 2c_4\left(\frac{\xi_5}{\xi_1\xi_2}\right),$$

$$c_1 = \frac{\varphi_1^2\xi_2^2}{2\xi_4^2} + \frac{\xi_1^2\xi_2^2}{\lambda_P\xi_4^2\gamma},\quad c_2 = \frac{\xi_2}{\xi_1\xi_4^2\gamma}\left(\varphi_1\left(\varphi_1\xi_5\gamma - \varepsilon\xi_4\gamma\right) + \frac{2\xi_1^2\xi_5}{\lambda_P}\right),\quad c_3 = \frac{\xi_5^2}{\lambda_P\xi_4^2} + \frac{1}{2\xi_1^2}\left(\frac{\varphi_1\xi_5}{\xi_4} - \varepsilon\right)^2,\quad c_4 = c_1 + \Theta_m,$$

$$\upsilon_1 = \frac{\varphi_1^2\xi_2^2\gamma}{2\xi_3^2} + \frac{\xi_1^2\xi_2^2}{\lambda_P\xi_3^2},\ \ \upsilon_2 = \frac{\xi_2}{\xi_1\xi_3^2}\left(\varphi_1\left(\varphi_1\xi_5\gamma + \varepsilon\xi_3\sqrt{\gamma}\right) + \frac{2\xi_1^2\xi_5}{\lambda_P}\right),\ \ \upsilon_3 = \frac{\xi_5^2}{\lambda_P\xi_3^2} + \frac{1}{2\xi_1^2}\left(\frac{\varphi_1\xi_5\sqrt{\gamma}}{\xi_3} + \varepsilon\right)^2,\ \ \upsilon_4 = \upsilon_1 + \Theta_m,$$

$$\Xi_4 = \frac{\xi_1\xi_2^2\sqrt{\delta}}{\lambda_P\xi_3^2},\quad \Xi_5 = 2\upsilon_1\left(\frac{\xi_5}{\xi_1\xi_2}\right) - \upsilon_2,\quad \text{and } \Xi_6 = 2\upsilon_4\left(\frac{\xi_5}{\xi_1\xi_2}\right) - \upsilon_2.$$

By substituting (10) and (32) to (33) using (34), then with the help of [28, eq. (2.33.1)], P_{out} can be obtained as

$$P_{out} = \mathcal{A}_1 - \mathcal{A}_2 - \mathcal{A}_3, \tag{38}$$

where $\mathcal{A}_1$, $\mathcal{A}_2$, and $\mathcal{A}_3$ are given at the top of this page.

IV. Results and Discussions

This section provides numerical and simulation results to confirm the benefits of applying the RIS technology in the proposed system model. Unless otherwise stated, we set $\mathcal{R}_b$ = 1 b/s/Hz, $\mathcal{Q}$ = 10 dBW, $\bar{\gamma}_{se}$ = 5 dB, δ = 2, and $\mathcal{R}_s$ = 1 b/s/Hz.

In Fig. 2, we investigate the PN secrecy enhancement due to the deployment of the RIS technology. In this respect, the SOP of the PN is evaluated for the SC and MRC techniques versus ω_p, at Eav, for different values of N, where ω_e = 10 dB. The PN secrecy performance is improved as N increases, showing the effect of the RIS's jamming signals toward Eav. Consequently, the PLS of the PN is increased. Moreover, the SOP is enhanced as ω_p increases. As revealed in our analysis and simulation, improved secrecy performance can be achieved using RIS as a friendly jammer. This is because the wiretapped signal is degraded at Eav due to the jamming signals generated by the RIS, resulting in a more secure PN transmission. Since the MRC technique produces a higher SNR gain at Eav over the SC technique, the PN secrecy performance is degraded when Eav utilizes the MRC technique, as illustrated in Fig. 2. The asymptotic analyses are included, and perfect agreement with the theoretical results can be seen when $\omega_p \to \infty$, confirming the preciseness of the asymptotic expressions. Finally, it is evident that theoretical and simulation results have an excellent match, confirming the exactness of the derived expressions.

Figure 3 plots the PNSC versus $\bar{\gamma}_p$. It can be noted that the PNSC improves as $\bar{\gamma}_p$ increases for a fixed $\bar{\gamma}_e$. Moreover, the PNSC improves with decreasing $\bar{\gamma}_e$. Further, it is also remarkable that the PNSC increases as N increases. Interestingly, secure transmission is guaranteed as N increases. As

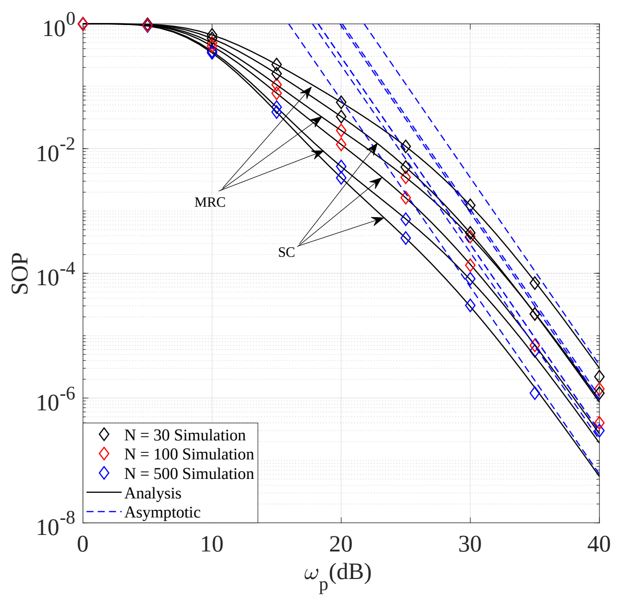

Fig. 2. The PN's SOP vs. ω_p, for different values of the number of reflecting elements, N, where $N_P = N_E = 3$.

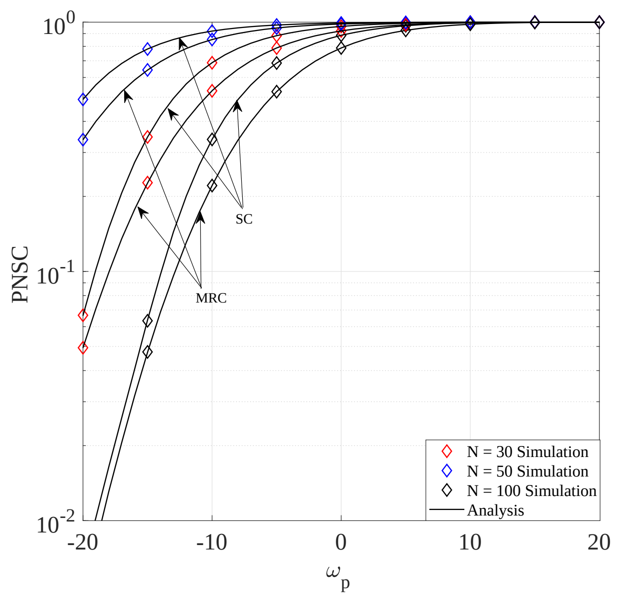

Fig. 3. The PN's PNSC vs. ω_p, for different values of the number of reflecting elements, N, where $N_P = N_E = 3$.

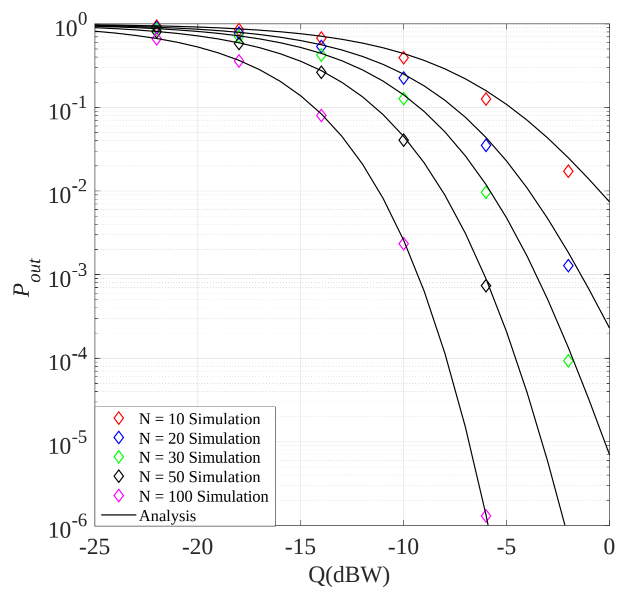

Fig. 4. The SN's P_{out} vs. $\mathcal{Q}$, for different values of the number of reflecting elements, N, where $\mathcal{R}_d = 1$ b/s/Hz.

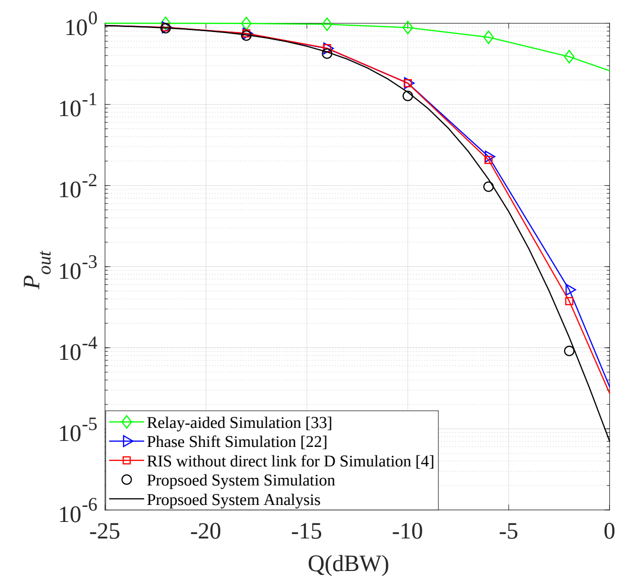

Fig. 5. The SN's P_{out} vs. $\mathcal{Q}$, for different scenarios, where $N = 30$, $\mathcal{R}_d = 1$ b/s/Hz.

expected, for the SC technique, the PNSC is lower than that of the MRC technique. Analytical results are also found to match simulation results, validating the accuracy of our analysis.

The SN outage probability, P_{out}, is presented in Fig. 4, where the numerical results are provided and compared with the simulated ones. Towards this end, the effect of N on the RIS is evaluated. As shown in this figure, P_{out} of the SN transmission decreases dramatically when $\mathcal{Q}$ increases. With this in mind, the reliability of SN communication increases as N increases. As an illustration, $\mathcal{Q}$ decreases by nearly 4 dB, deploying an RIS technology with N = 20 compared with N = 50 to reach P_{out} = 10^{-2}.

In Fig. 5, the reliability of the proposed system model is studied and compared with different scenarios. Towards this end, the relay-aided transmission [33], phase shift error, and unavailability of the line of sight between S and D scenarios are introduced and the results obtained through Monte-Carlo simulations. To evaluate the influence of the discrete phase shifts, simulation results where the phase error is uniformly distributed in $[-\frac{\pi}{4}, \frac{\pi}{4}]$ [22] are provided. Interestingly, the SN's reliability is enhanced by utilizing the RIS in the presence of the S-D link compared to other scenarios. This is due to the fact that the RIS can maximize the received SNR at D and thus improve the channel quality of the SN. It is also noteworthy that simulation and numerical results match impeccably, verifying the correctness of our analysis. Furthermore, theoretical results and simulation results agree perfectly, verifying the exactness of our analysis.

V. Conclusion

In this work, the RIS technology is employed to simultaneously assist SN transmission and enhance the PN's secrecy performance in a CR environment. New analytical expressions are provided for the SN's outage probability and the PN's SOP, considering practical combining techniques. The accuracy of the provided expressions is confirmed via extensive Monte-Carlo simulations. Furthermore, the benefits of the proposed system model are verified through numerical and simulation results.

References

[1] E. Basar, M. Di Renzo, J. De Rosny, M. Debbah, M.-S. Alouini, and R. Zhang, "Wireless communications through reconfigurable intelligent surfaces," *IEEE Access*, vol. 7, pp. 116 753–116 773, Jul. 2019.

[2] Q. Wu and R. Zhang, "Towards smart and reconfigurable environment: Intelligent reflecting surface aided wireless network," *IEEE Commun. Mag.*, vol. 58, no. 1, pp. 106–112, Jan. 2020.

[3] Q. Wu, S. Zhang, B. Zheng, C. You, and R. Zhang, "Intelligent reflecting surface aided wireless communications: A tutorial," *IEEE Trans. Commun.*, vol. 69, no. 5, pp. 3313–3351, May 2021.

[4] M. H. Khoshafa, T. M. Ngatched, and M. H. Ahmed, "Reconfigurable intelligent surfaces-aided physical layer security enhancement in D2D underlay communications," *IEEE Commun. Lett.*, vol. 25, no. 5, pp. 1443–1447, May 2021.

[5] M. H. Khoshafa, T. M. Ngatched, M. H. Ahmed, and A. R. Ndjiongue, "Active reconfigurable intelligent surfaces-aided wireless communication system," *IEEE Commun. Lett.*, vol. 25, no. 11, pp. 3699–3703, Nov. 2021.

[6] R. Fara, P. Ratajczak, D.-T. Phan-Huy, A. Ourir, M. Di Renzo, and J. De Rosny, "A prototype of reconfigurable intelligent surface with continuous control of the reflection phase," *IEEE Wireless Commun.*, vol. 29, no. 1, pp. 70–77, Feb. 2022.

[7] G. C. Trichopoulos, P. Theofanopoulos, B. Kashyap, A. Shekhawat, A. Modi, T. Osman, S. Kumar, A. Sengar, A. Chang, and A. Alkhateeb, "Design and evaluation of reconfigurable intelligent surfaces in real-world environment," *IEEE Open J. Commun. Soc.*, vol. 3, pp. 462–474, Dec. 2022.

[8] L. Dai, B. Wang, M. Wang, X. Yang, J. Tan, S. Bi, S. Xu, F. Yang, Z. Chen, M. Di Renzo *et al.*, "Reconfigurable intelligent surface-based wireless communications: Antenna design, prototyping, and experimental results," *IEEE access*, vol. 8, pp. 45 913–45 923, Mar. 2020.

[9] A. Chorti, A. N. Barreto, S. Köpsell, M. Zoli, M. Chafii, P. Sehier, G. Fettweis, and H. V. Poor, "Context-aware security for 6G wireless: the role of physical layer security," *IEEE Commun. Standards Mag.*, vol. 6, no. 1, pp. 102–108, Mar. 2022.

[10] S. Basharat, S. A. Hassan, H. Pervaiz, A. Mahmood, Z. Ding, and M. Gidlund, "Reconfigurable intelligent surfaces: Potentials, applications, and challenges for 6G wireless networks," *IEEE Wireless Commun.*, vol. 28, no. 6, pp. 184–191, Dec. 2021.

[11] A. D. Wyner, "The wire-tap channel," *Bell sys. tech. j.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[12] S. Fang, G. Chen, Z. Abdullah, and Y. Li, "Intelligent omni surface-assisted secure MIMO communication networks with artificial noise," *IEEE Commun. Lett.*, 2022.

[13] X. Guan, Q. Wu, and R. Zhang, "Intelligent reflecting surface assisted secrecy communication: Is artificial noise helpful or not?" *IEEE Wireless Commun. Lett.*, vol. 9, no. 6, pp. 778–782, Jun. 2020.

[14] Z. Zhang, C. Zhang, C. Jiang, F. Jia, J. Ge, and F. Gong, "Improving physical layer security for reconfigurable intelligent surface aided NOMA 6G networks," *IEEE Trans. Veh. Technol.*, vol. 70, no. 5, pp. 4451–4463, May 2021.

[15] *Cisco Annual Internet Report (2018–2023) White Paper*. Available [Online]: http://goo.gl/ylTuVx, Mar. 2020.

[16] M. H. Khoshafa, J. M. Moualeu, T. M. Ngatched, and M. H. Ahmed, "On the performance of secure underlay cognitive radio networks with energy harvesting and dual-antenna selection," *IEEE Commun. Lett.*, vol. 25, no. 6, pp. 1815–1819, Jun. 2021.

[17] C. Pan, H. Ren, K. Wang, J. F. Kolb, M. Elkashlan, M. Chen, M. Di Renzo, Y. Hao, J. Wang, A. L. Swindlehurst *et al.*, "Reconfigurable intelligent surfaces for 6G systems: Principles, applications, and research directions," *IEEE Commun. Mag.*, vol. 59, no. 6, pp. 14–20, Jun. 2021.

[18] L. Zhang, Y. Wang, W. Tao, Z. Jia, T. Song, and C. Pan, "Intelligent reflecting surface aided MIMO cognitive radio systems," *IEEE Trans. Veh. Technol.*, vol. 69, no. 10, pp. 11 445–11 457, Oct. 2020.

[19] J. Yuan, Y.-C. Liang, J. Joung, G. Feng, and E. G. Larsson, "Intelligent reflecting surface-assisted cognitive radio system," *IEEE Trans. Commun.*, vol. 69, no. 1, pp. 675–687, Jan. 2021.

[20] E. Shi, J. Zhang, S. Chen, J. Zheng, Y. Zhang, D. W. K. Ng, and B. Ai, "Wireless energy transfer in RIS-aided cell-free massive MIMO systems: Opportunities and challenges," *IEEE Commun. Mag.*, vol. 60, no. 3, pp. 26–32, Mar. 2022.

[21] H. Wang, et al., "Intelligent reflecting surfaces assisted secure transmission without eavesdropper's CSI," *IEEE Signal Process. Lett.*, vol. 27, pp. 1300–1304, Jul. 2020.

[22] P. Xu, et al., "Ergodic secrecy rate of RIS-assisted communication systems in the presence of discrete phase shifts and multiple eavesdroppers," *IEEE Wireless Commun. Lett.*, vol. 10, no. 3, pp. 629–633, Mar. 2021.

[23] J. Lee, H. Wang, J. G. Andrews, and D. Hong, "Outage probability of cognitive relay networks with interference constraints," *IEEE Trans. Wireless Commun.*, vol. 10, no. 2, pp. 390–395, Feb. 2011.

[24] H. Lei, H. Zhang, I. S. Ansari, Z. Ren, G. Pan, K. A. Qaraqe, and M.-S. Alouini, "On secrecy outage of relay selection in underlay cognitive radio networks over Nakagami-m fading channels," *IEEE Trans. Cognitive Commun. Netw.*, vol. 3, no. 4, pp. 614–627, Dec. 2017.

[25] E. Björnson, Ö. Özdogan, and E. G. Larsson, "Intelligent reflecting surface versus decode-and-forward: How large surfaces are needed to beat relaying?" *IEEE Wireless Commun. Lett.*, vol. 9, no. 2, pp. 244–248, Feb. 2020.

[26] M.-A. Badiu and J. P. Coon, "Communication through a large reflecting surface with phase errors," *IEEE Wireless Commun. Lett.*, vol. 9, no. 2, pp. 184–188, Feb. 2020.

[27] M. H. Khoshafa, T. M. Ngatched, M. H. Ahmed, and A. Ibrahim, "Improving physical layer security of cellular networks using full-duplex jamming relay-aided D2D communications," *IEEE Access*, vol. 8, pp. 53 575–53 586, Mar. 2020.

[28] I. S. Gradshteyn and I. M. Ryzhik, *Table of integrals, series, and products*. Academic press, 2014.

[29] M. H. Khoshafa, T. M. Ngatched, and M. H. Ahmed, "On the physical layer security of underlay relay-aided device-to-device communications," *IEEE Trans. Veh. Technol.*, vol. 69, no. 7, pp. 7609–7621, Jul. 2020.

[30] L. Yang, J. Yang, W. Xie, M. O. Hasna, T. Tsiftsis, and M. Di Renzo, "Secrecy performance analysis of RIS-aided wireless communication systems," *IEEE Trans. Veh. Technol.*, Jul. 2020.

[31] A. Papoulis and S. U. Pillai, *Probability, random variables, and stochastic processes*. Tata McGraw-Hill Education, 2002.

[32] D. Sadhwani, R. N. Yadav, and S. Aggarwal, "Tighter bounds on the gaussian q function and its application in Nakagami-m fading channel," *IEEE Wireless Commun. Lett.*, vol. 6, no. 5, pp. 574–577, Oct. 2017.

[33] M. H. Khoshafa, T. M. N. Ngatched, M. H. Ahmed, and A. Ibrahim, "Secure transmission in wiretap channels using full-duplex relay-aided D2D communications with outdated CSI," *IEEE Wireless Commun. Lett.*, vol. 9, no. 8, pp. 1216–1220, Aug. 2020.