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

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

Abstract—Reconfigurable intelligent surface (RIS) technology is considered one of the leading technologies for sixth-generation wireless communication, and it has also been revealed to be effective in enhancing secure and reliable communications. This article investigates using RIS to improve physical layer security and data transmission in underlay cognitive radio networks (CRNs). Because of its capability to control the wireless environment, RIS can enhance the security of the primary network (PN) and increase the reliability of the secondary network (SN) data transmission. This approach is practical and beneficial for both the PN and SN in terms of reliability and security. The study focuses on a scenario where the eavesdropper is passive and uses either selection or maximal ratio combining to combine the signals from the PN. Analytical expressions for the secrecy outage probability and the probability of nonzero secrecy capacity of the PN are derived. Additionally, an expression for the SN outage probability is also provided. The results from simulations and the numerical analysis confirm the benefits of the proposed system model and validate the accuracy of the derived expressions. This work provides valuable insights into the integration of RIS with CRNs and highlights the potential role of RIS in the future of wireless communication systems.

Index Terms—Cognitive radio network (CRN), physical layer security (PLS), reconfigurable intelligent surface (RIS), secrecy outage probability (SOP).

I. INTRODUCTION

The reconfigurable intelligent surface (RIS) is attracting much consideration as a leading technology to achieve an intelligent wireless channels environment for the next-generation networks [2]. The RIS is a planar surface 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, enhance the quality of the received signals at the destination, reduce the power consumption compared with other technologies, increase the physical layer security (PLS), and alleviate the undesired interference [3], [4], [5], [6]. Passive RIS prototypes were assembled in [7], [8], and [9] to acquire more practical and precise results regarding the actual performance of RIS-aided systems by taking experimental measurements. Furthermore, Qian et al. in [10] utilized the RIS as a relay-assisted satellite to facilitate information transmission. This approach enables the user to concurrently receive information directly from the satellite and information relayed by the satellite through the RIS.

With the envision of new technologies and utilizing higher frequency bands, secure communications are significant in sixth-generation (6G) wireless networks, where new security challenges arise [11]. Present research contributions have established RIS as a cutting-edge technology with promising research directions toward the 6G. To take things further, the integration of RIS and cutting-edge communication technologies yields higher performance increases [12]. Wyner [13] initially investigated PLS, which has now become an attractive technique for improving the security level of cellular networks against signal leakage. In this respect, PLS utilizes the inherent characteristics of wireless communication channels and interference to secure the transmission of data by reducing the amount of information that unauthorized users can access at the bit level [14]. The RIS can be employed to enhance PLS in wireless communication systems [15]. One way this can be achieved is by using the RIS to create virtual beamforming, which can be used to create multiple beams that can be directed to different users. This can increase the secrecy performance of the cellular networks by reducing the signal strength at the unintended receivers, making it more challenging for an eavesdropper to intercept the signal. Additionally, the RIS can be used to create a secure zone for communication by directing the signal toward the intended receiver and away from the eavesdropper. Another way to use RISs for PLS is by creating artificial noise with the RIS to mask the signals [16]. This can be done by creating a beam that interferes with the signal and makes it more challenging to decode. Moreover, the RIS can be used to create a jamming signal that can be used to disrupt the communication of an eavesdropper [5], [17]. The RIS can also be used to detect and identify the location of the eavesdropper. By measuring the channel state information (CSI), the RIS can determine if there is an unintended receiver in the vicinity and can then adjust the beamforming to reduce the signal strength at that location.
Thanks to their distinctive characteristics, which enable them to manipulate the transmission environment, RIS technology has the ability to improve the received signal without using active elements and eliminate interference effects. Therefore, the RIS technology has recently been employed to improve the security of wireless communication systems [18], [19]. To guarantee secure transmission, the RIS was positioned close to the eavesdropper to counteract the eavesdropping signal [16]. This approach can effectively decrease the amount of information that is disclosed and enhance the confidentiality of the wireless network.

The rapid growth of smart devices has led to a significant increase in mobile wireless communication data traffic, putting a strain on the available radio spectrum resources such as energy and bandwidth. As a result, energy and spectral efficiency have become critical design considerations for the next wireless networks. To address the above challenges, the concept of a cognitive radio network (CRN) has been introduced as an efficient solution for improving the utilization of the spectrum. In CRN, which is composed of the primary network (PN) and the secondary network (SN), the secondary users (SUs) are permitted to transmit simultaneously with primary users (PUs) but at a power level below a certain threshold so as not to interfere with PUs’ communications. Therefore, CRN adjusts the transmission power of the SUs accordingly, ensuring that the interference generated by SUs to the PUs stays less than a predetermined level. In CRN, where multiple users share the same spectrum, PLS is critical because it can protect the communication link from unauthorized access and interference. Moreover, CRN has unique security challenges, such as the dynamic and uncertain nature of the wireless environment and the need to protect both PUs and SUs. Consequently, PLS is crucial for maintaining the integrity and confidentiality of the communication link and ensuring that the CRN can operate effectively and efficiently in a shared spectrum environment [20]. The study in [21] examined the secrecy performance of energy harvesting in CRN through the use of cooperative jamming.

The RIS-aided CRN has the potential to significantly improve the performance of both the PN and the SN. The ability of RIS to control the propagation of radio waves in a wireless environment can be leveraged to enhance the transmission of the SN by improving the signal-to-noise ratio (SNR) and increasing the capacity of the network [22]. Additionally, the RIS can be employed to improve the PLS of the PN by creating a more secure wireless environment. The benefit of RIS to control the propagation of radio waves can be used to create more secure wireless communications by reducing the PNs transmitted power and increasing the secrecy of the PNs communication. Moreover, by modifying the amplitude and phase of the incoming signal on the RIS, the network’s power consumption can be decreased, thereby enhancing the energy efficiency of the network [23]. A common technique is to employ beamforming to improve the performance of the SN while guaranteeing that the interference power received by the PUs stays below a specified limit [24]. Nevertheless, the beamforming gain is restricted when the link between the SN source and SN destination is weak as a result of severe attenuation.

The works mentioned above reflect the fact that passive RIS technology plays an essential role in the evolution of wireless communication systems. Using RIS in CRN is to improve the PLS of the network. A highly directional and manipulable wireless transmission environment can be established by leveraging the abundant reflecting elements in the RIS. This can be used to selectively enhance or null the signal strength of legitimate or malicious signals, respectively, to improve the network’s overall security. In addition, using RIS allows for creating multiple virtual channels, which can be used to separate legitimate and malicious signals and provide additional protection against eavesdropping and jamming attacks. These insights motivate us to explore a new RIS architecture that can boost the secrecy capacity of the PN and strengthen the SN transmission simultaneously. Our proposed novel RIS-assisted CRN architecture (as depicted in Fig. 1) can accomplish this objective by reflecting the incoming SN EM waves toward the SU and simultaneously redirecting the interference toward the eavesdropper through the RIS. In this work, we present a secure RIS-assisted underlay CRN. To the best of our knowledge, no previous studies have examined the benefits of RIS technology for securing PN and enhancing SN transmission simultaneously. The main contributions of this article can be summarized as follows.

1) The RIS technology is presented to improve both the reliability of the SN and the PLS of the PN concurrently.
2) 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 mutually beneficial situation for both networks, i.e., security provisioning for the PN and high reliability and robustness for the SN.
3) The secrecy performance of the PN is examined and closed-form expressions for the secrecy outage probability (SOP) and the probability of nonzero secrecy capacity (PNSC), considering practical combining techniques, namely, selection combining (SC) and maximum ratio combining (MRC) at the eavesdropper side are presented. Furthermore, the outage probability of the SN is explored and an analytical expression is provided.
4) The impact of the location of the secondary receiver on the SNs performance is investigated, providing insights into...
optimal positioning strategies and offering valuable guidelines for deploying and optimizing RIS-aided systems in underlay CRNs.

5) Asymptotic analysis in the high transmit power regime in the PN is carried out and concise expressions for the SOP of the PN are presented. These expressions demonstrate that SC and MRC techniques achieve identical secrecy diversity orders. The benefits of the proposed system model are demonstrated and validated through numerical and simulation results.

A list of symbols utilized in this paper is presented in Table I.

### II. SYSTEM MODEL

A proposed RIS-aided underlay CRN, 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, whereas the PN comprises a primary transmitter (PT) and a single-antenna primary receiver (PR). The PT is equipped with \( N_{PR} \geq 1 \) antennas. In addition, an eavesdropper (Eav), equipped with \( N_{E} \geq 1 \) antennas, intends to overhear the PNs data streams. Therefore, the 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 noteworthy that a field-programmable gate array (FPGA) is utilized as a controller to adjust the phase and amplitude of the RIS in practice. It often coordinates and communicates with other elements of the network, such as the BS and users, through dedicated connections [25]. Recently, advanced techniques for channel estimation in RIS-assisted systems have been proposed, e.g., [26], [27]. Consequently, we assume that the CSI of all channels is perfectly known at the RIS for reflecting/transmitting data. As we consider a passive Eav, its CSI is unknown at both the PT and the RIS.

The channel coefficients for the PT → PR, PT → Eav, RIS → Eav, RIS → PR, S → Eav, S → PR, S → D, S → RIS, and RIS → D links are denoted as \( h_{pp}, h_{pe}, h_{e}^{2}, h_{p}, h_{se}, h_{sp}, h_{sd}, h_{s}, \) and \( h_{D} \), respectively. The above channel coefficients are assumed to undergo Rayleigh fading. To elaborate, \( h_{k} \in \mathbb{C}^{N \times 1} \), \( h_{D} \in \mathbb{C}^{1 \times N} \), \( h_{e}^{2} \in \mathbb{C}^{1 \times N} \), and \( h_{D} \in \mathbb{C}^{1 \times N} \) 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 \( S \rightarrow RIS \), RIS → D, S → D, PT → PR, PT → Eav, RIS → Eav, RIS → PR, S → Eav, and S → 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, \( n_{o} \) is the additive white Gaussian noise (AWGN) at D, PR, and E, respectively, where \( o \in \{d, p, e\} \), with zero mean and variance \( \sigma_{o}^{2} \). Consequently, the received signal at D can be written as

\[
y_{D} = \sqrt{P_{S}} x_{s} \left[ \left( \frac{d_{sr} d_{rd}}{d_{o}} \right)^{2} \sum_{i=1}^{N} h_{s_{i}} h_{d_{i}} e^{j\phi_{i}} + h_{sd} \left( \frac{d_{sd}}{d_{o}} \right)^{2} \right] + n_{d}
\]

where \( x_{s} \) is the SN transmitted signal, \( P_{S} \) denotes the SN transmitted power, \( d_{o} \) is a reference distance, and \( n_{o} \) is the path loss exponent. In addition, \( h_{s} \) and \( h_{d} \) are complex Gaussian random variables (RV) with a zero mean and unit variance, and \( \phi_{i} \) is the alterable phase coefficient of the \( i \)-th element of the RIS. It is assumed that the PT position is distant from both the D and the RIS, thus causing no significant interference. This is a widely accepted assumption in literature [22], [28], [31], [32], [33]. Additionally, it is also assumed that the phases of the channels \( h_{s} \) and \( h_{d} \) are perfectly available at the RIS.

1The traditional pilot signaling techniques can be utilized to estimate the CSI of the legitimate transmission links. Moreover, due to the advanced channel estimation techniques, the CSI can be easily estimated, which explains why the assumption of perfect knowledge of the CSI is commonly used in the literature [2], [19], [28], [29], [30]. The findings obtained in this work are considered an upper bound on the performance increase that the RIS can achieve because it is an ideal situation.

2The bold font is used to indicate vectors.

3Since the transmission links experience blockages and the RISs location cannot be optimized to guarantee reliable line-of-sight links, similar to [19], [29], and [30], Rayleigh fading environment is assumed in this work.

| Symbol | Description |
|--------|-------------|
| S      | Secondary transmitter |
| D      | Secondary receiver |
| PT     | Primary transmitter |
| PR     | Primary receiver |
| Eav    | Eavesdropper |
| \( N_{PR} \) | 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 |
| \( \sigma_{a}^{2} \) | AWGN variance at node a |
| \( y_{a} \) | Received signal at node a |
| \( s_{x} \) | SN transmitted signal |
| \( x_{p} \) | PN transmitted signal |
| \( P_{S} \) | SN transmitted power |
| \( P_{D} \) | PN transmitted power |
| \( d_{o} \) | Reference distance |
| \( \phi_{i} \) | Phase coefficient of the \( i \)-th element of the RIS |
| \( \delta_{i} \) | Residual phase errors affecting the PR |
| \( \psi_{i} \) | Residual phase errors affecting the Eav |
| \( \gamma_{a} \) | SINR at node a |
| \( \eta_{a} \) | Average SNR at node a |
| \( \eta \) | Path loss exponent |
| \( f_{X}(\cdot) \) | PDF of random variable \( X \) |
| \( F_{X}(\cdot) \) | CDF of random variable \( X \) |
| \( F_{X}^{*}(\cdot) \) | Asymptotic CDF of random variable \( X \) |
| \( C \) | PN secrecy capacity |
| \( C_{p} \) | PN capacity |
| \( C_{B} \) | Eav capacity |
| \( R_{S} \) | SN achievable data rate |
| \( R_{e} \) | PN target secrecy rate |
| \( Pr(\cdot) \) | Probability of an event |
| SOP    | Secrecy outage probability |
| \( P_{out} \) | SN outage probability |
| SOP*   | Asymptotic SOP |
| \( g_{a} \) | Secrecy diversity order |
| \( g_{d} \) | Secrecy array gain |
| \( \mathcal{O}(\cdot) \) | Higher order term |
allowing the optimal phase shift to be selected for maximizing the instantaneous SNR at D [2], [34]. It is also assumed that the reflected gain of each reflecting element is equal to one [2], [19]. As a result, the received signal at the PR can be written as

\[ y_p = \sqrt{P_p} \left( \frac{d_{pp}}{d_o} \right)^{-\frac{\eta}{2}} h_{pp} x_p + \sqrt{P_s} \sum_{i=1}^{N} h_i s_i e^{j\psi_i} + h_{sp} \left( \frac{d_{sp}}{d_o} \right)^{-\frac{\eta}{2}} x_s + n_p \]  

(2)

where \( x_p \) is the PN-transmitted signal, \( P_p \) denotes the PN-transmitted power, and \( \theta_i \) is the residual phase errors affecting the PR. In a similar way, the wiretapped signal at Eav can be written as

\[ y_{Eav} = \sqrt{P_p} \left( \frac{d_{pe}}{d_o} \right)^{-\frac{\eta}{2}} h_{pe} x_p + \sqrt{P_s} \sum_{i=1}^{N} h_i s_i e^{j\psi_i} + h_{se} \left( \frac{d_{se}}{d_o} \right)^{-\frac{\eta}{2}} x_s + n_c \]  

(3)

where \( \psi_i \) is the residual phase errors affecting the Eav. The instantaneous SNR at D, \( \Xi_D \), is given by

\[ \Xi_D = \frac{P_S}{\sigma_{d}^2} \left( \frac{d_{sd}}{d_o} \right)^{-\frac{\eta}{2}} \sum_{i=1}^{N} h_i s_i h_d e^{j\psi_i} + h_{sd} \left( \frac{d_{sd}}{d_o} \right)^{-\frac{\eta}{2}} \right]^2 . \]  

(4)

Moreover, the instantaneous signal-to-interference-and-noise ratio (SINR) at PR and Eav, denoted as \( \Xi_P \) and \( \Xi_{Eav} \), respectively, are given by

\[ \Xi_P = \left( \frac{P_P}{\phi_P} \right)^{-\frac{\eta}{2}} |h_{pp}|^2 \]  

\[ \Xi_{Eav} = \left( \frac{P_P}{\phi_P} \right)^{-\frac{\eta}{2}} |h_{pe}|^2 \]  

(5)

and

\[ \Xi_{Eav} = \left( \frac{P_P}{\phi_P} \right)^{-\frac{\eta}{2}} |h_{pe}|^2 \]  

\[ \Xi_{Eav} = \left( \frac{P_P}{\phi_P} \right)^{-\frac{\eta}{2}} |h_{pe}|^2 \]  

(6)

which can be rewritten as

\[ \Xi_{E} = \frac{\Psi_{PE}}{\phi_P + 1} \]  

(7)

where

\[ \Psi_E = \left| L_1 \sum_{i=1}^{N} h_i s_i e^{j\psi_i} + \Lambda_2 h_{se} \right|^2 \]  

\[ L_1 = \sqrt{\eta \sigma_{se} \left( \frac{d_{sd}}{d_o} \right)^{-\frac{\eta}{2}}}, \quad \Lambda_2 = \sqrt{\eta \sigma_{se} \left( \frac{d_{se}}{d_o} \right)^{-\frac{\eta}{2}}}, \quad \gamma_{se} = \frac{\phi_P}{\phi_P}, \quad \Psi_{PE} = \omega_{e} |h_{pe}|^2, \quad \omega_c = \gamma_{ce} \left( \frac{d_{se}}{d_o} \right)^{-\frac{\eta}{2}}, \quad \gamma_{ce} = \frac{\phi_P}{\phi_P} \]  

As the phase shifts of the RIS elements are designed based on the legitimate SN link, the resulting phase distributions for each RIS \( \rightarrow E \) link \( \psi_i \) are i.i.d. and uniformly distributed RVs by virtue of the work in [29]. Thus, \( \Psi_E \) can be approximated by an exponential RV according to [35, Corollary 2] with a parameter \( \Lambda_{PE} = N \Lambda_1^2 + \Lambda_2^2 \). Therefore, the probability density function (pdf) of \( \Psi_E \) is given by

\[ f_{\Psi_E}(\gamma) = \frac{1}{\Lambda_{PE}} e^{-\frac{\gamma}{\Lambda_{PE}}} \]  

(8)

It should be noted that the power transmitted by the SN \( P_S \) should be below a certain limit to prevent excessive interference. In underlay CRN, the PN and the SN can coexist, considering that \( S \) does not generate excessive interference to the PR. The worst case scenario for the PR perspective is expressed by \( P_S = \frac{P_S}{\phi_P} \). However, even under this scenario, the PR will still operate reliably. When \( P_{\text{max}} < \frac{P_S}{\phi_P}, \) \( P_S \) would be equal to the maximum power limit \( P_{\text{max}} \) but this will not impact the reliability of the PR. Therefore, our expression performs as an upper bound. However, it is common for \( P_{\text{max}} \) to be greater than \( \frac{P_S}{\phi_P} \) in practical scenarios [22], [28]. Consequently, the power of the interfering signal toward the PR must be limited by \( P_S, \Psi_P \leq Q, \) with \( \Psi_P \) being the sum of the channel power gains from \( S \) and the RIS, and \( Q \) expresses the maximum tolerable interference imposed on the PR. Precisely, \( \Psi_P \) consists of the reflected link RIS \( \rightarrow \) PR and the \( S \rightarrow \) PR link. From (5), \( \Psi_P \) can be expressed as

\[ \Psi_P = \left( \frac{d_{sd}}{d_o} \right)^{-\frac{\eta}{2}} \sum_{i=1}^{N} h_i s_i h_d e^{j\psi_i} + h_{sd} \left( \frac{d_{sd}}{d_o} \right)^{-\frac{\eta}{2}} |h_{sp}|^2 . \]  

(9)

Similar to \( \Psi_E, \Psi_P \) also can be approximated as an exponential RV with a parameter \( \lambda_P = \left( \frac{d_{sd}}{d_o} \right)^{-\frac{\eta}{2}} N + \left( \frac{d_{se}}{d_o} \right)^{-\frac{\eta}{2}} \), where the pdf of \( \Psi_P \) is given by

\[ f_{\Psi_P}(\gamma) = \frac{1}{\lambda_P} e^{-\frac{\gamma}{\lambda_P}} . \]  

(10)

### III. PERFORMANCE ANALYSIS

#### A. PN Secrecy Outage Probability

In this section, we focus on investigating the secrecy capacity \( C \) of the PN by analyzing the SOP. SOP is the probability that the achievable secrecy rate for PN transmission falls below a certain predefined target secrecy rate \( R_s \). Mathematically, it is represented as

\[ \text{SOP} = \Pr(C < R_s) \]  

(11)

where \( C \) is the PN secrecy capacity and \( R_s \) is the PN target secrecy rate. In this regard, \( C_S \) can be obtained by

\[ C = |C_P - C_E| \]  

(12)

where \( C_P \) and \( C_E \) are the PN and the Eav capacities, respectively, and \( [x]^+ = \max(x, 0) \). Accordingly, \( C_P \) is given by

\[ C_P = \log_2 (1 + \Xi_P) \]  

(13)

where \( \Xi_P \) is given by

\[ \Xi_P = \frac{P_P}{P_S \Psi_P + \sigma_P^2} = \frac{P_P}{P_S \Psi_P + \sigma_P^2} = \frac{P_P}{P_S \Psi_P + \sigma_P^2} \]  

(14)
where $Q = P_{b} \Psi_{p}, \Phi = \omega_{p}, \vartheta, \omega_{p} = \frac{d_{p}}{\sigma_{p}} \vartheta^{\gamma},$ and $\vartheta = (\frac{D}{\sigma_{p}^{2}} + 1)^{-1}$. Employing the antenna selection technique at the PT is to maintain the advantages of multiple antenna diversity while minimizing the hardware complexity. The principal benefit of using this technique is that it reduces power consumption and signal processing overhead compared to other techniques, such as beamforming. 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:

$$|h_{pp}|^2 = \max_{n \in \{1, \ldots, N_{p}\}} |h_{p,n}|^2.$$  \hspace{1cm} (15)

The cumulative distribution function (cdf) of $\Xi_{p}$ is given by

$$F_{\Xi_{p}}(\gamma) = N_{p} \sum_{n=0}^{N_{p}-1} (-1)^{n} \frac{(N_{p}-1)}{(n+1)} \left(1 - e^{-\frac{(n+1)}{(\alpha+1)}}\right).$$ \hspace{1cm} (16)

Moreover, $C_{E}$ is given by $C_{E} = \log_{2}(1 + \Xi_{E})$, where $\Xi_{E}$ is given in (6). Now, the SOP can be derived as

$$\text{SOP}_{\xi} = \int_{0}^{\infty} F_{\Xi_{p}}(\beta \gamma + \alpha) f_{\Xi_{p}}(\gamma) d\gamma$$ \hspace{1cm} (17)

where $\alpha = \beta - 1$, $\beta = 2^{2\zeta}$, and $\zeta \in \{\text{SC}, MRC\}$.

1) SC Approach: SC is a widely employed diversity-combining technique in wireless communication systems. It encompasses selecting the optimal signal among a set of received replicas, often originating from different antennas. This selection is based on predetermined criteria, such as the magnitude or quality of signal strength [36]. Using the SC approach at the Eav side is essential because it allows for the advantages of multiple antenna technology, such as diversity and increased throughput, to be maintained while avoiding high hardware complexity. The SC approach is significant because it has low power consumption and minimal signal processing overhead compared to other techniques. The SC technique has essential advantages, such as diversity and spectral efficiency gains, reduced hardware complexity and signaling overheads, flexibility, and minimal feedback.

**Theorem 1:** The SOP for SC, $\text{SOP}_{\text{SC}}$, can be derived as

$$\text{SOP}_{\text{SC}} = N_{p} \sum_{n=0}^{N_{p}-1} (-1)^{n} \frac{(N_{p}-1)}{(n+1)} \left[ 1 - \frac{N_{E}}{\omega_{p} \Lambda_{E}} \sum_{k=0}^{N_{E}-1} (-1)^{k} \frac{(N_{E}-1)}{(n+1)} \right] \left( \frac{\Lambda_{E}}{\omega_{p}} + \Theta \right)$$ \hspace{1cm} (18)

where $\Theta = \frac{\Lambda_{E}}{\omega_{p}} + \Theta, \Theta = \frac{\Lambda_{E}}{\omega_{p}}$, and $\Gamma(\cdot, \cdot)$ denotes the upper incomplete gamma function [37, eq. (8.350.2)].

**Proof:** See Appendix A. \hfill \blacksquare

2) MRC Approach: MRC is an alternative diversity-combining technique that combines multiple received signals through scaling based on their respective SNR ratios, followed by their summation [36]. The MRC is a coherent technique that linearly combines the signals received from multiple antennas at the receiver. However, digital signal processing makes it practical. This work considers the MRC at Eav because it is the worst case scenario from the PN perspective. When Eav deploys the MRC on the eavesdropping signals from the PT, the PLS of the PN decreases dramatically, as shown in the obtained results.

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. Furthermore, the MRC technique is commonly used in the literature.

**Theorem 2:** The SOP for MRC, $\text{SOP}_{\text{MRC}}$, can be derived as

$$\text{SOP}_{\text{MRC}} = \frac{N_{p} \sum_{n=0}^{N_{p}-1} (-1)^{n} \frac{(N_{p}-1)}{(n+1)} \left[ 1 - \frac{N_{E}}{\omega_{p} \Lambda_{E}} \sum_{k=0}^{N_{E}-1} (-1)^{k} \frac{(N_{E}-1)}{(n+1)} \right] \left( \frac{\Lambda_{E}}{\omega_{p}} + \Theta \right) \left( \frac{\Lambda_{E}}{\omega_{p}} + \Theta \right)}{e^{\frac{\omega_{p} \Lambda_{E}}{\omega_{p}} \Theta}}$$ \hspace{1cm} (19)

where $\Theta = \frac{\Lambda_{E}}{\omega_{p}} * (n+1)$, and $W_{\alpha, \beta}(\cdot)$ denotes the Whittaker function [37, eq. (9.220.4)].

**Proof:** See Appendix B. \hfill \blacksquare

**B. Asymptotic PN SOP Analysis**

The asymptotic SOP is analyzed at high SNR, when the value of $\omega_{p} \rightarrow \infty$, to understand better the impact of key parameters that influence the performance of the proposed system in terms of the SOP. The focus is on the secrecy array gain ($G_{s}$) and the secrecy diversity order ($G_{d}$). In this scenario, it is assumed that the PT and PR are located close to each other and that $\omega_{p} \gg \omega_{r}$.

As $\omega_{p} \rightarrow \infty$, the asymptotic expression of $\text{SOP}^{\infty}$ can be expressed as

$$\text{SOP}^{\infty} = (G_{d} \omega_{p})^{-G_{d}} + O(\omega_{p}^{-G_{d}}).$$ \hspace{1cm} (20)

The expression implies that the higher-order terms are represented by $O(\cdot)$. The shape of the SOP$^{\infty}$ curve is defined by $G_{d}$ and the difference in SNR between the SOP$^{\infty}$ curve and the reference curve ($\omega_{p}^{-G_{d}}$) is quantified by $G_{d}$. To obtain $F_{\Xi_{p}}(\cdot)$, the exponential functions in (16) are expanded using the Taylor series method presented in [37, eq. (1.211.1)]. Only the first two terms of the expansion are retained, and the remainder of the higher-order terms are disregarded. After some simple algebraic manipulations, $F_{\Xi_{p}}(\cdot)$ can be derived.

1) SC Approach: For the SC technique, the pdf of $\Xi_{E}$, $f_{\Xi_{p}}^{\text{SC}}(\gamma)$, is given in (39). By plugging $F_{\Xi_{p}}(\cdot)$ and (39) into (17), and after simple algebraic manipulations, then with the help of [37, eq. (3.382.4)], the SOP$^{\infty}_{\text{SC}}$, can be derived as

$$\text{SOP}^{\infty}_{\text{SC}} = (G_{d}^{\text{SC}} \omega_{p})^{-G_{d}^{\text{SC}}} + O(\omega_{p}^{-G_{d}^{\text{SC}}}).$$ \hspace{1cm} (21)
where $G_{d}^{SC} = N_p$ and $G_{a}^{SC}$ is derived as

$$G_{a}^{SC} = \left[1 + \frac{N_{E}}{\eta} \sum_{k=0}^{N_{E}} \frac{N_{P} \left(N_{P} - 1\right)}{k} \frac{Z_{1}}{\left(k + 1\right)} \left(W_{\frac{1}{\sqrt{N_{E}}}} + W_{\frac{1}{\sqrt{N_{E}}} + \frac{1}{\sqrt{N_{E}}}} \left(1 + \frac{1}{\sqrt{N_{E}}}\right)\right) \right]$$

where $Z_{1} = \frac{N_{E}^{2} \omega_{p} e^{-\frac{\eta}{N_{E}}} \Gamma(N+1)}{N_{P} \omega_{p} e^{-\frac{\eta}{N_{E}}} \Gamma(N+1)}$.

2) MRC Approach: For the MRC technique, the pdf of $\Xi_{E}$, $f_{\Xi_{E}}^{MRC}(\gamma)$, is given in (42). By plugging $F_{\Xi_{E}}(\cdot)$ and (42) into (17), and after simple algebraic manipulations, then with the help of [37, eq. (383.4)], the SOP$_{MRC}$ can be derived as

$$\text{SOP}_{MRC} = \left(\frac{G_{a}^{MRC}}{N_{P}} + O\left(\frac{1}{\sqrt{N_{P}}}\right)\right)$$

where $G_{a}^{MRC} = N_p$ and $G_{a}^{MRC}$ is derived as

$$G_{a}^{MRC} = \left[1 + \frac{N_{E}}{\eta} \sum_{k=0}^{N_{E}} \frac{N_{P} \left(N_{P} - 1\right)}{k} \frac{Z_{2}}{\left(k + 1\right)} \left(W_{\frac{1}{\sqrt{N_{E}}}} + W_{\frac{1}{\sqrt{N_{E}}} + \frac{1}{\sqrt{N_{E}}}} \left(1 + \frac{1}{\sqrt{N_{E}}}\right)\right) \right]$$

where $Z_{2} = \frac{N_{E}^{2} \omega_{p} e^{-\frac{\eta}{N_{E}}} \Gamma(N+1)}{N_{P} \omega_{p} e^{-\frac{\eta}{N_{E}}} \Gamma(N+1)}$.

C. Probability of Nonzero Secrecy Capacity

PNSC for the PN is investigated in this section. It should be noted that nonzero secrecy capacity can only be achieved when $C > 0$. According to (11), the PNSC can be expressed as follows:

$$\text{PNSC}_{C} = \text{Pr}(C > 0) = \text{Pr} \left(1 + \frac{\Xi_{P}}{1 + \Xi_{E}} > 1\right) = 1 - \int_{0}^{\infty} F_{\Xi_{E}}(\gamma) f_{\Xi_{E}}(\gamma) d\gamma.$$ (25)

1) SC Approach: By plugging (16) and (39) into (25), and after simple algebraic manipulations, then with the help of [37, eq. (383.9)], the PNSC for SC, PNSC$_{SC}$, can be derived as

$$P_{\text{NSC}}^{SC} = 1 - \frac{N_{P} - 1}{N_{P} + 1} \left(1 - \frac{1}{\sqrt{N_{E}}} \sum_{k=0}^{N_{E}} \frac{N_{P} \left(N_{P} - 1\right)}{k} \frac{Z_{1}}{\left(k + 1\right)} \left(W_{\frac{1}{\sqrt{N_{E}}}} + W_{\frac{1}{\sqrt{N_{E}}} + \frac{1}{\sqrt{N_{E}}}} \left(1 + \frac{1}{\sqrt{N_{E}}}\right)\right) \right]$$

where $Z_{1} = \frac{N_{E}^{2} \omega_{p} e^{-\frac{\eta}{N_{E}}} \Gamma(N+1)}{N_{P} \omega_{p} e^{-\frac{\eta}{N_{E}}} \Gamma(N+1)}$.

2) MRC Approach: By plugging (16) and (42) into (25), and after simple algebraic manipulations, then with the help of [37, eq. (383.4)], the PNSC for MRC, PNSC$_{MRC}$, can be derived as

$$P_{\text{NSC}}^{MRC} = 1 - \frac{N_{P} - 1}{N_{P} + 1} \left(1 - \frac{1}{\sqrt{N_{E}}} \sum_{k=0}^{N_{E}} \frac{N_{P} \left(N_{P} - 1\right)}{k} \frac{Z_{2}}{\left(k + 1\right)} \left(W_{\frac{1}{\sqrt{N_{E}}}} + W_{\frac{1}{\sqrt{N_{E}}} + \frac{1}{\sqrt{N_{E}}}} \left(1 + \frac{1}{\sqrt{N_{E}}}\right)\right) \right]$$

where $Z_{2} = \frac{N_{E}^{2} \omega_{p} e^{-\frac{\eta}{N_{E}}} \Gamma(N+1)}{N_{P} \omega_{p} e^{-\frac{\eta}{N_{E}}} \Gamma(N+1)}$.

D. SN Outage Probability

For the SN, the outage probability, $P_{\text{out}}$ is given by

$$P_{\text{out}} = \text{Pr} (\Xi_{D} \leq 2^{R_{d} - 1}) = F_{\Xi_{D}}(2^{R_{d} - 1})$$ (28)

where $R_{d}$ is the SN achievable data rate, and $\Xi_{D}$ is the instantaneous SNR of the SN link. By substituting $P_{3}$ with $\frac{N_{P}}{N_{P} - 1}$ in (4), the expression for $\Xi_{D}$ can be rewritten as follows:

$$\Xi_{D} = \left[\frac{Q}{ \sqrt{\frac{P}{\sigma_{d}^{2}}} } \left(\frac{d_{e} d_{sd}}{d_{l}^{2}}\right)^{2} \left(\frac{d_{e} d_{sd}}{d_{l}^{2}}\right)^{2}\right] \left(\frac{h_{e} h_{d} e^{j\phi_{e}} + h_{sd} \left(\frac{d_{e} d_{sd}}{d_{l}^{2}}\right)^{2}}{\left(\frac{d_{e} d_{sd}}{d_{l}^{2}}\right)^{2}}\right)$$ (29)

which can be rewritten as $\Xi_{D} = \frac{\psi_{D}}{\sigma_{d}^{2}}$, where $\psi_{D} = \Omega_{1} + \sum_{i=1}^{N} |h_{e} | |h_{d} | + |h_{sd}|^{2}$, $\Omega_{1} = \frac{N_{P}}{\sigma_{d}^{2}} \left(\frac{d_{e} d_{sd}}{d_{l}^{2}}\right)^{2}$, and $\Omega_{2} = \frac{N_{P}}{\sigma_{d}^{2}} \left(\frac{d_{e} d_{sd}}{d_{l}^{2}}\right)^{2}$. $P_{\text{out}}$ can be further written mathematically as [38]

$$P_{\text{out}} = \int_{0}^{\psi_{D}} F_{\psi_{D}}(\cdot) f_{\psi_{D}}(\cdot) d\gamma.$$ (30)

Theorem 3: $P_{\text{out}}$ can be obtained as

$$P_{\text{out}} = I_{1} - I_{2} - I_{3}$$ (31)

where $I_{1}$, $I_{2}$, and $I_{3}$ are given in (32), (33), and (34), respectively, at the bottom of the next page, where the symbols are defined in Appendix C.

Proof: See Appendix C.

IV. RESULTS AND DISCUSSIONS

Numerical and simulation results that confirm the benefits of applying the RIS technology in the proposed system model are provided in this section. Unless otherwise stated, we set $R_{d} = 1$ b/s/Hz, $\gamma_{sc} = 5$ dB, $\sigma_{d}^{2} = \sigma_{e}^{2} = 0$ dBm, $\delta = 2$, $\eta = 3$, $d_{o} = 10$ m, and $R_{e} = 1$ b/s/Hz. From Fig. 2, the position of $S$ in meters is $(0, 10)$ m, where 0 is the coordinate of $S$ along the $x$-axis, and 10 is the coordinate of $S$ along the $y$-axis. Likewise, the coordinates of RIS, D, PR, PT, and Eav are $(10, 20)$ m, $(100, 0)$, $(50, 0)$, $(100, 10)$ m, and $(50, 5)$ m, respectively. The Matlab platform is utilized to perform the simulations. The results are obtained by averaging $10^{7}$ channel realizations via Monte Carlo simulations.

In Fig. 3, we investigate the PN secrecy enhancement due to the deployment of the RIS technology. In this respect, the SOP$_{SC}$ of the PN is evaluated for the SC technique at Eav...
versus $P_p$ for different values of $N$ and $Q$, where $\gamma_c = 30$ dB. As the value of $N$ increases, the security of the PN improves, demonstrating the impact of the RIS’s jamming signals on $\text{Eav}$. Consequently, the PLS of the PN is enhanced. Moreover, the SOP_{SC} improves as $P_p$ increases. As demonstrated through our analysis and simulations, integrating the RIS technology with CRN can enhance the PLS of the PN by functioning as a friendly jammer. The RIS can degrade the quality of the signal intercepted by the $\text{Eav}$, leading to a more secure transmission for the PN. To illustrate, SOP_{SC} can be decreased by approximately 0.05, using an RIS with $N = 1000$ compared with $N = 10$ at $P_p = 20$ dBW and $Q = 10$ dB. It is essential to highlight that a decrease in the level of $Q$ leads to a corresponding reduction in the SOP_{SC}, thereby enhancing the security of the transmission for the PN. This can be attributed to the fact that a lower level of $Q$ results in reduced interference generated by the SN, consequently improving the security capacity at the PR. As an example, $P_p$ can be decreased by approximately 8 dB when $Q = 0$ dB compared with $Q = 10$ dB to achieve an SOP_{SC} of $10^{-2}$ at $N = 1000$.

Fig. 2. Simulations setup.

Fig. 3. PNs SOP_{SC} versus $P_p$, for different values of $N$ and $Q$, where $N_P = N_E = 3$.

Fig. 4 illustrates the secrecy improvement of the PN as a result of deploying the RIS technology. The evaluation focuses on the SOP_{MRC} of the PN as a function of $P_p$ under the MRC technique, considering different values of $N$ and $Q$. The security of the PN improves as $N$ increases. This indicates that the jamming signals emitted by the RIS significantly impact the $\text{Eav}$, enhancing the PLS of the PN. For Figs. 3 and 4, the analysis and simulations demonstrate that integrating the RIS technology with the CRN can significantly enhance the PLS of the PN by effectively functioning as a friendly jammer. The presence of the RIS degrades the quality of the signal intercepted by the $\text{Eav}$, resulting in a more secure transmission for the PN. Moreover, the MRC technique yields a higher SNR gain at the $\text{Eav}$ than the

$$I_1 = \frac{Q_4}{2\lambda_p} + \frac{A_1}{2\pi Q_2^2} \left(2e^{-\frac{Q_2^2}{\pi}} - 1\right) + \sum_{m=1}^4 \frac{C_m}{2} \left[ e^{\frac{Q_2^2(A_2+1)}{Q_2}} \left(\sqrt{\frac{Q_2}{\pi}} \frac{\Theta_m Q_2 e^{-\frac{Q_2^2(A_2+1)^2}{Q_2^2}}}{A_2} \right) \right]$$

$$I_2 = \frac{q^2 e^{-D_4}}{2\beta Q_6^2} \left[ \frac{1}{D_2^{3/2}} \left(\sqrt{\frac{D_6}{2\sqrt{D_2}}} \left(\text{erf} \left(\frac{D_3}{2\sqrt{D_2}}\right) - \text{erf} \left(\frac{D_6}{2\sqrt{D_2}}\right)\right) - \sqrt{\frac{D_7}{2\sqrt{D_2}}} \text{erfc} \left(\frac{D_3}{2\sqrt{D_2}}\right) \right) \right] + \sum_{m=1}^4 \frac{C_m}{D_5^{3/2}} \left[ \frac{\sqrt{\frac{D_7}{2\sqrt{D_5}}} \left(\text{erf} \left(\frac{D_7}{2\sqrt{D_2}}\right) - \text{erf} \left(\frac{D_7}{2\sqrt{D_5}}\right)\right) \right]$$

$$I_3 = \frac{q^2 e^{-B_4}}{2\beta Q_8^2} \left[ \frac{Q_4 B_6}{B_2^2} \left(\sqrt{\frac{B_6}{2\sqrt{B_2}}} + 1\right) + 2\sqrt{B_2} \right] - \sum_{m=1}^4 \frac{C_m}{B_5^2} \left[ \frac{\sqrt{\frac{D_7}{2\sqrt{B_5}}} \left(\text{erf} \left(\frac{B_7}{2\sqrt{B_5}}\right) + 1\right) + 2\sqrt{B_5} \right]$$

(33)
SC technique. Therefore, employing the MRC technique at $E_{av}$ leads to a more degradation in the PNs secrecy performance, as depicted in Fig. 4. To illustrate, $SOP_{SC} = 0.02$ compared with $SOP_{MRC} = 0.075$, using an RIS with $N = 1000$ at $P_p = 20$ dBW and $Q = 0$ dB. The asymptotic analyses are included, and a perfect match with the theoretical results can be seen when $P_p \to \infty$, confirming the preciseness of the asymptotic expressions. Finally, it is evident that theoretical and simulation results have an excellent match, verifying the exactness of the derived expressions.

The SOP is examined in Figs. 5 and 6 as a function of $N_P$ and $N_E$, respectively, considering both SC and MRC techniques. The figures also present the asymptotic SOP results for SC and MRC. Fig. 5 reveals that the SOP increases for both SC and MRC as $N_P$ decreases. This behavior can be attributed to the increase in the PN capacity $C_p$, which occurs as $N_P$ increases. In Fig. 6, it can be observed that with an increase in $N_E$, the SOP increases for both the SC and MRC. Notably, the increase in SOP is due to the array gain, as $N_E$ does not affect the diversity order. The analysis of Figs. 5 and 6 shows that both SC and MRC have the same secrecy diversity orders $N_P$ and that the MRC has a higher SOP than SC. The results provide valuable insights into the impact of $N_P$ and $N_E$ on the SOP for the SC and MRC techniques.

Figs. 7 and 8 depict the PNSC as a function of $P_p$, considering both SC and MRC techniques, $PNSC_{SC}$ and $PNSC_{MRC}$, respectively. It can be observed that, for a fixed $\omega_e$, as $P_p$ increases, $PNSC_{SC}$ and $PNSC_{MRC}$ improve. Additionally, a decrease in $Q$ leads to an improvement in PNSC. Furthermore, it is noteworthy that PNSC increases with the increase in $N$. This implies that the larger the value of $N$, the more secure the transmission becomes. As expected, PNSC of the SC technique is lower compared to PNSC of the MRC technique. Both analytical and simulation results match, demonstrating the validity of our analysis.

The SN outage probability $P_{out}$ is presented in Fig. 9, where numerical results are provided and compared with the simulated ones. To evaluate the impact of the number of reflecting elements
$N$, the effect of $Q$ on $P_{\text{out}}$ of the SN transmission is investigated. The figure shows that $P_{\text{out}}$ of the SN transmission decreases significantly when $Q$ increases. With this in mind, the reliability of SN communication improves as the value of $N$ increases. For example, deploying the RIS technology with $N=1000$ instead of $N=50$ leads to a decrease of nearly 12.7 dBW in $Q$ to reach $P_{\text{out}}=10^{-2}$. In addition, the reliability of the proposed system model is studied and compared with different scenarios. To assess the effectiveness of the proposed system model relative to alternative scenarios, we examine the influence of phase-shift error \cite{30} and the relay-aided transmission \cite{39} scenarios. In this respect, Monte Carlo simulations are utilized to obtain the results. To examine the effect of the discrete phase shifts error, simulations are performed where the phase error is uniformly distributed between $[-\frac{\pi}{4}, \frac{\pi}{4}]$ \cite{30}. When compared to alternative scenarios, the utilization of RIS is observed to enhance the SNR at the SN destination, thereby improving the channel quality of the SN and subsequently enhancing its transmission reliability. Additionally, it is noted that the simulation results perfectly match the numerical ones, confirming the accuracy of our analysis.

Fig. 10 illustrates the impact of the location of $D$ on $P_{\text{out}}$ of the SN for different values of the number of reflecting elements $N$. It is seen that increasing the number of reflecting elements leads to a notable improvement in $P_{\text{out}}$. Moreover, a distinct trend emerges from the figure, indicating that $P_{\text{out}}$ initially decreases to its minimum values when $D$ is situated at a distance of 50 m. Subsequently, it increases beyond this distance. This trend can be explained by the fact that 50 m corresponds to the point of the minimum distance between the RIS and $D$, thus resulting in minimal fading on the RIS–$D$ link. Consequently, $P_{\text{out}}$ for the SN is reduced. In doing so, we gain insights into the optimal positioning strategies that can maximize the performance of the SN. Valuable guidelines for deploying and optimizing RIS-aided systems in underlay CRNs can be obtained from Fig. 10.

V. CONCLUSION

In this article, a new system model that employs RIS technology to improve the performance of simultaneous wireless communication and security in a CR environment has been proposed and evaluated. The proposed system model is designed to enhance the SNs transmission simultaneously and improve the PN's secrecy performance by using RIS. Using RIS can enhance the SNs transmission by boosting the SNR and increasing the network’s capacity by controlling the propagation of radio waves in the wireless environment. Additionally, employing RIS improves the PLS of the PN by creating a more secure wireless environment. A thorough analysis is conducted to assess the performance of the proposed system model, wherein novel closed-form expressions for the SNs outage probability and the PN's SOP, considering practical combining techniques, namely, SC and MRC, are provided. Additionally, the asymptotic analysis is
carried out to gain more in-depth insights into the impact of various system parameters on the SOP. The results of the asymptotic analysis demonstrate that both SC and MC techniques achieve the same diversity order of $N_P$. Interestingly, it is observed that the diversity order remains unaffected by $N_E$. Furthermore, it is verified that increasing $N$ and $N_P$ enhances the secrecy performance of the PN. Moreover, the impact of the location of the secondary receiver on the SNs performance is investigated, providing insights into optimal positioning strategies and offering valuable guidelines for deploying and optimizing RIS-aided systems in underlay CRNs. The validity of these expressions was verified through extensive Monte Carlo simulations. These simulations’ results demonstrate the proposed system model’s benefits in improving the performance of both SN and PN.

VI. FUTURE WORK

This research opens the potential for further studies. Future research could investigate RIS-assisted PLS enhancement in next-generation wireless communication networks while considering the challenges of imperfect or outdated CSI. One solution could be to employ machine learning methods, such as deep reinforcement learning, to design secure RIS-aided systems. Integrating RIS with machine learning and artificial intelligence to enable self-optimizing wireless networks is a potential area for future research.

APPENDIX

A. Appendix A

The SINR at Eav, $\Xi_E$, can be rewritten as

$$\Xi_E = \frac{\Psi_{PE}}{\Psi_{E} + 1}. \quad (35)$$

For the SC approach, the pdf of $\Xi_E$, $f^{SC}_{\Xi_E}(\cdot)$, can be derived using \[38\]

$$f^{SC}_{\Xi_E}(\gamma) = \int_0^\infty (z + 1) f^{SC}_{\Psi_{PE}}(\gamma(z + 1)) f_{\Psi_E}(z) \, dz \quad (36)$$

where $f^{SC}_{\Psi_E}(\cdot)$ is given by

$$f^{SC}_{\Psi_E}(\gamma) = \frac{N_E}{\omega_e} \sum_{k=0}^{N_E-1} (-1)^k \binom{N_E - 1}{k} \exp\left(-\frac{\gamma(k + 1)}{\omega_e}\right) \quad (37)$$

and $f_{\Psi_E}(\cdot)$ is given by

$$f_{\Psi_E}(\gamma) = \frac{1}{\Lambda_E} \exp\left(-\frac{\gamma}{\Lambda_E}\right). \quad (38)$$

By substituting (37) and (38) into (36), then with the help of [37, eq. (3.351.3)] and after simple algebraic manipulations, the pdf of $\gamma_E$, $f^{SC}_{\gamma_E}(\gamma)$, can be derived as

$$f^{SC}_{\gamma_E}(\gamma) = \sum_{k=0}^{N_E-1} \frac{N_E(-1)^k(N_E-1)}{\omega_e \Lambda_E} \exp\left(-\frac{\gamma(k + 1)}{\omega_e}\right) \times \left(1 + \frac{2(k+1)}{\omega_e} + \frac{1}{\Lambda_E}\right). \quad (39)$$

By plugging (16) and (39) into (17), and after simple algebraic manipulations, then with the help of [37, eq. (3.383.9)], the SOP for SC, $SOP_{SC}$, can be derived as in (18).

B. Appendix B

For the MRC approach, the pdf of $\Xi_E$, $f^{MRC}_{\Xi_E}(\cdot)$, can be derived using [38]

$$f^{MRC}_{\Xi_E}(\gamma) = \int_0^\infty (z + 1) f^{MRC}_{\Psi_{PE}}(\gamma(z + 1)) f_{\Psi_E}(z) \, dz \quad (40)$$

where $f^{MRC}_{\Psi_E}(\cdot)$ is given by

$$f^{MRC}_{\Psi_E}(\gamma) = \frac{\gamma N_E - 1}{\Gamma(N_E) \omega_e} \sum_{k=0}^{N_E} \frac{(N_E - 1)^k}{k!} \frac{1}{\omega_e^k \Lambda_E^{k+1}}. \quad (42)$$

By plugging (16) and (42) into (17), and after simple algebraic manipulations, then with the help of [37, eq. (3.383.4)], the SOP for MRC, $SOP_{MRC}$, can be derived as in (19).

C. Appendix C

Based on the central limit theorem, $\gamma = \sum_{i=1}^{N} |h_i| |h_{di}|$ can be modeled as a Gaussian random variable with mean $\varepsilon = \frac{N\pi}{\omega_e}$ and variance $\sigma^2 = N(1 - \frac{\pi^2}{\omega_e^2})$ \[2\]. Additionally, $\gamma = |h_{di}|$ follows a Rayleigh distribution with parameter $\delta$. The pdfs for $\gamma_1$ and $\gamma_2$ are expressed as $f_{\chi_1}(\gamma) = \frac{1}{\sqrt{2\pi}\sigma^2} \exp\left(-\frac{(\gamma - \mu)^2}{2\sigma^2}\right)$, and $f_{\chi_2}(\gamma) = \frac{1}{\sqrt{2\pi}\sigma^2} \exp\left(-\frac{(\gamma - \mu)^2}{2\sigma^2}\right)$, respectively. Thus, $\Psi_D$ can be expressed as $\Psi_D = (\Omega_2 + \Omega_1)^2$, leading to the cdf given in \[40\] $F_{\Psi_D}(\gamma) = \frac{1}{2} (\text{erf}(Q_1 \sqrt{7} - Q_2) + Q_1) = -\frac{1}{2} \left(\text{erf}(Q_1 \sqrt{7}) + \text{erf}(Q_2 \sqrt{7} + Q_1)\right)$, where $Q_1 = \frac{(\gamma_1 + \gamma_2)}{\sqrt{2}\sigma}$, $Q_2 = \frac{(\gamma_1 + \gamma_2)}{\sqrt{2}\sigma}$, and $\text{erf}(x)$ is the error function \[37, eq. (8.250.1)]}. However, utilizing $F_{\Psi_D}(\gamma)$ to derive $P_{out}$ is not mathematically tractable. Therefore, the following approximation of the erf(·) function is utilized \[41\]:

$$\text{erf}(x) \approx \begin{cases} 1 - \frac{1}{2}\sum_{m=1}^{\infty} c_m e^{-\Theta_m x^2} & x \geq 0 \\ -1 - \frac{1}{2}\sum_{m=1}^{\infty} c_m e^{-\Theta_m x^2} & x < 0 \end{cases} \quad (43)$$
where $\Theta = [1, 2, 20/3, 20/17]$, and $C = [1/8, 1/4, 1/4, 1/4]$. By plugging $F_{\Psi_0}(\gamma)$ and (10) into (30), we get

$$P_{out} = \int_{0}^{\infty} \left( \text{erf} \left( \frac{Q_1 \sqrt{\beta \gamma} - Q_2}{Q_3} \right) + Q_4 \right) \frac{e^{-\frac{u}{2}}}{\lambda_2^p} du$$

$$- \int_{0}^{\infty} q_1 e^{-\left( \frac{Q_1 \sqrt{\beta \gamma} - Q_2}{Q_3} \right)^2} \text{erf} \left( \frac{Q_6 \sqrt{\beta \gamma} - Q_2}{Q_7} \right) e^{-\frac{u}{2}} du$$

$$- \int_{0}^{\infty} q_1 e^{-\left( \frac{Q_1 \sqrt{\beta \gamma} - Q_2}{Q_3} \right)^2} \text{erf} \left( \frac{Q_8 \sqrt{\beta \gamma} + Q_2}{Q_9} \right) e^{-\frac{u}{2}} du.$$

From (44), $I_1$ can be evaluated as

$$I_1 = \frac{1}{A_1} \int_{0}^{\infty} \left( u + Q_2 \right) \text{erf}(u) e^{-\frac{(u+Q_2)^2}{4}} du + \frac{Q_3}{2\lambda_2^p}$$

$$+ \frac{1}{A_1} \int_{0}^{\infty} \left( u + Q_2 \right) e^{-\frac{(u+Q_2)^2}{4}} \left[ 1 - \sum_{m=1}^{4} \frac{C_m}{\xi^{\left( m, u^2 \gamma \right)}} \right] du$$

$$- \sum_{m=1}^{4} \frac{C_m}{\xi^{\left( m, u^2 \gamma \right)}} \int_{-Q_2}^{0} \left( u + Q_2 \right) e^{-\frac{(u+Q_2)^2}{4}} du$$

$$+ \frac{1}{A_1} \int_{-Q_2}^{0} \left( u + Q_2 \right) e^{-\frac{(u+Q_2)^2}{4}} \left[ 1 - \sum_{m=1}^{4} \frac{C_m}{\xi^{\left( m, u^2 \gamma \right)}} \right] du$$

$$+ \frac{1}{2\lambda_2^p} \frac{Q_3}{Q_7} \left( 2e^{-\frac{Q_3^2}{4}} - 1 \right).$$

where $A_1 = \lambda_1^p Q_1^2$, $A_2 = A_1 \Theta + 1$, (a) follows by substituting $u = Q_1 \sqrt{\beta \gamma} - Q_2$, (b) follows by using the approximation of the erf(·) function in (43), (c) follows by rearranging the integration parts and utilizing the square completion method. With the help of [37, eq. (2.33.1)], and after simple algebraic manipulations, $I_3$ can be obtained as in (32). From (44), $I_2$ can be evaluated as

$$I_2 = \frac{2q_1}{B_2^2} \int_{-Q_2}^{0} (u + Q_2) u^{-\frac{(u+Q_2)^2}{4}} du$$

$$+ \frac{2q_1}{B_2^2} \int_{0}^{\infty} \left( u + Q_2 \right) e^{-\frac{(u+Q_2)^2}{4}} \left[ 1 - \sum_{m=1}^{4} \frac{C_m}{\xi^{\left( m, u^2 \gamma \right)}} \right] du$$

$$+ \frac{2q_1}{B_2^2} \int_{-Q_2}^{0} \left( u + Q_2 \right) e^{-\frac{(u+Q_2)^2}{4}} \left[ 1 - \sum_{m=1}^{4} \frac{C_m}{\xi^{\left( m, u^2 \gamma \right)}} \right] du$$

$$+ \frac{4}{\beta_2^2} \int_{0}^{\infty} \left( u + Q_2 \right) e^{-\frac{(u+Q_2)^2}{4}} \left[ 1 - \sum_{m=1}^{4} \frac{C_m}{\xi^{\left( m, u^2 \gamma \right)}} \right] du.$$

where $q_1 = \frac{\sqrt{\gamma}}{2\lambda_2^p}$, $D_1 = \beta_1^p Q_2^2$, $D_2 = \left( \frac{Q_4 \frac{\xi}{Q_1} Q_2 - Q_5}{Q_6} \right)^2 + \frac{1}{\lambda_2^p}$, $D_3 = \frac{(Q_4 \frac{\xi}{Q_1} Q_2 - Q_5)^2 + \frac{1}{\lambda_2^p}}{2\lambda_2^p} \left( Q_2 Q_7 - Q_5 \right) + \frac{Q_7}{Q_7} Q_5$, $D_4 = \left( \frac{Q_4 \frac{\xi}{Q_1} Q_2 - Q_5}{Q_6} \right)^2 + \frac{1}{\lambda_2^p}$, $D_5 = D_2 + \Theta m$, $D_6 = D_3 - 2D_2 Q_7$, $D_7 = D_1 - 2D_2 Q_7$, (a) follows by substituting $u = Q_1 \sqrt{\beta \gamma} - Q_2$, (b) follows by using the approximation of the erf(·) function in (43), (c) follows by rearranging the integration parts and utilizing the square completion method. With the help of [37, eq. (2.33.1)], and after simple algebraic manipulations, $I_3$ can be obtained as in (34).

REFERENCES

[1] M. H. Khoshafa, “Physical layer security in 5G and beyond wireless networks enabling technologies,” Ph.D. dissertation, Elect. Comput. Eng. Dept., Memorial Univ. Newfoundland, St. John’s, NL, Canada, Feb. 2022.

[2] 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. 116753–116773, Jul. 2019.

[3] 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.

[4] 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.

[5] M. H. Khoshafa, T. M. Ngactched, and M. H. Ahmad, “Reconfigurable intelligent surfaces-aided physical layer security enhancement in D2D underlay communications,” IEEE Commun. Lett., vol. 25, no. 5, pp. 1443–1447, May 2021.

[6] M. H. Khoshafa, T. M. Ngactched, M. H. Ahmad, and A. R. Ndjigoe, “Active reconfigurable intelligent surfaces-aided wireless communication system,” IEEE Commun. Lett., vol. 25, no. 11, pp. 3699–3703, Nov. 2021.

[7] R. Fara, P. Rajaczak, 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.

[8] G. C. Trichopoulos et al., “Design and evaluation of reconfigurable intelligent surfaces in real-world environment,” IEEE Open J. Commun. Soc., vol. 3, pp. 462–474, Dec. 2022.

[9] L. Dai et al., “Reconfigurable intelligent surface-based wireless communications: Antenna design, prototyping, and experimental results,” IEEE Access, vol. 8, pp. 45934–45923, Mar. 2020.

[10] L. Qian et al., “Multi-dimensional polarized modulation for land mobile satellite communications,” IEEE Trans. Cogn. Commun. Net., vol. 7, no. 2, pp. 383–397, Jun. 2021.

[11] A. Cherti et al., “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.
[12] S. Basharat, S. A. Hassan, H. Pervaz, A. Mahmood, Z. Ding, and M. Gildan, “Reconfigurable intelligent surfaces: Potentials, applications, and challenges for 6G wireless networks,” IEEE Wireless Commun., vol. 28, no. 6, pp. 184–191, Dec. 2021.

[13] A. D. Wyner, “The wire-tap channel,” Bell Syst. Tech. J., vol. 54, no. 8, pp. 1335–1387, Oct. 1975.

[14] 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.

[15] J. Zhang, H. Du, Q. Sun, B. Ai, and D. W. K. Ng, “Physical layer security enhancement with reconfigurable intelligent surface-aided networks,” IEEE Trans. Info. Forensics Secur., vol. 16, pp. 3480–3495, Jun. 2021.

[16] 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.

[17] X. Tang, X. Lan, D. Zhai, R. Zhang, and Z. Han, “Securing wireless transmissions with RIS-receiver coordination: Passive beamforming and active jamming,” IEEE Trans. Veh. Technol., vol. 70, no. 6, pp. 6260–6265, Jun. 2021.

[18] X. Gu, W. Duan, G. Zhang, Q. Sun, M. Wen, and P.-H. Ho, “Physical layer security for RIS-aided wireless communications with uncertain eavesdropper distributions,” IEEE Syst. J., vol. 17, no. 1, pp. 848–859, Mar. 2023.

[19] 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.

[20] D. H. Tashman and W. Hamouda, “An overview and future directions on physical-layer security for cognitive radio networks,” IEEE Netw., vol. 35, no. 3, pp. 205–211, May/Jun. 2021.

[21] 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.

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

[23] C. Pan 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.

[24] B. Zhao, M. Lin, S. Xiao, M. Cheng, W.-P. Zhu, and N. Al-Dhahir, “Robust beamforming for RIS enhanced transmissions in cognitive radio networks,” IEEE Trans. Veh. Technol., vol. 72, no. 5, pp. 6800–6804, May 2023.

[25] E. Shi et al., “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.

[26] J. Chen, Y.-C. Liang, H. V. Cheng, and W. Yu, “Channel estimation for reconfigurable intelligent surface aided multi-user MIMO systems,” IEEE Trans. Wireless Commun., early access, 2023, doi: 10.1109/TWC.2023.3246264.

[27] B. Zheng, C. You, and R. Zhang, “Intelligent reflecting surface assisted multi-user OFDMA: Channel estimation and training design,” IEEE Trans. Wireless Commun., vol. 19, no. 12, pp. 8315–8329, Dec. 2020.

[28] 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. 11445–11457, Oct. 2020.

[29] 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.

[30] P. Xu, G. Chen, G. Pan, and M. D. Renzo, “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. 5, pp. 629–633, Mar. 2021.

[31] L. Zhang, C. Pan, Y. Wang, H. Ren, and K. Wang, “Robust beamforming design for intelligent reflecting surface aided cognitive radio systems with imperfect cascaded CSI,” IEEE Trans. Cogn. Commun. Netw., vol. 8, no. 1, pp. 186–201, Mar. 2022.

[32] 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.

[33] H. Lei et al., “On secrecy outage of relay selection in underlay cognitive radio networks over Nakagami-m fading channels,” IEEE Trans. Cogn. Commun. Netw., vol. 3, no. 4, pp. 614–627, Dec. 2017.

[34] E. Björnson, O. 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.

[35] M.-A. Badu 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.

[36] P. Xu, G. Chen, G. Pan, and M. D. Renzo, “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. 5, pp. 629–633, Mar. 2021.

[37] A. Papoulis and S. U. Pillai, Probability, Random Variables, and Stochastic Processes, 2nd ed. Upper Saddle River, NJ, USA: Prentice-Hall, 2002.

[38] I. S. Gradshteyn and I. M. Ryzhik, Table of Integrals, Series, and Products. New York, NY, USA: Academic, 2014.

[39] M. H. Khoshafa, T. M. 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.

[40] E. Björnson, O. Özdogan, and E. G. Larsson, “Intelligent reflecting surface with phase errors,” IEEE Wireless Commun. Lett., vol. 9, no. 2, pp. 184–188, Feb. 2020.

[41] D. Sadhwa, 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.