IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received March 16, 2021, accepted March 29, 2021, date of publication April 20, 2021, date of current version April 30, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3074507

Secrecy Performance of SIMO Underlay Cognitive Radio Networks Over $\alpha - \mu$ Fading Channels

SUNEEL YADAV[1], (Member, IEEE), AND DEVENDRA SINGH GURJAR[2], (Member, IEEE)
[1]Department of Electronics and Communication Engineering, Indian Institute of Information Technology, Allahabad, Prayagraj 211012, India
[2]Department of Electronics and Communication Engineering, National Institute of Technology Silchar, Silchar 788010, India

Corresponding author: Suneel Yadav (suneel@iiita.ac.in)

ABSTRACT This paper investigates the secrecy performance of a single-input multiple-output (SIMO) based underlay cognitive radio networks. In particular, a single-antenna secondary transmitter transmits its secret message to a multi-antenna equipped secondary node in the presence of a multi-antenna equipped passive eavesdropper under a peak interference constraint at the single-antenna primary receiver. We proficiently derive the expressions for secrecy outage probability (SOP), intercept probability, and ergodic secrecy capacity (ESC) for the considered system over $\alpha - \mu$ fading channels. Further, we carry out the asymptotic analysis of SOP and intercept probability under two cases of interest; 1) when the average signal-to-noise ratio (SNR) of the main link, i.e., between the secondary source and secondary destination, goes to infinity with a fixed average SNR of wiretap link between the secondary source and secondary eavesdropper, and 2) when the SNRs of both the main and wiretap links tend to infinity. We can infer that a secrecy diversity order of $\frac{\alpha_D N_D \mu_D}{2}$ can be achieved under case 1, where α_D and μ_D are the main link fading parameters, and N_D denotes the number of antennas at the destination. Whereas, under case 2, the system's secrecy diversity order becomes zero. Moreover, we also present some interesting findings for the ESC when the interference constrained secondary transmitter power is considerably high. Further, we validate our analytical framework through extensive simulation and numerical results, and demonstrate the effects of system/channel parameters on the secrecy performance of the considered system. Our results reveal that the higher number of eavesdropper antennas can have a more deleterious impact on the system's secrecy performance.

INDEX TERMS Physical layer security, cognitive radio networks, fading channels, secrecy performance.

I. INTRODUCTION

A. BACKGROUND

In the recent years, the demand of various wireless communication services has been exponentially increased, which has exhausted the available spectrum resources and setup a strong demand for new technologies to solve radio spectrum scarcity. Therefore, to meet such an unprecedented requirement, cognitive radio technology has been advanced as a potential solution that can improve spectrum utilization owing to its spectrum sensing capability and adaptability to operate opportunistically in the licensed and unlicensed bands [1], [4]. In the cognitive radio networks (CRNs), all the secondary users (unlicensed users) can share the licensed band with the primary users (licensed users) in different modes, namely, underlay, overlay, and interweave, by guaranteeing the quality-of-service of the primary users. Our particular interest in this paper is the underlay mode of operation, where the secondary users are allowed to utilize the licensed spectrum with a strict constraint that the secondary users maintain the transmit power within a tolerable interference limit of the primary nodes. Good amount of literature on investigating the performance of CRNs is available (see [5], [11] and the references therein). However, the security against jamming and eavesdropping attacks in CRNs is of prime concern, which occurs due to its highly adaptive nature and functionality in open wireless communication medium [12], [13]. Traditionally, the security in wireless communications mainly depends on the encryption based techniques applicable in upper layers, e.g., advanced encryption standard and data encryption standard algorithms that require a powerful computational processing. Therefore, information

The associate editor coordinating the review of this manuscript and approving it for publication was Ding Xu.

security in wireless communications is a challenging task. Recently, with the proliferation of cooperative communications, multi-antennas, and coding technologies, physical layer security (PHY-security) has envisioned as an effective method to secure wireless communications. Different from the traditional encryption techniques, there is no need of employing encryption key in PHY-security technologies, since it exploits the properties of wireless channels, e.g., fading, interference, and path-loss [13], to realize secure communications.

B. RELATED WORKS

The secrecy performance of underlay CRNs over different fading channels under PHY-security aspects has been studied in [14], [28]. The authors in [14] and [15] have comprehensively discussed various PHY-security aspects in CRNs. The authors in [16] have evaluated the secrecy performance of single-input single-output (SISO) CRNs under the impact of nodes' mobility and imperfect channel estimates over Rayleigh fading channels. Moreover, the secrecy performance of SISO cooperative cognitive relay networks has been evaluated in [17] over Rayleigh fading channels. The authors in [18] have investigated the secrecy performance of relay assisted CRNs in the presence of primary transceiver network over Rayleigh fading channels. Recently, PHY-security in SISO cooperative cognitive vehicular relay networks has been studied in [19], [20] over mixed Rayleigh and double-Rayleigh fading channels. The authors in [21] have evaluated the secrecy outage analysis of SISO underlay CRNs over Nakagami-*m* fading channels. Furthermore, the secrecy outage performance of an underlay cognitive decode-and-forward relay network over Nakagami-*m* fading channels is investigated in [22]. Moreover, the secrecy performance of single-input multiple-output (SIMO) based CRNs has been widely analyzed for Rayleigh fading channels in [23], [24] and for Nakagami-*m* fading channels in [25]. PHY-security in multiple-input multiple-output (MIMO) supported cognitive radio wiretap channels has been examined by considering Rayleigh fading scenario in [26], [27] and Nakagami-*m* fading scenario in [28].

In particular, the works mentioned earlier [14], [28] on PHY-security in CRNs have adopted an impractical postulate related to homogeneous diffuse scattering scenario to model the small-scale fading. As a consequence, the $\alpha - \mu$ distribution has drawn significant consideration as it has the ability to characterize non-homogeneous fading situations encountered in practical wireless communications systems. It can also be applied to model both the fading scenarios, i.e., small-scale fading and large-scale fading [29], [30]. Herein, the parameter α defines the non-linearity of the propagation environment, and μ characterizes the clustering of multipath waves. Therefore, the $\alpha - \mu$ distribution can be utilized to model a wide range of fading distributions, such as, exponential, Rayleigh, Nakagami-*m*, Gamma, and Weibull. Further, PHY-security for wireless networks by considering single-antenna/multiple-antennas scenario has been studied over $\alpha - \mu$ fading in [31], [35], however these works were carried out over non-cognitive framework. Recently, the secrecy performance of SISO underlay CRNs over $\alpha - \mu$ fading channels has been investigated in terms of secrecy outage probability (SOP) in [36], and in terms of intercept probability and ergodic secrecy capacity (ESC) in [37]. To the best of our knowledge, the benefits of considering multiple antennas in the considered underlay CRN and comprehensively investigation of the secrecy performance over $\alpha - \mu$ fading channels have not been done so far. Therefore, our aim in this paper is to fill this critical gap.

C. MOTIVATION AND CONTRIBUTIONS

Motivated by the above studies, this paper analyzes the secrecy performance of SIMO underlay CRNs over $\alpha - \mu$ fading channels. Specifically, we consider a secure underlay CRN which consists a single-antenna primary receiver, a single-antenna secondary transmitter, a multi-antenna secondary destination, and a multi-antenna passive eavesdropper. We employ a peak interference constraint at the primary receiver. For the considered setup, we derive the SOP, intercept probability, and ESC expressions over $\alpha - \mu$ fading channels. The main contributions of this paper are listed as follows.

1) Compared to [36] and [37], in which the destination and eavesdropper receivers were deployed with a single antenna devices, a more generalized system model is considered in this paper, as both the destination and eavesdropper are equipped with multi-antenna devices.
2) We derive the exact expression for the SOP of the considered system under the $\alpha - \mu$ fading scenario. Besides, we perform the asymptotic SOP analysis for two cases of interest; 1) when the average transmit signal-to-noise ratio (SNR) of the main channel, i.e., between the secondary source and secondary destination goes to infinity with fixed average SNR at the eavesdropper, and 2) when the SNRs of both the main channel and wiretap channel (i.e., between secondary source and secondary eavesdropper) go to infinity. Further, we note that a secrecy diversity order of $\frac{\alpha_D N_D \mu_D}{2}$ (α_D and μ_D are the fading parameters of the main link, and N_D denotes the number of antennas at the legitimate destination) can be achieved under case 1.
3) We also derive the intercept probability and asymptotic intercept probability expressions for the considered system. From the asymptotic intercept probability analysis in the high transmit average SNR regime, we show that a secrecy diversity order of $\frac{\alpha_D N_D \mu_D}{2}$ can be achieved.
4) We deduce the exact ESC expression for the considered system by taking the $\alpha - \mu$ fading scenario into account. We also depict some critical observations related to system performance in terms of ESC. For instance, when secondary source power with interference constraint is kept very high, two phenomena can be observed;

1) there exists a ceiling of ESC, and 2) the ESC follows a scaling law of $\Theta\big(\ln\big(\frac{\Omega_D}{\Omega_E}\big)\big)$, where Ω_E and Ω_D represent the average channel gains of wiretap link and main link.
5) Finally, we verify our analytical and theoretical findings via simulations studies. Our results show the impact of various channel/system parameters on the system's secrecy performance. It is also revealed that the system's secrecy performance increases significantly with the increased number of destination antennas, and reduces as number of eavesdropper antennas increases.

D. ORGANIZATION

The remainder of this paper is organized as follows. The description of the considered system model is given in Section II. Section III presents the expressions for the exact SOP followed by its asymptotic form, intercept probability, and ESC. In section IV, we show the convergence of infinite summations. In Section V, we perform the numerical and simulation experiments to validate our analysis, and finally, Section VI summarizes the contributions of this work.

Notations: $\Upsilon(\cdot,\cdot)$ and $\Gamma(\cdot)$ are used to denote the lower incomplete gamma function and complete gamma function, respectively, [38, eq. (8.350)]. $G_{p,q}^{m,n}(x|_{b_1,\cdots,b_q}^{a_1,\cdots,a_p})$ is the Meijer-G function [38, eq. (9.301)]. I_N denotes the $N\times N$ identity matrix, $\mathcal{H}$ and T are the hermitian transpose and transpose, respectively, and $||\cdot||$ and $|\cdot|$ are the Frobenius norm and absolute value, respectively. $\mathbb{Z}_+$ denotes the set of positive integers.

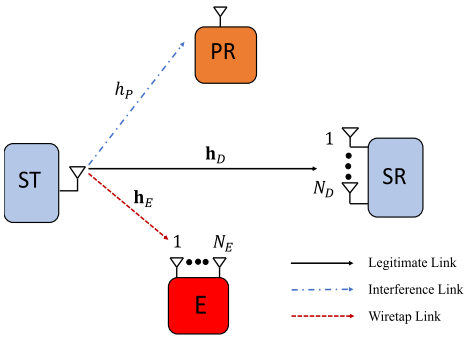

FIGURE 1. System model for the secure SIMO underlay CRNs.

II. SYSTEM AND CHANNEL MODELS

A secure CRN as depicted in Fig. 1 has been considered in this work that utilizes an underlay spectrum sharing technique, where a secondary user pair makes use of the same licensed band assigned to the primary system for its communication in a specified propagation medium. In particular, a single-antenna equipped secondary source (ST) realizes its communication with an N_D-antenna equipped secondary destination (SR) in the presence of an N_E-antenna equipped secondary passive eavesdropper (E) in the secondary network and a primary receiver (PR) in the primary network. Furthermore, the transmit power at the secondary source power is compelled to have the interference on PR below a certain maximum level of tolerable interference Q due to the inability of detecting the interference at PR imposed by ST. Thereby, the transmit power of ST is given as $P_s=\frac{Q}{|h_P|^2}$. Such a peak interference type of power control strategy is popularly used in the literature [16], [17], [19], [20]. Furthermore, it is assumed that all the participating nodes communicate in a half-duplex mode. Because of the availability of multiple antennas at SR and E, $\mathbf{h}_D$ and $\mathbf{h}_E$ can be denoted as the channel vectors for the links ST $\rightarrow$ SR and ST $\rightarrow$ E, and can be expressed, respectively, as $\mathbf{h}_D=[h_{D,1}\,h_{D,2}\,\cdots\,h_{D,N_D}]^T$ and $\mathbf{h}_E=[h_{E,1}\,h_{E,2}\,\cdots\,h_{E,N_E}]^T$. Whereas, h_P denotes the channel coefficients for ST $\rightarrow$ PR link. In addition, we assume the perfect channel state information (CSI)[1] for all the links. We also assume that all the channels are quasi-static and modeled as independent and identically distributed (i.i.d.) $\alpha-\mu$ flat-fading, where μ and α represent the number of multipath clusters and nonlinearity of the propagation medium, respectively. The $\alpha-\mu$ flat-fading is a generalized fading distribution that can characterize different small-scale fading models [29], viz., Weibull ($\mu=1$), Rayleigh ($\alpha=2,\mu=1$), One-sided Gaussian ($\alpha=2,\mu=1/2$), Nakagami-m ($\alpha=2,\mu=m$), and Negative Exponential ($\alpha=1,\mu=1$). The noise at each node is modeled as additive white Gaussian noise (AWGN), which is defined as $\mathcal{CN}(0,\sigma_n^2)$.

In the information transmission process, ST sends its confidential information to the destination node SR over the main link. Thereby, the received signal at SR can be given as

$$\underbrace{\begin{bmatrix} y_{D,1}\\ y_{D,2}\\ .\\ .\\ .\\ y_{D,N_D}\end{bmatrix}}_{\mathbf{Y}_D}=\sqrt{P_s}\underbrace{\begin{bmatrix} h_{D,1}\\ h_{D,2}\\ .\\ .\\ .\\ h_{D,N_D}\end{bmatrix}}_{\mathbf{h}_D}x_s+\underbrace{\begin{bmatrix} n_{D,1}\\ n_{D,2}\\ .\\ .\\ .\\ n_{D,N_D}\end{bmatrix}}_{\mathbf{n}_D}, \tag{1}$$

where $\mathbf{n}_D=[n_{D,1}\,n_{D,2}\,\cdots\,n_{D,N_D}]^T$ is the noise vector at SR, whose entries $n_{D,i}$, for $i\in\{1,2,\cdots,N_D\}$ can be modeled as $\mathcal{CN}(0,\sigma_n^2)$. Furthermore, we can compactly represent (1) as

$$\mathbf{Y}_D=\sqrt{P_s}\mathbf{h}_D x_s+\mathbf{n}_D. \tag{2}$$

Since, E overhears the confidential message transmitted by ST via the wiretap channel, therefore, the signal received at E

[1]It should be noted that i) the statistical CSI corresponding to ST $\rightarrow$ SR link is available at ST, ii) under passive eavesdropping, the eavesdropper is generally not cooperative and not willing to feedback its instantaneous CSI to the legitimate node, therefore, the instantaneous CSI between ST and E is not available at ST and only statistical CSI of the eavesdropper is considered to be known at ST [39], and iii) the PR is capable to feedback its instantaneous CSI to ST, so that ST can adjust its transmit power to satisfy the interference constraint [40]. This can be achieved via a spectrum band manager that mediates between the primary and secondary users.

can be expressed as

$$\underbrace{\begin{bmatrix} y_{E,1} \\ y_{E,2} \\ \cdot \\ \cdot \\ \cdot \\ y_{E,N_E} \end{bmatrix}}_{\mathbf{Y}_E} = \sqrt{P_s} \underbrace{\begin{bmatrix} h_{E,1} \\ h_{E,2} \\ \cdot \\ \cdot \\ \cdot \\ h_{E,N_E} \end{bmatrix}}_{\mathbf{h}_E} x_s + \underbrace{\begin{bmatrix} n_{E,1} \\ n_{E,2} \\ \cdot \\ \cdot \\ \cdot \\ n_{E,N_E} \end{bmatrix}}_{\mathbf{n}_E}, \tag{3}$$

where $\mathbf{n}_E = [n_{E,1}\, n_{E,2} \cdots n_{E,N_E}]^T$ is the noise vector at E, whose entries $n_{E,j}$, for $j \in \{1, 2, \cdots, N_E\}$ are modeled as $\mathcal{CN}(0, \sigma_n^2)$. Also, (3) can be shown in the compact form as

$$\mathbf{Y}_E = \sqrt{P_s}\mathbf{h}_E x_s + \mathbf{n}_E. \tag{4}$$

Now, by applying the maximal ratio combining (MRC) scheme at SR and E, we can express (2) and (4) as

$$\begin{aligned} \mathbf{R}_D &= \mathbf{W}_D^{\mathcal{H}}\mathbf{Y}_D \\ &= \sqrt{P_s}\mathbf{W}_D^{\mathcal{H}}\mathbf{h}_D x_s + \mathbf{W}_D^{\mathcal{H}}\mathbf{n}_D, \end{aligned} \tag{5}$$

$$\begin{aligned} \mathbf{R}_E &= \mathbf{W}_E^{\mathcal{H}}\mathbf{Y}_E \\ &= \sqrt{P_s}\mathbf{W}_E^{\mathcal{H}}\mathbf{h}_E x_s + \mathbf{W}_E^{\mathcal{H}}\mathbf{n}_E, \end{aligned} \tag{6}$$

respectively, where $\mathbf{W}_D = \frac{\mathbf{h}_D}{||\mathbf{h}_D||}$ is the $N_D \times 1$ receive weight vector at SR and $\mathbf{W}_E = \frac{\mathbf{h}_E}{||\mathbf{h}_E||}$ is the $N_E \times 1$ receive weight vector at E. In addition, we make the reasonable assumption that the noise samples across the different antennas are independent, i.e., $\mathbb{E}\{n_{J,u}n_{J,v}^*\} = 0$ for $u \neq v$ and $J \in \{D, E\}$. This can also be expressed using the covariance matrix $\mathbb{R}_{\mathbf{n}_J}$ of the noise vector $\mathbf{n}_J$, for $J \in \{D, E\}$, as $\mathbb{R}_{\mathbf{n}_J} = \mathbb{E}\{n_{J,u}n_{J,v}^*\} = \sigma_n^2 I_{N_J}$.

Furthermore, after some simplifications, the instantaneous end-to-end SNRs at SR and E can be expressed as

$$\digamma_D = \frac{P_s||\mathbf{h}_D||^2}{\sigma_n^2} \text{ and } \digamma_E = \frac{P_s||\mathbf{h}_E||^2}{\sigma_n^2}, \tag{7}$$

respectively, where $||\mathbf{h}_D||^2 = \sum_{i=1}^{N_D}|h_{D,i}|^2$ and $||\mathbf{h}_E||^2 = \sum_{j=1}^{N_E}|h_{E,j}|^2$. Note that we adopt the peak interference power control mechanism to satisfy the required constraint, i.e., $P_s = \frac{Q}{|h_P|^2}$, the instantaneous end-to-end SNRs $\digamma_D$ and $\digamma_E$ in (7) can be expressed, respectively, as

$$\digamma_D = \frac{\gamma_D}{|h_P|^2} \text{ and } \digamma_E = \frac{\gamma_E}{|h_P|^2}, \tag{8}$$

where $\gamma_D = \frac{Q}{\sigma_n^2}||\mathbf{h}_D||^2$ and $\gamma_E = \frac{Q}{\sigma_n^2}||\mathbf{h}_E||^2$. Also, $\overline{\gamma}_D = \frac{Q}{\sigma_n^2}\Omega_D$ and $\overline{\gamma}_E = \frac{Q}{\sigma_n^2}\Omega_E$ represent the average transmit SNRs of main and wiretap links, respectively.

The achievable rates for the main and the wiretap links are given as $\mathcal{C}_D = \log_2(1 + \digamma_D)$ and $\mathcal{C}_E = \log_2(1 + \digamma_E)$, respectively. With the help of achievable rates, the secrecy capacity can be formulated as

$$\mathcal{C}_{\text{sec}} = \max\{\mathcal{C}_D - \mathcal{C}_E, 0\}. \tag{9}$$

III. PERFORMANCE ANALYSIS

In this section, we first derive the cumulative distribution function (CDF) and the probability density function (PDF) of $\gamma_J = \frac{Q}{\sigma_n^2}||\mathbf{h}_J||^2$, where $J \in \{D, E\}$, under $\alpha-\mu$ fading channels. Using these, we evaluate some key performance measures, viz., SOP, asymptotic SOP, intercept probability alongwith its asymptotic form, and ESC, for the SIMO underlay CRNs by employing MRC at both SR and E.

A. CDFs AND PDFs OF γ_D AND γ_E

Under i.i.d. $\alpha-\mu$ fading channels, the CDF and PDF of the channel gain $|h_\iota|^2$, for $\{\iota\} \in \big(\{D, i\}, \{E, j\}, \{P\}\big)$, $i \in \{1, 2, \cdots, N_D\}$ and $j \in \{1, 2, \cdots, N_E\}$, can be given, respectively, by [29]

$$F_{|h_\iota|^2}(x) = \frac{1}{\Gamma(\mu_\kappa)}\Upsilon\Big(\mu_\kappa, \mu_\kappa\Big(\frac{x}{\Omega_\kappa}\Big)^{\frac{\alpha_\kappa}{2}}\Big), \tag{10}$$

$$f_{|h_\iota|^2}(x) = \frac{\alpha_\kappa \mu_\kappa^{\mu_\kappa}}{2\Gamma(\mu_\kappa)} \frac{x^{\frac{\mu_\kappa\alpha_\kappa}{2}-1}}{\Omega_\kappa^{\frac{\mu_\kappa\alpha_\kappa}{2}}} \mathrm{e}^{-\mu_\kappa\left(\frac{x}{\Omega_\kappa}\right)^{\frac{\alpha_\kappa}{2}}}, \tag{11}$$

where $\{\kappa\} \in (\{D\}, \{E\}, \text{ and } \{P\})$ correspond to $\{\iota\} \in \big(\{D, i\}, \{E, j\}, \text{ and } \{P\}\big)$, respectively.

Furthermore, based on the properties of MRC, the CDF and PDF of $\gamma_J = \frac{Q}{\sigma_n^2}||\mathbf{h}_J||^2$, for $J \in \{D, E\}$, under i.i.d. $\alpha-\mu$ fading channels can be given, respectively, as [31]

$$F_{\gamma_J}(x) = \frac{1}{\Gamma(N_J\mu_J)}\Upsilon\Big(N_J\mu_J, N_J\mu_J\Big(\frac{x}{N_J\overline{\gamma}_J}\Big)^{\frac{\alpha_J}{2}}\Big), \tag{12}$$

$$f_{\gamma_J}(x) = \frac{\alpha_J(N_J\mu_J)^{N_J\mu_J}}{2\Gamma(N_J\mu_J)} \frac{x^{\frac{N_J\mu_J\alpha_J}{2}-1}}{(N_J\overline{\gamma}_J)^{\frac{N_J\mu_J\alpha_J}{2}}} \mathrm{e}^{-\frac{N_J\mu_J}{(N_J\overline{\gamma}_J)^{\frac{\alpha_J}{2}}}x^{\frac{\alpha_J}{2}}} \tag{13}$$

These CDFs and PDFs will help us to evaluate the performance measures under consideration.

B. EXACT SOP ANALYSIS

A secrecy outage event happens when $\mathcal{C}_{\text{sec}}$ falls below a certain target secrecy rate $\mathcal{R}_s$ (bps/Hz), and therefore the SOP can be formulated as

$$\mathbb{P}_{\text{out}}^{\text{sec}} = \Pr[\max\{\mathcal{C}_D - \mathcal{C}_E, 0\} < \mathcal{R}_s]. \tag{14}$$

However, it is important to observe that when $\mathcal{C}_D \leq \mathcal{C}_E$, the SOP is compromised, i.e., $\mathbb{P}_{\text{out}}^{\text{sec}} = 1$. Therefore, we can evaluate the SOP for the case when $\mathcal{C}_D > \mathcal{C}_E$ as

$$\begin{aligned} \mathbb{P}_{\text{out}}^{\text{sec}} &= \Pr[\mathcal{C}_D - \mathcal{C}_E < \mathcal{R}_s] \\ &= \Pr\left[\frac{1 + \frac{\gamma_D}{|h_P|^2}}{1 + \frac{\gamma_E}{|h_P|^2}} < \eta\right] \\ &= \int_0^\infty \Bigg[\underbrace{\int_0^\infty F_{\gamma_D}\big((\eta-1)w + \eta y\big) f_{\gamma_E}(y)dy}_{\triangleq \mathbb{I}_1}\Bigg] \\ &\quad \times f_{|h_P|^2}(w)dw, \end{aligned} \tag{15}$$

where $\eta = 2^{\mathcal{R}_s}$ is the secrecy target threshold. For solving (15), we first need to simplify the inner integral $\mathbb{I}_1$ according to Theorem 1.

Theorem 1: The integral term $\mathbb{I}_1$ in (15) can be expressed as

$$\mathbb{I}_1 = \frac{2^{-\alpha_E}\xi_E}{\pi^{\alpha_E-\frac{1}{2}}\eta^{\frac{\alpha_E N_E\mu_E}{2}}\Gamma(N_D\mu_D)}\sum_{n=0}^{\infty}\frac{(-1)^n}{n!}\frac{\lambda_D^{N_D\mu_D+n}}{N_D\mu_D+n} \times \frac{(\eta-1)^{\frac{\alpha_D(N_D\mu_D+n)}{2}+\frac{\alpha_E N_E\mu_E}{2}}}{\Gamma\big(-\frac{\alpha_D(N_D\mu_D+n)}{2}\big)\alpha_E^{\frac{\alpha_D(N_D\mu_D+n)}{2}}} w^{\frac{\alpha_D(N_D\mu_D+n)}{2}+\frac{\alpha_E N_E\mu_E}{2}} \times G_{\alpha_E,\alpha_E+2}^{\alpha_E+2,\alpha_E}\left(\frac{\lambda_E^2(\eta-1)^{\alpha_E}w^{\alpha_E}}{4\eta^{\alpha_E}} \middle| \begin{matrix}\Delta\big(\alpha_E,1-\frac{\alpha_E N_E\mu_E}{2}\big)\\ \Delta(2,0),\Delta\big(\alpha_E,-\frac{\alpha_D(N_D\mu_D+n)}{2}-\frac{\alpha_E N_E\mu_E}{2}\big)\end{matrix}\right), \quad (16)$$

where $\Delta(a,b)=\frac{b}{a},\frac{b+1}{a},\cdots,\frac{b+a-1}{a}$, $\lambda_D=\frac{N_D\mu_D}{(N_D\overline{\gamma}_D)^{\frac{\alpha_D}{2}}}$, $\lambda_E=\frac{N_E\mu_E}{(N_E\overline{\gamma}_E)^{\frac{\alpha_E}{2}}}$, and $\xi_E=\frac{(N_E\mu_E)^{N_E\mu_E}}{\Gamma(N_E\mu_E)(N_E\overline{\gamma}_E)^{\frac{\alpha_E N_E\mu_E}{2}}}$.

Proof: Please see Appendix A. ∎

Then, invoking (16) alongwith the PDF $f_{|h_P|^2}(w)$ into (15), the SOP, $\mathbb{P}_{\text{out}}^{\text{sec}}(\eta)$, can be given by

$$\mathbb{P}_{\text{out}}^{\text{sec}}(\eta) = \frac{2^{-\alpha_E}\xi_E\xi_P}{\pi^{\alpha_E-\frac{1}{2}}\eta^{\frac{\alpha_E N_E\mu_E}{2}}\Gamma(N_D\mu_D)}\sum_{n=0}^{\infty}\frac{(-1)^n}{n!}\frac{\lambda_D^{N_D\mu_D+n}}{N_D\mu_D+n} \times \frac{1}{\Gamma\big(-\frac{\alpha_D(N_D\mu_D+n)}{2}\big)}\frac{(\eta-1)^{\frac{\alpha_D(N_D\mu_D+n)}{2}+\frac{\alpha_E N_E\mu_E}{2}}}{\alpha_E^{\frac{\alpha_D(N_D\mu_D+n)}{2}}} \times \left[\int_0^{\infty} w^{\frac{\alpha_D(N_D\mu_D+n)}{2}+\frac{\alpha_E N_E\mu_E}{2}+\frac{\alpha_P\mu_P}{2}-1} \times \mathrm{e}^{-\lambda_P w^{\frac{\alpha_P}{2}}} G_{\alpha_E,\alpha_E+2}^{\alpha_E+2,\alpha_E}\left(\frac{\lambda_E^2(\eta-1)^{\alpha_E}w^{\alpha_E}}{4\eta^{\alpha_E}} \middle| \begin{matrix}\Delta\big(\alpha_E,1-\frac{\alpha_E N_E\mu_E}{2}\big)\\ \Delta(2,0),\Delta\big(\alpha_E,-\frac{\alpha_D(N_D\mu_D+n)}{2}-\frac{\alpha_E\mu_E}{2}\big)\end{matrix}\right)dw\right], \quad (17)$$

where $\xi_P=\frac{\alpha_P\mu_P^{\mu_P}}{2\Gamma(\mu_P)\Omega_P^{\frac{\alpha_P\mu_P}{2}}}$ and $\lambda_P=\frac{\mu_P}{\Omega_P^{\frac{\alpha_P}{2}}}$. Now, applying $\mathrm{e}^{-x}=G_{0,1}^{1,0}(x|_0^-)$ [41] into (17) alongwith the change of variables $w^{\frac{\alpha_E}{2}}=t$, and simplifying further by utilizing the fact [42, eq. (2.24.1.1)], the exact expression of SOP is given by (18), as mentioned at the bottom of the page, where $\phi_1(n)=\frac{1}{\alpha_E}\big(\frac{\alpha_D(\mu_D N_D+n)}{2}+\frac{\alpha_P\mu_P}{2}\big)$ and $\phi_2(n)=\phi_1(n)+\frac{N_E\mu_E}{2}$.

Remark 1: It can be seen from (18) that the SOP expression mainly consists of powers and Meijer-G function containing channel/system parameters, such as, number of antennas (N_D, N_E), fading parameters $(\mu_D, \alpha_D, \mu_E, \alpha_E, \mu_P, \alpha_P)$, maximum tolerable interference level (Q), average channel gains $(\Omega_D, \Omega_E, \Omega_P)$, and secrecy target rate $(\mathcal{R}_s)$, which can readily be evaluated for the various involved parameters via Mathematica software, as shown numerically in Section V. Furthermore, it should also be noted that the infinite summation that appears in (18) can be avoided by assuming that $\mu_J\in\mathbb{Z}_+$, where $J\in\{D,E\}$.

C. ASYMPTOTIC SOP ANALYSIS

In this section, we evaluate the asymptotic SOP expressions under two cases of interest, i.e., 1) when $\overline{\gamma}_D\to\infty$ and fixed $\overline{\gamma}_E$, and 2) when $\overline{\gamma}_D\to\infty$ and $\overline{\gamma}_E\to\infty$. By doing so, we present the impact of key system/channel parameters on the secrecy diversity order of the considered system.

1) WHEN $\overline{\gamma}_D\to\infty$ AND FIXED $\overline{\gamma}_E$

By applying the approximation $\Upsilon(\beta,x)\underset{x\to 0}{\approx}\frac{x^\beta}{\beta}$ in the high $\overline{\gamma}_D$ regime, the CDF $F_{\gamma_D}(x)$ in (12) can be given by

$$F_{\gamma_D}(x)\underset{\overline{\gamma}_D\to\infty}{\approx}\frac{(N_D\mu_D)^{N_D\mu_D-1}}{\Gamma(N_D\mu_D)}\Big(\frac{x}{N_D\overline{\gamma}_D}\Big)^{\frac{N_D\mu_D\alpha_D}{2}}. \quad (19)$$

To reveal the asymptotic SOP behavior under $\overline{\gamma}_D\to\infty$ with fixed $\overline{\gamma}_E$, we need to simplify the inner integral $\mathbb{I}_1$ of (15) in the high $\overline{\gamma}_D$ region, according to Theorem 2.

Theorem 2: The integral $\mathbb{I}_1$ in (15) can be expressed for $\overline{\gamma}_D\to\infty$ with fixed $\overline{\gamma}_E$, as

$$\mathbb{I}_1\underset{\overline{\gamma}_D\to\infty}{\approx}\frac{2^{-\alpha_E}\alpha_E\xi_E(N_D\mu_D)^{N_D\mu_D-1}}{\pi^{\alpha_E-\frac{1}{2}}\Gamma(N_D\mu_D)}((\eta-1)w)^{\frac{\alpha_D N_D\mu_D}{2}} \times\frac{((\eta-1)w)^{\frac{\alpha_E N_E\mu_E}{2}}}{(N_D\overline{\gamma}_D)^{\frac{\alpha_D N_D\mu_D}{2}}\eta^{\frac{\alpha_E N_E\mu_E}{2}}}G_{\alpha_E,\alpha_E+2}^{\alpha_E+2,\alpha_E}\left(\frac{\lambda_E^2((\eta-1)w)^{\alpha_E}}{4\eta^{\alpha_E}} \times \middle| \begin{matrix}\Delta\big(\alpha_E,1-\frac{\alpha_E N_E\mu_E}{2}\big)\\ \Delta(2,0),\Delta\big(\alpha_E,-\frac{\alpha_D N_D\mu_D}{2}-\frac{\alpha_E N_E\mu_E}{2}\big)\end{matrix}\right), \quad (20)$$

Proof: By invoking the CDF $F_{\gamma_D}(x)$ from (19) alongwith the PDF of γ_E into the inner integral $\mathbb{I}_1$ of (15), and by using the transformations $(1+x)^\beta=\frac{1}{\Gamma(-\beta)}G_{1,1}^{1,1}(x|_0^{\beta+1})$ and

$$\mathbb{P}_{\text{out}}^{\text{sec}}(\eta) = \frac{2^{2-\alpha_E-\alpha_P(\alpha_E+1)}\xi_E\xi_P}{\pi^{\alpha_E+\alpha_P(\alpha_E+1)-2}\Gamma(N_D\mu_D)}\sum_{n=0}^{\infty}\frac{(-1)^n}{n!}\frac{\lambda_D^{N_D\mu_D+n}}{N_D\mu_D+n}\frac{\eta^{\alpha_E\phi_1(n)}(\eta-1)^{\frac{\alpha_P\mu_P}{2}}}{\Gamma\big(-\frac{\alpha_D(N_D\mu_D+n)}{2}\big)\alpha_E^{\frac{\alpha_D(N_D\mu_D+n)}{2}+\frac{1}{2}}} \times\left(\frac{\lambda_E^2}{4}\right)^{-\phi_2(n)}\alpha_P^{2\phi_2(n)-\frac{\alpha_D(N_D\mu_D+n)}{2}-\frac{3}{2}}G_{\alpha_P(\alpha_E+2),\alpha_P(\alpha_E+2)}^{\alpha_E(\alpha_P+2),\alpha_P(\alpha_E+2)}\left(\left(\frac{\lambda_E^2(\eta-1)^{\alpha_E}}{4\eta^{\alpha_E}}\right)^{-\alpha_P}\frac{\lambda_P^{2\alpha_E}\alpha_P^{2\alpha_P}}{(2\alpha_E)^{2\alpha_E}} \times \left| \begin{matrix}\Delta(\alpha_P,1-\phi_2(n)),\Delta(\alpha_P,\frac{1}{2}-\phi_2(n)),\Delta(\alpha_P,1-\frac{\alpha_P\mu_P}{2\alpha_E}),\Delta(\alpha_P,1-\frac{1}{\alpha_E}-\frac{\alpha_P\mu_P}{2\alpha_E}),\Delta(\alpha_P,1-\frac{2}{\alpha_E}-\frac{\alpha_P\mu_P}{2\alpha_E}),\cdots,\Delta(\alpha_P,1-\frac{\alpha_E-1}{\alpha_E}-\frac{\alpha_P\mu_P}{2\alpha_E})\\ \Delta(2\alpha_E,0),\Delta(\alpha_P,1-\frac{1}{\alpha_E}-\phi_1(n)),\Delta(\alpha_P,1-\frac{2}{\alpha_E}-\phi_1(n)),\cdots,\Delta(\alpha_P,1-\frac{\alpha_E-1}{\alpha_E}-\phi_1(n)),\Delta(\alpha_P,-\phi_1(n))\end{matrix}\right), \quad (18)$$

$\mathrm{e}^{-x} = G_{0,1}^{1,0}(x|_0^-)$ [41], and then simplifying the resultant integral $\mathbb{I}_1$ via [42, eq. (2.24.1.1)], $\mathbb{I}_1$ for the case $\overline{\gamma}_D \to \infty$ with fixed $\overline{\gamma}_E$ can be obtained, as presented in (20). ■

Furthermore, invoking (20) alongwith the PDF of $|h_P|^2$ into (15), and then by the use of the fact that $\mathrm{e}^{-x} = G_{0,1}^{1,0}(x|_0^-)$ [41] and the change of variables $w^{\alpha_E} = t$, and simplifying the required integral via [42, eq. (2.24.1.1)], the asymptotic SOP in this case can be expressed as

$$\mathbb{P}_{\text{out, asy}}^{\text{sec}}(\eta) \underset{\overline{\gamma}_D \to \infty}{\simeq} \mathbb{G}_{\text{C}} \overline{\gamma}_D^{-\frac{\alpha_D N_D \mu_D}{2}}, \tag{21}$$

where $\mathbb{G}_{\text{C}}$ denotes the secrecy array gain, as shown in (22) at the bottom of the page, where $\phi_3(n) = \frac{1}{\alpha_E}\left(\frac{\alpha_D N_D \mu_D}{2} + \frac{\alpha_P \mu_P}{2}\right)$ and $\phi_4(n) = \phi_3(n) + \frac{N_E \mu_E}{2}$.

Remark 2: It is evident from (21) that the system's achievable secrecy diversity order is $\frac{\alpha_D N_D \mu_D}{2}$, which is independent of fading parameters of E (i.e., α_E, μ_E) and PR (i.e., α_P, μ_P), and number of E's antennas (i.e., N_E).

2) WHEN $\overline{\gamma}_D \to \infty$ AND $\overline{\gamma}_E \to \infty$

For the case when $\overline{\gamma}_D \to \infty$ and $\overline{\gamma}_E \to \infty$ with fixed ratio of SNRs (i.e., $\frac{\overline{\gamma}_D}{\overline{\gamma}_E}$), $\mathbb{P}_{\text{out, asy}}^{\text{sec}}(\eta)$ can be expressed as

$$\begin{aligned}\mathbb{P}_{\text{out, asy}}^{\text{sec}}(\eta) &= \Pr\left[\frac{1+\frac{\gamma_D}{|h_P|^2}}{1+\frac{\gamma_E}{|h_P|^2}} < \eta\right] \underset{\overline{\gamma}_D, \overline{\gamma}_E \to \infty}{\approx} \Pr\left[\frac{\gamma_D}{\gamma_E} < \eta\right] \\ &= \int_0^\infty F_{\gamma_D}(\eta y) f_{\gamma_E}(y) dy. \end{aligned} \tag{23}$$

On inserting the CDF of γ_D after applying the well known relation $\Upsilon(\beta, x) = \Gamma(\beta)[1 - e^{-x}\sum_{r=0}^{\beta-1}\frac{x^r}{r!}]$ [38, eq. (8.352.6)] and the PDF $f_{\gamma_E}(x)$ into (23), we can express $\mathbb{P}_{\text{out, asy}}^{\text{sec}}(\eta)$ as

$$\begin{aligned}\mathbb{P}_{\text{out, asy}}^{\text{sec}}(\eta) = &\frac{\alpha_E \xi_E}{2}\int_0^\infty y^{\frac{\alpha_E N_E \mu_E}{2}-1}\mathrm{e}^{-\lambda_E y^{\frac{\alpha_E}{2}}} dy \\ &- \frac{\alpha_E \xi_E}{2}\sum_{r=0}^{N_D\mu_D-1}\frac{1}{r!}\left(\lambda_D \eta^{\frac{\alpha_D}{2}}\right)^r \\ &\times \int_0^\infty y^{\frac{r\alpha_D}{2}+\frac{\alpha_E N_E \mu_E}{2}-1}\mathrm{e}^{-\lambda_D(\eta y)^{\frac{\alpha_D}{2}}}\mathrm{e}^{-\lambda_E y^{\frac{\alpha_E}{2}}} dy. \end{aligned} \tag{24}$$

The first integral in (24) can be obtained by using the change of variables $\lambda_E y^{\frac{\alpha_E}{2}} = t$ and [38, eq. (8.310.1)]. Whereas, the second integral in (24) can be evaluated by first utilizing the relation $\mathrm{e}^{-x} = G_{0,1}^{1,0}(x|_0^-)$ [41] and then performing the change of variables $y^{\frac{\alpha_D}{2}} = t$ and using [42, eq. (2.24.1.1)]. Subsequently, the asymptotic SOP can be expressed as

$$\begin{aligned}&\mathbb{P}_{\text{out, asy}}^{\text{sec}}(\eta) \\ &\underset{\overline{\gamma}_D, \overline{\gamma}_E \to \infty}{\approx} 1 - \frac{(N_E\mu_E)^{N_E\mu_E}}{\Gamma(N_E\mu_E)\alpha_D^{\frac{1}{2}}}\frac{\alpha_E^{\frac{\alpha_E N_E \mu_E}{\alpha_D}+\frac{1}{2}}}{(2\pi)^{\frac{\alpha_E+\alpha_D}{2}-1}} \\ &\quad\times \frac{\eta^{-\frac{\alpha_E N_E \mu_E}{2}}}{(N_D\mu_D)^{\frac{\alpha_E N_E \mu_E}{\alpha_D}}}\left(\frac{N_D}{N_E}\right)^{\frac{\alpha_E N_E \mu_E}{2}}\left(\frac{\overline{\gamma}_D}{\overline{\gamma}_E}\right)^{\frac{\alpha_E N_E \mu_E}{2}} \\ &\quad\times \sum_{r=0}^{N_D\mu_D-1}\frac{\alpha_E^r}{r!}G_{\alpha_E,\alpha_D}^{\alpha_D,\alpha_E}\left(\frac{(N_E\mu_E)^{\alpha_D}}{(N_D\mu_D)^{\alpha_E}}\frac{\alpha_E^{\alpha_E}}{\alpha_D^{\alpha_D}}\right. \\ &\quad\times \left.\left(\frac{N_D\overline{\gamma}_D}{\eta N_E \overline{\gamma}_E}\right)^{\frac{\alpha_E N_E \mu_E}{2}}\Bigg|_{\Delta(\alpha_D,0)}^{\Delta(\alpha_E,1-r-\frac{\alpha_E N_E \mu_E}{\alpha_D})}\right). \end{aligned} \tag{25}$$

Remark 3: We can clearly reveal from (25) that the system's secrecy performance for fixed $\frac{\overline{\gamma}_D}{\overline{\gamma}_E}$ turns to a constant, and hence the secrecy diversity order in this case becomes zero. Also, the expression in (25) is valid for $\mu_D \in \mathbb{Z}_+$.

D. INTERCEPT PROBABILITY ANALYSIS

When the capacity of the main link becomes lower than that of the wiretap link's capacity, the eavesdropper can have the ability to intercept the signal transmitted by the transmitter, and therefore an intercept event happens. By contrast, the SOP is defined as the probability that the difference between the capacity of the main channel and that of the wiretap channel becomes less than a predefined secrecy rate. Therefore, It can be observed that the intercept probability is a special case of SOP with the secrecy target rate $\mathcal{R}_s = 0$ (such that $\eta = 1$). Now, substituting $\mathcal{R}_s = 0$ into (15), the intercept probability can be expressed as

$$\begin{aligned}\mathbb{P}_{\text{int}} &= \Pr[\mathcal{C}_D < \mathcal{C}_E] \\ &= \Pr[\digamma_D < \digamma_E] \\ &= \int_0^\infty F_{\gamma_D}(y) f_{\gamma_E}(y) dy. \end{aligned} \tag{26}$$

Furthermore, the intercept probability in (26) can be evaluated as per the below theorem.

$$\begin{aligned}\mathbb{G}_{\text{C}} = &\frac{2^{2-\alpha_E-\alpha_P(\alpha_E+1)}\sqrt{\alpha_E}\xi_E\xi_P(N_D\mu_D)^{N_D\mu_D-1}}{\pi^{\alpha_E+\alpha_P(\alpha_E+1)-2}\Gamma(N_D\mu_D)}\frac{(\eta-1)^{\frac{\alpha_D N_D\mu_D}{2}+\frac{\alpha_E N_E\mu_E}{2}}}{\eta^{\frac{\alpha_E N_E\mu_E}{2}}}\alpha_P^{2\phi_4(n)-\frac{\alpha_D N_D\mu_D}{2}-\frac{3}{2}} \\ &\times N_D^{-\frac{\alpha_D N_D\mu_D}{2}}\left(\frac{\lambda_E^2(\eta-1)^{\alpha_E}}{4\eta^{\alpha_E}}\right)^{-\phi_4(n)}G_{\alpha_P(\alpha_E+2),\alpha_P(\alpha_E+2)}^{\alpha_E(\alpha_P+2),\alpha_P(\alpha_E+2)}\left(\frac{\lambda_P^{2\alpha_E}\alpha_P^{2\alpha_P}}{(2\alpha_E)^{2\alpha_E}}\left(\frac{\lambda_E^2(\eta-1)^{\alpha_E}}{4\eta^{\alpha_E}}\right)^{-\alpha_P}\right. \\ &\times \left.\Bigg|_{\Delta(2\alpha_E,0),\Delta(\alpha_P,1-\frac{1}{\alpha_E}-\phi_3(n)),\Delta(\alpha_P,1-\frac{2}{\alpha_E}-\phi_3(n)),\cdots,\Delta(\alpha_P,1-\frac{\alpha_E-1}{\alpha_E}-\phi_3(n)),\Delta(\alpha_P,-\phi_3(n))}^{\Delta(\alpha_P,1-\phi_4(n)),\Delta(\alpha_P,\frac{1}{2}-\phi_4(n)),\Delta(\alpha_P,1-\frac{\alpha_P\mu_P}{2\alpha_E}),\Delta(\alpha_P,1-\frac{1}{\alpha_E}-\frac{\alpha_P\mu_P}{2\alpha_E}),\Delta(\alpha_P,1-\frac{2}{\alpha_E}-\frac{\alpha_P\mu_P}{2\alpha_E}),\cdots,\Delta(\alpha_P,1-\frac{\alpha_E-1}{\alpha_E}-\frac{\alpha_P\mu_P}{2\alpha_E})}\right), \end{aligned} \tag{22}$$

Theorem 3: The intercept probability for the considered system over $\alpha-\mu$ fading channels can be expressed as

$$\mathbb{P}_{\text{int}} = 1 - \frac{(N_E\mu_E)^{N_E\mu_E}}{\Gamma(N_E\mu_E)\alpha_D^{\frac{1}{2}}}\frac{(N_D\mu_D)^{-\frac{\alpha_E N_E\mu_E}{\alpha_D}}}{(2\pi)^{\frac{\alpha_E+\alpha_D}{2}-1}} \times \alpha_E^{\frac{\alpha_E N_E\mu_E}{\alpha_D}+\frac{1}{2}}\left(\frac{N_D\overline{\gamma}_D}{N_E\overline{\gamma}_E}\right)^{\frac{\alpha_E N_E\mu_E}{2}}\sum_{r=0}^{N_D\mu_D-1}\frac{\alpha_E^r}{r!} \times G_{\alpha_E,\alpha_D}^{\alpha_D,\alpha_E}\left(\frac{(N_E\mu_E)^{\alpha_D}}{(N_D\mu_D)^{\alpha_E}}\frac{\alpha_E^{\alpha_E}}{\alpha_D^{\alpha_D}}\left(\frac{N_D\overline{\gamma}_D}{N_E\overline{\gamma}_E}\right)^{\frac{\alpha_E N_E\mu_E}{2}} \times \Bigg|_{\Delta(\alpha_D,0)}^{\Delta\left(\alpha_E,1-r-\frac{\alpha_E N_E\mu_E}{\alpha_D}\right)}\right). \quad (27)$$

Proof: See Appendix B for the detailed proof. ■

Remark 4: The expression of intercept probability given by (27) comprises the Meijer-*G* function with the finite summation that can simply be solved for different values of the system/channel parameters with the help of the Mathematica computational software package. Moreover, it should be noted that (27) is valid for $\mu_D \in \mathbb{Z}_+$.

E. ASYMPTOTIC INTERCEPT PROBABILITY ANALYSIS

This section examines the achievable secrecy diversity order and reveals some critical insights for the considered system in the $\alpha-\mu$ fading scenario, which has not been done so far in the literature to the best of the authors' knowledge. Specifically, we obtain the secrecy diversity order by deriving the asymptotic intercept probability expression for the case when $\overline{\gamma}_D \to \infty$ and $\overline{\gamma}_E$ is fixed.

Now, on inserting the CDF expression given in (19) for high $\overline{\gamma}_D$ region and the PDF expression of γ_E into (26), we can get the expression of asymptotic intercept probability with fixed $\overline{\gamma}_E$, considering high $\overline{\gamma}_D$ regime, as

$$\mathbb{P}_{\text{int}}^{\text{asy}} \underset{\overline{\gamma}_D\to\infty}{\simeq} \frac{\alpha_E\xi_E(N_D\mu_D)^{N_D\mu_D-1}}{2\Gamma(N_D\mu_D)(N_D\overline{\gamma}_D)^{\frac{N_D\mu_D\alpha_D}{2}}} \times \int_0^\infty y^{\frac{N_D\mu_D\alpha_D}{2}+\frac{\alpha_E N_E\mu_E}{2}-1}\mathrm{e}^{-\lambda_E y^{\frac{\alpha_E}{2}}}dy. \quad (28)$$

Furthermore, on applying the change of variables $\lambda_E y^{\frac{\alpha_E}{2}} = t$, we can get

$$\mathbb{P}_{\text{int}}^{\text{asy}} \underset{\overline{\gamma}_D\to\infty}{\simeq} \frac{\xi_E(N_D\mu_D)^{N_D\mu_D-1}}{\Gamma(N_D\mu_D)(N_D\overline{\gamma}_D)^{\frac{N_D\mu_D\alpha_D}{2}}}\frac{1}{\lambda_E^{\frac{\alpha_D N_D\mu_D+\alpha_E N_E\mu_E}{\alpha_E}}} \times \int_0^\infty y^{\frac{\alpha_D N_D\mu_D+\alpha_E N_E\mu_E}{\alpha_E}-1}\mathrm{e}^{-t}dt. \quad (29)$$

Now, on utilizing [38, eq. (8.310.1)] to solve the integral in (29) and applying some mathematical formulations, one can get $\mathbb{P}_{\text{int}}^{\text{asy}}$ in the high $\overline{\gamma}_D$ region with fixed $\overline{\gamma}_E$ as

$$\mathbb{P}_{\text{int}}^{\text{asy}} \underset{\overline{\gamma}_D\to\infty}{\simeq} \frac{(N_D\mu_D)^{N_D\mu_D-1}(N_E\mu_E)^{-\frac{\alpha_D N_D\mu_D}{\alpha_E}}}{\Gamma(N_D\mu_D)\Gamma(N_E\mu_E)} \times \frac{(N_E\overline{\gamma}_E)^{\frac{\alpha_D N_D\mu_D}{2}}}{(N_D\overline{\gamma}_D)^{\frac{\alpha_D N_D\mu_D}{2}}}\Gamma\left(\frac{\alpha_D N_D\mu_D+\alpha_E N_E\mu_E}{\alpha_E}\right). \quad (30)$$

Remark 5: With the help of (30), we unveil two important insights: 1) the system can achieve a secrecy diversity order of $\frac{\alpha_D N_D\mu_D}{2}$, and 2) if both the average SNRs of main and wiretap links tend to infinity, i.e., $\overline{\gamma}_D \to \infty$ and $\overline{\gamma}_E \to \infty$, while maintaining the ratio $\frac{\overline{\gamma}_E}{\overline{\gamma}_D}$ in (30) as finite constant, then the system will become exposed to the perfect eavesdropping that yields into a zero system secrecy diversity order.

F. EXACT ESC ANALYSIS

The expression for the instantaneous secrecy capacity for the considered system can be formulated as

$$\begin{aligned}\mathcal{C}_{\text{sec}} &= \max\{\mathcal{C}_D - \mathcal{C}_E, 0\} \\ &= \max\{\log_2(1+\digamma_D) - \log_2(1+\digamma_E), 0\}. \end{aligned} \quad (31)$$

Further, by considering the case $\gamma_D > \gamma_E$ and averaging (31) over the distributions of $\digamma_D$ and $\digamma_E$, one can get the ESC expression as

$$\begin{aligned}\overline{\mathcal{C}}_{\text{sec}} &= \mathbb{E}\big[\log_2(1+\digamma_D) - \log_2(1+\digamma_E)\big] \\ &= \mathbb{E}_{\{|h_P|^2,\gamma_D,\gamma_E\}}\left[\log_2\left(1+\frac{\gamma_D}{|h_P|^2}\right) - \log_2\left(1+\frac{\gamma_E}{|h_P|^2}\right)\right], \end{aligned} \quad (32)$$

that can be expanded in the integral form as

$$\begin{aligned}\overline{\mathcal{C}}_{\text{sec}} = \frac{1}{\ln(2)}\int_0^\infty \Bigg[&\underbrace{\int_0^\infty y\ln(1+x)f_{\gamma_D}(xy)F_{\gamma_E}(xy)dx}_{\triangleq \mathbb{J}_1} \\ &+ \underbrace{\int_0^\infty y\ln(1+x)f_{\gamma_E}(xy)F_{\gamma_D}(xy)dx}_{\triangleq \mathbb{J}_2} \\ &- \underbrace{\int_0^\infty y\ln(1+x)f_{\gamma_E}(xy)dx}_{\triangleq \mathbb{J}_3}\Bigg] f_{|h_P|^2}(y)dy. \end{aligned} \quad (33)$$

$$\mathbb{J}_1 = \frac{2^{-\alpha_D}\xi_D}{\pi^{\alpha_D-\frac{1}{2}}\Gamma(N_E\mu_E)}\sum_{n=0}^\infty\frac{(-1)^n}{n}\lambda_E^{N_E\mu_E+n}y^{\phi_5(n)}G_{2\alpha_D,2\alpha_D+2}^{2\alpha_D+2,\alpha_D}\left(\frac{\lambda_D^2 y^{\alpha_D}}{4}\Big|\begin{matrix}\Delta(\alpha_D,-\phi_5(n)),\Delta(\alpha_D,1-\phi_5(n))\\ \Delta(2,0),\Delta(\alpha_D,-\phi_5(n)),\Delta(\alpha_D,-\phi_5(n))\end{matrix}\right), \quad (34)$$

$$\mathbb{J}_2 = \frac{2^{-\alpha_E}\xi_E}{\pi^{\alpha_E-\frac{1}{2}}\Gamma(N_D\mu_D)}\sum_{n=0}^\infty\frac{(-1)^n}{n!}\lambda_D^{N_D\mu_D+n}y^{\phi_6(n)}G_{2\alpha_E,2\alpha_E+2}^{2\alpha_E+2,\alpha_E}\left(\frac{\lambda_E^2 y^{\alpha_E}}{4}\Big|\begin{matrix}\Delta(\alpha_E,-\phi_6(n)),\Delta(\alpha_E,1-\phi_6(n))\\ \Delta(2,0),\Delta(\alpha_E,-\phi_6(n)),\Delta(\alpha_E,-\phi_6(n))\end{matrix}\right), \quad (35)$$

$$\mathbb{J}_3 = \frac{2^{-\alpha_E}\xi_E}{\pi^{\alpha_E-\frac{1}{2}}}y^{\frac{N_E\mu_E\alpha_E}{2}}G_{2\alpha_D,2\alpha_D+2}^{2\alpha_D+2,\alpha_D}\left(\frac{\lambda_E^2 y^{\alpha_E}}{4}\Big|\begin{matrix}\Delta(\alpha_E,-\frac{N_E\mu_E\alpha_E}{2}),\Delta(\alpha_E,1-\frac{N_E\mu_E\alpha_E}{2})\\ \Delta(2,0),\Delta(\alpha_D,-\frac{N_E\mu_E\alpha_E}{2}),\Delta(\alpha_D,-\frac{N_E\mu_E\alpha_E}{2})\end{matrix}\right), \quad (36)$$

For evaluating $\overline{\mathcal{C}}_{\text{sec}}$ in (33), the integrals $\mathbb{J}_1, \mathbb{J}_2$, and $\mathbb{J}_3$ are first simplified as per Theorem 4.

Theorem 4: The integrals $\mathbb{J}_1, \mathbb{J}_2$, and $\mathbb{J}_3$ in (33) can be expressed in (34), (35), and (36), respectively, as shown at the bottom of the previous page, where $\xi_D = \frac{(N_D\mu_D)^{N_D\mu_D}}{\Gamma(N_D\mu_D)} \frac{1}{(N_D\overline{\gamma}_D)^{\frac{\alpha_D N_D\mu_D}{2}}}$, $\phi_5(n) = \frac{N_D\mu_D\alpha_D}{2} + \frac{(N_E\mu_E+n)\alpha_E}{2}$, and $\phi_6(n) = \frac{N_E\mu_E\alpha_E}{2} + \frac{(N_D\mu_D+n)\alpha_D}{2}$.

Proof: Please see Appendix C. ∎

On invoking (34), (35), and (36) alongwith the PDF of $|h_P|^2$ into (33), and applying the change of variables $y^{\frac{\alpha_P}{2}} = t$ and then using [42, eq. (2.24.3.1)], $\overline{\mathcal{C}}_{\text{sec}}$ can be obtained as

$$\begin{aligned}\overline{\mathcal{C}}_{\text{sec}} = \frac{1}{\ln(2)}\Bigg[&\frac{\xi_D\xi_P}{\pi^{\alpha_D+\alpha_P(\alpha_D+1)-2}\Gamma(N_E\mu_E)}\sum_{n=0}^{\infty}\frac{(-1)^n}{n!}\\ &\times 2^{\phi_7(n)-\alpha_D}2^{-\alpha_P(\alpha_D+1)-2}\alpha_P^{-\frac{3}{2}}\alpha_D^{\phi_7(n)-\frac{1}{2}}\lambda_E^{N_E\mu_E+n}\\ &\times \mathcal{S}(\alpha_D,\lambda_D,\phi_7(n),\phi_5(n)) + \frac{\xi_E\xi_P}{\Gamma(N_D\mu_D)}\sum_{n=0}^{\infty}\frac{(-1)^n}{n!}\\ &\times \frac{2^{\phi_8(n)-\alpha_E-\alpha_P(\alpha_E+1)-2}}{\pi^{\alpha_E+\alpha_P(\alpha_E+1)-2}}\alpha_P^{-\frac{3}{2}}\alpha_E^{\phi_8(n)-\frac{1}{2}}\lambda_D^{N_D\mu_D+n}\\ &\times \mathcal{S}(\alpha_E,\lambda_E,\phi_8(n),\phi_6(n))\frac{2\pi^{-\alpha_E}\xi_E\xi_P}{\pi^{\alpha_P(\alpha_E+1)-2}}\alpha_P^{-\frac{3}{2}}\alpha_E^{\phi_9-\frac{1}{2}}\\ &- 2^{\phi_9-\alpha_E-\alpha_P(\alpha_E+1)}\mathcal{S}\Big(\alpha_E,\lambda_E,\phi_5,\frac{N_E\mu_E\alpha_E}{2}\Big)\Bigg],\end{aligned} \tag{37}$$

where $\phi_7(n) = \frac{2}{\alpha_P}\big(\frac{\alpha_P\mu_P}{2} + \phi_5(n)\big)$, $\phi_8(n) = \frac{2}{\alpha_P}\big(\frac{\alpha_P\mu_P}{2} + \phi_6(n)\big)$, $\phi_9 = \frac{2}{\alpha_P}\big(\frac{\alpha_P\mu_P}{2} + \frac{\alpha_E N_E\mu_E}{2}\big)$, and $\mathcal{S}(a,b,c,d)$ is shown in (38) at the bottom of the next page.

Remark 6: The ESC in (32) for $\gamma_D \geq \gamma_E$ can be given by

$$\overline{\mathcal{C}}_{\text{sec}} = \frac{1}{\ln(2)}\int_0^{\infty} f_{\gamma_E}(\gamma_E)\int_{\gamma_E}^{\infty}\ln\left(\frac{1+\frac{\gamma_D}{|h_P|^2}}{1+\frac{\gamma_E}{|h_P|^2}}\right) \times f_{\gamma_D}(\gamma_D)d\gamma_D d\gamma_E. \tag{39}$$

On inserting $\gamma_D = \frac{Q}{\sigma_n^2}\Omega_D x$ and $\gamma_E = \frac{Q}{\sigma_n^2}\Omega_E y$ in (39) and performing some simple mathematical formulations, we can get (39) in the high $\frac{Q}{\sigma_n^2}$ regime (i.e., $\frac{Q}{\sigma_n^2} \to \infty$) as

$$\overline{\mathcal{C}}_{\text{sec}} \underset{\frac{Q}{\sigma_n^2}\to\infty}{\simeq} \frac{1}{\ln(2)}\int_0^{\infty}\int_{\frac{\Omega_E}{\Omega_D}y}^{\infty}\ln\left(\frac{\Omega_D x}{\Omega_E y}\right)\Psi(x,y)dxdy, \tag{40}$$

where $\Psi(x,y) = \frac{\alpha_D\alpha_E(N_D\mu_D)^{N_D\mu_D}(N_E\mu_E)^{N_E\mu_E}}{4\Gamma(N_D\mu_D)\Gamma(N_E\mu_E)}x^{\frac{N_D\mu_D\alpha_D}{2}-1} \times y^{\frac{N_E\mu_E\alpha_E}{2}-1}\mathrm{e}^{-N_D\mu_D x^{\frac{\alpha_D}{2}}}\mathrm{e}^{-N_E\mu_E y^{\frac{\alpha_E}{2}}}$. On utilizing [38, eq. (3.351.1)] and [38, eq. (3.351.2)], and performing some algebraic formulations, we can obtain the ESC expression in (40) at high $\frac{Q}{\sigma_n^2}$ regime, which is not derived here for brevity. From (40), one can note that the ESC improves with the increase in $\frac{Q}{\sigma_n^2}$, indicating an improvement in the source transmitting power. But, an error floor exists for ESC at high $\frac{Q}{\sigma_n^2}$ regime due to the concurrent rise in the SNRs at both SR and E. This behavior is also depicted numerically in Section V.

Remark 7: Note that (40) can also be expressed as

$$\begin{aligned}\overline{\mathcal{C}}_{\text{sec}} = \frac{1}{\ln(2)}\Bigg[&\int_0^{\infty}\int_{\frac{\Omega_E}{\Omega_D}y}^{\infty}\ln\left(\frac{x}{y}\right)\Psi(x,y)dxdy\\ &+ \ln\left(\frac{\Omega_D}{\Omega_E}\right)\int_0^{\infty}\int_{\frac{\Omega_E}{\Omega_D}y}^{\infty}\Psi(x,y)dxdy\Bigg].\end{aligned} \tag{41}$$

Herein, ESC follows the scaling law of $\Theta\big(\ln\big(\frac{\Omega_D}{\Omega_E}\big)\big)$ as $\frac{\Omega_D}{\Omega_E}$ increases due the fact that both integrals in (41) are consistent.

IV. CONVERGENCE FOR INFINITE SUMMATIONS

We can observe that the SOP analysis in Section III-B and ESC analysis in Section III-F rely on infinite summations. As a result, convergence of the infinite summations becomes important to obtain tractability, as given in Lemma 1.

Lemma 1: Considering a finite number of terms $\mathcal{M}$, we can have $\lim_{\mathcal{M}\to\infty}\epsilon = 0$, where ϵ represents the truncation error.

Proof: Assuming that the infinite summation under $\mathbb{I}_1$ in (16) converges for a finite $\mathcal{M}$ number of terms, therefore the corresponding truncation error can be given by

$$\begin{aligned}\epsilon = &\frac{2^{-\alpha_E}\xi_E}{\pi^{\alpha_E-\frac{1}{2}}\Gamma(N_D\mu_D)}(\eta-1)^{\frac{\alpha_D N_D\mu_D}{2}+\frac{\alpha_E N_E\mu_E}{2}}\\ &\times\frac{\lambda_D^{N_D\mu_D}\alpha_E^{\frac{\alpha_D N_D\mu_D}{2}}}{\eta^{\frac{\alpha_E N_E\mu_E}{2}}}w^{\frac{\alpha_D N_D\mu_D}{2}+\frac{\alpha_E N_E\mu_E}{2}}\\ &\times\sum_{n=\mathcal{M}}^{\infty}\frac{(-1)^n}{n!}\left(\frac{\lambda_D(\eta-1)^{\frac{\alpha_D}{2}}}{\alpha_E^{\frac{\alpha_D}{2}}}\right)^n\frac{w^{\frac{n\alpha_D}{2}}}{N_D\mu_D+n}\\ &\times\frac{1}{\Gamma\big(-\frac{\alpha_D(N_D\mu_D+n)}{2}\big)}G^{\alpha_E+2,\alpha_E}_{\alpha_E,\alpha_E+2}\left(\frac{\lambda_E^2(\eta-1)^{\alpha_E}w^{\alpha_E}}{4\eta^{\alpha_E}}\right.\\ &\times\left.\begin{matrix}\Delta\big(\alpha_E,1-\frac{\alpha_E N_E\mu_E}{2}\big)\\ \Delta(2,0),\Delta\big(\alpha_E,-\frac{\alpha_D(N_D\mu_D+n)}{2}-\frac{\alpha_E N_E\mu_E}{2}\big)\end{matrix}\right),\end{aligned} \tag{42}$$

from which it is clear that because $\frac{\big(\lambda_D(\eta-1)^{\frac{\alpha_D}{2}}\alpha_E^{\frac{-\alpha_D}{2}}\big)^n}{n!(N_D\mu_D+n)} \to 0$ for $\mathcal{M} \to \infty$, $n = \mathcal{M}, \cdots, \infty$, the truncation error approaches to zero, which proves the infinite summation convergence under $\mathbb{I}_1$. This proof can also be applicable for the other findings under Sections III-B and III-F to show the convergence behavior of the relevant infinite summations. ∎

V. NUMERICAL RESULTS AND DISCUSSION

In this section, we provide numerical and simulation results using the software tools like Mathematica and Matlab to validate our analytical findings. As the infinite series is involved in the SOP and ESC expressions, therefore, we show that the accurate results can be obtained by considering a few terms ($n = 5$) and after that, it converges.

Fig. 2 illustrates the SOP performance for the considered system versus $\overline{\gamma}_D$ for different values of α_D, μ_D, and N_D,

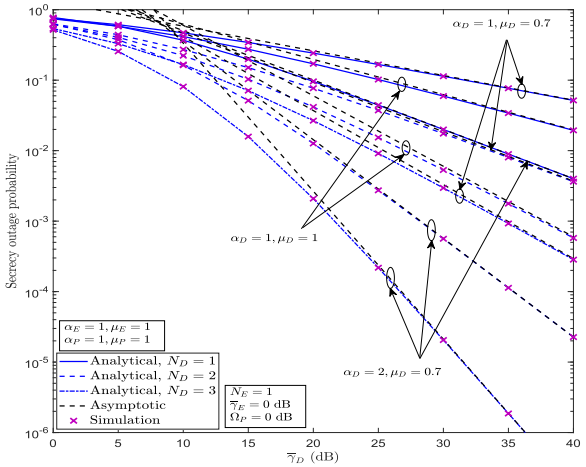

FIGURE 2. SOP performance with different values of α_D, μ_D, and N_D.

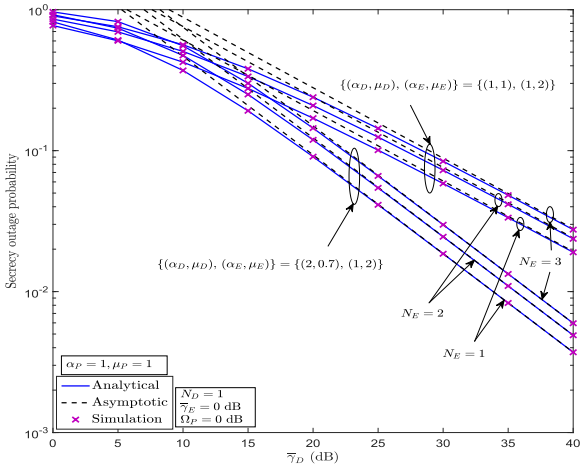

FIGURE 3. Effect of wiretap channel/system parameters on the SOP performance.

when $\mathcal{R}_s = 1$ bps/Hz, $\alpha_E = \mu_E = 1$, $\alpha_P = \mu_P = 1$, $N_E = 1$, and $\overline{\gamma}_E = \Omega_P = 0$ dB. It can be observed from this figure that the analytical results in (18) are matched perfectly with the simulation results over the entire range of $\overline{\gamma}_D$. Also, the asymptotic results in (21) are in good agreement with the exact results in the medium-to-high $\overline{\gamma}_D$ regime. This verifies the correctness of our derived theoretical results. As expected, the SOP performance increases as α_D and/or μ_D increases, irrespective of number of antennas N_D. This is due to the fact that the legitimate channel is lees faded and less vulnerable to the variations with the increased α_D and μ_D. In addition, the SOP performance increases significantly as number of antennas at the legitimated destination, N_D, increases, regardless of α_D and μ_D. Moreover, a secrecy diversity order of $\frac{\alpha_D \mu_D N_D}{2}$ (as proved analytically in Section III-C) can also be verified from the slope of the curves for different values of involved parameters.

In Fig. 3, we demonstrate the impact of wiretap channel/system parameters on the SOP performance, when when $\mathcal{R}_s = 1$ bps/Hz, $\alpha_P = \mu_P = 1$, $N_D = 1$, and $\overline{\gamma}_E = \Omega_P = 0$ dB. We can infer from this figure that the analytical results are in perfect consonance with the simulation results. From Fig. 3, it can be observed that the SOP decreases when the channel parameters of wiretap link (α_E and μ_E) are lower than the channel parameters of legitimated link (α_D and μ_D) (or in other words, when the fading severity of legitimate link is lower than the fading severity of wiretap link). Moreover, the SOP performance considerably deteriorates as the number of eavesdropper antennas N_E increases, irrespective of $\alpha_E, \mu_E, \alpha_D,$ and μ_D.

In Fig. 4, we show the SOP performance when $\overline{\gamma}_D$ and $\overline{\gamma}_E$ improve simultaneously, for different values of α_D, μ_D, N_D, and N_E. We set $\mathcal{R}_s = 1$ bps/Hz, $\alpha_E = 1, \mu_E = 2$,

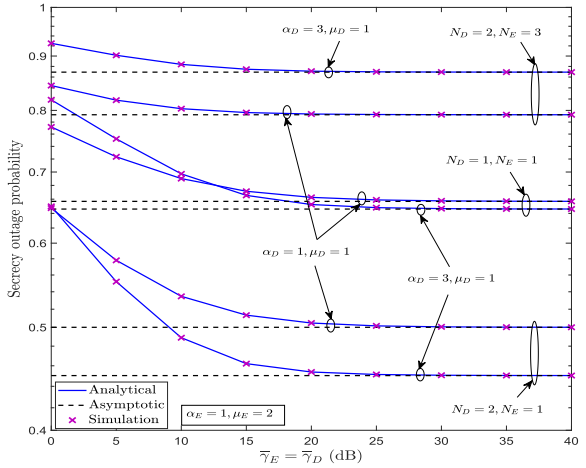

FIGURE 4. SOP performance of the considered system with simultaneous improvement in $\overline{\gamma}_D$ and $\overline{\gamma}_E$.

$\alpha_P = \mu_P = 1$, and $\Omega_P = 0$ dB. It can be seen from this figure that the SOP performance improves slightly in the low-to-medium SNR regime, however saturates in the high SNR regime, regardless of α_D, μ_D, N_D, and N_E. This is owing to the simultaneous improvement in both $\overline{\gamma}_D$ and $\overline{\gamma}_E$. Furthermore, as expected, the SOP performance improves as α_D and μ_D strengthen, irrespective of $\overline{\gamma}_D$ and $\overline{\gamma}_E$. In addition, for fixed values of α_D and μ_D, we can also observed that the SOP performance enhances as N_D increases (i.e., from $N_D = 1$ to $N_D = 2$ for fixed value of $N_E = 1$), however this SOP performance deteriorates significantly as N_E increases (i.e., from $N_E = 2$ to $N_E = 3$ for fixed value of $N_D = 2$).

Fig. 5 demonstrates the impact of Ω_P on the SOP performance for various values of α_D, μ_D, α_E, μ_E, N_D, and N_E,

$$\mathcal{S}(a,b,c,d) = G_{2a(\alpha_P+1),2\alpha_P(a+1)}^{2\alpha_P(a+1),a(\alpha_P+2)}\left(\left(\frac{b}{2\alpha_P}\right)^{2\alpha_P}\left(\frac{2a}{\lambda_P}\right)^{2a}\middle|\begin{matrix}\Delta(2a,1-c),\Delta(\alpha_P,\Delta(\alpha_E,-d)),\Delta(\alpha_P,\Delta(\alpha_E,1-d))\\ \Delta(\alpha_P,\Delta(2,0)),\Delta(\alpha_P,\Delta(\alpha_E,-d)),\Delta(\alpha_P,\Delta(\alpha_E,-d))\end{matrix}\right). \tag{38}$$

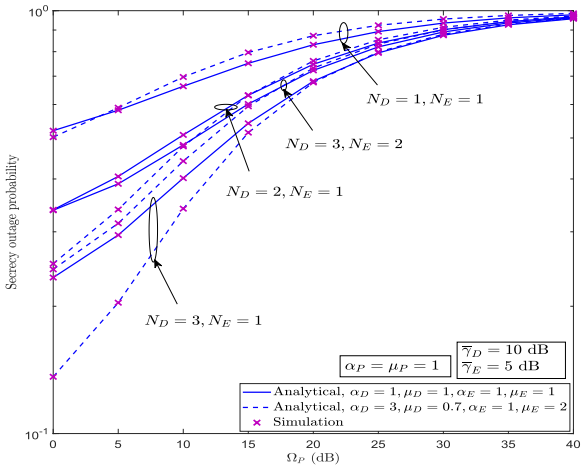

FIGURE 5. Effect of primary receiver on SOP performance.

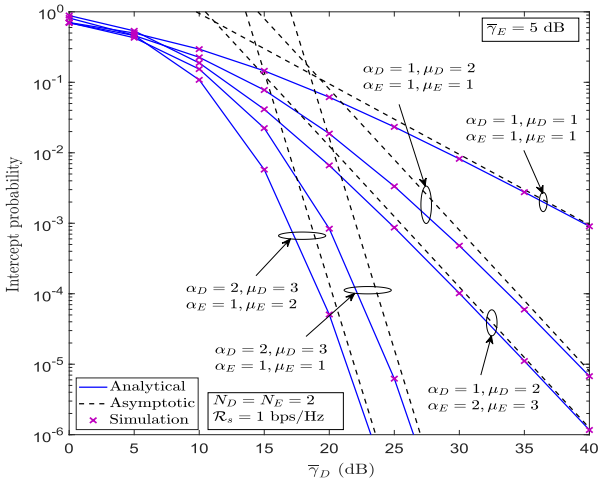

FIGURE 6. Intercept probability versus $\overline{\gamma}_D$ for various values of α_D, μ_D, α_E, and μ_E.

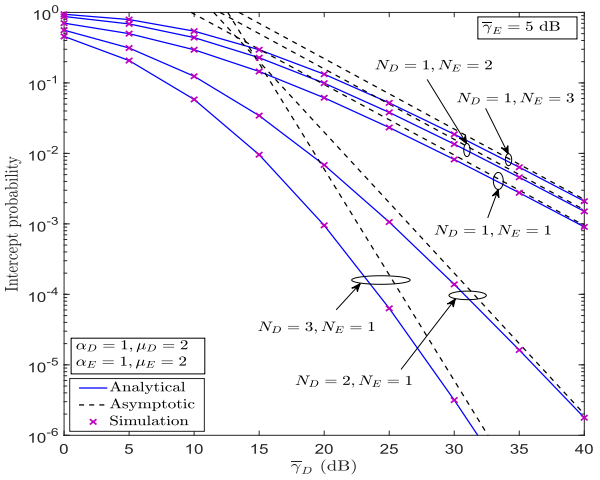

FIGURE 7. Impact of N_D and N_E on the Intercept probability performance.

when $\mathcal{R}_s = 1$ bps/Hz, $\alpha_P = \mu_P = 1$, and $\overline{\gamma}_D = 10$ dB, $\overline{\gamma}_E = 5$ dB. It can be observed from this figure that the SOP performance reduces significantly with the increase in Ω_P, irrespective of different values of α_D, μ_D, α_E, μ_E, N_D, and N_E. This is due to the fact that the transmit power at ST decreases as Ω_P increases, and hence less power is available at ST for transmitting the desired information successfully.

Fig. 6 depicts the intercept probability curves versus $\overline{\gamma}_D$ for different values of α_D, μ_D, α_E, and μ_E, when $\overline{\gamma}_E = 5$ dB, and $N_D = N_E = 2$. From this figure, one can perceive that all the analytical results based on (27) are in good consonance with the simulation results for the complete range of $\overline{\gamma}_D$. Moreover, the asymptotic results based on (30) are also in accordance with the exact ones in the medium-to-high $\overline{\gamma}_D$. Further, one can also note from Fig. 6 that as α_D and/or μ_D increases, the intercept probability decreases for fixed values of α_E and μ_E. This behavior is evinced because the channel is less faded and less vulnerable to the changes in higher values of α_D and μ_D. Also, for fixed values of α_D and μ_D, the intercept probability performance enhances significantly with the improvement in α_E and/or μ_E. This indicates that the higher values of α_E and μ_E will strengthen the wiretap link, and hence results into the high probability of eavesdropping. Also, the system's secrecy diversity order is $\frac{\alpha_D N_D \mu_D}{2}$ (as given analytically in Section III-E), which is consistent with the slope of the asymptotic curves in Fig. 6.

In Fig. 7, we demonstrate the impact of number of antennas (N_D and N_E) on the intercept probability, when $\overline{\gamma}_E = 5$ dB, $\alpha_D = 1$, $\mu_D = 2$, and $\alpha_E = 1$, $\mu_E = 2$. It can be observed from this figure that the intercept probability increases when N_D is increased for fixed value of N_E and vice-versa, for all values of γ_D. This implies that the higher values of N_D strengthen the main channel quality, which results into a low probability of eavesdropping. On the other hand, the higher values of N_E improve the wiretap channel quality, which results into a high probability of successful eavesdropping. Also, from the plots in Fig. 7, the secrecy diversity order of $\frac{\alpha_D N_D \mu_D}{2}$ is proved by the slope of the curves for different values of system/channel parameters.

In Fig. 8, we show the ESC performance versus $\overline{\gamma}_D$ curves for different values of $\overline{\gamma}_E$, α_D, μ_D, α_E, and μ_E, when $N_D = N_E = 2, \alpha_P = \mu_P = 1$, and $\Omega_P = 0$ dB. From this figure, one can manifestly see the accuracy of our derived ESC expression given in (37) by the close consonance between the simulation results and analytical results for the entire range of $\overline{\gamma}_D$. One can also note that the ESC performance degrades as $\overline{\gamma}_E$ increases, despite the values of α_D, μ_D, α_E, and μ_E. This is due to the fact that the increase in $\overline{\gamma}_E$ value improves the quality of wiretap link, and therefore enhances the capacity of wiretap channel. Further, the ESC performance becomes better for the case when the quality of main channel (i.e., α_D and μ_D) is superior than the wiretap channel (i.e., α_E and μ_E).

In Fig. 9, we demonstrate the impact of number of antennas (N_D and N_E) on the ESC performance, when $\alpha_D = \mu_D = 1$, $\alpha_E = \mu_E = 1$, $\alpha_P = \mu_P = 1$, $\overline{\gamma}_E = 5$ dB, and

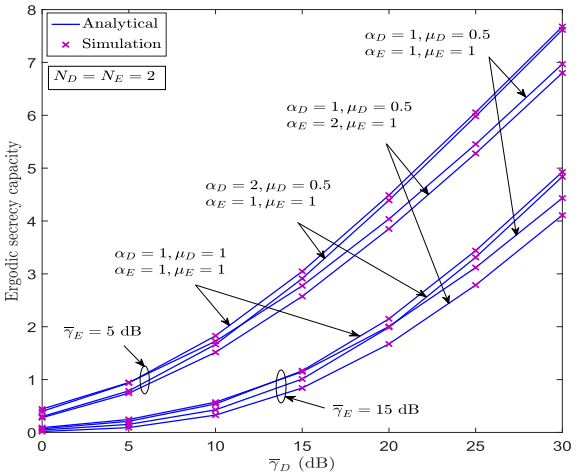

FIGURE 8. ESC performance versus $\overline{\gamma}_D$ for various $\overline{\gamma}_E$, α_D, μ_D, α_E, and μ_E.

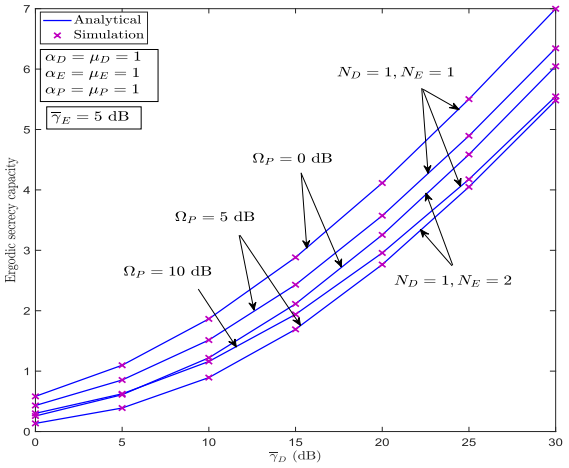

FIGURE 10. Impact of Ω_P on the ESC performance.

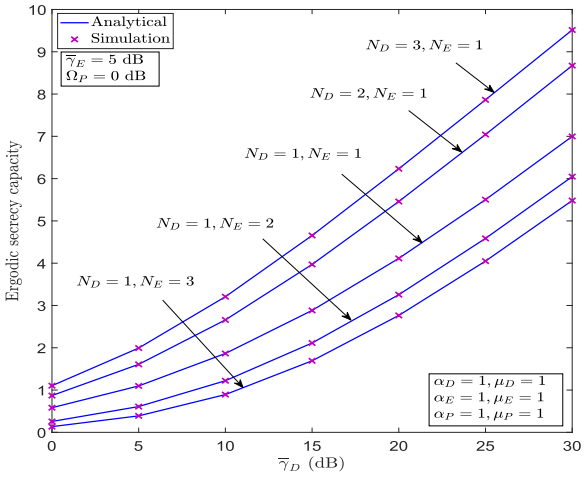

FIGURE 9. Impact of N_D and N_E on the ESC performance.

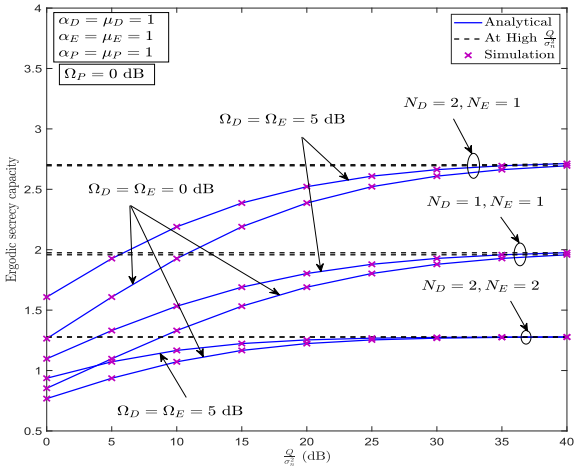

FIGURE 11. ESC versus $\frac{Q}{\sigma_n^2}$ for various values of Ω_D, Ω_E, N_D, and N_E.

$\Omega_P = 0$ dB. We can easily observe from this figure that the ESC performance significantly improves as the number of antennas at the legitimated destination, N_D, increases, for all values of $\overline{\gamma}_D$. Whereas, the ESC performance deteriorates with the increase in number of antennas at the eavesdropper terminal N_E, over the entire range of $\overline{\gamma}_D$.

Fig. 10 depicts the effect of Ω_P on the system performance in terms of ESC with $\overline{\gamma}_E = 5$ dB, $\alpha_D = \mu_D = 1$, $\alpha_E = \mu_E = 1$, $\alpha_P = \mu_P = 1$, $N_D = 1$, and $N_E = \{1, 2\}$. For fixed values of N_D and N_E, one can infer that the system's ESC performance is better with a lower value of Ω_P. Alternatively, we can say that the ESC performance degrades as Ω_P increases. This is because the transmit power at ST increases as the value of Ω_P decreases.

In Fig. 11, we demonstrate the ESC versus $\frac{Q}{\sigma_n^2}$ for various values of Ω_D, Ω_E, N_D, and N_E, when $\alpha_D = \mu_D = 1$, $\alpha_E = \mu_E = 1$, $\alpha_P = \mu_P = 1$, and $\Omega_P = 0$ dB. For fixed values of Ω_D and Ω_E, it can be observed from Fig. 11 that the ESC performance improves as N_D increases, and reduces with the increased in N_E. In addition, the ESC performance enhances when the value of $\frac{Q}{\sigma_n^2}$ increases in low region of $\frac{Q}{\sigma_n^2}$, whereas it starts saturating in the high $\frac{Q}{\sigma_n^2}$ region, regardless of Ω_D, Ω_E, N_D, and N_E. This is due to the fact that the ESC behaves independently from $\frac{Q}{\sigma_n^2}$ in the high $\frac{Q}{\sigma_n^2}$ region, which is theoretically specified in the Remark 6 of Section III-F.

VI. CONCLUSION

This paper examined the secrecy performance of a secure SIMO underlay CRN with peak interference type of power control for the $\alpha-\mu$ fading scenario. The exact expressions for the SOP, intercept probability, and ESC were derived and validated through Monte-Carlo simulations. Also, we obtained the asymptotic SOP expressions under two cases of interest; 1) when the main link SNR tends to infinity with fixed eavesdropper average SNR, and 2) when both the main link and eavesdropper link average SNRs go to infinity. From case 1, it is revealed that the system can achieve a secrecy diversity order of $\frac{\alpha_D N_D \mu_D}{2}$, whereas the diversity order reduces to zero under case 2. Moreover, we derived the asymptotic intercept probability expression in the high SNR regime (main link) with fixed eavesdropper

average SNR, from which a secrecy diversity order of $\frac{\alpha_D N_D \mu_D}{2}$ can also be obtained. Furthermore, based on the ESC analysis, we demonstrated that the ESC obeys a scaling law of $\Theta\big(\ln\big(\frac{\Omega_D}{\Omega_E}\big)\big)$ and converges when secondary source power with interference constraint is immense. We verified our analytical framework via numerical and simulation results and revealed the effect of different channel/system parameters on the secrecy performance.

APPENDIX A
PROOF OF THEOREM 1

On inserting the expressions of the CDF of γ_D and the PDF of γ_E into $\mathbb{I}_1$ of (15), we can express $\mathbb{I}_1$ as

$$\mathbb{I}_1 = \frac{\alpha_E \xi_E}{2\Gamma(N_D\mu_D)} \int_0^\infty y^{\frac{\alpha_E N_E \mu_E}{2}-1} e^{-\lambda_E y^{\frac{\alpha_E}{2}}} \times \Upsilon\Big(N_D\mu_D, \lambda_D((\eta-1)w+\eta y)^{\frac{\alpha_D}{2}}\Big) dy. \quad (43)$$

After that, on invoking the series expansion of lower incomplete gamma function, i.e., $\Upsilon(\beta,x) = \sum_{n=0}^{\infty} \frac{(-1)^n}{n!}\frac{x^{\beta+n}}{\beta+n}$ [38, eq. (8.354.1)] into (43), and making the transformations as $(1+x)^\beta = \frac{1}{\Gamma(-\beta)} G_{1,1}^{1,1}(x|_0^{\beta+1})$ and $e^{-x} = G_{0,1}^{1,0}(x|_0^-)$ [41], (43) is given as

$$\mathbb{I}_1 = \frac{\alpha_E \xi_E}{2\Gamma(N_D\mu_D)} \sum_{n=0}^{\infty} \frac{(-1)^n}{n!} \frac{\lambda_D^{N_D\mu_D+n}}{N_D\mu_D+n} w^{\frac{\alpha_D(N_D\mu_D+n)}{2}} \times \frac{(\eta-1)^{\frac{\alpha_D(N_D\mu_D+n)}{2}}}{\Gamma\big(-\frac{\alpha_D(N_D\mu_D+n)}{2}\big)} \int_0^\infty y^{\frac{\alpha_E N_E\mu_E}{2}-1} G_{0,1}^{1,0}\Big(\lambda_E y^{\frac{\alpha_E}{2}}\Big|_0^-\Big) \times G_{1,1}^{1,1}\Big(\frac{\eta y}{(\eta-1)w}\Big|_0^{\frac{\alpha_D(N_D\mu_D+n)}{2}+1}\Big) dy. \quad (44)$$

Further, the integral in (44) can be solved by using [42, eq. (2.24.1.1)], as shown at the bottom of the page, where $\tilde{\beta} = 1-\beta, b^* = s+t-\frac{u+v}{2}, c^* = m+n-\frac{p+q}{2}, \rho = \sum_{j=1}^{v} d_j - \sum_{j=1}^{u} c_j + \frac{u-v}{2}+1$, and $\chi = \sum_{j=1}^{q} b_j - \sum_{j=1}^{p} a_j + \frac{p-q}{2}+1$, and after some involved simplifications, $\mathbb{I}_1$ in (44) can be given by (16).

APPENDIX B
PROOF OF THEOREM 3

By invoking the CDF of γ_D with the fact that $\Upsilon(\beta,z) = \Gamma(\beta)[1-e^{-z}\sum_{n=0}^{\beta-1}\frac{z^n}{n!}]$ [38, eq. (8.352.6)] alongwith the PDF of γ_E into (26), $\mathbb{P}_{\text{int}}$ in (26) can be expressed as

$$\mathbb{P}_{\text{int}} = \frac{\alpha_E \xi_E}{2} \int_0^\infty y^{\frac{\alpha_E N_E\mu_E}{2}-1} e^{-\lambda_E y^{\frac{\alpha_E}{2}}} dy - \frac{\alpha_E \xi_E}{2} \times \sum_{r=0}^{N_D\mu_D-1} \frac{\lambda_D^r}{r!} \int_0^\infty y^{\frac{r\alpha_D}{2}+\frac{\alpha_E N_E\mu_E}{2}-1} e^{-\lambda_D y^{\frac{\alpha_D}{2}}} e^{-\lambda_E y^{\frac{\alpha_E}{2}}} dy. \quad (46)$$

The first integral (say $\mathbb{I}_1$) of (46) can be solved by using change of variables $\lambda_E y^{\frac{\alpha_E}{2}} = t$, and via [38, eq. (8.310.1)] as

$$\mathbb{I}_1 = \frac{2}{\alpha_E} \frac{\Gamma(N_E\mu_E)}{\lambda_E^{N_E\mu_E}}. \quad (47)$$

Moreover, the second integral (say $\mathbb{I}_2$) in (46) can be expressed by making the change of variables $y^{\frac{\alpha_D}{2}} = t$ as

$$\mathbb{I}_2 = \frac{2}{\alpha_D} \int_0^\infty t^{\frac{r\alpha_D+\alpha_E N_E\mu_E}{\alpha_E}-1} e^{-\lambda_D t} e^{-\lambda_E t^{\frac{\alpha_E}{\alpha_D}}} dt. \quad (48)$$

Furthermore, with the help of the representation of the exponential function in terms of the Meijer-G function, i.e., $e^{-x} = G_{0,1}^{1,0}(x|_0^-)$ [41, eq. (11)], we can re-express (48) as

$$\mathbb{I}_2 = \frac{2}{\alpha_D} \int_0^\infty t^{\frac{r\alpha_D+\alpha_E N_E\mu_E}{\alpha_E}-1} G_{0,1}^{1,0}\Big(\lambda_D t\Big|_0^-\Big) \times G_{0,1}^{1,0}\Big(\lambda_E t^{\frac{\alpha_E}{\alpha_D}}\Big|_0^-\Big) dt, \quad (49)$$

which can be then evaluated by using [42, eq. (2.24.1.1)] as

$$\mathbb{I}_2 = \frac{2}{\alpha_D^{\frac{1}{2}}} \frac{\alpha_E^{r+\frac{\alpha_E N_E\mu_E}{\alpha_D}-\frac{1}{2}}}{(2\pi)^{\frac{\alpha_E+\alpha_D}{2}-1}} \lambda_D^{-r-\frac{\alpha_E N_E\mu_E}{\alpha_D}} \times G_{\alpha_E,\alpha_D}^{\alpha_D,\alpha_E}\Bigg(\frac{\lambda_E^{\alpha_D}}{\lambda_D^{\alpha_E}}\frac{\alpha_E^{\alpha_E}}{\alpha_D^{\alpha_D}}\Bigg|_{\Delta(\alpha_D,0)}^{\Delta(\alpha_E,1-r-\frac{\alpha_E N_E\mu_E}{\alpha_D})}\Bigg). \quad (50)$$

Finally, invoking (47) and into (46), and after some involved simplifications, the intercept probability can be given as (27).

APPENDIX C
PROOF OF THEOREM 4

By invoking the PDF of γ_D and the CDF of γ_E with the identity $\Upsilon(\beta,x) = \sum_{n=0}^{\infty}\frac{(-1)^n}{n!}\frac{x^{\beta+n}}{\beta+n}$ [38, eq. (8.354.1)], and invoking the following transformations $\ln(1+x) = G_{2,2}^{1,2}(x|_{1,0}^{1,1})$ and $e^{-x} = G_{0,1}^{1,0}(x|_0^-)$ [41, eq. (11)] into $\mathbb{J}_1$ of (33), to get

$$\mathbb{J}_1 = \frac{\alpha_D \xi_D}{2\Gamma(N_E\mu_E)} \sum_{n=0}^{\infty} \frac{(-1)^n}{n!} \lambda_E^{N_E\mu_E+n} y^{\frac{\alpha_D N_D\mu_D}{2}} \times \int_0^\infty y^{\frac{\alpha_E(N_E\mu_E+n)}{2}} x^{\frac{\alpha_D N_D\mu_D}{2}} x^{\frac{\alpha_E(N_E\mu_E+n)}{2}-1} \times G_{2,2}^{1,2}\Big(x\Big|_{1,0}^{1,1}\Big) G_{0,1}^{1,0}\Big(\lambda_D(xy)^{\frac{\alpha_D}{2}}\Big|_0^-\Big) dx, \quad (51)$$

which can be further simplified via identity [42, eq. (2.24.1.1)], as given in (34).

On adopting the same steps as adopted to get $\mathbb{J}_1$ in (34), we can evaluate $\mathbb{J}_2$ by interchanging α_D with α_E and $N_D\mu_D$

$$\int_0^\infty \tau^{\beta-1} G_{u,v}^{s,t}(\sigma\tau|_{d_1,\cdots,d_v}^{c_1,\cdots,c_u}) G_{p,q}^{m,n}(\varpi\tau^{l/k}|_{b_1,\cdots,b_q}^{a_1,\cdots,a_p}) d\tau = \sigma^{-\beta} \frac{k^\chi l^{(v-u)\beta+\rho-1}}{(2\pi)^{(l-1)b^*+(k-1)c^*}} \times G_{kp+lv,kq+lu}^{km+lt,kn+ls}\Bigg(\frac{\varpi^k k^{k(p-q)}}{\sigma^l l^{l(u-v)}}\Bigg|_{\Delta(k,b_1),\cdots,\Delta(k,b_m),\Delta(l,\tilde{\beta}-c_1),\cdots,\Delta(l,\tilde{\beta}-c_u),\Delta(k,b_{m+1}),\cdots,\Delta(k,b_q)}^{\Delta(k,a_1),\cdots,\Delta(k,a_n),\Delta(l,\tilde{\beta}-d_1),\cdots,\Delta(l,\tilde{\beta}-d_v),\Delta(k,a_{n+1}),\cdots,\Delta(k,a_p)}\Bigg), \quad (45)$$

with $N_E\mu_E$ in (34), as given in (35). Further, the third integral $\mathbb{J}_3$ of (33) can be written by inserting the PDF $f_{\gamma_E}(x)$ as

$$\mathbb{J}_3 = \frac{\alpha_E \xi_E}{2} y^{\frac{\alpha_E N_E \mu_E}{2}} \int_0^\infty \ln(1+x) x^{\frac{\alpha_E N_E \mu_E}{2}-1} \mathrm{e}^{-\lambda_E (xy)^{\frac{\alpha_E}{2}}} dx. \tag{52}$$

On applying the transformations $\ln(1+x) = G_{2,2}^{1,2}(x|_{1,0}^{1,1})$ and $\mathrm{e}^{-x} = G_{0,1}^{1,0}(x|_0^-)$ [41, eq. (11)], and then utilizing [42, eq. (2.24.1.1)], $\mathbb{J}_3$ can be obtained as in (36).

REFERENCES

[1] S. Haykin, "Cognitive radio: Brain-empowered wireless communications," *IEEE J. Sel. Areas Commun.*, vol. 23, no. 2, pp. 201–220, Feb. 2005.

[2] F. Mehmeti and T. Spyropoulos, "Performance analysis, comparison, and optimization of interweave and underlay spectrum access in cognitive radio networks," *IEEE Trans. Veh. Technol.*, vol. 67, no. 8, pp. 7143–7157, Aug. 2018.

[3] A. Goldsmith, S. A. Jafar, I. Maric, and S. Srinivasa, "Breaking spectrum gridlock with cognitive radios: An information theoretic perspective," *Proc. IEEE*, vol. 97, no. 5, pp. 894–914, May 2009.

[4] K. B. Letaief and W. Zhang, "Cooperative communications for cognitive radio networks," *Proc. IEEE*, vol. 97, no. 5, pp. 878–893, May 2009.

[5] V. Kumar, B. Cardiff, and M. F. Flanagan, "Fundamental limits of spectrum sharing for NOMA-based cooperative relaying under a peak interference constraint," *IEEE Trans. Commun.*, vol. 67, no. 12, pp. 8233–8246, Dec. 2019.

[6] V. Kumar, Z. Ding, and M. F. Flanagan, "On the performance of downlink NOMA in underlay spectrum sharing," 2020, *arXiv:2011.08159*. [Online]. Available: http://arxiv.org/abs/2011.08159

[7] T. M. C. Chu and H.-J. Zepernick, "Performance optimization for hybrid two-way cognitive cooperative radio networks with imperfect spectrum sensing," *IEEE Access*, vol. 6, pp. 70582–70596, Nov. 2018.

[8] A. Alsharoa, H. Ghazzai, and M.-S. Alouini, "Optimal transmit power allocation for MIMO two-way cognitive relay networks with multiple relays using AF strategy," *IEEE Wireless Commun. Lett.*, vol. 3, no. 1, pp. 30–33, Feb. 2014.

[9] V. Blagojevic and P. Ivanis, "Ergodic capacity for TAS/MRC spectrum sharing cognitive radio," *IEEE Commun. Lett.*, vol. 16, no. 3, pp. 321–323, Mar. 2012.

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

[11] T. Q. Duong, V. N. Q. Bao, and H.-J. Zepernick, "Exact outage probability of cognitive AF relaying with underlay spectrum sharing," *Electron. Lett.*, vol. 47, no. 17, pp. 1001–1002, Aug. 2011.

[12] L. Sibomana, H.-J. Zepernick, and H. Tran, "Achievable secrecy capacity in an underlay cognitive radio network," in *Proc. IEEE Conf. Commun. Netw. Secur. (CNS)*, Oct. 2014, pp. 1–6.

[13] Y. Zou, J. Zhu, L. Yang, Y.-C. Liang, and Y.-D. Yao, "Securing physical-layer communications for cognitive radio networks," *IEEE Commun. Mag.*, vol. 53, no. 9, pp. 48–54, Sep. 2015.

[14] Y. Zou, X. Li, and Y.-C. Liang, "Secrecy outage and diversity analysis of cognitive radio systems," *IEEE J. Sel. Areas Commun.*, vol. 32, no. 11, pp. 2222–2236, Nov. 2014.

[15] Z. Shu, Y. Qian, and S. Ci, "On physical layer security for cognitive radio networks," *IEEE Netw.*, vol. 27, no. 3, pp. 28–33, May 2013.

[16] S. Yadav and A. Pandey, "Secrecy performance of cognitive vehicular radio networks: Joint impact of nodes mobility and imperfect channel estimates," in *Proc. IEEE Int. Black Sea Conf. Commun. Netw. (BlackSeaCom)*, Odesa, Ukraine, May 2020, pp. 1–7.

[17] P. Chakraborty and S. Prakriya, "Secrecy outage performance of a cooperative cognitive relay network," *IEEE Commun. Lett.*, vol. 21, no. 2, pp. 326–329, Feb. 2017.

[18] W. Saad, M. Shokair, and S. M. Ibraheem, "On the security of relay assisted cognitive radio networks in the presence of primary transceiver network," *Wireless Pers. Commun.*, vol. 104, no. 3, pp. 949–977, Feb. 2019.

[19] S. Yadav and A. Pandey, "On the secrecy performance of cooperative cognitive vehicular relay networks," in *Proc. IEEE Int. Conf. Adv. Netw. Telecommun. Syst. (ANTS)*. Goa, India: BITS Pilani, Dec. 2019, pp. 1–6.

[20] A. Pandey, S. Yadav, D.-T. Do, and R. Kharel, "Secrecy performance of cooperative cognitive AF relaying networks with direct links over mixed Rayleigh and double-Rayleigh fading channels," *IEEE Trans. Veh. Technol.*, vol. 69, no. 12, pp. 15095–15112, Dec. 2020, doi: 10.1109/TVT.2020.3034729.

[21] C. Tang, G. Pan, and T. Li, "Secrecy outage analysis of underlay cognitive radio unit over Nakagami-*m* fading channels," *IEEE Wireless Commun. Lett.*, vol. 3, no. 6, pp. 609–612, Dec. 2014.

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

[23] M. Elkashlan, L. Wang, T. Q. Duong, G. K. Karagiannidis, and A. Nallanathan, "On the security of cognitive radio networks," *IEEE Trans. Veh. Technol.*, vol. 64, no. 8, pp. 3790–3795, Aug. 2015.

[24] H. Zhao, D.-Y. Wang, C.-Q. Tang, Y.-P. Liu, G.-F. Pan, T.-T. Li, and Y.-F. Chen, "Physical layer security of underlay cognitive radio using maximal ratio combining," *Frontiers Inf. Technol. Electron. Eng.*, vol. 17, no. 9, pp. 929–937, Oct. 2016.

[25] H. Lei, H. Zhang, I. S. Ansari, C. Gao, Y. Guo, G. Pan, and K. A. Qaraqe, "Secrecy outage performance for SIMO underlay cognitive radio systems with generalized selection combining over Nakagami-*m* channels," *IEEE Trans. Veh. Technol.*, vol. 65, no. 12, pp. 10126–10132, Dec. 2016.

[26] S. Timilsina, G. A. A. Baduge, and R. F. Schaefer, "Secure communication in spectrum-sharing massive MIMO systems with active eavesdropping," *IEEE Trans. Cogn. Commun. Netw.*, vol. 4, no. 2, pp. 390–405, Jun. 2018.

[27] H. Zhao, Y. Tan, G. Pan, Y. Chen, and N. Yang, "Secrecy outage on transmit antenna selection/maximal ratio combining in MIMO cognitive radio networks," *IEEE Trans. Veh. Technol.*, vol. 65, no. 12, pp. 10236–10242, Dec. 2016.

[28] H. Lei, C. Gao, I. S. Ansari, Y. Guo, Y. Zou, G. Pan, and K. A. Qaraqe, "Secrecy outage performance of transmit antenna selection for MIMO underlay cognitive radio systems over Nakagami-*m* channels," *IEEE Trans. Veh. Technol.*, vol. 66, no. 3, pp. 2237–2250, Mar. 2017.

[29] M. D. Yacoub, "The $\alpha-\mu$ distribution: A physical fading model for the Stacy distribution," *IEEE Trans. Veh. Tecnhol.*, vol. 56, no. 1, pp. 27–34, Jan. 2007.

[30] U. S. Dias and M. D. Yacoub, "On the $\alpha-\mu$ autocorrelation and power spectrum functions: Field trials and validation," in *Proc. IEEE Global Telecommun. Conf. (GLOBECOM)*, Honolulu, HI, USA, Nov. 2009, pp. 1–6.

[31] J. M. Moualeu, D. B. da Costa, F. J. Lopez-Martinez, W. Hamouda, T. M. N. Ngatched, and U. S. Dias, "Secrecy analysis of a TAS/MRC scheme in $\alpha-\mu$ fading channels," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Marrakesh, Morocco, Apr. 2019, pp. 1–6.

[32] J. M. Moualeu, D. B. da Costa, F. J. Lopez-Martinez, W. Hamouda, T. M. N. Nkouatchah, and U. S. Dias, "Transmit antenna selection in secure MIMO systems over $\alpha-\mu$ fading channels," *IEEE Trans. Commun.*, vol. 67, no. 9, pp. 6483–6498, Sep. 2019.

[33] H. Lei, I. S. Ansari, G. Pan, B. Alomair, and M.-S. Alouini, "Secrecy capacity analysis over $\alpha-\mu$ fading channels," *IEEE Commun. Lett.*, vol. 21, no. 6, pp. 1445–1448, Jun. 2017.

[34] L. Kong, S. Vuppala, and G. Kaddoum, "Secrecy analysis of random MIMO wireless networks over $\alpha-\mu$ fading channels," *IEEE Trans. Veh. Technol.*, vol. 67, no. 12, pp. 11654–11666, Dec. 2018.

[35] J. M. Moualeu, D. B. da Costa, W. Hamouda, U. S. Dias, and R. A. A. de Souza, "Physical layer security over α-κ-μ and α-η-μ fading channels," *IEEE Trans. Veh. Technol.*, vol. 68, no. 1, pp. 1025–1029, Jan. 2019.

[36] S. Yadav, "Secrecy performance of cognitive radio sensor networks over $\alpha-\mu$ fading channels," *IEEE Sensors Lett.*, vol. 4, no. 9, Sep. 2020, Art. no. 6002004.

[37] S. Yadav and D. S. Gurjar, "Physical layer security in underlay cognitive radio networks over $\alpha-\mu$ fading channels," in *Proc. IEEE Latin-Amer. Conf. Commun. Virtual Conf. (LATINCOM)*, Santo Domingo, Dominican Republic, Nov. 2020, pp. 1–6.

[38] I. S. Gradshteyn and I. M. Ryzhik, *Tables of Integrals, Series, and Products*, 6th ed. New York, NY, USA: Academic, 2000.

[39] L. Fan, N. Yang, T. Q. Duong, M. Elkashlan, and G. K. Karagiannidis, "Exploiting direct links for physical layer security in multiuser multirelay networks," *IEEE Trans. Wireless Commun.*, vol. 15, no. 6, pp. 3856–3867, Jun. 2016.

[40] A. Ghasemi and E. Sousa, "Fundamental limits of spectrum-sharing in fading environments," *IEEE Trans. Wireless Commun.*, vol. 6, no. 2, pp. 649–658, Feb. 2007.
[41] V. S. Adamchik and O. I. Marichev, "The algorithm for calculating integrals of hypergeometric type functions and its realization in REDUCE system," in *Proc. Int. Symp. Symbolic Algebr. Comput. (ISSAC)*, New York, NY, USA, Jul. 1990, pp. 212–224.
[42] A. P. Prudnikov, Y. A. Brychkov, and O. I. Marichev, *Integrals and Series: More Special Functions*, vol. 3. New York, NY, USA: Gordon and Breach, 1990.

SUNEEL YADAV (Member, IEEE) received the B.Tech. degree in electronics and communication engineering from the Meerut Institute of Engineering and Technology, Meerut, India, in 2008, the M.Tech. degree in digital communications from the ABV-Indian Institute of Information Technology and Management, Gwalior, India, in 2012, and the Ph.D. degree in electrical engineering from the Indian Institute of Technology Indore, Indore, India, in 2016. He is currently working with the Department of Electronics and Communication Engineering, Indian Institute of Information Technology, Allahabad, Prayagraj, India, as an Assistant Professor. He is also serving as a Faculty in-Charge for the Mobile and Wireless Networking Laboratory (MoWiNeT), Indian Institute of Information Technology, Allahabad. He has numerous publications in peer-reviewed journals and conferences. He has served as a TPC member, a session chair, a program co-chair, and a reviewer, for various national and international conferences. He is also serving as a reviewer for a number of international journals, including the IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, the IEEE COMMUNICATIONS LETTERS, the IEEE TRANSACTIONS ON COMMUNICATIONS, the IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, the IEEE SYSTEMS JOURNAL, IEEE ACCESS, the IEEE INTERNET OF THINGS JOURNAL, the IEEE TRANSACTIONS ON SIGNAL AND INFORMATION PROCESSING OVER NETWORKS, and the *Physical Communication*. His current research interests include wireless relaying techniques, cooperative communications, cognitive relaying networks, device-to-device communications, reconfigurable intelligent surfaces, signal processing, physical layer security, and MIMO systems.

DEVENDRA SINGH GURJAR (Member, IEEE) received the B.Tech. degree in electronics and communications engineering from Uttar Pradesh Technical University, Lucknow, India, in 2011, the M.Tech. degree in wireless communications and computing from the Indian Institute of Information Technology, Allahabad, India, in 2013, and the Ph.D. degree in electrical engineering from the Indian Institute of Technology Indore, India, in 2017. He was with the Department of Electrical and Computer Engineering, University of Saskatchewan, Canada, as a Postdoctoral Research Fellow. He is currently working as an Assistant Professor with the Department of Electronics and Communication Engineering, National Institute of Technology Silchar, India. He has numerous publications in peer-reviewed journals and conferences. His research interests include MIMO communication systems, cooperative relaying, device-to-device communications, smart grid communications, physical layer security, and simultaneous wireless information and power transfer. He is also a member of the IEEE Communications Society and the IEEE Vehicular Technology Society. He was a recipient of Alain Bensoussan Fellowship, in 2019, from the European Research Consortium for Informatics and Mathematics (ERCIM).