sensors

MDPI

Article

Secure Cognitive Radio-Enabled Vehicular Communications under Spectrum-Sharing Constraints

Suneel Yadav [1,*], Anshul Pandey [2], Dinh-Thuan Do [3], Byung Moo Lee [4] and Adão Silva [5]

[1] Department of Electronics and Communication Engineering, Indian Institute of Information Technology Allahabad, Prayagraj 211015, India
[2] Secure Systems Research Center, Technology Innovation Institute, Abu Dhabi 9639, United Arab Emirates; anshul@ssrc.tii.ae
[3] Department of Computer Science and Information Engineering, College of Information and Electrical Engineering, Asia University, 500 Lioufeng Rd., Wufeng, Taichung 41354, Taiwan; dodinhthuan@asia.edu.tw
[4] Department of of Intelligent Mechatronics Engineering, and Convergence Engineering for Intelligent Drone, Sejong University, Seoul 05006, Korea; blee@sejong.ac.kr
[5] Instituto de Telecomunicações (IT) and Departamento de Eletrónica, Telecomunicações e Informática (DETI), University of Aveiro, 3810-193 Aveiro, Portugal; asilva@av.it.pt
* Correspondence: suneel@iiita.ac.in

Abstract: Vehicular communication has been envisioned to support a myriad of essential fifth-generation and beyond use-cases. However, the increasing proliferation of smart and intelligent vehicles has generated a lot of design and infrastructure challenges. Of particular interest are the problems of spectrum scarcity and communication security. Consequently, we considered a cognitive radio-enabled vehicular network framework for accessing additional radio spectrum and exploit physical layer security for secure communications. In particular, we investigated the secrecy performance of a cognitive radio vehicular network, where all the nodes in the network are moving vehicles and the channels between them are modeled as double-Rayleigh fading. Furthermore, adopting an underlay approach, the communication between secondary nodes can be performed by employing two interference constraint strategies at the primary receiver; (1) Strategy I: the secondary transmitter power is constrained by the interference threshold of the primary receiver, and (2) Strategy II: the secondary transmitter power is constrained by both the interference threshold of the primary receiver and the maximum transmit power of the secondary network. Under the considered strategies, we derive the exact secrecy outage probability (SOP) and ergodic secrecy capacity (ESC) expressions over double-Rayleigh fading. Moreover, by analyzing the asymptotic SOP behavior, we show that a full secrecy diversity of 1 can be achieved, when the average channel gain of the main link goes to infinity with a fixed average wiretap channel gain. From the ESC analysis, it is revealed that the ESC follows a scaling law of $\Theta\left(\ln\left(\frac{\Omega_m^2}{\Omega_e^2}\right)\right)$ for large Ω_m and Ω_e, where Ω_m and Ω_e are the average channel gains of the main link and wiretap link. The numerical and simulation results verify our analytical findings.

Keywords: physical-layer security; cognitive radio vehicular networks (CRVNs); secrecy outage probability (SOP); ergodic secrecy capacity (ESC); double-Rayleigh fading channels

Citation: Yadav, S.; Pandey, A.; Do, D.-T.; Lee, B.M.; Silva, A. Secure Cognitive Radio-Enabled Vehicular Communications under Spectrum-Sharing Constraints. *Sensors* **2021**, *21*, 7160. https://doi.org/10.3390/s21217160

Academic Editor: Omprakash Kaiwartya

Received: 10 August 2021
Accepted: 25 October 2021
Published: 28 October 2021

1. Introduction

With the advancement in wireless communication capabilities and increasing number of sensors, an ecosystem of automated connected vehicles has evolved into a network paradigm called the Internet of Vehicles (IoV) [1,2]. Such vehicular communication networks form an integral part of 5G and beyond wireless communication technologies. Moreover, vehicular communications can help us to realize an abundance of on the move intelligent transportation system (ITS) applications, such as safer and better travel experience to the users, infotainment services, efficient traffic management, vehicle platooning

etc. [3]. In addition, vehicular communications aim at realizing ubiquitous connectivity among the vehicles in a wireless manner [4]. Therefore, to support such massive connectivity with real-time network access, a substantial amount of energy and radio resources are needed. To this end, cognitive radio technology can be exploited in the vehicular communication networks to support the shared spectrum access [5,6]. The cognitive radio-enabled vehicular communications, named cognitive radio vehicular networks (CRVNs), can exploit the additional spectrum opportunities outside the IEEE 802.11p specified standard 5.9-GHz band [7]. However, such networks are susceptible to various serious security attacks as the bulk of communication occur over the open and vulnerable wireless medium [8]. The issues of mobility, cooperative infrastructure, dynamic nature of cognitive radios, and heterogeneity can further aggravate the security concerns, as these characteristics limit the implementation of the existing key-based cryptography security infrastructure [8,9]. As of late, physical-layer security (PHY-security) has arisen as an appealing way to guarantee secure wireless transmissions and to complement the existing security infrastructure further. In contrast to the key-based upper layer security mechanisms, PHY-security techniques provide secure transmissions at the physical layer by exploiting the inherent random nature of the wireless channels such as fading, interference, etc., through various coding, signal design, and signal processing approaches [10]. Therefore, this paper aims to provide a comprehensive performance analysis of PHY-security in CRVNs under spectrum-sharing constraints.

1.1. Related Works

PHY-security aspects have been thoroughly investigated in the literature for various network scenarios under different fading channels without considering the cognitive framework [11–20]. Furthermore, the authors in [21] have proposed a machine-learning-based method to locate the vehicles generating jamming signals by monitoring the physical channel parameters of the vehicles in the vehicular networks. Moreover, PHY-security performance in the cognitive radio networks has been explored broadly in the literature [22–31] with or without relaying scenarios. In addition, to guarantee the quality of service (QoS) at the primary receiver, these works have employed either the single-power constraint of the maximum interference tolerable limit for the primary network or the combined power constraint of the maximum interference tolerable limit for the primary network and the maximum allowable transmission power at the secondary network. For the relay-assisted cognitive radio networks, the secrecy performance of cooperative cognitive relay networks has been analyzed in [22–27] and the references therein. Specifically, the authors in [22] investigated the secrecy performance of the cooperative cognitive relay networks in the presence of direct links. The authors in [23,24] have proposed some relay selection strategies to enhance the secrecy performance of the secondary network in the cognitive relaying systems. Moreover, the authors in [25] employed external jamming techniques for improving the security of an underlay cognitive relaying systems. The authors in [26] studied the problem of residual energy maximization for the multiple eavesdropper scenario in cognitive relaying networks. Furthermore, the authors in [27] analyzed the PHY-security performance of multiple-input–multiple-output cognitive relaying networks under the impact of outdated channel estimates.

Of particular interest are the secure underlay cognitive radio networks, where the secondary transmitter communicates with the secondary receiver under the interference constraint imposed on primary receiver in the presence of active/passive eavesdropper. Specifically, the authors in [28–32] evaluated the secrecy performance for cognitive radio networks. For instance, the authors in [28] investigated the secrecy performance of an underlay cognitive wiretap secondary system with multiple secondary receivers and eavesdroppers by considering the joint power constraint under Rayleigh fading channels. In [29], the authors investigated the secrecy performance of multiinput, single-output, and single-eavesdropper cognitive radio networks over correlated fading channels. The authors in [30] analyzed the secrecy performance of a cognitive wiretap system with multiantenna

secondary terminals under Rayleigh fading channels. Further, the authors in [31] evaluated the secrecy performance of an underlay cognitive radio system in the presence of an active eavesdropper. Furthermore, for a single-input–multiple-output system, the authors in [32] investigated the impact of outdated channel estimates on PHY-security performance for cognitive radio networks.

However, all the aforesaid studies in [28–32] were limited to the scenarios where the nodes in the network are stationary (i.e., fixed infrastructures); therefore, the channel between the nodes is modeled as Rayleigh fading or Nakagami-*m* fading. In fact, the nodes in the wireless communication networks can be moving while exchanging the information, e.g., mobile of people driving on road, yielding the channel between the moving nodes as cascaded Rayleigh (double-Rayleigh) fading [33–35]. (It is to be emphasized that the vehicle-to-vehicle (V2V) links undergo multiple scattering phenomena and are moving in a relatively dense scattering environment; thus, from the theoretical and empirical studies, cascaded Rayleigh channel modeling is shown to be more appropriate in resembling the dynamic V2V communication links [33–35]). Therefore, such V2V communications-enabled cognitive radio networks are one of the most fascinating use-cases in the upcoming 5G networks, and it is very interesting to comprehensively investigate the PHY-security in CRVNs under double-Rayleigh fading channels. In this context, the secrecy performance over cascaded fading channels has been widely studied in [35–40]. Recently, the authors in [41] studied the secrecy capacity performance for vehicular communication networks. However, these works [35–41] were limited to the noncognitive networking setup. Moreover, the authors in [42,43] evaluated the performance of multihop cognitive radio networks over double-Rayleigh fading channels but without taking PHY-security aspects into account. Further, the authors in [44] investigated secrecy performance of CRVNs over N*Nakagami-m fading channels.

1.2. Motivation

From the aforementioned discussion, we can infer that the bulk of the works reported towards the investigation of PHY-security aspects in cognitive communication networks were limited to the scenario where the nodes are stationary. With the emerging varied form of ITS applications and user needs on the move, CRVNs have attracted great research interest. The authors in [35–40] evaluated PHY-security performance of cooperative vehicular relaying networks but without taking the spectrum-sharing cognitive framework into consideration. Moreover, the authors in [42,43] considered double-Rayleigh fading channels and evaluated the performance of cognitive radio-enabled V2V networks, but they did not emphasize the PHY-security aspects of the considered system. Therefore, exploitation of PHY-security benefits in underlay CRVNs over cascaded fading channels is still an open issue. To this end, a little effort has been directed to analyze the secrecy performance of CRVNs over N*Nakagami-m fading channels in [44]. Very recently, the authors in [45] analyzed the secrecy performance of cognitive radio networks over cascaded Rayleigh fading. However, there are several differences between this work and [44,45].

- In [44], the authors considered the following assumptions while analyzing the secrecy performance of CRVNs; (i) single-power constraint of the interference on the primary receiver, and (ii) N*Nakagami-m fading. In addition, the system's performance was evaluated in terms of secrecy outage probability (SOP).
- In [45], the authors considered the following assumptions while investigating the PHY-security performance of CRVNs; (i) single-power constraint of the interference on the primary receiver, (ii) cascaded Rayleigh fading for the main channel (between secondary source and secondary receiver), and Rayleigh fading for both the wiretap channel (between secondary source and secondary eavesdropper) and interference channel (between secondary source and primary receiver). However, for evaluating the system's performance, the cascaded Rayleigh fading was transformed into a Nakagami-m fading approximation, and assumed statistical independence among the

channel gains. In addition, the performance was evaluated in terms of SOP, intercept probability, and probability of non-zero secrecy capacity.

- Different from [44,45], in this paper, we adopt the following: (i) two power control strategies at the secondary transmitter, i.e., Strategy I: single-power constraint of the interference on the primary receiver, and Strategy II: combined power constraint of the interference on the primary receiver and the maximum transmission power at the secondary transmitter, (ii) double-Rayleigh fading for all the links, and (iii) statistical dependency among the channel gains. In addition, we evaluate the secrecy performance in terms of exact SOP, asymptotic SOP, and ergodic secrecy capacity (ESC), under Strategies I and II.

In addition, the proposed work and the works presented in [46,47] explored the cognitive radio networks under vehicular communications. However, there are several key differences between this work and [46,47], whose brief detail is as follows.

- This paper and the work presented in [46] consider all the nodes are equipped with single antenna, whereas the authors in [47] considered the secondary transmitter and primary receiver are equipped with single antenna and secondary receiver and eavesdropper are enabled with multiple antennas.
- In this work, we consider the channel between the moving vehicles to be quasistationary for a short duration (i.e., one fading block time), where the distance between the nodes is much greater than the scattering radii. Consequently, assuming the radio propagation between two moving vehicles undergoes independent double scattering events, the channel can be modeled as double-Rayleigh fading. By contrast, the works presented in [46,47] considered the scenario where the symbol period of the detected signal is larger than the coherence time of the channel, and hence, the system fading links can be characterized as time-selective. Particularly, the works [46,47] considered Rayleigh fading channels and Nakagami-m fading channels, respectively.
- In [46], the authors considered a single-power constraint of the interference on the primary receiver, whereas in [47], the authors adopted a combined power constraint of the interference on the primary receiver and the maximum transmission power at the secondary transmitter. Different from [46,47], this paper adopts both single-power- and combined-power-based control strategies for managing interference at the primary receiver.
- In [46], the authors evaluated the SOP and intercept probability expressions over Rayleigh fading channels, while in [47], the authors derived the expressions for the SOP and ESC over Nakagami-m fading channels. In this paper, we derived the SOP and ESC expressions over double-Rayleigh fading channels.

Therefore, the above differences make the contributions and results of this work fundamentally very different from [44–47]. Hence, this motivates us to develop a thorough and comprehensive investigation on the secrecy performance of CRVNs under both single and combined interference power constraints in the presence of double-Rayleigh fading channels.

1.3. Contributions

From the aforesaid discussion, it is obvious that there is a lack of PHY-security performance evaluation in CRVNs over double-Rayleigh fading channels by employing two power control strategies at the secondary transmitter vehicle, i.e., (1) Strategy I: where the transmit power of the secondary transmitter vehicle is only constrained by the interference threshold of the primary receiver vehicle, and (2) Strategy II: where the transmit power of the secondary transmitter vehicle is constrained by both the maximum transmit power and the interference threshold of the primary receiver vehicle. The analytical outcomes reported in this paper thus (1) face several mathematical challenges and complications under the considered strategies and double-Rayleigh fading, (2) are unique as efforts to investigate PHY-security in CRVNs under the consideration of two spectrum sharing constraints and double-Rayleigh fading channels is made first time in the literature, and (3) lay the

foundation for examining PHY-security in CRVNs over more generalized cascaded fading models, such as N*Rayleigh and N*Nakagami-m. Specifically, in this work, under the two considered power control strategies and by taking double-Rayleigh fading channels into account, we investigate SOP, asymptotic SOP behavior, and ESC, for the considered underlay CRVNs. The key contributions of the paper are summarized as follows.

1. We deduce the exact SOP expressions over double-Rayleigh fading channels in order to investigate the secrecy performance under two considered power control strategies. These SOP expressions enable us to effectively determine the impact of key system/channel parameters on the system's secrecy performance.
2. We further present the asymptotic SOP expressions for Strategy I and Strategy II over double-Rayleigh fading channels. These asymptotic expressions provide us some important insights related to the system's achievable secrecy diversity order. Based on these asymptotic results, it is observed that the system can achieve a secrecy diversity order of 1, when the average channel gain of the main link goes to infinity and the average channel gain of the wiretap link is fixed. However, the convergence of achieving the asymptotical secrecy diversity order of 1 is very slow, due the involvement of double-Rayleigh fading channels. In addition, the secrecy diversity order reduces to zero when the average channel gains of the main and wiretap links go to infinity.
3. Using the derived exact SOP expression under Strategy II, we demonstrate the impact of maximum tolerable interference level and maximum secondary transmitter power on the secrecy performance. Specifically, we analyze two cases, viz., (1) when maximum tolerable interference level is proportional to maximum secondary transmitter power, and (2) when maximum tolerable interference level is not related to maximum secondary transmitter power. It is revealed from these two cases that the SOP performance saturates when maximum secondary transmitter power is large enough, which results into a zero system' secrecy diversity gain.
4. Further, we deduce novel ESC expressions for Strategy I and Strategy II under double-Rayleigh fading, in order to analyze the impact of interference threshold, maximum transmit power, and average channel gains on the secrecy performance. We also present two key observations irrespective of two power control strategies, when the average channel gains of main and wiretap links are very large, i.e., (1) there exists a ceiling of ESC, and (2) the ESC follows a scaling law of $\Theta\big(\ln\big(\frac{\Omega_m^2}{\Omega_e^2}\big)\big)$, where Ω_m and Ω_e are the average channel gains of main and wiretap links, respectively.
5. We finally verify our analytical and theoretical findings via simulation studies. Our results show the impact of involved network parameters on the system's SOP and ESC performances under Strategy I and Strategy II.

1.4. Organization

The paper is structured as follows: Section 2 describes the considered system model for CRVNs. In Section 3, we analyze and present the exact and asymptotic SOP expressions under Strategy I and Strategy II for CRVNs. Section 4 presents the ESC expressions under Strategies I and II. Numerical results are provided in Section 5 to offer valuable insights onto the secrecy performance. Finally, Section 6 concludes the work.

Notations: $K_v(\cdot)$ is the v-th order modified Bessel function of second kind (eq. (8.432)) of [48], ${}_2\tilde{F}_1(m,n,p;z)$ is the Hypergeometric regularized function (eq. (9.10)) of [48], $\Psi(\cdot,\cdot,\cdot)$ being the Kummer hypergeometric function (eq. (9.238)) of [48], $G_{p,q}^{m,n}\left(y\middle|\begin{matrix}a_1,\cdots,a_p\\ b_1,\cdots,b_q\end{matrix}\right)$ is the Meijer-G function (eq. (9.301)) of [48], and $G_{p_1,q_1:\,p_2,q_2:\,p_3,q_3}^{m_1,n_1:\,n_2,m_2:\,n_3,m_3}\left(y,z\middle|\begin{matrix}a_1,\cdots,a_{p_1}\\ b_1,\cdots,b_{q_1}\end{matrix}\middle|\begin{matrix}c_1,\cdots,c_{p_2}\\ d_1,\cdots,d_{q_2}\end{matrix}\middle|\begin{matrix}e_1,\cdots,e_{p_3}\\ f_1,\cdots,f_{q_3}\end{matrix}\right)$ is the extended generalized bivariate Meijer-G function (eq. (07.34.21.0081.01)) of [49].

2. System and Channel Models

In the following subsections, we detail the adopted cascaded fading channel model for the V2V channels and the system model for our considered cognitive vehicular networks.

Further, we consider two power control strategies to minimize the interference at the primary receiver and present the end-to-end instantaneous signal-to-noise ratios for both the strategies.

2.1. Statistical Background: The Double-Rayleigh Distribution

As proposed in [33], for mobile-to-mobile links, the multiple Rayleigh propagation considers two or more independent Rayleigh fading processes generated by independent groups of scatterers around the two moving vehicles. The resulting transfer function, $H(t)$, can be expressed as a linear combination of components with Rayleigh, double-Rayleigh, triple-Rayleigh, etc., distributed amplitudes. For the case of only double-Rayleigh process, the narrow-band, base-band channel transfer function can be written as [37]

$$\overline{H}(t) = \sqrt{\frac{2}{\mathbb{N}_T \mathbb{N}_R}} \sum_{n=1}^{\mathbb{N}_T} \sum_{m=1}^{\mathbb{N}_R} e^{j2\pi(f_T \cos(\phi_n)t + f_R \cos(\phi_m)t + \theta_{nm})}, \tag{1}$$

where $\mathbb{N}_T$ and $\mathbb{N}_R$ are the respective numbers of scatterers generated around moving transmitter and receiver, f_T and f_R denote the respective maximum Doppler shift due to the motion (speed of mobility) of transmitter and receiver, ϕ_n and ϕ_m are the random angle of departure and the angle of arrival with respect to the velocity vectors, respectively, and θ_{nm} is the joint phase shift. It is important to note that the motions (speed of mobility) of transmitter and receiver are involved in the form of Doppler shifts to determine how fast the fading channel will be. For mathematical tractability, the channel between moving vehicles is assumed to be quasi-stationary for a short duration (i.e., one fading block time), and the distance between the nodes is much greater than the scattering radii, the channel between those moving vehicles can be distributed as double-Rayleigh fading (It is a more realistic channel model in a V2V scenario, especially when (i) the vehicles are moving in high scattering environment, e.g., high traffic scenarios and (ii) all the vehicles are equipped with low elevation antennas. Such a fading assumption which can find its applicability for vehicular communication scenarios in rush-hour traffic is widely investigated for vehicular networks in the literature [35–40,42,43]) [33–40,42–45,50–52].

Under double-Rayleigh fading, the resulting envelope $\mathbb{R}$ can be expressed as the product of $\mathbb{R}_1$ and $\mathbb{R}_2$, i.e., $\mathbb{R} = \mathbb{R}_1\mathbb{R}_2$, where $\mathbb{R}_1$ and $\mathbb{R}_2$ are independent Rayleigh fading processes with mean powers Ω_1 and Ω_2, respectively. Thus, the probability density function (PDF) and the cumulative distribution function (CDF) of $\mathbb{R}$ can be expressed as [37]

$$f_{\mathbb{R}}(r) = \frac{r}{\Omega_1\Omega_2} K_0\Big(\frac{r}{\sqrt{\Omega_1\Omega_2}}\Big), \tag{2}$$

$$F_{\mathbb{R}}(r) = 1 - \frac{r}{\sqrt{\Omega_1\Omega_2}} K_1\Big(\frac{r}{\sqrt{\Omega_1\Omega_2}}\Big), \tag{3}$$

respectively. Moreover, the PDF and CDF of the square to the envelope, i.e., $|\mathbb{R}|^2$, can be represented, respectively, as

$$f_{|\mathbb{R}|^2}(r) = \frac{2}{\Omega_1\Omega_2} K_0\Big(2\sqrt{\frac{r}{\Omega_1\Omega_2}}\Big), \tag{4}$$

$$F_{|\mathbb{R}|^2}(r) = 1 - 2\sqrt{\frac{r}{\Omega_1\Omega_2}} K_1\Big(2\sqrt{\frac{r}{\Omega_1\Omega_2}}\Big). \tag{5}$$

2.2. Cognitive Radio Vehicular System

We consider a secure CRVN, where primary user vehicle and secondary user vehicles share the same licensed spectrum band in a given propagation environment. In the secondary network, the secondary transmitter sends its message to secondary receiver in the presence of a primary receiver present in the primary network. Meanwhile, in the secondary network, a passive eavesdropper vehicle is able to intercept the information transmitted by the secondary transmitter. Under the passive eavesdropping scenario, the

instantaneous CSI between secondary transmitter and eavesdropper is not available at the secondary transmitter. During the whole process, the secondary transmitter imposes an interference to the primary receiver. Note that we highlight a practical consideration of the passive eavesdropping scenario since, in practice, the passive eavesdropper is noncooperative and does not feedback its instantaneous CSI to the trusted nodes. The assumption of known statistical CSI of eavesdropper's channel can be applied to the scenario where the eavesdropper is part of a system which in alternate time slots becomes an active trusted user in the system. As such, the instantaneous CSI of the eavesdropper can be available at the transmitter via a feedback channel for the time slot where it is being served. Therefore, from this information and assuming eavesdropper CSI does not change under the assumption of quasi-stationary channel for a short duration, statistical CSI of the passive eavesdropper can be available at the trusted node, for the time slots where it is not being served [17–30]. The detail of the interference constraints is discussed later in this section.

Figure 1 depicts the system model of the considered secure CRVN, which consists of a secondary transmitter vehicle ST, a secondary receiver vehicle SR, a primary receiver vehicle PR, and a passive eavesdropper vehicle E. All the terminals are equipped with a single antenna and operate in the half-duplex manner (note that the consideration of single-antenna at the terminals can reduce the system complexity and requirement of power-intensive signal processing modules and hence make them for practical use in various battery operated devices, such as wireless sensor applications. In addition, the assumption of half-duplex terminals can be practically applicable, as the half-duplex operation is much easier and does not require additional signal-processing operations compared to the full-duplex operation, because in the full-duplex operation, a significant amount of self-interference is observed at the receiving antenna as a result of the signal from the transmitting antenna of the same node). Since, all the nodes are moving vehicles; therefore, the channels for ST $\rightarrow$ SR (i.e., main link), ST $\rightarrow$ PR (i.e., interference link), and ST $\rightarrow$ E (i.e., wiretap link) links can be modeled as double-Rayleigh fading. We represent h_m, h_p, and h_e as the channel coefficients of ST $\rightarrow$ SR, ST $\rightarrow$ PR, and ST $\rightarrow$ E links, respectively. In addition, we consider the perfect CSI knowledge of the channels. In this paper, we consider the perfect channel estimation process. However, imperfect channel estimates may be available for transmission in such systems, which are generally inaccurate and outdated with respect to actual channel. Consequently, the imperfect/outdated CSI for the actual channel can be expressed as $h_\iota^{\text{imperfect}} = \varrho_\iota h_\iota + \sqrt{1-\varrho_\iota^2} w_\iota$, for $\iota \in \{m, e, p\}$, where ρ_ι denotes the normalized correlation coefficient between $h_\iota^{\text{imperfect}}$ and h_ι, and w_ι is a Gaussian random variable having the same variance as that of h_ι. Therefore, the performance evaluation of considered CRVNs under such imperfect/outdated CSI requires a fresh approach, which is studied thoroughly and comprehensively in the future work. Under double-Rayleigh fading, the channel coefficients h_ι, for $\iota \in \{m, e, p\}$, can be expressed as the product of $h_{\iota,1}$ and $h_{\iota,2}$, where $h_{\iota,1}$ and $h_{\iota,2}$ are independent complex Gaussian random variables having zero mean and variance (without loss of generality, we assume $\Omega_{\iota,1} = \Omega_{\iota,2} = \Omega_\iota$, for $\iota \in \{m, e, p\}$; however, the analysis can readily be extended for $\Omega_{\iota,1} \neq \Omega_{\iota,2}$). $\Omega_{\iota,1}$ and $\Omega_{\iota,2}$, respectively. P_s denotes the transmit power at ST. We also assume the additive white Gaussian noise (AWGN) with zero mean and N_0 variance for each link.

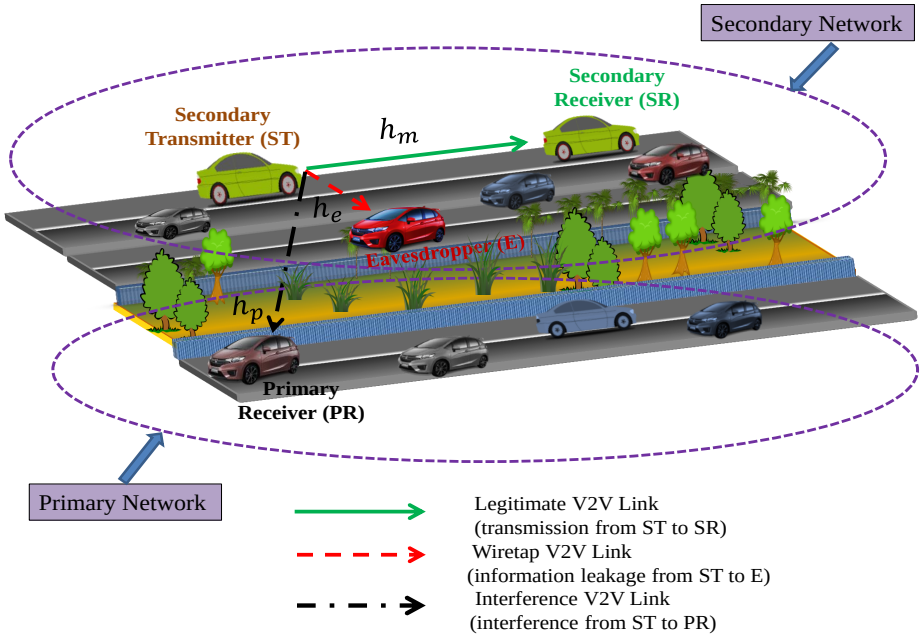

Figure 1. System model for the considered secure underlay CRVNs.

2.3. Instantaneous End-to-End Signal-to-Noise Ratio

Suppose that ST sends its confidential information to the legitimate SR over the main channel, and at the same time an E tries to decode this information through the wiretap channel; then, the signal received at SR and E can be given by $y_{\mathrm{SR}} = \sqrt{P_s} h_m x_s + n_m$ and $y_{\mathrm{E}} = \sqrt{P_s} h_e x_s + n_e$, respectively, where n_m and n_e are AWGNs at SR and E, respectively. The instantaneous end-to-end signal-to-noise ratios (SNRs) Λ_m and Λ_e at SR and E can be expressed as

$$\Lambda_m = \frac{P_s |h_m|^2}{N_0} \text{ and } \Lambda_e = \frac{P_s |h_e|^2}{N_0}. \tag{6}$$

Furthermore, we assume that PR feedbacks its instantaneous CSI to secondary transmitter ST, and ST accordingly adjusts its transmit power to satisfy the interference constraint [52]. Practically, a spectrum band manager can help to realize this task by mediating between the primary and the secondary users. Therefore, in order to protect the QoS of PR, we employ two power control strategies at ST, i.e., (1) Strategy I: single-power constraint of the interference on the PR, I_P [22,28,53] and (2) Strategy II: combined power constraint of the interference on the PR and the maximum transmit power at ST, Q [29,30,53].

Strategy I: Under Strategy I, the transmit power P_s at ST is constrained so that the interference impinged on PR remains below the maximum tolerable interference level I_P. Therefore, P_s at ST can be mathematically expressed as $P_s = \frac{I_P}{|h_p|^2}$. Therefore, with Strategy I, the instantaneous end-to-end SNRs at SR and E can be given as

$$\Lambda_m^{\mathrm{I}} = \frac{\rho |h_m|^2}{|h_p|^2} \text{ and } \Lambda_e^{\mathrm{I}} = \frac{\rho |h_e|^2}{|h_p|^2}, \tag{7}$$

respectively, where $\rho \triangleq \frac{I_P}{N_0}$.

Strategy II: In Strategy II, if ST is power limited terminal, then ST may transmit up to the maximum transmit power constraint of Q, and therefore P_s at ST can be expressed as

$P_s = \min\left(\frac{I_P}{|h_p|^2}, Q\right)$. Taking such strategy into account, the instantaneous end-to-end SNRs at SR and E can be given by

$$\Lambda_m^{\mathrm{II}} = \min\left(\frac{\rho}{|h_p|^2}, \rho_1\right)|h_m|^2, \tag{8}$$

$$\Lambda_e^{\mathrm{II}} = \min\left(\frac{\rho}{|h_p|^2}, \rho_1\right)|h_e|^2, \tag{9}$$

respectively, where $\rho_1 \triangleq \frac{Q}{N_0}$.

Under the two adopted strategies, the capacities corresponding to main link (i.e., ST $\rightarrow$ SR) and wiretap link (i.e., ST $\rightarrow$ E) can be given by $\mathcal{C}_m^{\jmath} = \log_2(1 + \Lambda_m^{\jmath})$ and $\mathcal{C}_e^{\jmath} = \log_2(1 + \Lambda_e^{\jmath})$, where $\jmath = \mathrm{I}$ for Strategy I and $\jmath = \mathrm{II}$ for Strategy II. Moreover, the secrecy capacity of the wireless transmission can be given as $\mathcal{C}_{sec}^{\jmath} = \max\{\mathcal{C}_m^{\jmath} - \mathcal{C}_e^{\jmath}, 0\}$, for $\jmath \in \{\mathrm{I}, \mathrm{II}\}$.

In addition, Figure 2 shows the overall representation of the proposed CRVN framework. Here, the secondary vehicular network operates in the underlay spectrum sharing context along with the presence of a primary vehicular network. The transmission in the secondary network can only be established as long as the resulting interference on the PR is maintained underneath a given threshold. Firstly, if the PR generates an instantaneous QoS requirements, then the transmit power at ST should be constrained so that the interference imposed on PR remains below the maximum tolerable interference level, and consequently the transmit power, P_s, at ST can be given as $P_s = \frac{I_P}{|h_p|^2}$. Thereafter, the secondary users are allowed to use the licensed band and perform their operations accordingly. On the other hand, if the PR generates a stringent requirement of protecting QoS of PR and maintaining secondary user throughput simultaneously, then the transmit power, P_s, at ST can be expressed as $P_s = \min\left(\frac{I_P}{|h_p|^2}, Q\right)$. Accordingly, the secondary users are allowed to start their transmissions. Finally, the performance of secure secondary network under the above two constraints can be evaluated in terms of SOP, asymptotic SOP, and ESC, as presented in subsequent Sections 3 and 4.

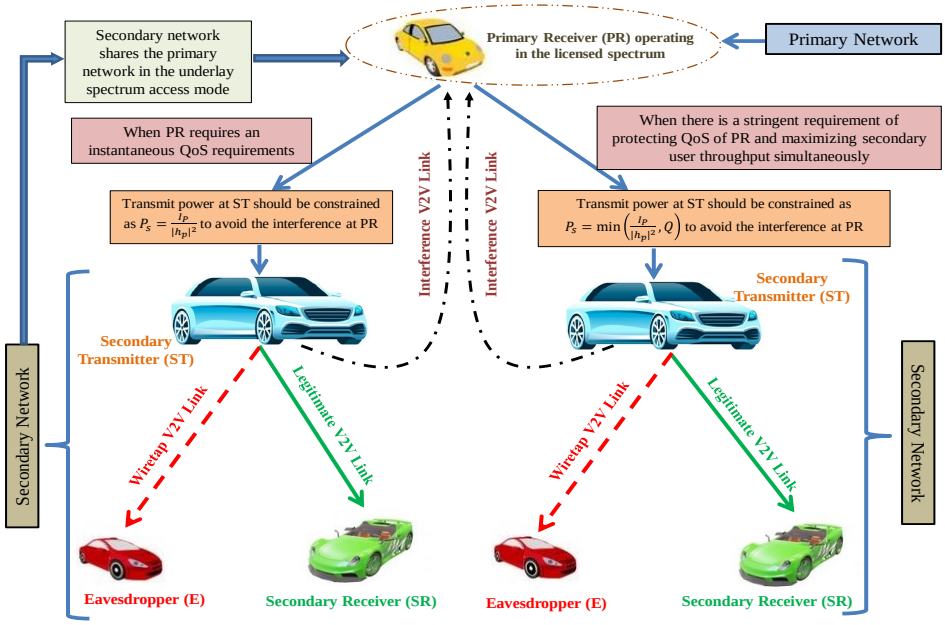

Figure 2. Overall representation of the considered CRVN framework.

2.4. Practical Applicability

The proposed analysis of the considered system by taking two power control strategies and double-Rayleigh fading channels into account can be applicable for various practical scenarios, as stated below.

- The proposed analysis under **Strategy I** can be more appropriate under the practical scenario when the service provided by the primary user has an instantaneous QoS requirement.
- The proposed analysis under **Strategy II** is suitable under the practical scenario when there is a stringent requirement of protecting QoS of primary user and maximizing secondary user throughput simultaneously.
- The proposed analysis under double-Rayleigh fading assumption is practically applicable for vehicular communication scenarios in rush-hour urban traffic.
- The proposed analysis is also applicable for the scenario when one mobile terminal is located indoors in low-ascent building, and the another mobile terminal is placed outdoors, as the cascaded fading envelope distribution is found suitable under such scenario.
- The proposed analysis can be applied to the scenario when the mobile nodes are located in a relatively dense scattering (e.g., vegetation) environment, as the channel between them will be a good fit for cascaded fading distribution.

It is to be noted that compared to the existing similar works presented in [44,45,47], the complexity of this work can be discussed as follows; (i) the paper [44] adopted N*Nakagami-m fading channels and [45] adopted cascaded fading channels, which implies that the cascading degree of order N imposes more computational resources in examining the performance of the considered system. Whereas this paper considers the double-Rayleigh fading channels, which allows one to operate with less computational resources (because of having cascading degree of order (2) while evaluating the system performance, without the loss of information, and (ii) the work presented in [47] considered the multiple-antennas at the legitimate destination and eavesdropper, which require several parallel radio frequency chains in the front-end architecture of the receiver. This increases the power consumption, complexity, cost, and size of the system, due to which the direct implementation of such systems is hindered in battery-operated sources, such as in wireless sensor applications. That said, this paper considers the single-antenna terminals which drastically reduce the system's complexity and can be efficiently applicable for the resource constraint devices.

Furthermore, we evaluate the SOP and ESC for Strategy I and Strategy II under double-Rayleigh fading channels, in what follows. Note that SOP is an appropriate metric for the block fading channels (such as, double-Rayleigh fading channels under multiple scattering phenomenon for vehicular scenario), where the maximum rate of reliable communication is supported only by the one channel realization. On the other hand, ESC is the maximum mutual information averaged over many independent fades of the channel. With the block fading, the time average should converge to the same limit for almost all channel realizations of the fading process (known as ergodicity); thus, ESC is only the long-term time average rate achieved, and not on how fast that rate fluctuates over the time. Therefore, we can evaluate the SOP and ESC in the one system assumption.

3. Exact and Asymptotic SOP Analyses under Strategies I and II

In the consequent subsections, we derive an analytical expression for a key secrecy metric and SOP to quantify the considered network secrecy performance under both Strategies I and II. Further, to provide meaningful insights, we also provide asymptotic SOP analysis under both the scenarios for the considered system.

3.1. Strategy I: Single-Power Constraint of the Interference on the PR

3.1.1. Exact Analysis for SOP

The SOP can be defined as the probability that the achievable secrecy capacity is less than a predefined secrecy transmission rate $\mathcal{R}_s$ (in bps/Hz). We can mathematically express the SOP under Strategy I as

$$\mathcal{P}_{out}^{sec,\mathrm{I}} = \Pr[\max\{\mathcal{C}_m^{\mathrm{I}} - \mathcal{C}_e^{\mathrm{I}}, 0\} < \mathcal{R}_s]. \tag{10}$$

Note that when $\mathcal{C}_m^{\mathrm{I}} \leq \mathcal{C}_e^{\mathrm{I}}$, the secrecy is compromised, i.e., $\mathcal{P}_{out}^{sec,\mathrm{I}} = 1$. Therefore, we analyze the SOP when $\mathcal{C}_m^{\mathrm{I}} > \mathcal{C}_e^{\mathrm{I}}$ as

$$\begin{aligned}\mathcal{P}_{out}^{sec,\mathrm{I}} &= \Pr[\mathcal{C}_m^{\mathrm{I}} - \mathcal{C}_e^{\mathrm{I}} < \mathcal{R}_s] = \Pr\left[\frac{1+\frac{\rho|h_m|^2}{|h_p|^2}}{1+\frac{\rho|h_e|^2}{|h_p|^2}} < \eta\right] \\ &= 1 - \Pr\left[|h_e|^2 < \frac{|h_m|^2}{\eta} - \frac{(\eta-1)|h_p|^2}{\eta\rho}\right].\end{aligned} \tag{11}$$

Since $|h_m|^2$ and $|h_e|^2$ consist of a common channel gain $|h_p|^2$; therefore, the SOP under this strategy can be expressed as

$$\mathcal{P}_{out}^{sec,\mathrm{I}} = 1 - \int_0^\infty \underbrace{\left[\int_{\frac{(\eta-1)w}{\rho}}^\infty F_{|h_e|^2}\left(\frac{y}{\eta} - \frac{(\eta-1)w}{\eta\rho}\right) f_{|h_m|^2}(y)dy\right]}_{\triangleq \mathbb{I}_1} f_{|h_p|^2}(w)dw, \tag{12}$$

where $\eta = 2^{\mathcal{R}_s}$ is the secrecy target threshold. To evaluate the SOP under Strategy I in (12), we first need to simplify the inner integral $\mathbb{I}_1$, which is given as per the following theorem.

Theorem 1. *The inner integral $\mathbb{I}_1$ of (12) can be expressed as*

$$\mathbb{I}_1 = \mathbb{I}_{1a} - \mathbb{I}_{1b}, \tag{13}$$

where

$$\mathbb{I}_{1a} = 2\sqrt{\frac{(\eta-1)w}{\rho\lambda_m}} K_1\left(2\sqrt{\frac{(\eta-1)w}{\rho\lambda_m}}\right), \tag{14}$$

$$\mathbb{I}_{1b} = \frac{\sqrt{\lambda_m}}{\sqrt{\eta\lambda_e}} \sum_{k=0}^{\infty} \frac{(-1)^k}{k!} \left(\frac{\eta-1}{\rho\lambda_m}\right)^k w^k G_{3,3}^{2,3}\left(\frac{\lambda_m}{\eta\lambda_e}\middle|_{\frac{1}{2},-\frac{1}{2},k-\frac{1}{2}}^{-\frac{1}{2},k-\frac{1}{2},k-\frac{1}{2}}\right), \tag{15}$$

where $\lambda_m = \Omega_m^2$ and $\lambda_e = \Omega_e^2$.

Proof. The proof is given in Appendix A. □

Furthermore, invoking (14) and (15) along with the PDF of $|h_p|^2$ into (12), we can represent the SOP as

$$\begin{aligned}\mathcal{P}_{out}^{sec,\mathrm{I}}(\eta) = 1 &- \frac{4}{\lambda_p}\sqrt{\frac{(\eta-1)}{\rho\lambda_m}}\left[\int_0^\infty w^{\frac{1}{2}} K_0\left(2\sqrt{\frac{w}{\lambda_p}}\right) K_1\left(2\sqrt{\frac{(\eta-1)w}{\rho\lambda_m}}\right) dw\right] \\ &+ \frac{2\sqrt{\lambda_m}}{\lambda_p\sqrt{\eta\lambda_e}} \sum_{k=0}^{\infty} \frac{(-1)^k}{k!} \left(\frac{\eta-1}{\rho\lambda_m}\right)^k G_{3,3}^{2,3}\left(\frac{\lambda_m}{\eta\lambda_e}\middle|_{\frac{1}{2},-\frac{1}{2},k-\frac{1}{2}}^{-\frac{1}{2},k-\frac{1}{2},k-\frac{1}{2}}\right)\left[\int_0^\infty w^k K_0\left(2\sqrt{\frac{w}{\lambda_p}}\right) dw\right],\end{aligned} \tag{16}$$

where $\lambda_p = \Omega_p^2$. Then, the first integral in (16) can be simplified using (eq. (03.04.26.0009.01)) of [49] and (eq. (07.34.21.0011.01)) of [49], and the second integral in (16) can be evaluated by

first using the transformation of variables $\frac{w}{\lambda_p} = \frac{t^2}{4}$ and then applying (eq. (6.561.16)) of [48]. Consequently, the SOP under Strategy I, $\mathcal{P}_{out}^{sec,\mathrm{I}}(\eta)$, can be expressed as

$$\mathcal{P}_{out}^{sec,\mathrm{I}}(\eta) = 1 - \sqrt{\frac{(\eta-1)\lambda_p}{\rho\lambda_m}} G_{2,2}^{2,2}\left(\frac{(\eta-1)\lambda_p}{\rho\lambda_m}\Big|_{\frac{1}{2},-\frac{1}{2}}^{-\frac{1}{2},-\frac{1}{2}}\right) + \frac{\sqrt{\lambda_m}}{\sqrt{\eta\lambda_e}} \sum_{k=0}^{\infty} \frac{(-1)^k}{k!} \left(\frac{\eta-1}{\rho\lambda_m}\right)^k \lambda_p^k (\Gamma(k+1))^2 G_{3,3}^{2,3}\left(\frac{\lambda_m}{\eta\lambda_e}\Big|_{\frac{1}{2},-\frac{1}{2},k-\frac{1}{2}}^{-\frac{1}{2},k-\frac{1}{2},k-\frac{1}{2}}\right). \quad (17)$$

Remark 1. *The SOP in (17) mainly consists of powers, complete Gamma function, and Meijer-G functions, containing maximum interference threshold limit (I_p), secrecy target threshold (η), and average channel gains (Ω_m, Ω_e, and Ω_p), which can effectively be evaluated using Mathematica software. The SOP behavior for various values of channel/system parameters is shown numerically in Section 5.*

Remark 2. *We infer that the SOP expression in (17) depends on the average channel gain of the interference link (ST → PR), i.e., $\lambda_p = \Omega_p^2$, which implies that the SOP performance degrades as λ_p increases and vice versa. This is due to the fact that the power at ST reduces with the increased λ_p, as also validated numerically in Section 5.*

3.1.2. Asymptotic Analysis for SOP

To gain more insights into the achievable secrecy diversity order of the considered system, we focus on the asymptotic analysis in the high average channel fading gains regime. Here, we specifically investigated two separate scenarios: (1) when $\lambda_m \to \infty$ and λ_e is fixed. In this scenario, the quality of the legitimated channel is better than the quality of wiretap channel (i.e., E is located far away from ST), and (2) when $\lambda_m \to \infty$ and $\lambda_e \to \infty$, where both the legitimated and wiretap channels experience similar fading conditions. Note that there may be another scenario where λ_m is fixed and $\lambda_e \to \infty$. However, this case significantly strengthens the quality of wiretap link and increases the probability of successful eavesdropping, as E, which implies that the secrecy diversity order becomes zero.

When $\lambda_m \to \infty$ and fixed λ_e

Under this scenario, we simplify (17) by ignoring the higher order infinitesimal terms to obtain the asymptotic SOP as

$$\mathcal{P}_{out,asy}^{sec,\mathrm{I}}(\eta) \underset{\lambda_m\to\infty}{\simeq} 1 - \sqrt{\frac{(\eta-1)\lambda_p}{\rho\lambda_m}} G_{2,2}^{2,2}\left(\frac{(\eta-1)\lambda_p}{\rho\lambda_m}\Big|_{\frac{1}{2},-\frac{1}{2}}^{-\frac{1}{2},-\frac{1}{2}}\right) + \frac{\sqrt{\lambda_m}}{\sqrt{\eta\lambda_e}} G_{3,3}^{2,3}\left(\frac{\lambda_m}{\eta\lambda_e}\Big|_{\frac{1}{2},-\frac{1}{2},-\frac{1}{2}}^{-\frac{1}{2},-\frac{1}{2},-\frac{1}{2}}\right). \quad (18)$$

Remark 3. *Secrecy diversity order analysis: When $\lambda_m \to \infty$ and λ_e are fixed, the secrecy diversity order can be defined as the ratio of asymptotic SOP to average channel gain of the main link λ_m, yielding*

$$\mathbb{G}_{\mathbb{D}} = -\lim_{\lambda_m\to\infty} \frac{\log \mathcal{P}_{out,asy}^{sec,I}(\eta)}{\log \lambda_m}. \quad (19)$$

From (18), we can observe that the term $G_{3,3}^{2,3}\left(\frac{\lambda_m}{\eta\lambda_e}\Big|_{\frac{1}{2},-\frac{1}{2},-\frac{1}{2}}^{-\frac{1}{2},-\frac{1}{2},-\frac{1}{2}}\right)$ converges to zero very quickly as $\lambda_m \to \infty$ for fixed η and λ_e, and hence, it can be ignored from (18) while evaluating the

secrecy diversity order. Consequently, we can re-express the resultant asymptotic SOP via (eq. (07.34.03.0871.01)) of [49], and after some simplifications, as

$$\mathcal{P}_{out,asy}^{sec,I}(\eta) \simeq 1 - \frac{\mathcal{A}(\eta)}{\lambda_m} {}_2\tilde{F}_1\left(2,2,3;1-\frac{\mathcal{A}(\eta)}{\lambda_m}\right), \tag{20}$$

where $\mathcal{A}(\eta) = \frac{(\eta-1)\lambda_p}{\rho}$. *Now, invoking (20) into (19), and by simplifying* ${}_2\tilde{F}_1(a,b,c;z)$ *using (eq. (07.24.26.0003.01)) of [49] and (eq. (07.23.03.3573.01)) of [49], and after some involved simplifications, we can express the secrecy diversity order as*

$$\mathbb{G}_{\mathbb{D}} = -\lim_{\lambda_m \to \infty} \frac{\log\left[1 - \frac{\lambda_m\left(-\mathcal{A}(\eta)+\lambda_m+\mathcal{A}(\eta)\log\left(\frac{\mathcal{A}(\eta)}{\lambda_m}\right)\right)}{(\mathcal{A}(\eta)-\lambda_m)^2}\right]}{\log \lambda_m}, \tag{21}$$

which can be further simplified with the assistance of L'Hospital's rule to obtain the secrecy diversity order as

$$\mathbb{G}_{\mathbb{D}} = 1. \tag{22}$$

Therefore, we can infer that the system can achieve a secrecy diversity order of 1 and does not depend on the parameters related to the wiretap link (i.e., ST → E) and interference link (i.e., ST → PR).

Remark 4. *The convergence behavior of secrecy diversity order is shown in Figure 3, from which it can be observed that the secrecy diversity order converges to its asymptotical value of 1 over double-Rayleigh fading channels, irrespective of the wiretap link strength* λ_e, ρ, *and* λ_p. *However, the convergence gets slower because of the involved double-Rayleigh fading channels. We can also infer that the convergence further slows down as* λ_e *and/or* λ_p *increases and vice versa.*

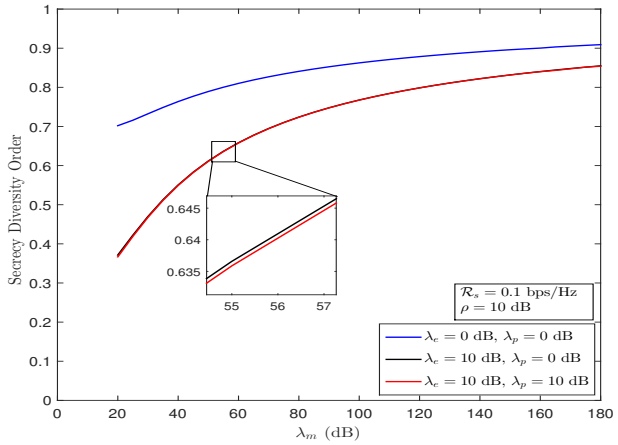

Figure 3. Secrecy diversity order behavior of the considered system under Strategy I for $\lambda_m \to \infty$ and fixed λ_e.

When $\lambda_m \to \infty$ and $\lambda_e \to \infty$

The asymptotic SOP for this case can be evaluated as per the following theorem.

Theorem 2. *The asymptotic SOP for the case when* $\lambda_m \to \infty$ *and* $\lambda_e \to \infty$ *(as the average channel gains of both the legitimated link and wiretap link are improved simultaneously) under double-Rayleigh fading channels can be expressed as*

$$\mathcal{P}_{out,asy}^{sec,I}(\eta) \underset{\lambda_m,\lambda_e \to \infty}{\simeq} 1 - \frac{\sqrt{\eta\lambda_e}}{\sqrt{\lambda_m}} G_{2,2}^{2,2}\left(\frac{\eta\lambda_e}{\lambda_m}\middle|_{\frac{1}{2},-\frac{1}{2}}^{-\frac{1}{2},-\frac{1}{2}}\right). \tag{23}$$

Proof. Under $\lambda_m \to \infty$ and $\lambda_e \to \infty$, we can approximate the SOP as $\mathcal{P}_{out}^{sec,\mathrm{I}}(\eta) = \Pr\left[\frac{1+\frac{\rho|h_m|^2}{|h_p|^2}}{1+\frac{\rho|h_e|^2}{|h_p|^2}} < \eta\right] \approx \Pr\left[\frac{|h_m|^2}{|h_e|^2} < \eta\right]$, which can be further expressed in the integral form as $\mathcal{P}_{out,asy}^{sec,\mathrm{I}}(\eta) \approx \int_0^\infty F_{|h_m|^2}(\eta y) f_{|h_e|^2}(y) dy$. Now, invoking the CDF of $|h_m|^2$ and the PDF of $|h_e|^2$ and simplifying with the aid of (eq. (07.34.21.0011.01)) of [49], we can obtain the asymptotic SOP expression, as given in (23). □

Remark 5. *From (23), we can infer that the secrecy outage floor occurs for fixed ratio $\frac{\lambda_e}{\lambda_m}$ (as $\lambda_m \to \infty$ and $\lambda_e \to \infty$), and hence, the secrecy diversity order cannot be attained. In addition, it is also worthwhile to note that the system's secrecy diversity order can also be realized by analyzing the asymptotic SOP behavior for the case when $\rho = \frac{I_p}{N_0} \to \infty$. Under this case, we can have the same asymptotic SOP expression as evaluated in (23), since ρ at both D and E are increased simultaneously. We can further reveal that the SOP expression under this case achieves an error floor and results in a zero secrecy diversity order.*

3.2. Strategy II: Combined Power Constraint of the Interference at the PR and Maximum Transmit Power at the ST

3.2.1. Exact Analysis for SOP

Considering $\mathcal{C}_m^{\mathrm{II}} > \mathcal{C}_e^{\mathrm{II}}$ and using (8) and (9), the SOP can be expressed as

$$\begin{aligned}\mathcal{P}_{out}^{sec,\mathrm{II}}(\eta) &= \Pr\left[\frac{1+\min\left(\frac{\rho}{|h_p|^2},\rho_1\right)|h_m|^2}{1+\min\left(\frac{\rho}{|h_p|^2},\rho_1\right)|h_e|^2} < \eta\right] \\ &= \underbrace{\Pr\left[\frac{1+\rho_1|h_m|^2}{1+\rho_1|h_e|^2} < \eta\right]\Pr\left[\frac{\rho}{\rho_1} \geq |h_p|^2\right]}_{\triangleq \Theta_1(\eta)} + \underbrace{\Pr\left[\frac{1+\frac{\rho|h_m|^2}{|h_p|^2}}{1+\frac{\rho|h_e|^2}{|h_p|^2}} < \eta, \frac{\rho}{\rho_1} < |h_p|^2\right]}_{\triangleq \Theta_2(\eta)}. \end{aligned} \tag{24}$$

Further, the SOP in (24) can be simplified as per Theorem 3.

Theorem 3. *The exact expression for the SOP under Strategy II using (24) can be expressed as*

$$\mathcal{P}_{out}^{sec,II}(\eta) = \Theta_1(\eta) + \Theta_2(\eta), \tag{25}$$

where

$$\begin{aligned}\Theta_1(\eta) = &\left[1 - 2\sqrt{\frac{\eta-1}{\rho_1\lambda_m}}K_1\left(2\sqrt{\frac{\eta-1}{\rho_1\lambda_m}}\right) + \frac{\sqrt{\lambda_m}}{\sqrt{\eta\lambda_e}}\sum_{k=0}^{\infty}\frac{(-1)^k}{k!}\left(\frac{\eta-1}{\rho_1\lambda_m}\right)^k\right. \\ &\left.\times G_{3,3}^{2,3}\left(\frac{\lambda_m}{\eta\lambda_e}\middle|_{\frac{1}{2},-\frac{1}{2},k-\frac{1}{2}}^{-\frac{1}{2},k-\frac{1}{2},k-\frac{1}{2}}\right)\right]\left[1 - \frac{2\sqrt{\rho}}{\sqrt{\rho_1\lambda_p}}K_1\left(\frac{2\sqrt{\rho}}{\sqrt{\rho_1\lambda_p}}\right)\right],\end{aligned} \tag{26}$$

$$\begin{aligned}\Theta_2(\eta) = &\frac{2\sqrt{\rho}}{\sqrt{\rho_1\lambda_p}}K_1\left(\frac{2\sqrt{\rho}}{\sqrt{\rho_1\lambda_p}}\right) - \frac{4}{\lambda_p}\sqrt{\frac{\eta-1}{\rho\lambda_m}}\left[\frac{\lambda_p^{\frac{3}{2}}}{4}G_{2,2}^{2,2}\left(\frac{(\eta-1)\lambda_p}{\rho\lambda_m}\middle|_{\frac{1}{2},-\frac{1}{2}}^{-\frac{1}{2},-\frac{1}{2}}\right)\right. \\ &\left. - \frac{\rho^{\frac{3}{2}}}{2\rho_1^{\frac{3}{2}}}\sum_{i=1}^{N}g_i t_i^2 G_{0,2}^{2,0}\left(\frac{(\eta-1)t_i^2}{\rho_1\lambda_m}\middle|\frac{1}{2},-\frac{1}{2}\right)G_{0,2}^{2,0}\left(\frac{\rho t_i^2}{\rho_1\lambda_p}\middle|0,0\right)\right] + \frac{\sqrt{\lambda_m}}{\sqrt{\eta\lambda_e}\lambda_p}\sum_{k=0}^{\infty}\frac{(-1)^k}{k!} \\ &\times\left(\frac{\rho}{\rho_1}\right)^{k+1}\left(\frac{\eta-1}{\rho\lambda_m}\right)^k G_{1,3}^{3,0}\left(\frac{\rho}{\rho_1\lambda_p}\middle|_{-k-1,0,0}^{-k}\right)G_{3,3}^{2,3}\left(\frac{\lambda_m}{\eta\lambda_e}\middle|_{\frac{1}{2},-\frac{1}{2},k-\frac{1}{2}}^{-\frac{1}{2},k-\frac{1}{2},k-\frac{1}{2}}\right),\end{aligned} \tag{27}$$

where $g_i = \left\{\sum_{j=0}^{N-1}[q_j(t_i)]^2\right\}^{-1}$ *and* t_i, $(i = 1, \cdots, N)$ *are the weights and zeros of* $N-$*order Gauss–Lobatto's polynomial (eq. (25.4.33)) of [54], respectively, and* $q_N(t) = \sqrt{2N+3}P_N^{(2,0)}(1-2t)$ *with* $P_N^{(2,0)}$ *as the Jacobi polynomial.*

Proof. The detailed analysis is given in Appendix B. □

Remark 6. *We highlight that (25) mainly involves powers, Meijer-G functions, and modified Bessel function of the second kind, consisting of network parameters* I_p, Q, η, Ω_m, Ω_e, *and* Ω_p, *which can readily be evaluated by the help of Mathematica software, as shown via numerical results in Section 5.*

Remark 7. *The SOP expression in (25) consists of Gauss–Lobatto's series expansion of order* N, *which converges to an arbitrarily accurate approximation by selecting the appropriate value of* N. *For instance, consider the term of (27), i.e.,* $\mathcal{Z} = G_{0,2}^{2,0}\left(\frac{(\eta-1)t_i^2}{\rho_1\lambda_m}\middle|\frac{1}{2},-\frac{1}{2}\right)G_{0,2}^{2,0}\left(\frac{\rho t_i^2}{\rho_1\lambda_p}\middle|0,0\right)$. *Note that the Meijer-G function can be expressed in terms of* v*-th order modified Bessel function of second kind using the transformation* $K_v(x) = \frac{1}{2}G_{0,2}^{2,0}(\frac{x^2}{4}\middle|\frac{v}{2},-\frac{v}{2})$ *(eq. (03.04.26.0009.01)) of [49], and* $K_v(x)$ *can further be expressed as* $\sqrt{\pi}e^{-x}(2x)^v\Psi(v+0.5,1+2v;2x)$ *(eq. (9.328)) of [48]. Realizing such representations in* $\mathcal{Z}$, *we can get* $\mathcal{Z} = 16\pi\sqrt{\frac{(\eta-1)t_i^2}{\rho_1\lambda_m}}e^{-2\sqrt{\frac{(\eta-1)t_i^2}{\rho_1\lambda_m}}}e^{-2\sqrt{\frac{\rho t_i^2}{\rho_1\lambda_p}}}\Psi\left(\frac{1}{2},1;4\sqrt{\frac{\rho t_i^2}{\rho_1\lambda_p}}\right)$ $\times\Psi\left(\frac{3}{2},3;4\sqrt{\frac{(\eta-1)t_i^2}{\rho_1\lambda_m}}\right)$. *From which, it can be clearly seen that the exponential terms in* $\mathcal{Z}$ *implies that (27) decreases rapidly as* N *increases, and only a few values of* N *are sufficient to obtain satisfactory accuracy, as also shown numerically in Section 5.*

3.2.2. Asymptotic Analysis for SOP

We analyze the asymptotic SOP performance of the considered system under Strategy II for two separate scenarios, i.e., (1) when $\lambda_m \to \infty$ and λ_e is fixed and (2) when $\lambda_m \to \infty$ and $\lambda_e \to \infty$, in what follows.

When $\lambda_m \to \infty$ and fixed λ_e

For $\lambda_m \to \infty$ and fixed λ_e, by neglecting the higher order infinitesimal terms in (26) and (27), and then invoking the resultant expressions on (25), the asymptotic SOP expression can be given as

$$\begin{aligned}\mathcal{P}_{out,asy}^{sec,II}(\eta) \simeq &\left[1-2\sqrt{\frac{\eta-1}{\rho_1\lambda_m}}K_1\left(2\sqrt{\frac{\eta-1}{\rho_1\lambda_m}}\right)+\frac{\sqrt{\lambda_m}}{\sqrt{\eta\lambda_e}}G_{3,3}^{2,3}\left(\frac{\lambda_m}{\eta\lambda_e}\middle|_{\frac{1}{2},-\frac{1}{2},-\frac{1}{2}}^{-\frac{1}{2},-\frac{1}{2},-\frac{1}{2}}\right)\right]\\ &\times\left[1-\frac{2\sqrt{\rho}}{\sqrt{\rho_1\lambda_p}}K_1\left(\frac{2\sqrt{\rho}}{\sqrt{\rho_1\lambda_p}}\right)\right]+\frac{2\sqrt{\rho}}{\sqrt{\rho_1\lambda_p}}K_1\left(\frac{2\sqrt{\rho}}{\sqrt{\rho_1\lambda_p}}\right)-\sqrt{\frac{(\eta-1)\lambda_p}{\rho\lambda_m}}\\ &\times G_{2,2}^{2,2}\left(\frac{(\eta-1)\lambda_p}{\rho\lambda_m}\middle|_{\frac{1}{2},-\frac{1}{2}}^{-\frac{1}{2},-\frac{1}{2}}\right)-\frac{2\rho}{\rho_1^{\frac{3}{2}}\lambda_p}\sqrt{\frac{(\eta-1)}{\lambda_m}}\sum_{i=1}^{N}g_it_i^2G_{0,2}^{2,0}\left(\frac{(\eta-1)t_i^2}{\rho_1\lambda_m}\middle|\frac{1}{2},-\frac{1}{2}\right)\\ &\times G_{0,2}^{2,0}\left(\frac{\rho t_i^2}{\rho_1\lambda_p}\middle|0,0\right)+\frac{\sqrt{\lambda_m}}{\sqrt{\eta\lambda_e}\lambda_p}G_{1,3}^{3,0}\left(\frac{\rho}{\rho_1\lambda_p}\middle|_{-k-1,0,0}^{-k}\right)G_{3,3}^{2,3}\left(\frac{\lambda_m}{\eta\lambda_e}\middle|_{\frac{1}{2},-\frac{1}{2},-\frac{1}{2}}^{-\frac{1}{2},-\frac{1}{2},-\frac{1}{2}}\right).\end{aligned} \tag{28}$$

Remark 8. *By following a similar approach used to evaluate (22), we can infer from (28) that the secrecy diversity order of 1 can also be achieved under Strategy II. Furthermore, Figure 4 shows that the secrecy diversity order convergence slows down because of the involvement of double-Rayleigh fading channels, for various values of* λ_e *and* ρ_1.

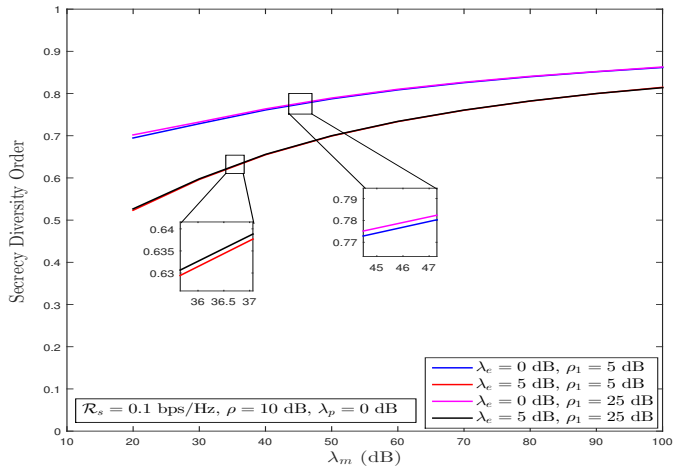

Figure 4. System's secrecy diversity order behavior under Strategy II for $\lambda_m \to \infty$ and fixed λ_e.

When $\lambda_m \to \infty$ and $\lambda_e \to \infty$

Using (24), the asymptotic SOP can be expressed as

$$\mathcal{P}_{out,asy}^{sec,\mathrm{II}}(\eta) \underset{\lambda_m,\lambda_e\to\infty}{\simeq} \Pr\left[\frac{|h_m|^2}{|h_e|^2} < \eta\right]\left(\Pr\left[|h_p|^2 \le \frac{\rho}{\rho_1}\right] + \Pr\left[|h_p|^2 > \frac{\rho}{\rho_1}\right]\right) = \int_0^\infty F_{|h_m|^2}(\eta y) f_{|h_e|^2}(y) dy. \tag{29}$$

Now, invoking the CDF of $|h_m|^2$ and the PDF of $|h_e|^2$ into (29), and simplifying it via (eq. (07.34.21.0011.01)) of [49], we can obtain the asymptotic SOP expression under the scenario when $\lambda_m \to \infty$ and $\lambda_e \to \infty$ as

$$\mathcal{P}_{out,asy}^{sec,\mathrm{II}}(\eta) \underset{\lambda_m,\lambda_e\to\infty}{\simeq} 1 - \frac{\sqrt{\eta\lambda_e}}{\sqrt{\lambda_m}} G_{2,2}^{2,2}\left(\frac{\eta\lambda_e}{\lambda_m}\middle|_{\frac{1}{2},-\frac{1}{2}}^{-\frac{1}{2},-\frac{1}{2}}\right). \tag{30}$$

Remark 9. *According to (30), the asymptotic SOP in this scenario depends on the wiretap channel gain to the legitimated channel gain ratio, i.e., $\frac{\lambda_e}{\lambda_m}$. Therefore, we can infer that the secrecy outage floor occurs, which yields into a zero secrecy diversity order.*

3.2.3. Impact of Maximum Tolerable Interference Level I_P and Maximum Secondary Transmitter Power Q

It can be observed in (25) that the SOP expression under Strategy II also depends on the maximum tolerable interference level I_P and maximum secondary transmitter power Q. Therefore, in order to study the impact of I_P and Q on the system's secrecy diversity gain, two cases, i.e., Case 1: when $\rho = \mu\rho_1$ and Case 2: when $\rho \neq \mu\rho_1$, where $\rho \triangleq \frac{I_P}{N_0}$ and $\rho_1 \triangleq \frac{Q}{N_0}$ are investigated in the following.

Case 1 ($\rho = \mu\rho_1$)

When ρ is proportional to ρ_1, i.e., $\rho = \mu\rho_1$, where μ is a positive constant. In the high SNR regime, i.e., $\rho_1 \to \infty$, the SOP in (25) can be approximated by applying the fact $K_1(x) \underset{x\to 0}{\approx} \frac{1}{x}$ (eq. (9.6.9)) of [54] and ignoring the higher order infinitesimal terms at high SNR, as

$$rl\mathcal{P}_{out}^{sec,\mathrm{II}}(\eta) \underset{\rho=\mu\rho_1,\rho_1\to\infty}{\approx} \frac{\sqrt{\lambda_m}}{\sqrt{\eta\lambda_e}} G_{3,3}^{2,3}\left(\frac{\lambda_m}{\eta\lambda_e}\Big|_{\frac{1}{2},-\frac{1}{2},-\frac{1}{2}}^{-\frac{1}{2},-\frac{1}{2},-\frac{1}{2}}\right)\left(1-\frac{2\sqrt{\rho}}{\sqrt{\lambda_p\rho_1}}K_1\left(\frac{2\sqrt{\rho}}{\sqrt{\lambda_p\rho_1}}\right)\right)+\frac{2\sqrt{\rho}}{\sqrt{\lambda_p\rho_1}} \times K_1\left(\frac{2\sqrt{\rho}}{\sqrt{\lambda_p\rho_1}}\right) frac\sqrt{\lambda_m}\rho\sqrt{\eta\lambda_e}\lambda_p\rho_1 G_{1,3}^{3,0}\left(\frac{\rho}{\rho_1\lambda_p}\Big|_{-1,0,0}^{0}\right) G_{3,3}^{2,3}\left(\frac{\lambda_m}{\eta\lambda_e}\Big|_{\frac{1}{2},-\frac{1}{2},-\frac{1}{2}}^{-\frac{1}{2},-\frac{1}{2},-\frac{1}{2}}\right). \tag{31}$$

Remark 10. *We can see from (31) that the SOP is independent of SNR ρ_1 with fixed ratio $\frac{\rho}{\rho_1}$, which implies that the secrecy diversity gain cannot be achieved in this case.*

Case 2 ($\rho \neq \mu\rho_1$)

When $\rho \neq \mu\rho_1$ and ρ is a constant. At high SNR range, i.e., $\rho_1 \to \infty$, we can approximate the SOP expression in (25) by using the fact $K_1(x) \underset{x\to 0}{\approx} \frac{1}{x}$ (eq. (9.6.9)) of [54] and eliminating the higher order terms under high SNR ($\rho_1 \to \infty$) regime, as

$$\mathcal{P}_{out}^{sec,\mathrm{II}}(\eta) \underset{\rho\neq\mu\rho_1,\rho_1\to\infty}{\approx} 1-\frac{\sqrt{(\eta-1)\lambda_p}}{\sqrt{\rho\lambda_m}} G_{2,2}^{2,2}\left(\frac{(\eta-1)\lambda_p}{\rho\lambda_m}\Big|_{\frac{1}{2},-\frac{1}{2}}^{-\frac{1}{2},-\frac{1}{2}}\right). \tag{32}$$

Remark 11. *From (32), it is noted that the SOP only depends on a constant ρ, although $\rho_1 \to \infty$. This implies that the secrecy diversity gain reduces to zero in this case as well.*

4. ESC Analysis under Strategies I and II

4.1. Strategy I: Single-Power Constraint of the Interference on the PR

The instantaneous secrecy capacity for the considered secure CRVN under Strategy I can be given as

$$\begin{aligned}\mathcal{C}_{sec}^{\mathrm{I}} &= \mathcal{C}_m^{\mathrm{I}} - \mathcal{C}_e^{\mathrm{I}} \\ &= \log_2(1+\Lambda_m^{\mathrm{I}}) - \log_2(1+\Lambda_e^{\mathrm{I}}).\end{aligned} \tag{33}$$

By averaging the instantaneous secrecy capacity expression over the distributions of the end-to-end SNRs Λ_m^{I} and Λ_e^{I} under Strategy I, the ESC can be expressed as

$$\begin{aligned}\overline{\mathcal{C}}_{sec}^{\mathrm{I}} &= \mathbb{E}[\log_2(1+\Lambda_m^{\mathrm{I}}) - \log_2(1+\Lambda_e^{\mathrm{I}})], \\ &= \frac{1}{\ln(2)}\mathbb{E}\left[\log\left(1+\frac{\rho|h_m|^2}{|h_p|^2}\right) - \log\left(1+\frac{\rho|h_e|^2}{|h_p|^2}\right)\right],\end{aligned} \tag{34}$$

which can be evaluated as per the following theorem.

Theorem 4. *The exact ESC expression for the considered system under Strategy I over double-Rayleigh fading channels can be represented as*

$$\begin{aligned}\overline{\mathcal{C}}_{sec}^{I} = \frac{1}{\ln(2)}\sum_{i=1}^{U} w_i e^{t_i}\Bigg[&\frac{t_i}{\rho\lambda_m} G_{2,4}^{4,1}\left(\frac{t_i}{\rho\lambda_m}\Big|_{0,0,-1,-1}^{-1,0}\right) \\ &- t_i^{\frac{3}{2}}\frac{\sqrt{\lambda_m}+\sqrt{\lambda_e}}{\rho^{\frac{3}{2}}\lambda_m\lambda_e}\mathcal{S}\left(\frac{t_i}{\rho}\right)\Bigg]\frac{1}{\lambda_p} G_{0,2}^{2,0}\left(\frac{t_i}{\lambda_p}\Big|0,0\right),\end{aligned} \tag{35}$$

where $\mathcal{S}(a) = G_{2,2:0,2:0,2}^{2,1:2,0:2,0}\left(\begin{matrix}-\frac{3}{2},-\frac{1}{2}\\ -\frac{3}{2},-\frac{3}{2}\end{matrix}\Big|0,0\Big|\frac{1}{2},-\frac{1}{2}\Big|\frac{a}{\lambda_m},\frac{a}{\lambda_e}\right)$. $w_i = \frac{t_i}{((U+1)L_{U+1}(t_i))^2}$ *and* t_i, $(i=1,\cdots,U)$ *are the weights and zeros of $U-$order Gauss–Laguerre polynomial (i.e., $L_U(t)$) (eq. (25.5.45)) of [54].*

Proof. See Appendix C for the proof. □

Remark 12. *It can be seen from (35) that the ESC expression consists of exponential, powers, and Meijer-G function, involving system parameters I_p, η, Ω_m, Ω_e, and Ω_p, and as such, it can be readily evaluated. In addition, the ESC expression in (35) consists of extended generalized bivariate Meijer-G function, which is not easily available in the Mathematica software computational package, but the work in [55] has proposed an efficient and accurate implementation in Mathematica. Moreover, from (35), we can see that the ESC expression consists of Gauss–Laguerre series expansion, which is convergent. We can achieve the accurate results by appropriately selecting the value of U (can be analytically proved as in Gauss–Lobatto's polynomial in Remark 7), as also shown numerically in Section 5.*

Remark 13. *Using (34) for $|h_m|^2 \geq |h_e|^2$, the ESC under strategy I can be expressed as*

$$\overline{C}_{sec}^{I} = \frac{1}{\ln(2)} \int_0^\infty f_{|h_e|^2}(|h_e|^2) \int_{|h_e|^2}^\infty \ln\left(\frac{1+\frac{\rho|h_m|^2}{|h_p|^2}}{1+\frac{\rho|h_e|^2}{|h_p|^2}}\right) \times f_{|h_m|^2}(|h_m|^2) d|h_m|^2 d|h_e|^2. \tag{36}$$

Substituting $|h_m|^2 = \lambda_m x$ and $|h_e|^2 = \lambda_e y$ into (36), and applying the scenario when the average power gains of both the main and wiretap channels go to infinity (i.e., $\lambda_m \to \infty$ and $\lambda_e \to \infty$), and after some involved mathematical simplifications, we can express (36) as

$$\overline{C}_{sec}^{I} \approx \frac{4}{\ln(2)} \int_0^\infty \int_{\frac{\lambda_e}{\lambda_m} y}^\infty \ln\left(\frac{\lambda_m x}{\lambda_e y}\right) K_0(2\sqrt{x}) K_0(2\sqrt{y}) dx dy. \tag{37}$$

Now, by using (eq. (6.561.8)) of [48] and the transformations $-\frac{z^a}{\pi(z+1)} \ln(z) = G_{3,3}^{2,2}\left(z|_{a,a,a+0.5}^{a,a,a+0.5}\right)$ (eq. (07.34.03.0919.01)) of [49] and $K_\nu(\sqrt{z}) = \frac{1}{2} G_{0,2}^{2,0}(\frac{z}{4}|\frac{\nu}{2}, \frac{\nu}{2})$, (eq. (03.04.26.0009.01)) of [49], into (37), and then simplifying it via (eq. (07.34.21.0011.01)) of [49] and (eq. (07.34.21.0081.01)) of [49], and after some algebraic simplifications, the ESC expression can be obtained, as shown in in (37), when $\lambda_m \to \infty$ and $\lambda_e \to \infty$. We skipped the detailed analysis here for brevity. Moreover, it can be seen from (37) that the ESC improves with λ_m and λ_e; however, an error floor can be seen in the ESC performance in the high λ_m and λ_e regime. This is because of the reason that the channel strengths of both main link and wiretap link are improved simultaneously. This behavior is also shown numerically in Section 5.

Remark 14. *We can further express (37) as*

$$\overline{C}_{sec}^{I} \approx \frac{4}{\ln(2)} \left[\int_0^\infty \int_{\frac{\lambda_e}{\lambda_m} y}^\infty \ln\left(\frac{x}{y}\right) K_0(2\sqrt{x}) K_0(2\sqrt{y}) dx dy + \ln\left(\frac{\lambda_m}{\lambda_e}\right) \int_0^\infty \int_{\frac{\lambda_e}{\lambda_m} y}^\infty K_0(2\sqrt{x}) K_0(2\sqrt{y}) dx dy \right]. \tag{38}$$

It can be seen from (38) that both the integrals are consistent and can easily be evaluated. Therefore, we can conclude that the asymptotic ESC follows the scaling law of $\Theta\left(\ln\left(\frac{\lambda_m}{\lambda_e}\right)\right)$ as $\frac{\lambda_m}{\lambda_e}$ increases and thus depends on the relative channel strengths of $ST \to SR$ and $ST \to E$ links, which is also demonstrated via numerical results in Section 5.

4.2. Strategy II: Combined Power Constraint of the Interference at the PR and Maximum Transmit Power at the ST

The ESC under Strategy II can be formulated as

$$\begin{aligned}\overline{C}_{sec}^{\mathrm{II}} &= \mathbb{E}\left[\log_2\left(1+\min\left(\frac{\rho}{|h_p|^2},\rho_1\right)|h_m|^2\right)-\log_2\left(1+\min\left(\frac{\rho}{|h_p|^2},\rho_1\right)|h_e|^2\right)\right]\\ &=\underbrace{\mathbb{E}\left[\log_2\left(1+\frac{\rho|h_m|^2}{|h_p|^2}\right)-\log_2\left(1+\frac{\rho|h_e|^2}{|h_p|^2}\right)\middle||h_p|^2>\frac{\rho}{\rho_1}\right]}_{\triangleq\,\overline{C}_{sec,1}^{\mathrm{II}}}\\ &+\underbrace{\mathbb{E}\left[\log_2\left(1+\rho_1|h_m|^2\right)-\log_2\left(1+\rho_1|h_e|^2\right)\middle||h_p|^2\le\frac{\rho}{\rho_1}\right]}_{\triangleq\,\overline{C}_{sec,2}^{\mathrm{II}}},\end{aligned}\tag{39}$$

which can be simplified as per the following theorem.

Theorem 5. *The exact expression of ESC under Strategy II over double-Rayleigh fading channels using (39) is given by*

$$\overline{C}_{sec}^{II}=\overline{C}_{sec,1}^{II}+\overline{C}_{sec,2}^{II},\tag{40}$$

where

$$\begin{aligned}\overline{C}_{sec,1}^{II} &= \frac{1}{\ln(2)}\sum_{i=1}^{U}\frac{w_i e^{t_i}}{\lambda_p}\left[\frac{t_i}{\rho\lambda_m}G_{2,4}^{4,1}\left(\frac{t_i}{\rho\lambda_m}\middle|_{0,0,-1,-1}^{-1,0}\right)-t_i^{\frac{3}{2}}\frac{\sqrt{\lambda_m}+\sqrt{\lambda_e}}{\rho^{\frac{3}{2}}\lambda_m\lambda_e}\mathcal{S}\left(\frac{t_i}{\rho}\right)\right]\\ &\times G_{0,2}^{2,0}\left(\frac{t_i}{\lambda_p}\middle|0,0\right)-\frac{2}{\ln(2)}\left[\sum_{k=1}^{N}\frac{g_k\rho}{\rho_1^2\lambda_m\lambda_p}G_{0,2}^{2,0}\left(\frac{\rho r_k^2}{\rho_1\lambda_p}\middle|0,0\right)G_{2,4}^{4,1}\left(\frac{r_k^2}{\rho_1\lambda_m}\middle|_{0,0,-1,-1}^{-1,0}\right)\right.\\ &\left.-\frac{\sqrt{\lambda_m}+\sqrt{\lambda_e}}{\lambda_m\lambda_e}\frac{\rho}{\rho_1^{\frac{5}{2}}}\sum_{k_1=1}^{M}\frac{g_{k_1}}{\lambda_p}G_{0,2}^{2,0}\left(\frac{\rho r_{k_1}^2}{\rho_1\lambda_p}\middle|0,0\right)\mathcal{S}\left(\frac{r_{k_1}^2}{\rho_1}\right)\right],\end{aligned}\tag{41}$$

$$\begin{aligned}\overline{C}_{sec,2}^{II} &= \frac{1}{\ln(2)}\left[\frac{1}{\rho_1\lambda_m}G_{2,4}^{4,1}\left(\frac{1}{\rho_1\lambda_m}\middle|_{0,0,-1,-1}^{-1,0}\right)-\frac{\sqrt{\lambda_m}+\sqrt{\lambda_e}}{\rho_1^{\frac{3}{2}}\lambda_m\lambda_e}\mathcal{S}\left(\frac{1}{\rho}\right)\right]\\ &\times\left[1-\frac{2\sqrt{\rho}}{\sqrt{\rho_1\lambda_p}}K_1\left(\frac{2\sqrt{\rho}}{\sqrt{\rho_1\lambda_p}}\right)\right],\end{aligned}\tag{42}$$

where $w_i=\frac{t_i}{((U+1)L_{U+1}(t_i))^2}$ *and* t_i, $(i=1,\cdots,U)$ *are the weights and zeros of* $U-$*order Gauss–Laguerre polynomial (i.e.,* $L_U(t)$*) [54, eq. (25.5.45)],* $g_k=\left\{\sum_{j=0}^{N-1}[q_j(r_k)]^2\right\}^{-1}$ *and* r_k, $(k=1,\cdots,N)$ *are the weights and zeros of* $N-$*order Gauss–Lobatto's polynomial [54, eq. (25.4.33)], respectively,* $q_N(r)=\sqrt{2N+4}P_N^{(3,0)}(1-2r)$ *with* $P_N^{(3,0)}$ *as Jacobi polynomial, and* $g_{k_1}=\left\{\sum_{j_1=0}^{M-1}[q_{j_1}(r_{k_1})]^2\right\}^{-1}$ *and* r_{k_1}, $(k_1=1,\cdots,M)$ *are the weights and zeros of* $M-$*order Gauss–Lobatto's polynomial, respectively,* $q_M(r)=\sqrt{2M+5}P_M^{(4,0)}(1-2r)$ *with* $P_M^{(4,0)}$ *as Jacobi polynomial.*

Proof. See Appendix D for the detailed proof. □

Remark 15. *It should be noted that (40) involves powers, exponential, Meijer-G functions, modified Bessel function of second kind, and extended generalized bivariate Meijer-G functions, consisting of network parameters* I_p, Q, η, Ω_m, Ω_e, *and* Ω_p, *which can be efficiently calculated via Mathematica software. We can achieve an arbitrary accurate approximation by appropriately selecting the values of* U, N, *and* M.

Remark 16. *Using (39) for $|h_m|^2 \geq |h_e|^2$, the ESC under strategy II can be expressed as*

$$\begin{aligned}\overline{\mathcal{C}}_{sec}^{II} = \frac{1}{\ln(2)} \int_{\frac{\rho}{\rho_1}}^{\infty} \Bigg[\int_0^{\infty} f_{|h_e|^2}(|h_e|^2) \int_{|h_e|^2}^{\infty} \ln\left(\frac{1+\frac{\rho|h_m|^2}{|h_p|^2}}{1+\frac{\rho|h_e|^2}{|h_p|^2}}\right) \\ \times f_{|h_m|^2}(|h_m|^2) d|h_m|^2 d|h_e|^2 \Bigg] f_{|h_p|^2}(|h_p|^2) d|h_p|^2 \\ + \frac{1}{\ln(2)} \int_{\frac{\rho}{\rho_1}}^{\infty} \Bigg[\int_0^{\infty} f_{|h_e|^2}(|h_e|^2) \int_{|h_e|^2}^{\infty} \ln\left(\frac{1+\rho_1|h_m|^2}{1+\rho_1|h_e|^2}\right) \\ \times f_{|h_m|^2}(|h_m|^2) d|h_m|^2 d|h_e|^2 \Bigg] f_{|h_p|^2}(|h_p|^2) d|h_p|^2. \end{aligned} \tag{43}$$

Substituting $|h_m|^2 = \lambda_m x$ and $|h_e|^2 = \lambda_e y$ into (43), and under the scenario when $\lambda_m \to \infty$ and $\lambda_e \to \infty$, and after some mathematical simplifications, we can express (43) as

$$\begin{aligned}\overline{\mathcal{C}}_{sec}^{\mathrm{II}} &\approx \frac{4}{\ln(2)} \int_0^{\infty} \int_{\frac{\lambda_e}{\lambda_m} y}^{\infty} \ln\left(\frac{\lambda_m x}{\lambda_e y}\right) K_0(2\sqrt{x}) K_0(2\sqrt{y}) dx dy \\ &\times \left[\int_{\frac{\rho}{\rho_1}}^{\infty} f_{|h_p|^2}(|h_p|^2) d|h_p|^2 + \int_0^{\frac{\rho}{\rho_1}} f_{|h_p|^2}(|h_p|^2) d|h_p|^2 \right] \\ &\approx \frac{4}{\ln(2)} \int_0^{\infty} \int_{\frac{\lambda_e}{\lambda_m} y}^{\infty} \ln\left(\frac{\lambda_m x}{\lambda_e y}\right) K_0(2\sqrt{x}) K_0(2\sqrt{y}) dx dy. \end{aligned} \tag{44}$$

Further, we can simplify (44) by using (eq. (6.561.8)) of [48], (eq. (07.34.03.0919.01)) of (eq. (03.04.26.0009.01)) of [49], (eq. (07.34.21.0011.01)) of [49], and (eq. (07.34.21.0081.01)) of [49], whose detailed analysis is skipped here for brevity. From (44), one can observe that the ESC performance increases with the increased in λ_m and λ_e but saturates in the high λ_m and λ_e regime because of the simultaneous improvement in the channel strengths of both the main link and the wiretap link, as shown numerically in Section 5.

Remark 17. *We can further express (44) as*

$$\begin{aligned}\overline{\mathcal{C}}_{sec}^{II} \approx \frac{4}{\ln(2)} \Bigg[\int_0^{\infty} \int_{\frac{\lambda_e}{\lambda_m} y}^{\infty} \ln\left(\frac{x}{y}\right) K_0(2\sqrt{x}) K_0(2\sqrt{y}) dx dy \\ + \ln\left(\frac{\lambda_m}{\lambda_e}\right) \int_0^{\infty} \int_{\frac{\lambda_e}{\lambda_m} y}^{\infty} K_0(2\sqrt{x}) K_0(2\sqrt{y}) dx dy \Bigg]. \end{aligned} \tag{45}$$

The integrals in (45) are consistent and can readily be simplified. Moreover, we can see from (45) that the asymptotic ESC follows the scaling law of $\Theta\big(\ln\left(\frac{\lambda_m}{\lambda_e}\right)\big)$ as $\frac{\lambda_m}{\lambda_e}$ increases, as shown numerically in Section 5.

5. Numerical Results and Discussion

In this section, we provide the numerical and simulation results to validate the effectiveness of our derived analytical findings under the consideration of Strategy I and Strategy II. To demonstrate, we plot various curves by varying the channel strengths (Ω_m, Ω_e, and Ω_p) of ST $\to$ SR, ST $\to$ E, and ST $\to$ PR links. Note that a path-loss channel modeling can also be adopted, where the average channel power gains of all channels can be denoted as $\Omega_\iota = d_\iota^{-\nu}$, for $\iota = \{m, e, p\}$, where ν denotes the path-loss exponent, and d_ι is the euclidean distance between the two nodes having the coordinates (x_ι, y_ι) and $(x_\jmath, y_\jmath)$, for $\iota = \{m, e, p\}$, $\jmath = \{m, e, p\}$, and $\iota \neq \jmath$. Such modeling indicates that, $\Omega_\iota \to \infty$ correspond to $d_\iota \to 0$, which implies that the nodes are located close to each other, whereas $\Omega_\iota \to 0$ correspond to $d_\iota \to \infty$, which indicates that two nodes are located far away from

each other. Furthermore, we consider the Gauss–Laguerre polynomial order $U = 30$ and Gauss–Lobatto's polynomial order $N = M = 50$, to obtain precise results.

5.1. SOP Performance under Strategies I and II

In Figure 5, we plot the SOP performance versus λ_m and λ_e for Strategy I. In Figure 5a, we show the SOP performance versus λ_m for different values of λ_e and $\mathcal{R}_s$, when $\rho = 10$ dB and $\lambda_p = 0$ dB. We can observed from Figure 5a that the derived analytical results are in good agreement with the simulation results over the entire range of λ_m. Further, we can see that the SOP performance improves as λ_m increases, and an effective secrecy diversity order of 1 can be verified irrespective of λ_e and $\mathcal{R}_s$, as also analytically demonstrated in Section 3-A. As expected, the SOP performance deteriorates with the improvement in wiretap channel strength λ_e, regardless of λ_m and $\mathcal{R}_s$. In Figure 5b, we demonstrate the SOP performance with average channel gains of both the main and wiretap links simultaneously varying (i.e., $\lambda_m = \lambda_e$ dB) for various values of $\mathcal{R}_s$, when $\rho = 10$ dB and $\lambda_p = 0$ dB. From which, it is observed that the SOP decreases as average channel gains ($\lambda_m = \lambda_e$ dB) increase, but saturates in the medium-to-high average channel gains regime, regardless of $\mathcal{R}_s$. This observation is also aligned with the derived asymptotic SOP results presented in (23), which depends on the fixed ratio $\frac{\lambda_e}{\lambda_m}$. In addition, we can see that the SOP performance decreases with the improvement in $\mathcal{R}_s$, since more power is needed to achieve the higher value of $\mathcal{R}_s$.

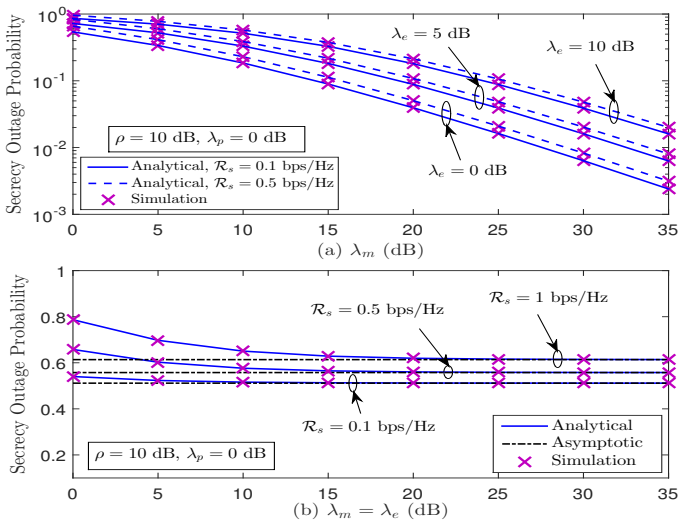

Figure 5. SOP performance for the considered system under Strategy I.

Figure 6 illustrates the impact of PR on the SOP performance for various values of ρ, λ_m, and λ_e, when $\mathcal{R}_s = 0.1$ bps/Hz. We can see from this figure that the SOP performance deteriorates as λ_p increases, irrespective of ρ, λ_m, and λ_e. This is because of the reason that the transmit power at ST decreases as λ_p increases. Moreover, for fixed value of ρ, the SOP performance improves when the legitimate channel quality is better than the wiretap channel quality, i.e., $\lambda_m > \lambda_e$, and vice versa. In addition, the SOP performance improves as ρ increases, i.e., the performance is better for $\rho = 20$ compared to $\rho = 10$ dB. This is due to the fact that an increase in ρ allows ST to transmit at a higher power level without interfering with the PR.

In Figure 7, we demonstrate the impact of λ_m, λ_e, and λ_p on the SOP performance under Strategy II. It can be observed from Figure 7 that the analytical results match perfectly with the simulation results, which corroborate the correctness of our derived theoretical findings. Figure 7a illustrates the SOP performance versus λ_m for various values of λ_e and $\mathcal{R}_s$, when $\rho = \rho_1 = 15$ dB and $\lambda_p = 0$ dB. We can observe that the SOP performance enhances as λ_m increases; however, it decreases with the improvement in λ_e. Moreover, the effective secrecy diversity order of 1 can also be achieved for different set of involved

parameters. As expected, the higher $\mathcal{R}_s$ results into the SOP performance degradation. In Figure 7b, we show the impact of PR on the SOP performance under Strategy II for various values of λ_m and λ_e, when $\mathcal{R}_s = 0.1$ bps/Hz and $\rho = \rho_1 = 20$ dB. It can be seen that the SOP performance degrades as λ_p increases, since power at ST reduces as λ_p improves. In addition, the SOP performance significantly improves if $\lambda_m > \lambda_e$, for all values of λ_p.

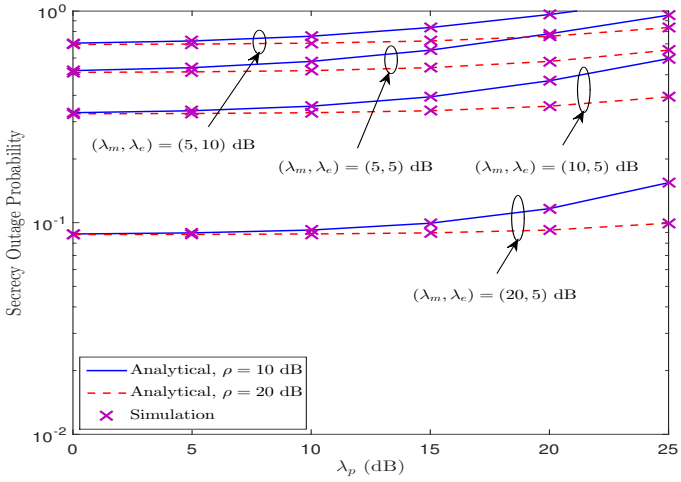

Figure 6. Impact of PR on the SOP performance under Strategy I.

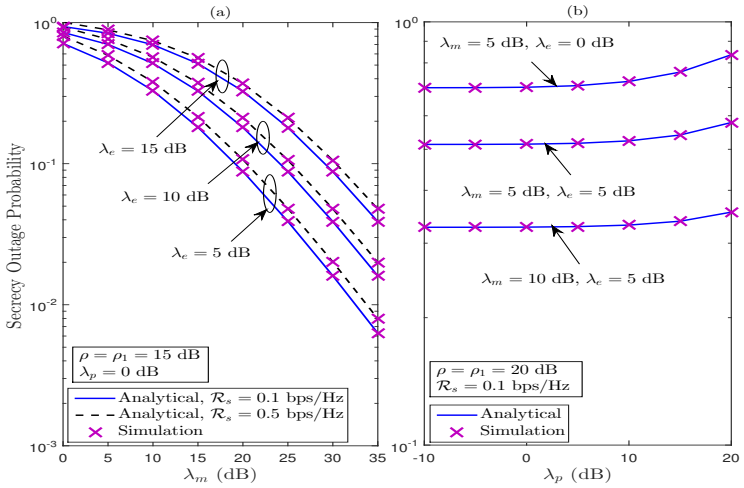

Figure 7. SOP performance for the considered system under Strategy II, (**a**) SOP versus λ_m, and (**b**) SOP versus λ_p.

In Figure 8, we illustrate the impact of maximum tolerable interference level I_P and maximum transmit power constraint Q on the SOP performance behavior under Strategy II. It can be observed from Figure 8a,b that the SOP performance deteriorates when $\lambda_e > \lambda_m$ in the low ρ and ρ_1 regimes; however, it saturates as ρ and ρ_1 increase (i.e., in the medium-to-high ρ and ρ_1 regimes). The secrecy floor in Figure 8a occurs because the SOP is independent of maximum secondary transmitter power, $\rho_1 \triangleq \frac{Q}{N_0}$, in the high ρ_1, and only depends on fixed ρ, as also theoretically verified in (32). Furthermore, the secrecy floor is observed in Figure 8b due to the limited impact of ρ on the SOP in the high ρ regime, since the SOP depends on the fixed ratio $\frac{\rho}{\rho_1}$, as also analytically validated in (31). In other words, the secrecy floor occurs in the high ρ region since the SNR both the legitimated link and wiretap link is improved simultaneously. In addition, Figure 8a,b implies that the secrecy diversity order reduces to zero, which is perfectly aligned with the theoretical findings obtained in Section 3-B.

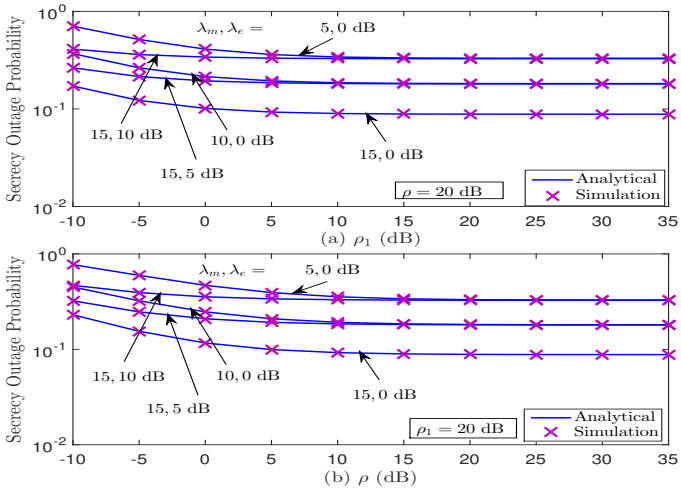

Figure 8. Impact of maximum tolerable interference level ($\rho = I_P/N_0$) and maximum transmit power constraint ($\rho_1 = Q/N_0$) on the SOP performance under Strategy II.

5.2. ESC Performance under Strategies I and II

Figure 9 illustrates the ESC curves for various values of λ_m and λ_e under Strategy I and Strategy II. We can observe that the analytical ESC results under Strategies I and II are in good agreement with the simulation results over the entire regime of λ_m and λ_e. We can observe from Figure 9a that the ESC performance increases as λ_m increases under both the considered strategies. In addition, the ESC performance decreases significantly as the quality of wiretap link improves. Further, in Figure 9b, the ESC performance increases as $\lambda_m = \lambda_e$ dB increases; however, the performance saturates in the high $\lambda_m = \lambda_e$ dB regime, which is aligned with the theoretical findings obtained in Section 4. The reason behind this behavior is that the quality of wiretap channel increases in the same proportion as of legitimate channel, hence restricting further improvement in the ESC performance.

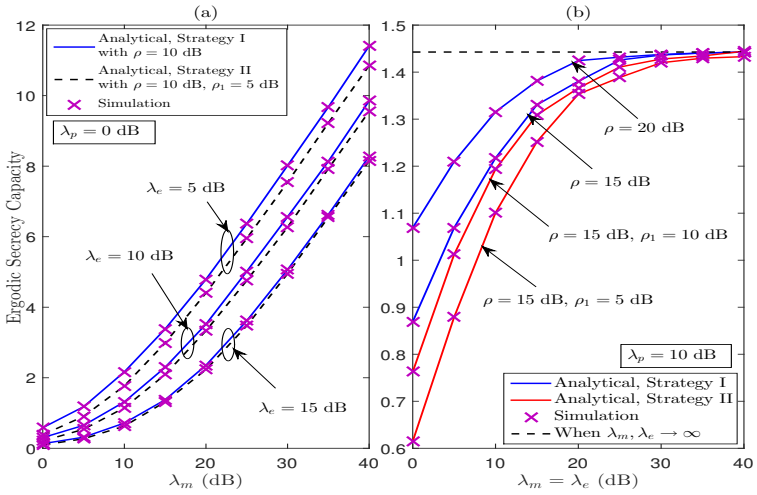

Figure 9. ESC performance for the considered system under Strategy I and Strategy II.

In Figure 10, we demonstrate the impact of primary user (λ_p), maximum tolerable interference level I_P, and maximum transmit power constraint Q on the ESC performance of the considered system. Figure 10a shows the ESC performance versus ρ under Strategy I for various values of λ_p, when $\lambda_m = 10$ dB and $\lambda_p = 5$ dB. The ESC performance increases as ρ increases; however, a secrecy floor is observed in the medium-to-high regime of ρ. This is because of the fact that an increase in ρ benefits both the legitimate destination and

the eavesdropper. Moreover, the performance significantly deteriorates as λ_p increases for all values of ρ. This degradation in ESC performance is because of the fact that the power at ST reduces as λ_p increases. Moreover, in Figure 10b, we plot the curves for ESC versus ρ_1 under Strategy II for various values of ρ and λ_p. We can observe from this figure that the ESC performance improves with ρ_1 when $\rho \geq \rho_1$ and saturates when $\rho < \rho_1$. In other words, the ESC is affected by the interaction of ρ and ρ_1. When ρ is smaller than ρ_1, the SOP is mainly affected by ρ, whereas when ρ_1 is smaller than ρ, then ρ_1 becomes the dominant factor. In addition, the secrecy floor behavior is also due to the fact that both the eavesdropper and the legitimate destination simultaneously extract the same benefits of increased transmit powers. Further, Figure 10b under Strategy II reveals that the ESC performance is better for lower values of λ_p than that of the one with higher values of λ_p.

Figure 11 illustrates the ESC versus $\frac{\lambda_m}{\lambda_e}$ for various ρ under Strategy I and for various ρ and ρ_1 under Strategy II, when $\lambda_p = 0$ dB. It can be observed from Figure 11 that the ESC improves with increasing $\frac{\lambda_m}{\lambda_e}$. This is owing to a higher λ_m than λ_e implying a superior channel quality of the legitimate channel when compared to the channel quality of the eavesdropper. This behavior is also depicted theoretically in (38) for Strategy I and in (45) for Strategy II. I addition, it is seen that there is a linear relationship between the ESC growth rate and $\frac{\lambda_m}{\lambda_e}$ at high $\frac{\lambda_m}{\lambda_e}$.

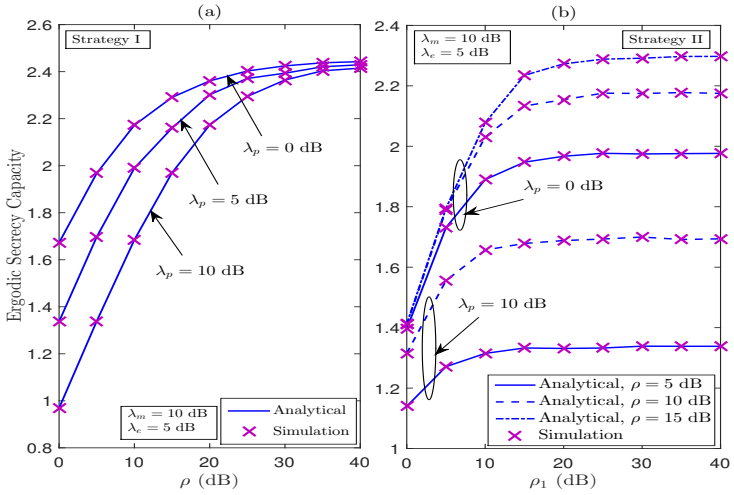

Figure 10. Impact of maximum tolerable interference level ($\rho = I_P/N_0$) and maximum transmit power constraint ($\rho_1 = Q/N_0$) on the ESC performance.

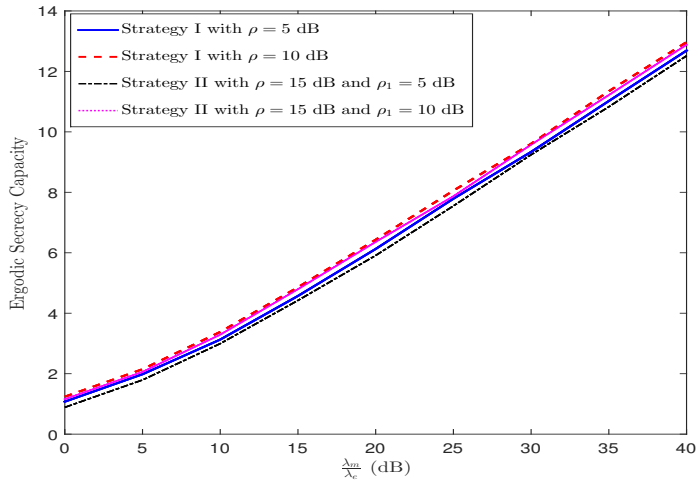

Figure 11. ESC performance versus $\frac{\lambda_m}{\lambda_e}$ under Strategy I and Strategy II.

6. Conclusions

This paper analyzed PHY-security in underlay CRVNs under spectrum-sharing constraints. Since all the nodes are in motion, the channels between the nodes are assumed to be modeled as double-Rayleigh fading. We assumed two different strategies to determine the transmit power of the secondary network. In Strategy I, the transmit power of the secondary transmitter is governed by the single-power constraint of the interference on the primary network, whereas in Strategy II, the transmit power of the secondary transmitter is governed by the combined power constraint of the interference on the primary network and the maximum transmission power at the secondary network. Under these two considered strategies, we deduced the exact SOP and ESC expressions for the considered system over double-Rayleigh fading channels. We also presented the asymptotic SOP analysis for the two considered strategies to reveal key insights into the system's secrecy diversity order. It was demonstrated that the system can achieve a full secrecy diversity order of 1, when the average channel gain of main link goes to infinity with fixed average wiretap channel gain. Furthermore, from the ESC analysis, it is reveled that the ESC follows a scaling law of $\Theta\big(\ln\big(\frac{\Omega_m^2}{\Omega_e^2}\big)\big)$, when Ω_m and Ω_e go to infinity. We also verified our analytical findings via simulation studies.

Author Contributions: Conceptualization, S.Y. and A.P.; methodology, S.Y., A.P., D.-T.D. and A.S.; software, S.Y. and A.P.; validation, S.Y. and A.P., D.-T.D., B.M.L. and A.S.; formal analysis, S.Y. and A.P.; investigation, S.Y., A.P. and A.S.; resources, A.S.; writing—original draft preparation, S.Y., A.P., D.-T.D., B.M.L. and A.S.; visualization, S.Y., A.P., D.-T.D., B.M.L. and A.S.; funding acquisition, A.S. All authors have read and agreed to the published version of the manuscript.

Funding: This work is funded by FCT/MCTES through national funds and when applicable co-funded EU funds under the project UIDB/50008/2020-UIDP/50008/2020.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: This study did not report any data.

Conflicts of Interest: The authors declare no conflict of interest.

Appendix A

Proof of Theorem 1

By invoking the CDF of $|h_e|^2$ and the PDF of $|h_m|^2$ into (12), we can express the integral $\mathbb{I}_1$ as

$$\mathbb{I}_1 = \mathbb{I}_{1a} - \mathbb{I}_{1b}, \tag{A1}$$

$$\text{where } \mathbb{I}_{1a} = \int_{\frac{(\eta-1)w}{\rho}}^{\infty} \frac{2}{\lambda_m} K_0\Big(2\sqrt{\frac{y}{\lambda_m}}\Big)dy, \tag{A2}$$

$$\mathbb{I}_{1b} = \frac{4}{\lambda_m\sqrt{\lambda_e}} \int_{\frac{(\eta-1)w}{\rho}}^{\infty} \sqrt{\frac{y}{\eta} - \frac{(\eta-1)w}{\eta\rho}} K_0\Big(2\sqrt{\frac{y}{\lambda_m}}\Big) K_1\Big(\frac{2}{\sqrt{\lambda_e}}\sqrt{\frac{y}{\eta} - \frac{(\eta-1)w}{\eta\rho}}\Big)dy. \tag{A3}$$

We can simplify $\mathbb{I}_{1a}$ in (A2) by first applying the relation $\int_{\alpha}^{\infty} g(x)dx = \int_0^{\infty} g(x)dx - \int_0^{\alpha} g(x)dx$ and then making use of the facts (eq. (6.561.16)) of [48] and (eq. (6.561.8)) of [48], as presented in (14). Moreover, $\mathbb{I}_{1b}$ in (A3) can be evaluated by first applying the change of variables $\frac{y}{\eta} - \frac{(\eta-1)w}{\eta\rho} = t$ and $\frac{\eta t}{\lambda_m} = r$ and the transformation $K_\nu(\sqrt{z}) = \frac{1}{2}G_{0,2}^{2,0}(\frac{z}{4}|\frac{\nu}{2}, -\frac{\nu}{2})$ (eq. (03.04.26.0009.01)) of [49] and then simplifying via (eq. (07.34.21.0082.01)) of [49], as shown in (15). Consequently, invoking (A2) and (A3) into (A1), we can obtain the inner integral $\mathbb{I}_1$ as presented in (13).

Appendix B

Proof of Theorem 3

We can simplify $\Theta_1(\eta)$ in (24) as

$$\begin{aligned}\Theta_1 &= \left[1 - \int_{\frac{\eta-1}{\rho_1}}^{\infty} F_{|h_e|^2}\left(\frac{y}{\eta} - \frac{\eta-1}{\eta\rho_1}\right) f_{|h_m|^2}(y)dy\right] F_{|h_p|^2}\left(\frac{\rho}{\rho_1}\right) \\ &= \left[1 - \int_{\frac{\eta-1}{\rho_1}}^{\infty} \frac{2}{\lambda_m} K_0\left(2\sqrt{\frac{y}{\lambda_m}}\right)dy \right. \\ &+ \frac{4}{\lambda_m\sqrt{\lambda_e}} \int_{\frac{\eta-1}{\rho_1}}^{\infty} \sqrt{\frac{y}{\eta} - \frac{\eta-1}{\eta\rho_1}} K_1\left(\frac{2}{\sqrt{\lambda_e}}\sqrt{\frac{y}{\eta} - \frac{\eta-1}{\eta\rho_1}}\right) \\ &\left. \times K_0\left(2\sqrt{\frac{y}{\lambda_m}}\right)dy\right]\left[1 - \frac{2\sqrt{\rho}}{\sqrt{\rho_1\lambda_p}} K_1\left(\frac{2\sqrt{\rho}}{\sqrt{\rho_1\lambda_p}}\right)\right]. \end{aligned} \tag{A4}$$

The first integral in (A4) can easily be simplified with the facts that $\int_{\alpha}^{\infty} g(x)dx = \int_0^{\infty} g(x)dx - \int_0^{\alpha} g(x)dx$ (eq. (6.561.16)) of [48] and (eq. (6.561.8)) of [48], whereas we can simplify the second integral in (A4) by first applying the transformations of variables $\frac{y}{\eta} - \frac{\eta-1}{\eta\rho_1} = t$ and $\frac{\eta t}{\lambda_m} = r$ and then using (eq. (03.04.26.0009.01)) of [49] and (eq. (07.34.21.0082.01)) of [49]. Consequently, $\Theta_1(\eta)$ can be given in (26).

Moreover, we can express $\Theta_2(\eta)$ in (24) as

$$\begin{aligned}\Theta_2(\eta) = &\int_{\frac{\rho}{\rho_1}}^{\infty} f_{|h_p|^2}(y)dy - \int_{\frac{\rho}{\rho_1}}^{\infty}\left\{\int_{\frac{y(\eta-1)}{\rho}}^{\infty} F_{|h_e|^2}\left(\frac{x}{\eta} - \frac{y(\eta-1)}{\eta\rho}\right)\right. \\ &\left. \times f_{|h_m|^2}(x)dx\right\} f_{|h_p|^2}(y)dy, \end{aligned} \tag{A5}$$

which can be further expressed after some simplifications as

$$\begin{aligned}\Theta_2(\eta) = &\frac{2\sqrt{\rho}}{\sqrt{\rho_1\lambda_p}} K_1\left(\frac{2\sqrt{\rho}}{\sqrt{\rho_1\lambda_p}}\right) - \int_{\frac{\rho}{\rho_1}}^{\infty}\left\{\int_{\frac{y(\eta-1)}{\rho}}^{\infty} f_{|h_m|^2}(x)\right. \\ &\left. \times F_{|h_e|^2}\left(\frac{x}{\eta} - \frac{y(\eta-1)}{\eta\rho}\right)dx\right\} f_{|h_p|^2}(y)dy. \end{aligned} \tag{A6}$$

The inner integral in (A6) can be evaluated by invoking the CDF of $|h_e|^2$ and the PDF of $|h_m|^2$ and following the same steps as used to simplify the integrals in (A4). Then, invoking the result along with the PDF of $|h_p|^2$ into (A6), and after some simplifications, $\Theta_2(\eta)$ can be expressed as

$$\begin{aligned}\Theta_2(\eta) = &\frac{2\sqrt{\rho}}{\sqrt{\rho_1\lambda_p}} K_1\left(\frac{2\sqrt{\rho}}{\sqrt{\rho_1\lambda_p}}\right)\frac{4}{\lambda_p}\sqrt{\frac{\eta-1}{\rho\lambda_m}} \int_{\frac{\rho}{\rho_1}}^{\infty} \sqrt{y} K_0\left(\frac{2\sqrt{y}}{\sqrt{\lambda_p}}\right) K_1\left(2\sqrt{\frac{(\eta-1)y}{\rho\lambda_m}}\right)dy \\ &+ \frac{2\sqrt{\lambda_m}}{\lambda_p\sqrt{\eta\lambda_e}} \sum_{k=0}^{\infty} \frac{(-1)^k}{k!}\left(\frac{\eta-1}{\rho\lambda_m}\right)^k G_{3,3}^{2,3}\left(\frac{\lambda_m}{\eta\lambda_e}\middle|_{\frac{1}{2},-\frac{1}{2},k-\frac{1}{2}}^{-\frac{1}{2},k-\frac{1}{2},k-\frac{1}{2}}\right) \int_{\frac{\rho}{\rho_1}}^{\infty} y^k K_0\left(\frac{2\sqrt{y}}{\sqrt{\lambda_p}}\right)dy. \end{aligned} \tag{A7}$$

The first integral (say χ_1) in (A7) can be expressed by using the facts that $\int_{\alpha}^{\infty} g(x)dx = \int_{0}^{\infty} g(x)dx - \int_{0}^{\alpha} g(x)dx$ and (eq. (03.04.26.0009.01)) of [49] as

$$\chi_1 = \frac{1}{4}\int_0^{\infty} \sqrt{y}\, G_{0,2}^{2,0}\left(\frac{(\eta-1)y}{\rho\lambda_m}\Big|\frac{1}{2},-\frac{1}{2}\right) G_{0,2}^{2,0}\left(\frac{y}{\lambda_p}\Big|0,0\right)dy$$
$$-\frac{1}{4}\int_0^{\frac{\rho}{\rho_1}} \sqrt{y}\, G_{0,2}^{2,0}\left(\frac{(\eta-1)y}{\rho\lambda_m}\Big|\frac{1}{2},-\frac{1}{2}\right) G_{0,2}^{2,0}\left(\frac{y}{\lambda_p}\Big|0,0\right)dy, \tag{A8}$$

where the first integral in (A8) can readily be simplified using (eq. (07.34.21.0011.01)) of [49], and the second integral in (A8) can be evaluated by first applying the transformation of variables $\frac{\rho_1 y}{\rho} = t^2$ and then applying Guass–Lobatto's quadrature integration [54]. Consequently, χ_1 can be given by

$$\chi_1 = \frac{\lambda_p^{\frac{3}{2}}}{4} G_{2,2}^{2,2}\left(\frac{(\eta-1)\lambda_p}{\rho\lambda_m}\Big|_{\frac{1}{2},-\frac{1}{2}}^{-\frac{1}{2},-\frac{1}{2}}\right) - \frac{\rho^{\frac{3}{2}}}{2\rho_1^{\frac{3}{2}}}\sum_{i=1}^{N} g_i t_i^2$$
$$\times\, G_{0,2}^{2,0}\left(\frac{(\eta-1)t_i^2}{\rho_1\lambda_m}\Big|\frac{1}{2},-\frac{1}{2}\right) G_{0,2}^{2,0}\left(\frac{\rho t_i^2}{\rho_1\lambda_p}\Big|0,0\right). \tag{A9}$$

Furthermore, we can simplify the second integral (say χ_2) of (A7) with the help of (eq. (03.04.26.0009.01)) of [49] and (eq. (07.34.21.0085.01)) of [49] as

$$\chi_2 = \left(\frac{\rho}{\rho_1}\right)^{k+1} G_{1,3}^{3,0}\left(\frac{\rho}{\rho_1\lambda_p}\Big|_{-k-1,0,0}^{-k}\right). \tag{A10}$$

Now, invoking (A9) and (A10) into (A7), and after some simplifications, we can express $\Theta_2(\eta)$ as presented in (27).

Appendix C

Proof of Theorem 4

With the aid of [56], we can express the ESC in (34) as

$$\overline{C}_{sec}^{\mathrm{I}} = \frac{1}{\ln(2)}\int_0^{\infty}\Bigg[\underbrace{\int_0^{\infty}\frac{y}{\rho}\ln(1+x) f_{|h_m|^2}\left(\frac{xy}{\rho}\right) F_{|h_e|^2}\left(\frac{xy}{\rho}\right)dx}_{\triangleq\, \mathbb{T}_1}$$
$$+\underbrace{\int_0^{\infty}\frac{y}{\rho}\ln(1+x) f_{|h_e|^2}\left(\frac{xy}{\rho}\right) F_{|h_m|^2}\left(\frac{xy}{\rho}\right)dx}_{\triangleq\, \mathbb{T}_2} \tag{A11}$$
$$-\underbrace{\int_0^{\infty}\frac{y}{\rho}\ln(1+x) f_{|h_e|^2}\left(\frac{xy}{\rho}\right)dx}_{\triangleq\, \mathbb{T}_3}\Bigg] f_{|h_p|^2}(y)dy.$$

By invoking the PDF of $|h_m|^2$ and the CDF of $|h_e|^2$ into $\mathbb{T}_1$ of (A11), and applying the transformations $\ln(1+z) = G_{2,2}^{1,2}(z|_{1,0}^{1,1})$ (eq. (01.04.26.0003.01)) of [49] and $K_{\nu}(\sqrt{z}) = \frac{1}{2}G_{0,2}^{2,0}(\frac{z}{4}|\frac{\nu}{2},-\frac{\nu}{2})$ (eq. (03.04.26.0009.01)) of [49], and then using (eq. (07.34.21.0011.01)) of [49] and (eq. (07.34.21.0081.01)) of [49], we can obtain $\mathbb{T}_1$ as

$$\mathbb{T}_1 = \frac{y}{\rho\lambda_m} G_{2,4}^{4,1}\left(\frac{y}{\rho\lambda_m}\Big|_{0,0,-1,-1}^{-1,0}\right) - \frac{y^{\frac{3}{2}}}{\rho^{\frac{3}{2}}\lambda_m\sqrt{\lambda_e}} G_{2,2:0,2:0,2}^{2,1:2,0:2,0}\left(\begin{matrix}-\frac{3}{2},-\frac{1}{2}\\ -\frac{3}{2},-\frac{3}{2}\end{matrix}\Big|0,0\Big|\frac{1}{2},-\frac{1}{2}\Big|\frac{y}{\rho\lambda_m},\frac{y}{\rho\lambda_e}\right). \tag{A12}$$

On the same line, we can evaluate the integrals $\mathbb{T}_2$ and $\mathbb{T}_3$ in (A11), respectively, as

$$\mathbb{T}_2 = \frac{y}{\rho\lambda_e} G_{2,4}^{4,1}\left(\frac{y}{\rho\lambda_e}\Big|_{0,0,-1,-1}^{-1,0}\right) - \frac{y^{\frac{3}{2}}}{\rho^{\frac{3}{2}}\lambda_e\sqrt{\lambda_m}} G_{2,2:0,2:0,2}^{2,1:2,0:2,0}\left(\begin{matrix}-\frac{3}{2},-\frac{1}{2}\\ -\frac{3}{2},-\frac{3}{2}\end{matrix}\Big|0,0\Big|\frac{1}{2},-\frac{1}{2}\Big|\frac{y}{\rho\lambda_m},\frac{y}{\rho\lambda_e}\right), \tag{A13}$$

$$\mathbb{T}_3 = \frac{y}{\rho\lambda_e} G_{2,4}^{4,1}\left(\frac{y}{\rho\lambda_e}\Big|_{0,0,-1,-1}^{-1,0}\right). \tag{A14}$$

Now, invoking (A12), (A13), and (A14) alongwith the PDF of $|h_p|^2$ into (A11), and applying the transformation $K_\nu(\sqrt{z}) = \frac{1}{2}G_{0,2}^{2,0}(\frac{z}{4}|\frac{\nu}{2},-\frac{\nu}{2})$ (eq. (03.04.26.0009.01)) of [49], it is observed that the solution of the resultant integral is tedious and intractable. To make the analysis tractable, we first multiply and divide the resultant integral by e^y, then simplifying it via Gauss–Laguerre numerical method [54]. Consequently, the ESC expression can be obtained, as shown in (35).

Appendix D

Proof of Theorem 5

The $\overline{C}_{sec,1}^{\mathrm{II}}$ of (39) can be expressed in the integral form as

$$\begin{aligned}\overline{C}_{sec,1}^{\mathrm{II}} = \frac{1}{\ln(2)}\int_{\frac{\rho}{\rho_1}}^{\infty}\Bigg[&\underbrace{\int_0^{\infty}\frac{y}{\rho}\ln(1+x)f_{|h_m|^2}\left(\frac{xy}{\rho}\right)F_{|h_e|^2}\left(\frac{xy}{\rho}\right)dx}_{\triangleq\,\mathbb{M}_1}\\ &+\underbrace{\int_0^{\infty}\frac{y}{\rho}\ln(1+x)f_{|h_e|^2}\left(\frac{xy}{\rho}\right)F_{|h_m|^2}\left(\frac{xy}{\rho}\right)dx}_{\triangleq\,\mathbb{M}_2}\\ &-\underbrace{\int_0^{\infty}\frac{y}{\rho}\ln(1+x)f_{|h_e|^2}\left(\frac{xy}{\rho}\right)dx}_{\triangleq\,\mathbb{M}_3}\Bigg]f_{|h_p|^2}(y)dy.\end{aligned} \tag{A15}$$

The integrals $\mathbb{M}_1$, $\mathbb{M}_2$, and $\mathbb{M}_3$ of (A15) can be evaluated by following the similar process as used to simplify $\mathbb{T}_1$ in (A12), $\mathbb{T}_2$ in (A13), and $\mathbb{T}_3$ in (A14), respectively. Then, invoking the results along with the PDF of $|h_p|^2$ into (A15), and further using the facts that $\int_\alpha^\infty g(x)dx = \int_0^\infty g(x)dx - \int_0^\alpha g(x)dx$ and (eq. (03.04.26.0009.01)) of [49], and after some mathematical simplifications, we can express $\overline{C}_{sec,1}^{\mathrm{II}}$ as

$$\begin{aligned}\overline{C}_{sec,1}^{\mathrm{II}} = \frac{1}{\ln(2)}\int_0^{\infty}&\left[\frac{y}{\rho\lambda_m}G_{2,4}^{4,1}\left(\frac{y}{\rho\lambda_m}\Big|_{0,0,-1,-1}^{-1,0}\right) - y^{\frac{3}{2}}\frac{\sqrt{\lambda_m}+\sqrt{\lambda_e}}{\rho^{\frac{3}{2}}\lambda_m\lambda_e}\mathcal{S}\left(\frac{y}{\rho}\right)\right]\\ &\times\frac{1}{\lambda_p}G_{0,2}^{2,0}\left(\frac{y}{\lambda_p}\Big|0,0\right)dy - \frac{1}{\ln(2)}\int_0^{\frac{\rho}{\rho_1}}\frac{1}{\lambda_p}G_{0,2}^{2,0}\left(\frac{y}{\lambda_p}\Big|0,0\right)\left[\frac{y}{\rho\lambda_m}G_{2,4}^{4,1}\left(\frac{y}{\rho\lambda_m}\Big|_{0,0,-1,-1}^{-1,0}\right)\right.\\ &\left.-y^{\frac{3}{2}}\frac{\sqrt{\lambda_m}+\sqrt{\lambda_e}}{\rho^{\frac{3}{2}}\lambda_m\lambda_e}\mathcal{S}\left(\frac{y}{\rho}\right)\right]dy.\end{aligned} \tag{A16}$$

The first integral in (A16) can be simplified by first multiplying and dividing it by e^y, and then applying the Guass–Laguarre quadrature method [54], whereas the second integral in (A16) can be evaluated by first using the transformation of variables $\frac{\rho_1 y}{\rho} = r^2$ and then applying Guass–Lobatto's integration method [54]. Consequently, the resultant expression of $\overline{C}_{sec,1}^{\mathrm{II}}$ can be obtained, as presented in (41).

Furthermore, we can express $\overline{C}^{\mathrm{II}}_{sec,2}$ of (39) as

$$\begin{aligned}\overline{C}^{\mathrm{II}}_{sec,2} = \frac{1}{\ln(2)}\Bigg[&\int_0^\infty \frac{1}{\rho_1}\ln(1+x) f_{|h_m|^2}\Big(\frac{x}{\rho_1}\Big) F_{|h_e|^2}\Big(\frac{x}{\rho_1}\Big)dx \\ &+ \int_0^\infty \frac{1}{\rho_1}\ln(1+x) f_{|h_e|^2}\Big(\frac{x}{\rho_1}\Big) F_{|h_m|^2}\Big(\frac{x}{\rho_1}\Big)dx \\ &- \int_0^\infty \frac{1}{\rho_1}\ln(1+x) f_{|h_e|^2}\Big(\frac{x}{\rho_1}\Big)dx\Bigg] F_{|h_p|^2}\Big(\frac{\rho}{\rho_1}\Big).\end{aligned} \tag{A17}$$

By invoking the PDFs and CDFs of $|h_m|^2$ and $|h_e|^2$ and applying the transformations $\ln(1+z) = G^{1,2}_{2,2}\big(z\big|^{1,1}_{1,0}\big)$ (eq. (01.04.26.0003.01)) of [49] and $K_\nu(\sqrt{z}) = \frac{1}{2}G^{2,0}_{0,2}\big(\frac{z}{4}\big|\frac{\nu}{2}, -\frac{\nu}{2}\big)$ (eq. (03.04.26.0009.01)) of [49], and then simplifying the integrals with the help of (eq. (07.34.21.0011.01)) of [49] and (eq. (07.34.21.0081.01)) of [49], we can obtain $\overline{C}^{\mathrm{II}}_{sec,2}$, as given in (42).

References

1. Zhou, H.; Xu, W.; Chen, J.; Weng, W. Evolutionary V2X technologies toward the Internet of vehicles: Challenges and opportunities. *Proc. IEEE*. **2020**, *108*, 308–320. [CrossRef]
2. Fallgren, M. 5GCAR: Executive Summary. 2019. Available online: https://5gcar.eu/wp-content/uploads/2019/12/5GCAR-Executive-Summary-White-Paper.pdf (accessed on 18 October 2021).
3. Wong, V.W.; Schober, R.; Ng, D.W.K.; Wang, L.C. *Key Technologies for 5G Wireless Systems*; Cambridge University Press: Cambridge, UK, 2017.
4. Kaiwartya, O.; Kumar, S. Enhanced caching for geocast routing in vehicular Ad Hoc network. In *Intelligent Computing, Networking, and Informatics*; Advances in Intelligent Systems and Computing; Springer: New Delhi, India, 2014; Volume 243, pp. 213–220.
5. Mumtaz, S.; Huq, K.M.S.; Ashraf, M.I.; Rodriguez, J.; Monteiro, V.; Politis, C. Cognitive vehicular communication for 5G. *IEEE Commun. Mag.* **2015**, *53*, 109–117. [CrossRef]
6. Eze, J.; Zhang, S.; Liu, E.; Eze, E. Cognitive radio-enabled Internet of Vehicles: A cooperative spectrum sensing and allocation for vehicular communication. *IET Netw.* **2018**, *7*, 190–199. [CrossRef]
7. Di Felice, M.; Doost-Mohammady, R.; Chowdhury, K.R.; Bononi, L. Smart Radios for Smart Vehicles: Cognitive Vehicular Networks. *IEEE Veh. Technol. Mag.* **2012**, *7*, 26–33. [CrossRef]
8. Zou, Y.; Zhu, J.; Yang, L.; Liang, Y.C.; Yao, Y.D. Securing physical-layer communications for cognitive radio networks. *IEEE Commun. Mag.* **2015**, *53*, 48–54. [CrossRef]
9. Shu, Z.; Qian, Y.; Ci, S. On physical layer security for cognitive radio networks. *IEEE Netw.* **2013**, *27*, 28–33.
10. Zou, Y.; Zhu, J.; Wang, X.; Hanzo, L. A survey on wireless security: Technical challenges, recent advances, and future trends. *Proc. IEEE*. **2016**, *104*, 1727–1765. [CrossRef]
11. Li, S.; Yang, L.; Hasna, M.O.; Alouini, M.S.; Zhang, J. Amount of secrecy loss: A novel metric for physical layer security analysis. *IEEE Commun. Lett.* **2020**, *24*, 1626–1630. [CrossRef]
12. Chen, X.; Ng, D.W.K.; Gerstacker, W.H.; Chen, H.H. A survey on multiple-antenna techniques for physical layer security. *IEEE Commun. Surv. Tut.* **2017**, *19*, 1027–1053. [CrossRef]
13. Moualeu, J.M.; da Costa, D.B.; Lopez-Martinez, F.J.; Hamouda, W.; Nkouatchah, T.M.; Dias, U.S. Transmit antenna selection in secure MIMO systems over $\alpha-\mu$ fading channels. *IEEE Trans. Commun.* **2019**, *67*, 6483–6498. [CrossRef]
14. Park, J.; Yun, S.; Kim, I.; Ha, J. Secure communications with a full-duplex relay network under residual self-interference. *IEEE Commun. Lett.* **2020**, *24*, 496–500. [CrossRef]
15. Le, K.N.; Bao, V.N.Q. Secrecy under Rayleigh-dual correlated Rician fading employing opportunistic relays and an adaptive encoder. *IEEE Trans. Veh. Technol.* **2020**, *69*, 5179–5192. [CrossRef]
16. Yang, L.; Chen, J.; Jiang, H.; Vorobyov, S.A.; Zhang, H. Optimal relay selection for secure cooperative communications with an adaptive eavesdropper. *IEEE Trans. Wirel. Commun.* **2017**, *16*, 6–42. [CrossRef]
17. Fan, L.; Lei, X.; Yang, N.; Duong, T.Q.; Karagiannidis, G.K. Secrecy cooperative networks with outdated relay selection over correlated fading channels. *IEEE Trans. Veh. Technol.* **2017**, *66*, 7599–7603. [CrossRef]
18. Zhao, H.; Liu, Z.; Yang, L.; Alouini, M.S. Secrecy analysis in DF relay over Generalized-K fading channels. *IEEE Trans. Commun.* **2019**, *67*, 7168–7182. [CrossRef]
19. Madeira, J.; Guerreiro, J.; Dinis, R.; Carvalho, P.; Campos, L. On the physical layer security characteristics for MIMO-SVD techniques for SC-FDE schemes. *Sensors* **2019**, *19*, 4757. [CrossRef]
20. Madeira, J.; Guerreiro, J.; Serra, H.; Dinis, R.; Carvalho, P.; Campos, L. A physical layer security technique for NOMA systems with MIMO SC-FDE schemes. *Electronics* **2020**, *9*, 240. [CrossRef]

21. Kumar, S.; Singh, K.; Kumar, S.; Kaiwartya, O.; Cao, Y.; Zhou, H. Delimitated anti jammer scheme for Internet of Vehicle: Machine learning based security approach. *IEEE Access* **2019**, *7*, 113311–113323. [CrossRef]
22. Chakraborty, P.; Prakriya, S. Secrecy outage performance of a cooperative cognitive relay network. *IEEE Commun. Lett.* **2017**, *21*, 326–329. [CrossRef]
23. Nguyen, M.N.; Nguyen, N.P.; Da Costa, D.B.; Nguyen, H.K.; De Sousa, R.T. Secure cooperative half-duplex cognitive radio networks with *K*-th best relay selection. *IEEE Access*. **2017**, *5*, 6678–6687. [CrossRef]
24. Chopra, K.; Bose, R.; Joshi, A. Secrecy performance of threshold-based cognitive relay network with diversity combining. *J. Commun. Netw.* **2018**, *20*, 383–395. [CrossRef]
25. Bouabdellah, M.; Bouanani, F.E.; Alouini, M.S. A PHY layer security analysis of uplink cooperative jamming-based underlay CRNs with multi-eavesdroppers. *IEEE Trans. Cog. Commun. Netw.* **2020**, *6*, 704–717. [CrossRef]
26. Banerjee, A.; Maity, S.P. On residual energy maximization in cognitive relay networks with eavesdropping. *IEEE Syst. J.* **2019**, *13*, 3836–3846. [CrossRef]
27. Zhang, T.; Cai, Y.; Huang, Y.; Duong, T.Q.; Yang, W. Secure transmission in cognitive MIMO relaying networks with outdated channel state information. *IEEE Access* **2016**, *4*, 8212–8224. [CrossRef]
28. Zou, Y.; Li, X.; Liang, Y. Secrecy outage and diversity analysis of cognitive radio systems. *IEEE J. Sel. Areas Commun.* **2014**, *32*, 2222–2236. [CrossRef]
29. Li, M.; Yin, H.; Huang, Y.; Fu, T.; Wang, Y.; Yu, R. Secrecy performance analysis in MISOSE cognitive radio networks over correlated fading. In Proceedings of the 2nd IEEE Advanced Information Management, Communicates, Electronic and Automation Control Conference (IMCEC 2018), Xi'an, China, 25–27 May 2018; pp. 875–879.
30. Singh, A.; Bhatnagar, M.R.; Mallik, R.K. Physical layer security of a multiantenna-based CR network with single and multiple primary users. *IEEE Trans. Veh. Technol.* **2017**, *66*, 11011–11022. [CrossRef]
31. Timilsina, S.; Baduge, G.A.A.; Schaefer, R.F. Secure communication in spectrum-sharing massive MIMO systems with active eavesdropping. *IEEE Trans. Cog. Commun. Netw.* **2018**, *4*, 390–405. [CrossRef]
32. Lei, H.; Zhang, J.; Park, K.H.; Ansari, I.S.; Pan, G.; Alouini, M.S. Secrecy performance analysis of SIMO underlay cognitive radio systems with outdated CSI. *IET Commun.* **2017**, *11*, 1961–1969. [CrossRef]
33. Andersen, J.B. Statistical distributions in mobile communications using multiple scattering. In Proceedings of the 27th URSI General Assembly, Maastricht, The Netherlands, 17–24 August 2002.
34. Salo, J.; El-Sallabi, H.M.; Vainikainen, P. Statistical analysis of the multiple scattering radio channel. *IEEE Trans. Antennas Propag.* **2006**, *54*, 3114–3124. [CrossRef]
35. Pandey, A.; Yadav, S. Physical layer security in cooperative AF relaying networks with direct links over mixed Rayleigh and double-Rayleigh fading channels. *IEEE Trans. Veh. Technol.* **2018**, *67*, 10615–10630. [CrossRef]
36. Kovács, I.Z.; Eggers, P.C.; Olesen, K.; Petersen, L.G. Radio channel description and quality of service for TETRA direct mode operation in forest environments. In Proceedings of the IEEE 54th Vehicular Technology Conference, VTC Fall, Atlantic City, NJ, USA, 7–11 October 2001; pp. 1970–1974.
37. Kovács, I.Z.; Eggers, P.C.; Olesen, K.; Petersen, L.G. Investigations of outdoor-to-indoor mobile-to-mobile radio communication channels. In Proceedings of the IEEE 56th Vehicular Technology Conference, Vancouver, BC, Canada, 24–28 September 2002; pp. 430–434.
38. Zhang, J.; Pan, G. Secrecy outage analysis with *K*th best relay selection in dual-hop inter-vehicle communication systems. *AEU—Int. J. Electron. Commun.* **2017**, *71*, 139–144. [CrossRef]
39. Pandey, A.; Yadav, S. Secrecy analysis of cooperative vehicular relaying networks over double-Rayleigh fading Channels. *Wirel. Pers. Commun.* **2020**, *114*, 2733–2753. [CrossRef]
40. Pandey, A.; Yadav, S. Physical layer security in cooperative amplify-and-forward relay networks over mixed Nakagami-*M* Double Nakagami-*m* Fading Channels: Perform. Eval. Optimisation. *IET Commun.* **2020**, *14*, 95–104. [CrossRef]
41. Ahn, N.; Lee, D.; Oh, S. Vehicle Communication Using Secrecy Capacity. In *Proceeding FTC*; Arai, K., Bhatia, R., Kapoor, S., Eds.; Springer International Publishing: Cham, Switzerland, 2019; pp. 158–172.
42. Duy, T.T.; Alexandropoulos, G.C.; Tung, V.T.; Son, V.N.; Duong, T.Q. Outage performance of cognitive cooperative networks with relay selection over double-Rayleigh fading channels. *IET Commun.* **2016**, *10*, 57–64. [CrossRef]
43. Lee, J.; Lee, J.H.; Bahk, S. Performance analysis for multi-hop cognitive radio networks over cascaded Rayleigh fading channels with imperfect channel state information. *IEEE Trans. Veh. Technol.* **2019**, *68*, 10335–10339. [CrossRef]
44. Ata, S.O.; Erdogan, E. Secrecy outage probability of inter-vehicular cognitive radio networks. *Int. J. Commun. Sys.* 2019, 33, e4244. [CrossRef]
45. Tashman, D.H.; Hamouda, W. Physical-layer security for cognitive radio networks over cascaded Rayleigh fading channels. In Proceedings of the IEEE Global Communications Conference (GLOBECOM 2020), Taipei, Taiwan, 7–11 December 2020; pp. 1–6.
46. Yadav, S; Pandey A. Secrecy performance of cognitive vehicular radio networks: Joint impact of nodes mobility and imperfect channel estimates. In Proceedings of the IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom), Odessa, Ukraine, 26–29 May 2020; pp. 1–7.
47. Pandey A.; Yadav, S. Joint impact of nodes mobility and imperfect channel estimates on the secrecy performance of cognitive radio vehicular networks over Nakagami-*M* Fading Channels. *IEEE Open J. Veh. Technol.* **2021**, *2*, 289–309. [CrossRef]
48. Gradshteyn I.S.; Ryzhik, I.M. *Tables of Integrals, Series, and Products*, 6th ed.; Academic Press: New York, NY, USA, 2000.

49. The Wolfram Functions Site [Online]. Available online: Http://functions.wolfram.com (accessed on 18 October 2021).
50. Patel, C.S.; Stuber G.L.; Pratt, T.G. Simulation of Rayleigh-faded mobile-to-mobile communication channels. *IEEE Trans. Commun.* **2005**, *53*, 1876–1884. [CrossRef]
51. Patzold, M.; Hogstad, B.O.; Youssef, N. Modeling, analysis, and simulation of MIMO mobile-to-mobile fading channels. *IEEE Trans. Wirel. Commun.* **2008**, *7*, 510–520. [CrossRef]
52. Ghasemi, A.; Sousa, E.S. Fundamental limits of spectrum-sharing in fading environments. *IEEE Trans. Wirel. Commun.* **2007**, *6*, 649–658. [CrossRef]
53. Duong, T.Q.; da Costa, D.B.; Elkashlan, M.; Bao, V.N.Q. Cognitive amplify-and-forward relay networks over Nakagami-*m* fading. *IEEE Trans. Veh. Technol.* **2012**, *61*, 2368–2374. [CrossRef]
54. Abramowitz, M.; Stegun, I.A. *Handbook of Mathematical Functions with Formulas, Graphs, and Mathematical Tables*; National Bureau of Standards: Washington, DC, USA, 1972.
55. Ansari, I.S.; Al-Ahmadi, S.; Yilmaz, F.; Alouini, M.S.; Yanikomeroglu, H. A new formula for the BER of binary modulations with dual-branch selection over generalized-K composite fading channels. *IEEE Trans. Commun.* **2011**, *59*, 2654–2658. [CrossRef]
56. Lei, H.; Zhang, H.; Ansari, I.S.; Gao, C.; Guo, Y.; Pan, G.; Qaraqe, K.A. Performance analysis of physical layer security over generalized-K fading channels using a mixture Gamma distribution. *IEEE Commun. Lett.* **2016**, *20*, 408–411.