IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received October 8, 2020, accepted October 21, 2020, date of publication October 26, 2020, date of current version November 9, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3033893

Achievable Physical-Layer Security Over Composite Fading Channels

OSAMAH S. BADARNEH[1], (Member, IEEE), PASCHALIS C. SOFOTASIOS[2,3], (Senior Member, IEEE), SAMI MUHAIDAT[2,4], (Senior Member, IEEE), SIMON L. COTTON[5], (Senior Member, IEEE), KHALED M. RABIE[6], (Senior Member, IEEE), AND NAOFAL ALDHAHIR[7], (Fellow, IEEE)

[1]Electrical and Communication Engineering Department, School of Electrical Engineering and Information Technology, German Jordanian University, Amman 11180, Jordan
[2]Center for Cyber-Physical Systems, Department of Electrical Engineering and Computer Science, Khalifa University, Abu Dhabi, United Arab Emirates
[3]Department of Electrical Engineering, Tampere University, 33101 Tampere, Finland
[4]Department of Systems and Computer Engineering, Carleton University, Ottawa, ON K1S 5B6, Canada
[5]Institute of Electronics, Communications and Information Technology, Queen's University Belfast, Belfast BT3 9DT, U.K.
[6]School of Engineering, Manchester Metropolitan University, Manchester M15 6BH, U.K.
[7]Department of Electrical and Computer Engineering, The University of Texas at Dallas, Richardson, TX 75080, USA

Corresponding author: Osamah S. Badarneh (osamah.badarneh@gju.edu.jo)

This work was supported in part by the Khalifa University under Grant KU/RC1-C2PS-T2/8474000137 and Grant No. KU/FSU-8474000122.

ABSTRACT We investigate the physical layer security limits of Wyner's wiretap model over Fisher-Snedecor $\mathcal{F}$ composite fading channels. $\mathcal{F}$ fading conditions have been recently shown to provide an accurate characterization of multipath fading and shadowing effects in emerging wireless transmission scenarios such as body centric, cellular and vehicular communications. To this end, we utilize a redefined analytic expression for the Fisher-Snedecor $\mathcal{F}$ distribution in order to ensure unconstrained validity and reliability when used in the analysis of various performance metrics of interest. In this context, we assume that the main channel (i.e., between the source and the legitimate destination) and the eavesdropper's channel (i.e., between the source and the illegitimate destination) undergo independent quasi-static Fisher-Snedecor $\mathcal{F}$ composite fading. Novel exact analytic expressions are then derived for the corresponding average secrecy capacity (ASC), secure outage probability (SOP) and probability of strictly positive secrecy capacity (SPSC) along with their insightful asymptotic representations. In addition, analytical expressions for the ASC, SOP and SPSC over mixed fading channels such as Nakagami-*m*/Nakagami-*m*, Nakagami-*m*/Fisher-Snedecor $\mathcal{F}$ and Fisher-Snedecor $\mathcal{F}$/Nakagami-*m* are derived. The new formulations are validated through comparisons with Monte-Carlo simulations and analyzed to gain useful insights into the impact of the fading parameters on the achievable accuracy and the overall system performance.

INDEX TERMS Average secrecy capacity, Fisher-Snedecor $\mathcal{F}$ distribution, physical layer security, secure outage probability.

I. INTRODUCTION

Due to the inherent broadcast nature of wireless communication systems, the message-bearing signal may be eavesdropped and decoded by illegitimate users. As a result, the information security in wireless communication systems has recently received considerable attention even at the physical layer of the Open System Interconnection (OSI) model. In his seminal contribution in [2], Shannon introduced the concept of information-theoretic secrecy by investigating the transmission of a secret message between a source, a legitimate receiver and an eavesdropper, where the source and the legitimate receiver share a secret key. To achieve perfect secrecy, it was shown that the key rate should be at least as large as the message rate. Subsequently, in [3], Wyner introduced the notion of a wiretap channel that enables a source to send a secret message to a legitimate receiver in the presence of an eavesdropper without using a shared key, such that almost no information about the secret message is leaked to the eavesdropper.

Based on the above considerations, earlier studies have analyzed the performance of physical-layer security (PLS)

The associate editor coordinating the review of this manuscript and approving it for publication was Maged Abdullah Esmail.

for several wireless applications, such as point-to-point, dual-hop and multi-hop communications, and cognitive radio networks (see e.g., [4]–[26] and the references therein). From these studies, a number of important performance measures such as the average secrecy capacity (ASC), secure outage probability (SOP), probability of strictly positive secrecy capacity (SPSC) and probability of nonzero secrecy capacity (PNSC) have been derived. In this context, a general and compact analysis framework for the wireless information-theoretic security of arbitrarily-distributed fading channels was presented in [4], whereas in [5], the authors investigated PLS in a random wireless network where both the legitimate and eavesdropping nodes are randomly deployed. The secrecy capacity of a wiretap broadcast channel with an external eavesdropper, where the source sends two private messages over a broadcast channel while keeping them secret from the eavesdropper, was studied in [6]. In addition, the authors in [7] evaluated the ASC performance of the classic Wyner's model over α-μ fading channels, while the authors in [8] derived closed-form expressions for the ASC, SOP and the SPSC assuming a classic Wyner's wiretap model over generalized-K fading channels.

In the same context, the performance of SOP and SPSC over generalized gamma fading channels was analyzed in [9]. Novel analytical expressions for the SPSC and a lower bound on the SOP were derived over independent and non-identically distributed (i.n.i.d) κ-μ fading channels in [10]. The derived expressions were then used to study the performance of different emerging wireless applications, such as cellular device-to-device, peer-to-peer, vehicle-to-vehicle and body centric communications. In [11], the same authors derived analytical expressions for the SPSC and a lower bound on the SOP over α-μ/κ-μ and κ-μ/α-μ fading channels, whereas the SPSC performance for wireless communication systems under Rician fading was analyzed in [12]. Furthermore, the effect of in-phase and quadrature imbalance on the ASC was studied in [13], whereas secure communications in terms of the ASC, SOP and PNSC over independent and correlated lognormal shadowing channels as well as composite fading channels were investigated in [14]. Finally, the wireless PLS performance in the presence of multiple eavesdroppers was evaluated in [15]–[17].

Recently, numerous studies have analyzed PLS performance in the context of dual- and multi-hop relaying systems [18]–[20], [27]–[30]. More specifically, the ergodic secrecy capacity performance in a dual-hop multiple-antenna amplify-and-forward (AF) relaying system was analyzed in [18]. To further enhance the ergodic secrecy capacity for a dual-hop decode-and-forward (DF) relaying system in the presence of an eavesdropper, a random phase shifting scheme was proposed in [19]. Similarly, an upper bound, lower bound and an approximate expression for the SOP of a dual-hop AF relaying system with relay selection and without the knowledge of the eavesdropper's instantaneous channel state information (CSI) were derived in [20]. Likewise, the impact of correlated Rayleigh fading on the security of multiple AF relaying networks was quantified in [31], whereas the performance of SOP in a dual-hop DF relaying system with diversity combining at the eavesdropper was considered in [32]. In [27], the authors jointly considered full-duplex and physical layer security by formulating a cross-layer optimization problem to maximize the secrecy rate in a multi-hop wireless network. The performance of PLS in DF full-duplex multi-hop relaying systems was investigated in [28], whereas the performance of PLS of a multi-hop DF relay network was analyzed in [29] in the presence of multiple passive eavesdroppers over Nakagami-m fading channels. Finally, the PNSC performance of a multi-hop relay network over Nakagami-m fading channels with hardware impairments was quantified in [30].

Multipath fading and shadowing phenomena are encountered in most practical wireless communication scenarios, such as in congested downtown areas with slow mobility or stationary users [33]–[35]. In addition, this type of composite fading is encountered in land–mobile satellite communication systems, subject to urban and/or vegetative shadowing [36]–[39]. However, even though the existing composite fading models can provide a fair characterization of the underlying fading phenomena, quite often their mathematical representation turns out to be inconvenient, leading to cumbersome or intractable analytic results for most critical performance metrics of interest. Unfortunately, this common analytical limitation impacts the formulation of important statistical metrics such as the probability density function, the cumulative distribution function and the moment generating function, which are required to evaluate important performance metrics, such as spectral efficiency, probability of error, channel capacity and outage probability. With this motivation, a composite fading model which is both accurate and tractable was recently proposed for characterizing the combined effects of multipath fading and shadowing. The so-called Fisher-Snedecor $\mathcal{F}$ fading model was introduced in [40] under the assumption that the scattered multipath follows a Nakagami-m distribution, while the root-mean-square signal is shaped by an inverse Nakagami-m random variable. The validity of this model was verified through extensive comparisons with field measurements obtained for a number of emerging wireless communications scenarios. Owing to its generality, several well-known fading models such as the Nakagami-m, Rayleigh and one-sided Gaussian can be obtained as special cases. In addition, the Fisher-Snedecor $\mathcal{F}$ distribution has been shown, both theoretically and experimentally, to outperform other frequently used composite fading distributions, such as the generalized-K distribution both in terms of modeling accuracy and computational complexity. For example, in [40], the authors demonstrated an important application of the Fisher-Snedecor $\mathcal{F}$ distribution for characterizing the composite fading observed in device-to-device (D2D) communications channels. It is worth mentioning here that D2D communication is expected to play an indispensable role in beyond fifth-generation (5G) wireless networks, see [41] and the references therein. In addition,

TABLE 1. Notations and symbols used throughout the paper.

Notation/Symbol	Definition/Explanation
y_D, y_E	Received signal at legitimate destination and eavesdropper's, respectively
h_D, h_E	Main channel and Eavesdropper's channel coefficients, respectively
n_D, n_E	AWGN at legitimate destination and eavesdropper's, respectively
σ_D^2, σ_E^2	Noise variances at legitimate destination and eavesdropper's, respectively
P_t	Transmitted power
$\overline{\gamma}_D, \overline{\gamma}_E$	Average SNR of the main and eavesdropper's links, respectively
m_D, m_E	Fading parameter of the main and eavesdropper's links, respectively
m_{s_D}, m_{s_E}	Shadowing parameter of the main and eavesdropper's links, respectively

it has been extensively shown that composite fading conditions are encountered in applications relating to both conventional and emerging wireless communication technologies, such as body area networks and vehicle-to-vehicle communications [42], [43].

Motivated by the above, in the present contribution we analyze a wireless communication system in the context of wireless PLS and Fisher-Snedecor $\mathcal{F}$ composite fading. Specifically, we consider a wireless system in which the main channel and the eavesdropper's channel experience independent quasi-static Fisher-Snedecor $\mathcal{F}$ fading effects. The main contributions of this work can be summarized as follows[1]:

- We utilize a redefined analytic expression for the probability density function (PDF) of the Fisher-Snedecor $\mathcal{F}$ fading distribution, which is a slight modification of the underlying inverse Nakagami-m PDF from that is used in [40]. While the PDF given in [40] corresponds to a valid model for physical channel characterization, the formulation of the underlying inverse Nakagami-m model renders the determination of the parameter range of numerous performance measures of interest problematic. On the contrary, the redefined PDF of the $\mathcal{F}$ model that is utilized in the present analysis is more generic and robust when employed in the analysis of digital communication systems.
- With the aid of the redefined PDF for the Fisher-Snedecor $\mathcal{F}$ fading model, we derive novel closed-form analytical expressions for the ASC, SOP and SPSC of the classic Wyner's model over Fisher-Snedecor $\mathcal{F}$ composite fading channels.
- Capitalizing on the derivation of the exact analytic expressions, we derive new asymptotic expressions for performance metrics of interest such as the ASC, SOP and SPSC when the destination node is located close to the source node (i.e., in the high signal-to-noise ratio (SNR) regime).
- Useful and simple closed-form analytical expressions for the ASC, SOP and SPSC are also derived for some specific cases of interest, such as Fisher-Snedecor $\mathcal{F}$/Nakagami-m, Nakagami-m/Fisher-Snedecor $\mathcal{F}$ and Nakagami-m/Nakagami-m distributions, which also include as a special case the standard Rayleigh fading conditions when the Nakagami fading parameter is set to unity (i.e., $m = 1$).
- Considering the derived results for the cases of interest introduced above, new asymptotic expressions for the ASC, SOP and SPSC are derived. These expressions provide useful insights into the effect of the involved system parameters on the overall security performance.

The rest of the paper is organized as follows: In Section II we present the considered system and channel models, whereas in Section III we derive the corresponding ASC, SOP and SPSC representations. The asymptotic analysis for the aforementioned metrics is provided in Section IV, whereas respective special cases are obtained from our general analysis in Section V. In Section VI, we investigate the impact of different system parameters on the overall security performance. Finally, useful concluding remarks are given in Section VII.

II. SYSTEM AND CHANNEL MODELS

A. SYSTEM MODEL

We consider a wiretap channel model [45], which consists of a source (S), a legitimate destination (D) and an eavesdropper (E). In this system, S sends a confidential message to D over the main channel while E attempts to decode this message from its received signal, as depicted in Fig. 1. Also, the main channel ($S \rightarrow D$) and the eavesdropper's channel ($S \rightarrow E$) experience independent quasi-static Fisher-Snedecor $\mathcal{F}$ fading conditions [40]. The fading coefficients for both links remain constant during the transmission time of a block but vary independently from one block to another. The CSI is assumed to be known at both the transmitter and the destination while we assume that the noise over all channels is zero-mean and unit-variance complex additive white

[1]It is noted that during the submission of this manuscript, it became apparent that [44] addressed in parallel some of the topics under study in the present work. However, the analytic and numerical results in the present contribution are different and more valid compared to those in [44] because they are based exclusively on a redefined analytic expression for the probability density function of the Fisher-Snedecor $\mathcal{F}$ fading distribution. Furthermore, this manuscript reports results that were not addressed in the independently carried out contribution.

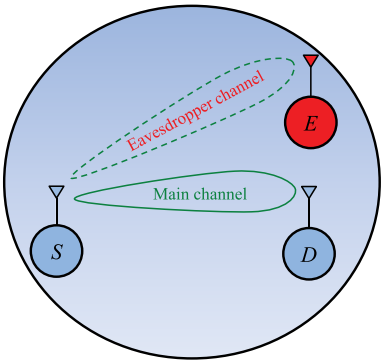

FIGURE 1. Illustration of a wireless communication system with potential eavesdropping.

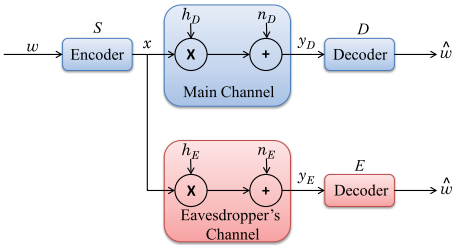

FIGURE 2. System model of the wiretap channel in the presence of Fisher-Snedecor $\mathcal{F}$ fading.

Gaussian noise (AWGN). Based on the system model of the wiretap channel shown in Fig. 2, the received signals at D and E can be expressed, respectively, as

$$y_D = \sqrt{P_t} h_D x + n_D, \tag{1}$$

and

$$y_E = \sqrt{P_t} h_E x + n_E, \tag{2}$$

where x is the normalized transmitted signal (i.e., $\mathbb{E}\{|x|^2\} = 1$, with $\mathbb{E}[\cdot]$ denoting statistical expectation). Based on the above, the instantaneous output SNRs at D and E are, respectively, given by

$$\gamma_D = \overline{\gamma}_D |h_D|^2 \tag{3}$$

and

$$\gamma_E = \overline{\gamma}_E |h_E|^2, \tag{4}$$

where $\overline{\gamma}_D = P_t/\sigma_D^2$ and $\overline{\gamma}_E = P_t/\sigma_E^2$.

In this work, we use the redefined version of the $\mathcal{F}$ distribution presented in [46]. As such, the PDF of the instantaneous SNR, γ_k (where $k \in \{D, E\}$), of the Fisher-Snedecor $\mathcal{F}$ fading distribution can be expressed as follows

$$f_k(\gamma_k) = \frac{m_k^{m_k} (m_{s_k} - 1)^{m_{s_k}} \overline{\gamma}_k^{m_{s_k}} \gamma^{m_k - 1}}{B(m_k, m_{s_k})(m_k \gamma + (m_{s_k} - 1)\overline{\gamma}_k)^{m_k + m_{s_k}}}, \tag{5}$$

where m_k and $m_{s_k} > 1$ denote the fading severity and shadowing parameters, respectively, $\overline{\gamma}_k = \mathbb{E}[\gamma_k]$ is the corresponding mean power and $B(\cdot, \cdot)$ denotes the beta function [47, Eq. (8.384.1)].

The representation in (5) is based on a slight modification of the underlying inverse Nakagami-m PDF from that used in [40]. While the PDF given in [40] corresponds to a valid model for physical channel characterization, the form of the underlying inverse Nakagami-m model renders the determination of the parameter range of many performance measures of interest problematic. On the contrary, the redefined PDF of the $\mathcal{F}$ model in (5) is more generic and robust when employed in the analysis of digital communication systems.

Based on the above and with the aid of [48, Eq. (8.4.2.5)] and [48, Eq. (8.2.2.15)], it follows that

$$f_k(\gamma_k) = \frac{1}{\Gamma(m_k)\Gamma(m_{s_k})} \gamma_k^{-1} \mathrm{G}_{1,1}^{1,1}\left(a_k \gamma_k \middle| \begin{matrix} 1 - m_{s_k} \\ m_k \end{matrix} \right), \tag{6}$$

where $a_k = \frac{m_k}{(m_{s_k} - 1)\overline{\gamma}_k}$ and $\mathrm{G}_{u,v}^{s,t}(\cdot)$ is the Meijer's G-function defined in Appendix A Eq. (37). It is also worth noting that the Fisher-Snedecor $\mathcal{F}$ distribution includes as special cases the Nakagami-m distribution ($m_s \to \infty$), Rayleigh distribution ($m_s \to \infty$ and $m = 1$) and one-sided Gaussian distribution ($m_s \to \infty$ and $m = \frac{1}{2}$). In addition, the corresponding cumulative distribution function (CDF) of γ_k can be expressed as follows:

$$F_k(\gamma_k) = \frac{1}{\Gamma(m_k)\Gamma(m_{s_k})} \mathrm{G}_{2,2}^{1,2}\left(a_k \gamma_k \middle| \begin{matrix} 1 - m_{s_k}, 1 \\ m_k, 0 \end{matrix} \right). \tag{7}$$

The above redefined measures are essential for performing a valid evaluation of the PHY layer security over $\mathcal{F}$ composite fading channels.

III. PHY LAYER SECURITY OVER $\mathcal{F}$ FADING CHANNELS

Based on the new analytic expressions for the PDF and CDF of the Fisher-Snedecor $\mathcal{F}$ fading distribution given in (6) and (7), we analyze the average secrecy capacity, the secrecy outage probability, and the strictly-positive secrecy capacity.

A. AVERAGE SECRECY CAPACITY (ASC)

We consider an active eavesdropping scenario [49], where the CSI of the eavesdropper's channel is known at S. Hence, S can adapt the achievable secrecy rate R such that $R \leq R_s$. In this context, the maximum achievable secrecy rate $C_s = R_s$ can be written as [49]

$$C_s = [C_D - C_E]^+, \tag{8}$$

where $C_D = \ln(1 + \gamma_D)$ and $C_E = \ln(1 + \gamma_E)$ denote the capacities in the main and eavesdropper channels with AWGN, respectively, whereas $[z]^+ = \max\{z, 0\}$.

Theorem 1 (Average Secrecy Capacity): The ASC for the Fisher-Snedecor $\mathcal{F}$ composite fading channels is given by (9), at the bottom of the next page, where $\mathrm{G}_{p_1,q_1:p_2,q_2:p_3,q_3}^{m_1,n_1:m_2,n_2:m_3,n_3}(\cdot)$ is the bivariate Meijer's G-function (BVMGF) defined in Appendix A Eq. (35).

Proof: The proof is provided in Appendix B.1. ■

Notably, even though the ASC in (9) is expressed in terms of the BVMGF, which is not a built-in function in standard scientific software packages, it can be efficiently computed with the aid of the methods outlined in [50]–[52].

B. SECURE OUTAGE PROBABILITY (SOP)

In this subsection, we consider a passive eavesdropper where the source S and destination D have no CSI knowledge about the eavesdropper. In this scenario, the SOP can be used as a key performance metric to characterize the wireless fading channel [49] since it denotes the probability that the instantaneous secrecy capacity falls below a target secrecy rate $R_s \geq 0$.

Theorem 2 (Secure Outage Probability): The SOP for Fisher-Snedecor $\mathcal{F}$ composite fading channels is given by

$$C_s^{SOP} = \sum_{n=0}^{\infty} \frac{(-1)^n a_D^n (\Psi-1)^n}{n!\Gamma(m_D)\Gamma(m_{s_D})\Gamma(m_E)\Gamma(m_{s_E})} \times \mathrm{G}_{4,4}^{3,3}\left(\frac{a_E}{a_D\Psi}\middle| \begin{matrix} 1, 1-m_{s_E}, 1+n-m_D, 1+n \\ m_E, n+m_{s_D}, n, 1+n \end{matrix}\right), \tag{10}$$

where $\Psi = \exp(R_s) \geq 1$.

Although (10) is expressed in terms of an infinite series, it converges rapidly and requires few terms (as little as three in certain cases) to achieve an acceptable target accuracy.

Proof: The proof is provided in Appendix B.2. ■

C. STRICTLY POSITIVE SECRECY CAPACITY (SPSC)

Likewise, the SPSC is another important metric in secure communications as it accounts for the probability that the secrecy rate for the $S \to D$ link is positive, i.e., $C_s > 0$.

Corollary 1 (Strictly Positive Secrecy Capacity): The SPSC for Fisher-Snedecor $\mathcal{F}$ composite fading channels is given by

$$C_s^{SPSC} = 1 - \frac{\mathrm{G}_{3,3}^{3,2}\left(\frac{a_E}{a_D}\middle| \begin{matrix} 1-m_{s_E}, 1-m_D, 1 \\ m_E, m_{s_D}, 0 \end{matrix}\right)}{\Gamma(m_D)\Gamma(m_{s_D})\Gamma(m_E)\Gamma(m_{s_E})}. \tag{11}$$

The SPSC in (11) is expressed in terms of the Meijer's G-function, which is a well known special built-in function in most scientific software packages such as Matlab and Mathematica. *Proof:* The proof is provided in Appendix B.3. ■

The validity of the new results were verified through comparisons with respective results from computer simulations. To the best of the authors' knowledge, these results have not been reported in the open technical literature.

IV. ASYMPTOTIC ANALYSIS

Capitalizing on the exact analytic results derived in Sec. III, we quantify the asymptotic performance when $\overline{\gamma}_D \to \infty$, which can be also viewed as the scenario where the destination D is located close to the source S. As such, the asymptotic behavior can be derived based on the behavior of the PDF of γ_k around the origin. Thus, the PDF, given in (5) or (6), and the CDF, given in (7), at high SNR regime can be rewritten as

$$f_k(\gamma_k) = \frac{a_k^{m_k}}{B(m_k, m_{s_k})}\gamma_k^{m_k-1} + \mathcal{O}\left((a_k\gamma_k)^{m_k}\right), \tag{12}$$

and

$$F_k(\gamma_k) = \frac{a_k^{m_k}\Gamma(m_k+m_{s_k})}{\Gamma(m_k+1)\Gamma(m_{s_k})}\gamma_k^{m_k} + \mathcal{O}\left((a_k\gamma_k)^{m_k}\right), \tag{13}$$

respectively, where $\mathcal{O}(\cdot)$ stands for higher-order terms.

A. ASYMPTOTIC ANALYSIS OF AVERAGE SECRECY CAPACITY

Proposition 1 (Asymptotic Average Secrecy Capacity): The asymptotic ASC for Fisher-Snedecor $\mathcal{F}$ composite fading channels is given by (14), at the bottom of the next page.

Proof: The proof is provided in Appendix B.4. ■

B. ASYMPTOTIC ANALYSIS OF SECURE OUTAGE PROBABILITY

Likewise, the asymptotic analysis for the corresponding SOP is provided in the following Proposition.

Proposition 2 (Asymptotic Secure Outage Probability): The asymptotic SOP is given by

$$C_s^{SOP,asym} = \frac{(a_D\Psi)^{m_D}\Gamma(m_D+m_{s_D})}{B(m_E, m_{s_E})\Gamma(m_D+1)\Gamma(m_{s_D})}\sum_{n=0}^{m_D}\binom{m_D}{n} \times \left(\frac{\Psi-1}{\Psi}\right)^{m_D-n} a_E^{-n}B(m_E+n, m_{s_E}-n). \tag{15}$$

The above representation provides useful insights into the impact of the involved parameters on the overall performance. For example, it demonstrates that the diversity gain is proportional to the fading parameter of the main link, m_D.

Proof: The proof is provided in Appendix B.5. ■

Fisher-Snedecor $\mathcal{F}$/Fisher-Snedecor $\mathcal{F}$:

$$\overline{C}_s^{ASC} = \frac{\mathrm{G}_{2,2:1,1:2,2}^{2,1:1,1:1,2}\left(a_D, a_E\middle| \begin{matrix} 0,1 \\ 0,0 \end{matrix}\middle| \begin{matrix} 1-m_{s_D} \\ m_D \end{matrix}\middle| \begin{matrix} 1-m_{s_E}, 1 \\ m_E, 0 \end{matrix}\right)}{\Gamma(m_D)\Gamma(m_{s_D})\Gamma(m_E)\Gamma(m_{s_E})} + \frac{\mathrm{G}_{2,2:1,1:2,2}^{2,1:1,1:1,2}\left(a_E, a_D\middle| \begin{matrix} 0,1 \\ 0,0 \end{matrix}\middle| \begin{matrix} 1-m_{s_E} \\ m_E \end{matrix}\middle| \begin{matrix} 1-m_{s_D}, 1 \\ m_D, 0 \end{matrix}\right)}{\Gamma(m_D)\Gamma(m_{s_D})\Gamma(m_E)\Gamma(m_{s_E})} - \frac{\mathrm{G}_{3,3}^{3,2}\left(a_E\middle| \begin{matrix} 1-m_{s_E}, 0, 1 \\ m_E, 0, 0 \end{matrix}\right)}{\Gamma(m_E)\Gamma(m_{s_E})} \tag{9}$$

C. ASYMPTOTIC ANALYSIS OF STRICTLY POSITIVE SECRECY CAPACITY

Finally, a simple asymptotic expression is also derived for the corresponding SPSC.

Proposition 3 (Asymptotic Strictly Positive Secrecy Capacity): The asymptotic SPSC is given by

$$C_s^{SPSC,asym} = \frac{B(m_E+m_D, m_{s_E}-m_D)\Gamma(m_D+m_{s_D})a_D^{m_D}}{B(m_E, m_{s_E})\Gamma(m_D+1)\Gamma(m_{s_D})a_E^{m_D}} = \frac{\Gamma(m_E+m_D)\Gamma(m_{s_E}-m_D)\Gamma(m_D+m_{s_D})}{\Gamma(m_D+1)\Gamma(m_D)\Gamma(m_E)\Gamma(m_{s_E})a_E^{m_D}a_D^{-m_D}}. \tag{16}$$

Equation (16) is also insightful since it shows that the diversity gain is proportional to the fading parameter of the main link, m_D.

Proof: The proof is provided in Appendix B.6. ■

V. SPECIAL CASES

The $\mathcal{F}$ composite fading model is extremely versatile and includes as special cases other well-known fading models. Therefore, following the derivation of the exact and asymptotic analytical framework in the previous section, we also derive analytic expressions for a number of special cases of interest which are encountered in practical wireless communication scenarios.

A. FISHER-SNEDECOR $\mathcal{F}$/Nakagami-m

First, we provide exact and asymptotic expressions for the ASC, SOP and SPSC when the legitimate link experiences Fisher-Snedecor $\mathcal{F}$ fading, while the eavesdropper's link experiences Nakagami-m fading (i.e., $m_{s_E} \to \infty$).

Corollary 2 (Average Secrecy Capacity): The ASC when the legitimate link experiences Fisher-Snedecor $\mathcal{F}$ fading, while the eavesdropper's link experiences Nakagami-m fading is given by (17), as shown at the bottom of the page.

Proof: The proof is provided in Appendix B.7. ■

Corollary 3 (Secure Outage Probability): The SOP when the legitimate link experiences Fisher-Snedecor $\mathcal{F}$ fading, while the eavesdropper's link experiences Nakagami-m fading is given by

$$C_s^{SOP} = \frac{1}{\Gamma(m_D)\Gamma(m_{s_D})\Gamma(m_E)} \sum_{n=0}^{\infty} \frac{(-1)^n a_D^n (\Psi-1)^n}{n!} \times \mathrm{G}_{3,4}^{3,2}\left(\frac{m_E}{a_D\Psi\overline{\gamma}_E}\middle| \begin{matrix}1, 1+n-m_D, 1+n\\ m_E, n+m_{s_D}, n, 1+n\end{matrix}\right). \tag{18}$$

Proof: The proof follows with the aid of equations (10), [48, Eq. (8.2.2.14)], [48, Eq. (8.2.2.12)] and [47, Eq. (8.328.2)]. ■

Corollary 4 (Strictly Positive Secrecy Capacity): The SPSC when the legitimate link experiences Fisher-Snedecor $\mathcal{F}$ fading, while the eavesdropper's link experiences Nakagami-m fading is expressed as

$$C_s^{SPSC} = 1 - \frac{\mathrm{G}_{2,3}^{3,1}\left(\frac{m_E}{a_D\overline{\gamma}_E}\middle| \begin{matrix}1-m_D, 1\\ m_E, m_{s_D}, 0\end{matrix}\right)}{\Gamma(m_D)\Gamma(m_{s_D})\Gamma(m_E)}. \tag{19}$$

Proof: The proof follows with the aid of equations (11), [48, Eq. (8.2.2.14)] and [48, Eq. (8.2.2.12)]. ■

As in the previous section, we capitalize on the exact analytic results derived for the aforementioned special case to derive asymptotic representations that provide useful insights into the impact of the involved parameters on the overall system performance.

Proposition 4 (Asymptotic Average Secrecy Capacity): The asymptotic ASC when the legitimate link experiences Fisher-Snedecor $\mathcal{F}$ fading, while the eavesdropper's link experiences Nakagami-m fading is given by (20), shown at the bottom of the next page.

Proof: The first and third terms in (14), when $m_{s_E} \to \infty$, reduce to the Nakagami-m case using [48, Eq. (8.2.2.12)] and [48, Eq. (8.2.2.14)]. While, the second term reduces to

---

Fisher-Snedecor $\mathcal{F}$/Fisher-Snedecor $\mathcal{F}$:

$$\overline{C}_s^{ASC,asym} = \underbrace{\frac{a_D^{m_D}\mathrm{G}_{4,4}^{3,3}\left(a_E\middle| \begin{matrix}1-m_{s_E}, 1, -m_D, 1-m_D\\ m_E, -m_D, -m_D, 0\end{matrix}\right)}{B(m_D, m_{s_D})\Gamma(m_E)\Gamma(m_{s_E})}}_{\text{1st term}} + \underbrace{\frac{\mathrm{G}_{2,2:1,1:2,2}^{2,1:1,1:1,2}\left(a_E, a_D\middle| \begin{matrix}0,1\\0,0\end{matrix}\middle| \begin{matrix}1-m_{s_E}\\ m_E\end{matrix}\middle| \begin{matrix}1-m_{s_D}, 1\\ m_D, 0\end{matrix}\right)}{\Gamma(m_D)\Gamma(m_{s_D})\Gamma(m_E)\Gamma(m_{s_E})}}_{\text{2nd term}} - \underbrace{\frac{\mathrm{G}_{3,3}^{3,2}\left(a_E\middle| \begin{matrix}1-m_{s_E}, 0, 1\\ m_E, 0, 0\end{matrix}\right)}{\Gamma(m_E)\Gamma(m_{s_E})}}_{\text{3rd term}}. \tag{14}$$

Fisher-Snedecor $\mathcal{F}$/Nakagami-m:

$$\overline{C}_s^{ASC} = \frac{\mathrm{G}_{2,2:1,1:1,2}^{2,1:1,1:1,1}\left(a_D, \frac{m_E}{\overline{\gamma}_E}\middle| \begin{matrix}0,1\\0,0\end{matrix}\middle| \begin{matrix}1-m_{s_D}\\ m_D\end{matrix}\middle| \begin{matrix}1\\ m_E, 0\end{matrix}\right)}{\Gamma(m_D)\Gamma(m_{s_D})\Gamma(m_E)} + \frac{\mathrm{G}_{2,2:0,1:2,2}^{2,1:1,0:1,2}\left(\frac{m_E}{\overline{\gamma}_E}, a_D\middle| \begin{matrix}0,1\\0,0\end{matrix}\middle| \begin{matrix}-\\ m_E\end{matrix}\middle| \begin{matrix}1-m_{s_D}, 1\\ m_D, 0\end{matrix}\right)}{\Gamma(m_D)\Gamma(m_{s_D})\Gamma(m_E)} - \frac{\mathrm{G}_{2,3}^{3,1}\left(\frac{m_E}{\overline{\gamma}_E}\middle| \begin{matrix}0,1\\ m_E, 0, 0\end{matrix}\right)}{\Gamma(m_E)}. \tag{17}$$

the Nakagami-m case when the BVMGF is represented by its integral form using (35) in Appendix A, followed by applying [47, Eq. (8.328.2)], and then using (35) in Appendix A, (20) is obtained, which completes the proof. ■

Proposition 5 (Asymptotic Secure Outage Probability): The asymptotic SOP when the legitimate link experiences Fisher-Snedecor $\mathcal{F}$ fading, while the eavesdropper's link experiences Nakagami-m fading is given by

$$C_s^{SOP,asym} = \frac{(a_D\Psi)^{m_D}\,\Gamma(m_D+m_{s_D})}{\Gamma(m_D+1)\Gamma(m_{s_D})\Gamma(m_E)}\sum_{n=0}^{m_D}\binom{m_D}{n} \times\left(\frac{\Psi-1}{\Psi}\right)^{m_D-n}\frac{\overline{\gamma}_E^n\Gamma(m_E+n)}{m_E^n}. \quad (21)$$

Proof: The proof follows using (15) and [47, Eq. (8.328.2)]. ■

Proposition 6 (Asymptotic Strictly Positive Secrecy Capacity): The asymptotic SPSC when the legitimate link experiences Fisher-Snedecor $\mathcal{F}$ fading, while the eavesdropper's link experiences Nakagami-m fading is given by

$$C_s^{SPSC,asym} = 1-\frac{a_D^{m_D}\overline{\gamma}_E^{m_D}\Gamma(m_D+m_{s_D})\Gamma(m_D+m_E)}{m_E^{m_D}\Gamma(m_D+1)\Gamma(m_{s_D})\Gamma(m_E)}. \quad (22)$$

Proof: The proof follows using equations (16) and [47, Eq. (8.328.2)]. ■

B. NAKAGAMI-m/FISHER-SNEDECOR $\mathcal{F}$

Conversely, in this subsection we derive exact and asymptotic expressions for the case of Nakagami-m/Fisher-Snedecor $\mathcal{F}$ fading conditions.

Corollary 5 (Average Secrecy Capacity): The ASC when the legitimate link experiences Nakagami-m fading, while the eavesdropper's link suffers Fisher-Snedecor $\mathcal{F}$ fading is given by (23), as shown at the bottom of the page.

Proof: The proof is provided in Appendix B.8. ■

Corollary 6 (Secure Outage Probability): The SOP when the legitimate link experiences Nakagami-m fading, while the eavesdropper's link experiences Fisher-Snedecor $\mathcal{F}$ fading is given by

$$C_s^{SOP} = \sum_{n=0}^{\infty}\frac{m_D^n\,(1-\Psi)^n}{n!\overline{\gamma}_D^n\Gamma(m_D)\Gamma(m_E)\Gamma(m_{s_E})} \times \mathrm{G}_{4,3}^{2,3}\left(\frac{a_E\overline{\gamma}_D}{m_D\Psi}\middle|\begin{matrix}1,\,1-m_{s_E},\,1+n-m_D,\,1+n\\ m_E,\,n,\,1+n\end{matrix}\right). \quad (24)$$

Proof: The proof follows with the aid of equations (10), [48, Eq. (8.2.2.14)] and [48, Eq. (8.2.2.12)]. ■

Corollary 7 (Strictly Positive Secrecy Capacity): The SOP when the legitimate link experiences Nakagami-m fading, while the eavesdropper's link experiences Fisher-Snedecor $\mathcal{F}$ fading is given by

$$C_s^{SPSC} = 1-\frac{\mathrm{G}_{3,2}^{2,2}\left(\frac{a_E\overline{\gamma}_D}{m_D}\middle|\begin{matrix}1-m_{s_E},\,1-m_D,\,1\\ m_E,\,0\end{matrix}\right)}{\Gamma(m_D)\Gamma(m_E)\Gamma(m_{s_E})}. \quad (25)$$

Proof: The proof follows using (11) and [48, Eq. (8.2.2.12)]. ■

Likewise, the corresponding asymptotic representations for this scenario are derived in the following propositions.

Proposition 7 (Asymptotic Average Secrecy Capacity): The asymptotic ASC when the legitimate link experiences Nakagami-m fading, while the eavesdropper's link suffers Fisher-Snedecor $\mathcal{F}$ fading is given by (26), as shown at the bottom of the next page.

Proof: The proof is provided in Appendix B.9. ■

Proposition 8 (Asymptotic Secure Outage Probability): The asymptotic SOP when the legitimate link experiences Nakagami-m fading, while the eavesdropper's link suffers Fisher-Snedecor $\mathcal{F}$ fading is given by

$$C_s^{SOP,asym} = \frac{1}{B(m_E,m_{s_E})\Gamma(m_D+1)}\left(\frac{m_D\Psi}{\overline{\gamma}_D}\right)^{m_D} \times\sum_{n=0}^{m_D}\binom{m_D}{n}\left(\frac{\Psi-1}{\Psi}\right)^{m_D-n} \times a_E^{-n}B(m_E+n,m_{s_E}-n). \quad (27)$$

Proof: The proof follows using (15) and [47, Eq. (8.328.2)]. ■

Fisher-Snedecor $\mathcal{F}$/Nakagami-m:

$$\overline{C}_s^{ASC,asym} = \frac{a_D^{m_D}\mathrm{G}_{3,4}^{3,2}\left(\frac{m_E}{\overline{\gamma}_E}\middle|\begin{matrix}1,\,-m_D,\,1-m_D\\ m_E,\,-m_D,\,-m_D,\,0\end{matrix}\right)}{B(m_D,m_{s_D})\Gamma(m_E)} + \frac{\mathrm{G}_{2,2:0,1:2,2}^{2,1:1,0:1,2}\left(\frac{m_E}{\overline{\gamma}_E},\,a_D\middle|\begin{matrix}0,1\\0,0\end{matrix}\middle|-\middle|\begin{matrix}1-m_{s_D},1\\ m_D,0\end{matrix}\right)}{\Gamma(m_D)\Gamma(m_{s_D})\Gamma(m_E)} - \frac{\mathrm{G}_{2,3}^{3,1}\left(\frac{m_E}{\overline{\gamma}_E}\middle|\begin{matrix}0,1\\ m_E,0,0\end{matrix}\right)}{\Gamma(m_E)} \quad (20)$$

Nakagami-m/Fisher-Snedecor $\mathcal{F}$:

$$\overline{C}_s^{ASC} = \frac{\mathrm{G}_{2,2:0,1:2,2}^{2,1:1,0:1,2}\left(\frac{m_D}{\overline{\gamma}_D},\,a_E\middle|\begin{matrix}0,1\\0,0\end{matrix}\middle|-\middle|\begin{matrix}1-m_{s_E},1\\ m_E,0\end{matrix}\right)}{\Gamma(m_D)\Gamma(m_E)\Gamma(m_{s_E})} + \frac{\mathrm{G}_{2,2:1,1:1,1}^{2,1:1,1:1,1}\left(a_E,\,\frac{m_D}{\overline{\gamma}_D}\middle|\begin{matrix}0,1\\0,0\end{matrix}\middle|\begin{matrix}1-m_{s_E}\\ m_E\end{matrix}\middle|\begin{matrix}1\\ m_D,0\end{matrix}\right)}{\Gamma(m_D)\Gamma(m_E)\Gamma(m_{s_E})} - \frac{\mathrm{G}_{3,3}^{3,2}\left(a_E\middle|\begin{matrix}1-m_{s_E},0,1\\ m_E,0,0\end{matrix}\right)}{\Gamma(m_E)\Gamma(m_{s_E})} \quad (23)$$

Proposition 9 (Asymptotic Strictly Positive Secrecy Capacity): The asymptotic SSPC when the legitimate link experiences Nakagami-m fading, while the eavesdropper's link suffers Fisher-Snedecor $\mathcal{F}$ fading is given by

$$C_s^{SPSC,asym} = 1 - \frac{m_D^{m_D}\Gamma(m_D+m_E)\Gamma(m_{s_E}-m_D)}{a_E^{m_D}\overline{\gamma}_D^{m_D}\Gamma(m_D+1)\Gamma(m_E)\Gamma(m_{s_E})}. \quad (28)$$

Proof: The proof follows using (16) and [47, Eq. (8.328.2)]. ■

C. NAKAGAMI-m/NAKAGAMI-m

Finally, capitalizing on the above results, we derive exact and asymptotic expressions for the classical case of Nakagami-*m*/Nakagami-*m* fading conditions.

In this case, the ASC, SOP and SPSC can be obtained either from the Fisher-Snedecor $\mathcal{F}$/Nakagami-*m* case or the Nakagami-*m*/Fisher-Snedecor $\mathcal{F}$ case.

Corollary 8 (Average Secrecy Capacity): The ASC when both the legitimate and the eavesdropper's links experience Nakagami-m fading is given by (29), as shown at the bottom of the page.

Proof: The proof is provided in Appendix B.10. ■

Corollary 9 (Secure Outage Probability): The SOP when both the legitimate and the eavesdropper's links experience Nakagami-m fading is given by

$$C_s^{SOP} = \frac{1}{\Gamma(m_D)\Gamma(m_E)}\sum_{n=0}^{\infty}\frac{\left(-\frac{m_D}{\overline{\gamma}_D}(\Psi-1)\right)^n}{n!} \times \mathrm{G}_{3,3}^{2,2}\left(\frac{m_E\overline{\gamma}_D}{m_D\overline{\gamma}_E\Psi}\middle|\begin{matrix}1,1+n-m_D,1+n\\ m_E,n,1+n\end{matrix}\right). \quad (30)$$

Proof: With the help of [48, Eq. (8.2.2.12)] and [48, Eq. (8.2.2.14)], (24) reduces to (30), which completes the proof. ■

Corollary 10 (Strictly Positive Secrecy Capacity): The SPSC when both the legitimate and the eavesdropper's links suffer Nakagami-m fading is given by

$$C_s^{SPSC} = 1 - \frac{\mathrm{G}_{2,2}^{2,1}\left(\frac{m_E\overline{\gamma}_D}{m_D\overline{\gamma}_E}\middle|\begin{matrix}1-m_D,1\\ m_E,0\end{matrix}\right)}{\Gamma(m_D)\Gamma(m_E)}. \quad (31)$$

Proof: With the help of [48, Eq. (8.2.2.12)] and [48, Eq. (8.2.2.14)], (25) reduces to (31), which completes the proof. ■

Proposition 10 (Asymptotic Average Secrecy Capacity): The asymptotic ASC when both the legitimate and the eavesdropper's links undergo Nakagami-m fading is given by (32), as shown at the bottom of the page.

Proof: The proof is provided in Appendix B.11. ■

Proposition 11 (Asymptotic Secure Outage Probability): The asymptotic SOP when both the legitimate and the eavesdropper's links suffer Nakagami-m fading is given by

$$C_s^{SOP,asym} = \frac{1}{\Gamma(m_D+1)\Gamma(m_E)}\left(\frac{m_D\Psi}{\overline{\gamma}_D}\right)^{m_D}\sum_{n=0}^{m_D}\binom{m_D}{n} \times \left(\frac{\Psi-1}{\Psi}\right)^{m_D-n}\frac{\overline{\gamma}_E^n\Gamma(m_E+n)}{m_E^n}. \quad (33)$$

Proof: With the aid of [47, Eq. (8.328.2)], (21) reduces to (33), which completes the proof. ■

Proposition 12 (Asymptotic Strictly Positive Secrecy Capacity): The asymptotic SPSC when both the legitimate and eavesdropper's links experience Nakagami-m fading is

---

Nakagami-*m*/Fisher-Snedecor $\mathcal{F}$:

$$\overline{C}_s^{ASC,asym} = \frac{\left(\frac{m_D}{\overline{\gamma}_D}\right)^{m_D}\mathrm{G}_{4,4}^{3,3}\left(a_E\middle|\begin{matrix}1-m_{s_E},1,-m_D,1-m_D\\ m_E,-m_D,-m_D,0\end{matrix}\right)}{\Gamma(m_D)\Gamma(m_E)\Gamma(m_{s_E})} + \frac{\mathrm{G}_{2,2:1,1:1,2}^{2,1:1,1:1,1}\left(a_E,\frac{m_D}{\overline{\gamma}_D}\middle|\begin{matrix}0,1\\0,0\end{matrix}\middle|\begin{matrix}1-m_{s_E}\\ m_E\end{matrix}\middle|\begin{matrix}1\\ m_D,0\end{matrix}\right)}{\Gamma(m_D)\Gamma(m_E)\Gamma(m_{s_E})} - \frac{\mathrm{G}_{3,3}^{3,2}\left(a_E\middle|\begin{matrix}1-m_{s_E},0,1\\ m_E,0,0\end{matrix}\right)}{\Gamma(m_E)\Gamma(m_{s_E})} \quad (26)$$

Nakagami-*m*/Nakagami-*m*:

$$\overline{C}_s^{ASC} = \frac{\mathrm{G}_{2,2:0,1:1,2}^{2,1:1,0:1,1}\left(\frac{m_D}{\overline{\gamma}_D},\frac{m_E}{\overline{\gamma}_E}\middle|\begin{matrix}0,1\\0,0\end{matrix}\middle|-\middle|m_D\middle|\begin{matrix}1\\ m_E,0\end{matrix}\right)}{\Gamma(m_D)\Gamma(m_E)} + \frac{\mathrm{G}_{2,2:0,1:1,2}^{2,1:1,0:1,1}\left(\frac{m_E}{\overline{\gamma}_E},\frac{m_D}{\overline{\gamma}_D}\middle|\begin{matrix}0,1\\0,0\end{matrix}\middle|-\middle|m_E\middle|\begin{matrix}1\\ m_D,0\end{matrix}\right)}{\Gamma(m_D)\Gamma(m_E)} - \frac{\mathrm{G}_{2,3}^{3,1}\left(\frac{m_E}{\overline{\gamma}_E}\middle|\begin{matrix}0,1\\ m_E,0,0\end{matrix}\right)}{\Gamma(m_E)}. \quad (29)$$

Nakagami-*m*/Nakagami-*m*:

$$\overline{C}_s^{ASC,asym} = \frac{\mathrm{G}_{3,4}^{3,2}\left(\frac{m_E}{\overline{\gamma}_E}\middle|\begin{matrix}1,-m_D,1-m_D\\ m_E,-m_D,-m_D,0\end{matrix}\right)}{\Gamma(m_D)\Gamma(m_E)}\left(\frac{m_D}{\overline{\gamma}_D}\right)^{m_D} + \frac{\mathrm{G}_{2,2:0,1:1,2}^{2,1:1,0:1,1}\left(\frac{m_E}{\overline{\gamma}_E},\frac{m_D}{\overline{\gamma}_D}\middle|\begin{matrix}0,1\\0,0\end{matrix}\middle|-\middle|m_E\middle|\begin{matrix}1\\ m_D,0\end{matrix}\right)}{\Gamma(m_D)\Gamma(m_E)} - \frac{\mathrm{G}_{2,3}^{3,1}\left(\frac{m_E}{\overline{\gamma}_E}\middle|\begin{matrix}0,1\\ m_E,0,0\end{matrix}\right)}{\Gamma(m_E)} \quad (32)$$

given by

$$C_s^{SPSC,asym} = 1 - \frac{\Gamma(m_D + m_E) m_D^{m_D} \overline{\gamma}_E^{m_D}}{\Gamma(m_D + 1)\Gamma(m_E) m_E^{m_D} \overline{\gamma}_D^{m_D}}. \quad (34)$$

Proof: Using [47, Eq. (8.328.2)], (22) reduces to (34), which completes the proof. ∎

The above-mentioned scenarios include the classical Rayleigh case which can be obtained by setting the corresponding fading parameters to unity.

VI. NUMERICAL RESULTS AND DISCUSSIONS

In this section, we present numerical results corresponding to the derived analytical representations in order to quantify the achievable performance and limitations of the considered setup under different multipath and shadowing conditions. Monte-Carlo simulations are also provided to demonstrate the validity of the derived analytical results. It can be observed from the figures that there is an excellent agreement between the analytical and simulation results, thereby confirming the validity of the derived expressions. Furthermore, it can be observed that the curves that correspond to the asymptotic representations are in close agreement with those that correspond to the exact representations in the high average SNR regime.

Fig. 3 illustrates the impact of the average SNR of the eavesdropper's link, $\overline{\gamma}_E$, on the ASC as a function of $\overline{\gamma}_D$ for $m_D = m_E = 2$ and $m_{s_D} = m_{s_E} = 5$. The results demonstrate that the ASC increases as $\overline{\gamma}_E$ decreases, which means that the transmitter S can transmit at a higher rate to the legitimate destination D. In the same context, the impact of various fading conditions on the ASC performance is illustrated in Fig. 4 for $m_E = 3$, $m_{s_E} = 20$, $m_D = \{5, 3, 1, 0.5\}$ and $m_{s_D} = 20$. It is evident that as the severity of the fading conditions decreases, i.e., the fading parameter of the main link m_D increases, the ASC improves. This is due to the fact that as m_D increases, the number of multipath clusters arriving

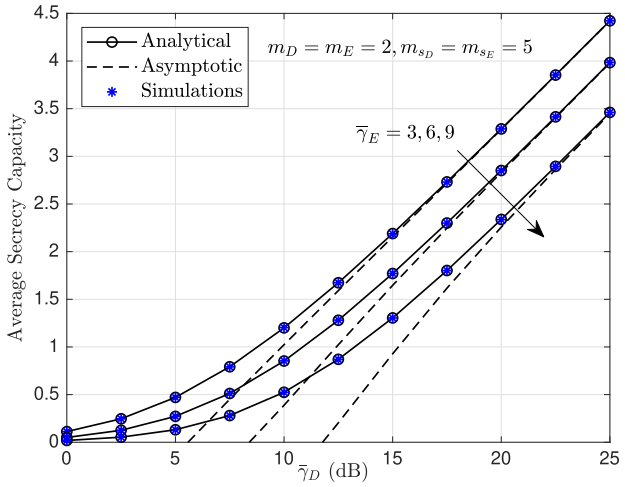

FIGURE 3. Impact of the average SNR of the eavesdropper's link, $\overline{\gamma}_E$, on the ASC as a function of $\overline{\gamma}_D$.

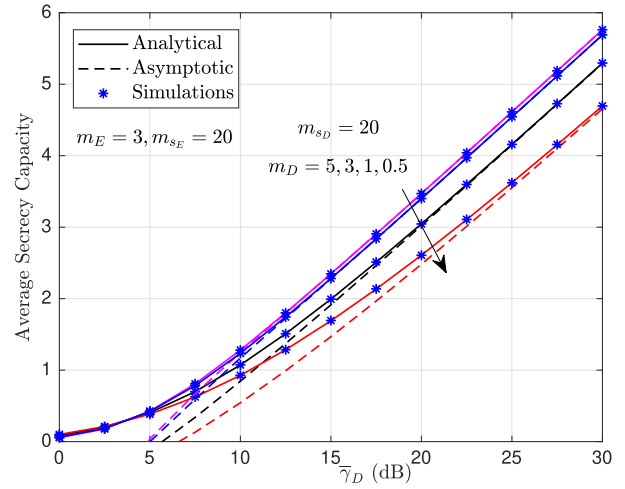

FIGURE 4. Impact of fading of the main link, m_D, on the ASC versus $\overline{\gamma}_D$.

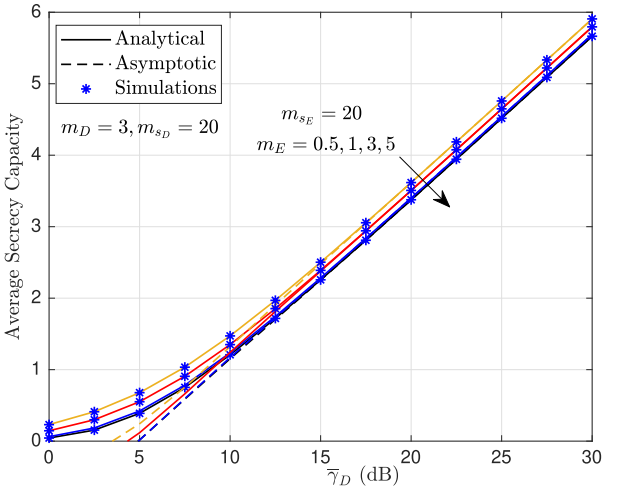

FIGURE 5. Impact of fading of the eavesdropper's link, m_E, on the ASC versus $\overline{\gamma}_D$.

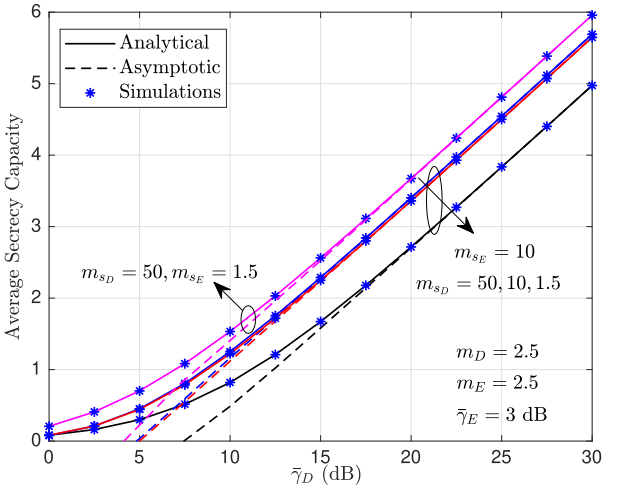

FIGURE 6. Impact of shadowing of the main link, m_{s_D}, and eavesdropper's link, m_{s_E}, on the ASC versus $\overline{\gamma}_D$.

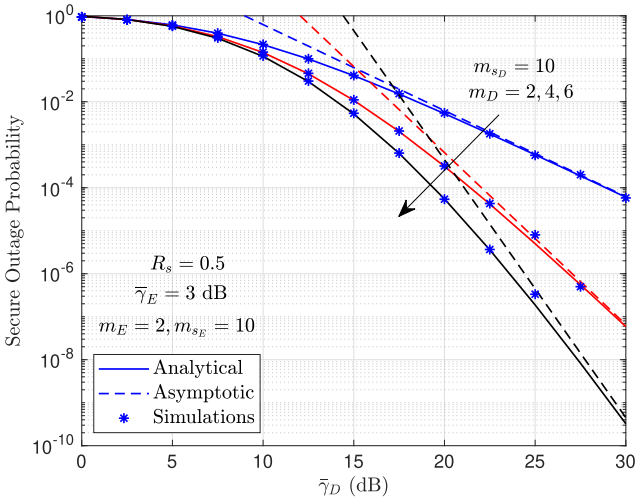

FIGURE 7. Impact of fading of the main link, m_D, on the SOP versus $\bar{\gamma}_D$.

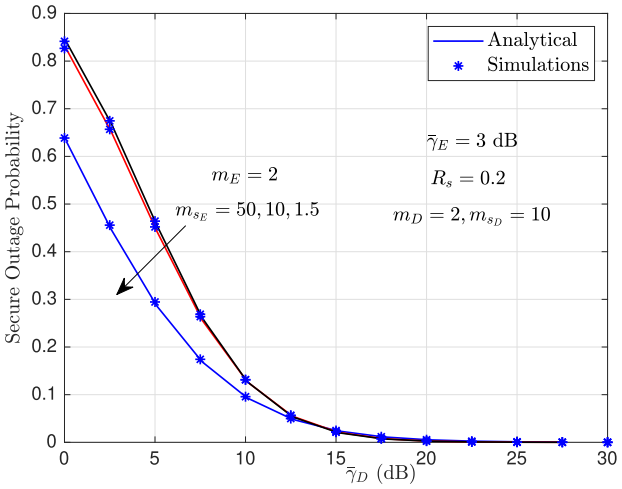

FIGURE 9. Impact of shadowing of the eavesdropper's link on the SOP. $m_D = 2, m_{s_D} = 10, m_E = 2, \bar{\gamma}_E = 3$ dB, $R_s = 0.2$..

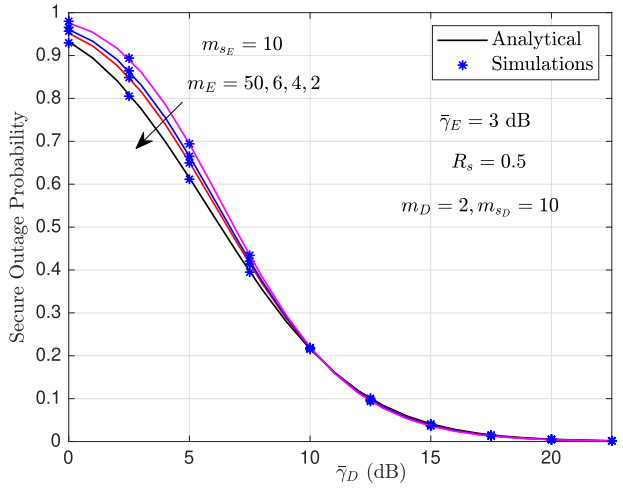

FIGURE 8. Impact of fading of the eavesdropper's link, m_E, on the SOP versus $\bar{\gamma}_D$.

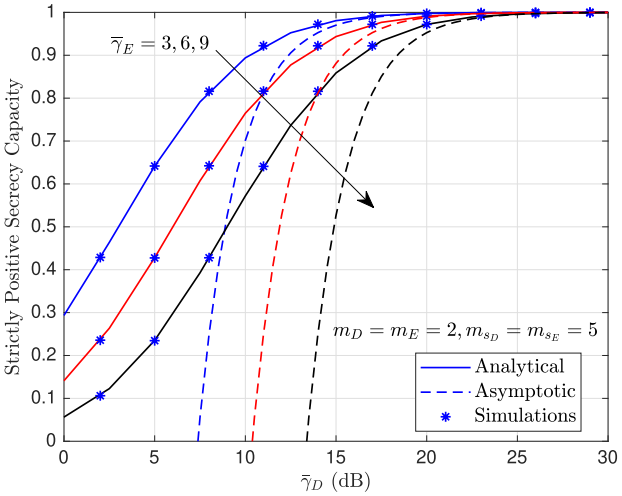

FIGURE 10. Impact of the average SNR of the eavesdropper's link, $\bar{\gamma}_E$, on the SPSC as a function of $\bar{\gamma}_D$.

at D also increases and thus, the received SNR increases. On the contrary, Fig. 5 demonstrates that the ASC improves as the fading parameter of the eavesdropper's channel, i.e., m_E, decreases. More striking though is the positive effect that m_D can have on the ASC performance since it is in fact more pronounced than that of m_E.

The influence that the shadowing effects encountered on the main link, m_{s_D}, and eavesdropper's link, m_{s_E}, can have on the ASC is demonstrated in Fig. 6 for $m_D = m_E = 2.5$ and $\bar{\gamma}_E = 3$ dB. When $m_{s_E} = 10$ and m_{s_D} increases from $m_{s_D} = 1.5$ (heavy shadowing) to $m_{s_D} = 50$ (light shadowing), the ASC performance improves noticeably. The results also show that when m_{s_D} changes from characterizing moderate shadowing (i.e., $m_{s_D} = 10$) towards light shadowing (i.e., $m_{s_D} = 50$), the ASC performance becomes independent of m_{s_D}. However, in contrast to m_{s_D}, when m_{s_E} decreases from $m_{s_E} = 10$ (moderate shadowing) to $m_{s_E} = 1.5$ (heavy shadowing), the ASC improves, i.e., S can transmit at a higher rate to D.

The results depicted in Fig. 7 illustrate the effect the encountered fading conditions in the main link, m_D, have on the SOP when $R_s = 0.5$ and $\bar{\gamma}_D = 3$ dB. It can be seen that as the value of m_D increases, the SOP performance improves. This is due to increasing m_D which leads to the diversity order in (15). On the other hand, Fig. 8 shows the effect of the fading conditions in the eavesdropper's link, m_E, on the SOP when $R_s = 0.5$ and $\bar{\gamma}_D = 3$ dB. Here too, it can be seen that as the value of m_E increases, the eavesdropper's link undergoes less severe fading conditions, which in turn reduces the overall SOP performance. It is also noted that the influence of increasing m_D is more pronounced than that of m_E.

Fig. 9 illustrates the impact of the shadowing conditions of the eavesdropper's link on the corresponding SOP

performance. It is evident that the SOP improves considerably as the severity of shadowing in the eavesdropper's link changes from light to heavy, i.e., when m_{s_E} decreases. This can be related to the fact that as the severity of shadowing increases, the eavesdropper's link experiences increasingly poorer reception. In the same context, Fig. 10 shows the impact of varying the average SNR of the eavesdropper's link, $\overline{\gamma}_E$, upon the SPSC for moderate multipath fading and shadowing conditions, namely $m_D = m_E = 2$ and $m_{s_D} = m_{s_E} = 5$. It is observed that as $\overline{\gamma}_E$ increases, the corresponding SPSC performance exhibits a noticeable decrease. Hence, the greater $\overline{\gamma}_E$ is, the better the quality of the eavesdropper's channel will be and thus the SPSC performance degrades, as expected.

VII. CONCLUSION

In this article, we have presented a systematic analysis of the Physical Layer Security of digital communications over Fisher-Snedecor $\mathcal{F}$ composite fading channels in the presence of an eavesdropper. Exact and asymptotic expressions for a number of important related performance metrics, namely the ASC, SOP and SPSC have been derived using a redefined form for the Fisher Snedecor $\mathcal{F}$ fading model, which leads to more unconstrained and reliable results. Using these formulations and considering both general and special cases, it has been demonstrated that the system performance improves considerably when the value of the fading parameter of the main link, m_D, increases. A similar observation has been made when the shadowing parameter of the main link, m_{s_D}, increases, i.e., its severity changes from heavy shadowing to light shadowing. It was also shown that performance improvements occur when the value of the fading parameter of the eavesdropper's link, m_E and the average SNR of the eavesdropper's link, $\overline{\gamma}_E$, decrease. Additionally, the performance deteriorates when the shadowing parameter of the eavesdropper's link, m_{s_E} increases, i.e., it changes from heavy shadowing to light shadowing. Lastly, the results have shown that the positive effect of m_D on the system performance is more pronounced than that of m_E.

As a final note, with the prevalence of multiple-input multiple-output in many emerging wireless applications such as those used in 5G cellular, a direct extension of this work will be to consider PLS for multi-antenna scenarios. Additionally, to further improve the practical applicability of the proposed framework, situations were the PLS is impacted by Fisher-Snedecor $\mathcal{F}$ composite fading and artificial noise should be considered.

APPENDIX
PRELIMINARIES

In this appendix, we provide some preliminary results that assist in the analysis of the system under consideration. To this end, it is recalled that the BVMGF is defined in terms of a two-fold contour integral in the complex plane [53, Eq. (13.1)], namely

$$\mathrm{G}_{p_1,q_1:p_2,q_2:p_3,q_3}^{m_1,n_1:m_2,n_2:m_3,n_3}\left(x, y \left| \begin{matrix} \mathbf{a_{1p_1}} \\ \mathbf{b_{1q_1}} \end{matrix} \right| \begin{matrix} \mathbf{a_{2p_2}} \\ \mathbf{b_{2q_2}} \end{matrix} \left| \begin{matrix} \mathbf{a_{3p_3}} \\ \mathbf{b_{3q_3}} \end{matrix} \right.\right) = \frac{1}{(2\pi i)^2} \int_{L_1}\int_{L_2} \Psi_1(s+t)\,\Psi_2(s)\,\Psi_3(t)\,x^{-s}y^{-t}\,ds\,dt, \tag{35}$$

where

$$\Psi_k(\tau) = \frac{\prod_{j=1}^{m_k}\Gamma(b_{kj}+\tau)\prod_{j=1}^{n_k}\Gamma(1-a_{kj}-\tau)}{\prod_{j=n_k+1}^{p_k}\Gamma(a_{kj}+\tau)\prod_{j=m_k+1}^{q_k}\Gamma(1-b_{kj}-\tau)} \tag{36}$$

with $k \in \mathbb{N}$. The contour L_1, in the complex s-plane, separates the poles of $\Gamma(1-a_{1j}-s)$ $(j=1,\ldots,n_1)$ and $\Gamma(1-a_{2j}-s)$ $(j=1,\ldots,n_2)$ from the poles of $\Gamma(b_{1j}+s)$ $(j=1,\ldots,m_1)$ and $\Gamma(b_{2j}+s)$ $(j=1,\ldots,m_2)$, when $t \in L_2$. Likewise, the contour L_2, in the complex s-plane, separates the poles of $\Gamma(1-a_{1j}-s)$ $(j=1,\ldots,n_1)$ and $\Gamma(1-a_{3j}-s)$ $(j=1,\ldots,n_3)$ from the poles of $\Gamma(b_{1j}+s)$ $(j=1,\ldots,m_1)$ and $\Gamma(b_{3j}+s)$ $(j=1,\ldots,m_3)$, when $s \in L_1$. Note that the BVMGF converges if the conditions listed in [53, Sec. 13.2] are satisfied. However, It is straightforward to show that the parameters of the BVMGF in (9), (14), (17), (20), (23), (26), (29), and (32) satisfy these sufficient conditions, and therefore the BVMGF converges.

The Meijer's G-function is defined by means of a one-fold contour integral in the complex plane [48, Eq. (8.3.1.1)], i.e.,

$$\mathrm{G}_{p_0,q_0}^{m_0,n_0}\left(x \left| \begin{matrix} a_1,\cdots,a_{p_0} \\ b_1,\cdots,b_{q_0} \end{matrix} \right.\right) = \frac{1}{2\pi i}\int_L \Psi(s)x^{-s}ds, \tag{37}$$

where

$$\Psi_k(s) = \frac{\prod_{j=1}^{m_0}\Gamma(b_j+s)\prod_{k=1}^{n_0}\Gamma(1-a_k-s)}{\prod_{k=n_0+1}^{p_0}\Gamma(a_k+s)\prod_{j=m_0+1}^{q_0}\Gamma(1-b_j-s)}.$$

The contour L is a suitable closed contour in the complex s-plane which can be chosen among three types of integration paths. Also, it is noted that the poles $\Gamma(b_j+s)$ must not coincide with the poles of $\Gamma(1-a_k-s)$ (with $j=1,\ldots,m_0$ and $k=1,\ldots,n_0$).

APPENDIX
A. PROOF OF THEOREM 1

Since both the main and eavesdropper channels experience independent fading, the corresponding ASC is given by

$$\begin{aligned}\overline{C}_s^{ASC} &= \mathbb{E}\left[C_s(\gamma_D,\gamma_E)\right] \\ &= \int_0^\infty\int_0^\infty C_s(\gamma_D,\gamma_E) f(\gamma_D,\gamma_E)\,d\gamma_D d\gamma_E \\ &= \mathcal{J}_1 + \mathcal{J}_2 - \mathcal{J}_3,\end{aligned} \tag{38}$$

where $f(\gamma_D,\gamma_E)$ is the joint PDF of γ_D and γ_E, and

$$\mathcal{J}_1 = \int_0^\infty \ln(1+\gamma_D) f_D(\gamma_D) F_E(\gamma_D)\,d\gamma_D, \tag{39}$$

$$\mathcal{J}_2 = \int_0^\infty \ln\left(1+\gamma_E\right) f_E\left(\gamma_E\right) F_D\left(\gamma_E\right) d\gamma_E, \tag{40}$$

and

$$\mathcal{J}_3 = \int_0^\infty \ln\left(1+\gamma_E\right) f_E\left(\gamma_E\right) d\gamma_E. \tag{41}$$

Performing a change of variables in (6) and (7), $\mathcal{J}_1$ becomes

$$\mathcal{J}_1 = \frac{1}{\Gamma(m_D)\Gamma(m_{s_D})\Gamma(m_E)\Gamma(m_{s_E})} \int_0^\infty \gamma_D^{-1} \ln\left(1+\gamma_D\right) \times \mathrm{G}_{1,1}^{1,1}\left(a_D\gamma_D \middle| \begin{matrix} 1-m_{s_D} \\ m_D \end{matrix}\right) \mathrm{G}_{2,2}^{1,2}\left(a_E\gamma_D \middle| \begin{matrix} 1-m_{s_E}, 1 \\ m_E, 0 \end{matrix}\right) d\gamma_D. \tag{42}$$

Representing the logarithmic function in terms of Meijer's G-function [48, Eq. (3.4.6.5)], (42) becomes

$$\mathcal{J}_1 = \frac{1}{\Gamma(m_D)\Gamma(m_{s_D})\Gamma(m_E)\Gamma(m_{s_E})} \int_0^\infty \gamma_D^{-1} \mathrm{G}_{2,2}^{1,2}\left(\gamma_D \middle| \begin{matrix} 1, 1 \\ 1, 0 \end{matrix}\right) \times \mathrm{G}_{1,1}^{1,1}\left(a_D\gamma_D \middle| \begin{matrix} 1-m_{s_D} \\ m_D \end{matrix}\right) \mathrm{G}_{2,2}^{1,2}\left(a_E\gamma_D \middle| \begin{matrix} 1-m_{s_E}, 1 \\ m_E, 0 \end{matrix}\right) d\gamma_D. \tag{43}$$

With the aid of [54], $\mathcal{J}_1$ can be obtained in closed-form as

$$\mathcal{J}_1 = \frac{\mathrm{G}_{2,2:1,1:2,2}^{2,1:1,1:1,2}\left(a_D, a_E \middle| \begin{matrix} 0, 1 \\ 0, 0 \end{matrix} \middle| \begin{matrix} 1-m_{s_D} \\ m_D \end{matrix} \middle| \begin{matrix} 1-m_{s_E}, 1 \\ m_E, 0 \end{matrix}\right)}{\Gamma(m_D)\Gamma(m_{s_D})\Gamma(m_E)\Gamma(m_{s_E})} \tag{44}$$

Likewise, the integral $\mathcal{J}_2$ can be obtained as

$$\mathcal{J}_2 = \frac{\mathrm{G}_{2,2:1,1:2,2}^{2,1:1,1:1,2}\left(a_E, a_D \middle| \begin{matrix} 0, 1 \\ 0, 0 \end{matrix} \middle| \begin{matrix} 1-m_{s_E} \\ m_E \end{matrix} \middle| \begin{matrix} 1-m_{s_D}, 1 \\ m_D, 0 \end{matrix}\right)}{\Gamma(m_D)\Gamma(m_{s_D})\Gamma(m_E)\Gamma(m_{s_E})} \tag{45}$$

Similarly, using (6) and (41), the integral $\mathcal{J}_3$ can be rewritten as

$$\mathcal{J}_3 = \int_0^\infty \frac{\gamma_E^{-1}\mathrm{G}_{2,2}^{1,2}\left(\gamma_E \middle| \begin{matrix} 1, 1 \\ 1, 0 \end{matrix}\right) \mathrm{G}_{1,1}^{1,1}\left(a_E\gamma_E \middle| \begin{matrix} 1-m_{s_E} \\ m_E \end{matrix}\right) d\gamma_E}{\Gamma(m_E)\Gamma(m_{s_E})}, \tag{46}$$

which can be solved with the help of [48, Eq. (2.24.1.1)] as

$$\mathcal{J}_3 = \frac{\mathrm{G}_{3,3}^{3,2}\left(a_E \middle| \begin{matrix} 1-m_{s_E}, 0, 1 \\ m_E, 0, 0 \end{matrix}\right)}{\Gamma(m_E)\Gamma(m_{s_E})}. \tag{47}$$

Finally, substituting (44), (45) and (47) into (38), yields (9).

B. PROOF OF THEOREM 2

The SOP in the considered set up can be obtained via

$$\begin{aligned} C_s^{SOP} &= \Pr\left\{C_s\left(\gamma_D, \gamma_E\right) < R_s\right\} = \Pr\left\{\gamma_D < \Psi\gamma_E + \Psi - 1\right\} \\ &= \int_0^\infty f_E\left(\gamma_E\right) \left(\int_0^{\Psi\gamma_E+\Psi-1} f_D\left(\gamma_D\right) d\gamma_D\right) d\gamma_E \\ &= \int_0^\infty F_D\left(\Psi\gamma_E + \Psi - 1\right) f_E\left(\gamma_E\right) d\gamma_E, \end{aligned} \tag{48}$$

where it is recalled that $\Psi = \exp(R_s) \geq 1$. To this effect and using (6) along with (7), it follows that

$$C_s^{SOP} = \frac{\int_0^\infty \gamma_E^{-1}\mathrm{G}_{1,1}^{1,1}\left(a_E\gamma_E \middle| \begin{matrix} 1-m_{s_E} \\ m_E \end{matrix}\right)}{\Gamma(m_D)\Gamma(m_{s_D})\Gamma(m_E)\Gamma(m_{s_E})} \times \mathrm{G}_{2,2}^{1,2}\left(a_D\left(\Psi\gamma_E + \Psi - 1\right) \middle| \begin{matrix} 1-m_{s_D}, 1 \\ m_D, 0 \end{matrix}\right) d\gamma_E. \tag{49}$$

After making the change of variable $x = a_D\Psi\gamma_E$ in (49) and using [48, Eq. (2.24.1.3)], then the SOP in (10) is obtained, which completes the proof.

C. PROOF OF COROLLARY 1

The corresponding SPSC can be obtained using

$$\begin{aligned} C_s^{SPSC} &= \Pr\left\{C_s\left(\gamma_D, \gamma_E\right) > 0\right\} = 1 - \Pr\left\{C_s\left(\gamma_D, \gamma_E\right) < 0\right\} \\ &= 1 - C_s^{SOP}\big|_{R_s=0}. \end{aligned} \tag{50}$$

Substituting $R_s = 0$ (i.e., $\Psi = 1$) and $n = 0$ into (10), and using [48, Eq. (8.2.2.8)], the SPSC in (11) is obtained, which completes the proof.

D. PROOF OF PROPOSITION 1

The asymptotic ASC can be evaluated via

$$C_s^{ASC,asym} = \mathcal{J}_1^{asym} + \mathcal{J}_2 - \mathcal{J}_3, \tag{51}$$

where $\mathcal{J}_2$ and $\mathcal{J}_3$ are defined in (45) and (47), respectively, whereas $\mathcal{J}_1^{asym}$ can be obtained using (39) and (12) as

$$\mathcal{J}_1^{asym} = \frac{a_D^{m_D}}{B(m_D, m_{s_D})\Gamma(m_E)\Gamma(m_{s_E})} \int_0^\infty \gamma_D^{m_D-1} \ln\left(1+\gamma_D\right) \times \mathrm{G}_{2,2}^{1,2}\left(a_E\gamma_D \middle| \begin{matrix} 1-m_{s_E}, 1 \\ m_E, 0 \end{matrix}\right) d\gamma_D. \tag{52}$$

The above integral can be solved in closed-form as follows:

$$\mathcal{J}_1^{asym} = \frac{a_D^{m_D}\mathrm{G}_{4,4}^{3,3}\left(a_E \middle| \begin{matrix} 1-m_{s_E}, 1, -m_D, 1-m_D \\ m_E, -m_D, -m_D, 0 \end{matrix}\right)}{B(m_D, m_{s_D})\Gamma(m_E)\Gamma(m_{s_E})}. \tag{53}$$

Based on this, substituting (53), (45) and (47) into (51) yields (14), which completes the proof.

E. PROOF OF PROPOSITION 2

The asymptotic SOP can be obtained using (5), (48), and (13), yielding

$$C_s^{SOP,asym} = \frac{a_D^{m_D} a_E^{m_E} \Psi^{m_D} \Gamma(m_D + m_{s_D})}{B(m_E, m_{s_E})\Gamma(m_D+1)\Gamma(m_{s_D})} \int_0^\infty \gamma_E^{m_E-1} \times (1+a_E\gamma_E)^{-(m_E+m_{s_E})} \left(\frac{\Psi-1}{\Psi}+\gamma_E\right)^{m_D} d\gamma_E. \quad (54)$$

Using the power series expansion in [47, Eq. (1.111)], one obtains

$$C_s^{SOP,asym} = \frac{a_D^{m_D} a_E^{m_E} \Psi^{m_D} \Gamma(m_D + m_{s_D})}{B(m_E, m_{s_E})\Gamma(m_D+1)\Gamma(m_{s_D})} \sum_{n=0}^{m_D} \binom{m_D}{n} \times \left(\frac{\Psi-1}{\Psi}\right)^{m_D-n} \int_0^\infty \gamma_E^{m_E+n-1} \times (1+a_E\gamma_E)^{-(m_E+m_{s_E})} d\gamma_E. \quad (55)$$

Notably, the above integral can be expressed in closed-form using [47, Eq. (3.194.3)] as in (15). This completes the proof.

F. PROOF OF PROPOSITION 3

The asymptotic SPSC can be obtained using

$$C_s^{SPSC,asym} = 1 - C_s^{SOP,asym}\big|_{R_s=0, n\to m_D}. \quad (56)$$

Thus, with the aid of (15) and after some algebraic manipulations, the asymptotic SPSC is obtained as in (16), which completes the proof.

G. PROOF OF COROLLARY 2

For the specific case of Nakagami-m fading conditions, i.e., $m_{s_E} \to \infty$, $\mathcal{J}_1$ and $\mathcal{J}_2$ in (44) and (45), reduce to (57) and (58), namely

$$\mathcal{J}_1 = \frac{\mathrm{G}_{2,2:1,1:1,2}^{2,1:1,1:1,1}\left(a_D, \frac{m_E}{\overline{\gamma}_E} \middle| \begin{matrix}0,1\\0,0\end{matrix} \middle| \begin{matrix}1-m_{s_D}\\m_D\end{matrix} \middle| \begin{matrix}1\\m_E,0\end{matrix}\right)}{\Gamma(m_D)\Gamma(m_{s_D})\Gamma(m_E)} \quad (57)$$

and

$$\mathcal{J}_2 = \frac{\mathrm{G}_{2,2:0,1:2,2}^{2,1:1,0:1,2}\left(\frac{m_E}{\overline{\gamma}_E}, a_D \middle| \begin{matrix}0,1\\0,0\end{matrix} \middle| \begin{matrix}-\\m_E\end{matrix} \middle| \begin{matrix}1-m_{s_D},1\\m_D,0\end{matrix}\right)}{\Gamma(m_D)\Gamma(m_{s_D})\Gamma(m_E)}. \quad (58)$$

It is noted here that (57) is obtained by first representing the BVMGF in (44) by its integral representation using (35) in Appendix A and then applying [47, Eq. (8.328.2)]. Finally, by using (35) in Appendix A again, one can obtain (57). Likewise, the evaluation of the integral $\mathcal{J}_2$, i.e., (58) can be obtained in the same manner.

However, a closed-form expression for $\mathcal{J}_3$ is obtained differently since [48, Eq. (8.2.2.14)] is first used and then [48, Eq. (8.2.2.12)] is applied. To this effect and by using [48, Eq. (8.2.2.14)] once more, it follows that

$$\mathcal{J}_3 = \frac{\mathrm{G}_{2,3}^{3,1}\left(\frac{m_E}{\overline{\gamma}_E} \middle| \begin{matrix}0,1\\m_E,0,0\end{matrix}\right)}{\Gamma(m_E)}. \quad (59)$$

Finally, substituting (57), (58) and (59) into (38), (17) is obtained, which completes the proof.

H. PROOF OF COROLLARY 5

For the special case of Nakagami-m fading, i.e., $m_{s_D} \to \infty$, $\mathcal{J}_1$ and $\mathcal{J}_2$ in (44) and (45) reduce to (60) and (61), namely

$$\mathcal{J}_1 = \frac{\mathrm{G}_{2,2:0,1:2,2}^{2,1:1,0:1,2}\left(\frac{m_D}{\overline{\gamma}_D}, a_E \middle| \begin{matrix}0,1\\0,0\end{matrix} \middle| \begin{matrix}-\\m_D\end{matrix} \middle| \begin{matrix}1-m_{s_E},1\\m_E,0\end{matrix}\right)}{\Gamma(m_D)\Gamma(m_E)\Gamma(m_{s_E})} \quad (60)$$

and

$$\mathcal{J}_2 = \frac{\mathrm{G}_{2,2:1,1:1,2}^{2,1:1,1:1,1}\left(a_E, \frac{m_D}{\overline{\gamma}_D} \middle| \begin{matrix}0,1\\0,0\end{matrix} \middle| \begin{matrix}1-m_{s_E}\\m_E\end{matrix} \middle| \begin{matrix}1\\m_D,0\end{matrix}\right)}{\Gamma(m_D)\Gamma(m_E)\Gamma(m_{s_E})}. \quad (61)$$

It is noted that the above expressions are obtained by first representing the BVMGF in (44) by its integral representation using (35) in Appendix A, then applying [47, Eq. (8.328.2)], and finally using (35) in Appendix A again. To this effect, substituting (47), (60), and (61) into (38), then (23) is obtained, which completes the proof.

I. PROOF OF PROPOSITION 7

The first term in (14) reduces to the Nakagami-m case after using the relation in [47, Eq. (8.328.2)], i.e.,

$$\mathcal{J}_1^{asym} = \frac{\left(\frac{m_D}{\overline{\gamma}_D}\right)^{m_D} \mathrm{G}_{4,4}^{3,3}\left(a_E \middle| \begin{matrix}1-m_{s_E},1,-m_D,1-m_D\\m_E,-m_D,-m_D,0\end{matrix}\right)}{\Gamma(m_D)\Gamma(m_E)\Gamma(m_{s_E})}. \quad (62)$$

The second term in (14) can be reduced using the definition of the BVMGF in (35) in Appendix A and the relation in [47, Eq. (8.328.2)], which yields

$$\mathcal{J}_2 = \frac{\mathrm{G}_{2,2:1,1:1,2}^{2,1:1,1:1,1}\left(a_E, \frac{m_D}{\overline{\gamma}_D} \middle| \begin{matrix}0,1\\0,0\end{matrix} \middle| \begin{matrix}1-m_{s_E}\\m_E\end{matrix} \middle| \begin{matrix}1\\m_D,0\end{matrix}\right)}{\Gamma(m_D)\Gamma(m_E)\Gamma(m_{s_E})}. \quad (63)$$

It is noted here that there is no change in the third term in (14). Thus, the asymptotic ASC is obtained as in (26), which completes the proof.

J. PROOF OF COROLLARY 8

The first and second terms in (17) can be reduced to the Nakagami-m case with the aid of (35) in Appendix A and [47, Eq. (8.328.2)], yielding (64) and (65) below

$$\mathcal{J}_1 = \frac{\mathrm{G}_{2,2:0,1:1,2}^{2,1:1,0:1,1}\left(\frac{m_D}{\overline{\gamma}_D}, \frac{m_E}{\overline{\gamma}_E} \middle| \begin{matrix}0,1\\0,0\end{matrix} \middle| \begin{matrix}-\\m_D\end{matrix} \middle| \begin{matrix}1\\m_E,0\end{matrix}\right)}{\Gamma(m_D)\Gamma(m_E)}, \quad (64)$$

and

$$\mathcal{J}_2 = \frac{\mathrm{G}_{2,2:0,1:1,2}^{2,1:1,0:1,1}\left(\frac{m_E}{\overline{\gamma}_E}, \frac{m_D}{\overline{\gamma}_D} \middle| \begin{matrix}0,1\\0,0\end{matrix} \middle| \begin{matrix}-\\m_E\end{matrix} \middle| \begin{matrix}1\\m_D,0\end{matrix}\right)}{\Gamma(m_D)\Gamma(m_E)}. \quad (65)$$

Based on the above and after some algebraic manipulations, (29) is deduced, which completes the proof.

K. PROOF OF PROPOSITION 10

The first term in (20) can be reduced to the Nakagami-m case, with the aid of [47, Eq. (8.328.2)], namely

$$\mathcal{J}_1^{asym} = \frac{\left(\frac{m_D}{\overline{\gamma}_D}\right)^{m_D}}{\Gamma(m_D)\Gamma(m_E)} \mathrm{G}_{3,4}^{3,2}\left(\frac{m_E}{\overline{\gamma}_E}\middle| \begin{matrix} 1, -m_D, 1-m_D \\ m_E, -m_D, -m_D, 0 \end{matrix}\right). \tag{66}$$

Likewise, the second term in (20) can be reduced to the Nakagami-m case using (35) in Appendix A and [47, Eq. (8.328.2)], which yields

$$\mathcal{J}_2^{asym} = \frac{\mathrm{G}_{2,2:0,1:1,2}^{2,1:1,0:1,1}\left(\frac{m_E}{\overline{\gamma}_E}, \frac{m_D}{\overline{\gamma}_D}\middle| \begin{matrix} 0, 1 \\ 0, 0 \end{matrix}\middle| \begin{matrix} - \\ m_E \end{matrix}\middle| \begin{matrix} 1 \\ m_D, 0 \end{matrix}\right)}{\Gamma(m_D)\Gamma(m_E)}. \tag{67}$$

Therefore, using (66) and (67), the asymptotic ASC for the case of Nakagami-m/Nakagami-m fading conditions is readily deduced in (32), which completes the proof.

ACKNOWLEDGMENT

This article was presented in part at the IEEE WiMob, Limassol, Cyprus, 2018. The authors would like to thank Dr. S. K. Yoo for the useful discussions during the early preparation of this manuscript.

REFERENCES

[1] O. S. Badarneh, P. C. Sofotasios, S. Muhaidat, S. L. Cotton, K. Rabie, and N. Al-Dhahir, "On the secrecy capacity of Fisher-Snedecor $\mathcal{F}$ fading channels," in *Proc. 14th Int. Conf. Wireless Mobile Comput., Netw. Commun. (WiMob)*, Oct. 2018, pp. 102–107.

[2] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, no. 4, pp. 656–715, Oct. 1949.

[3] A. D. Wyner, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[4] J. M. Romero-Jerez, G. Gomez, and F. J. Lopez-Martinez, "On the outage probability of secrecy capacity in arbitrarily-distributed fading channels," in *Proc. 21th Eur. Wireless Conf.*, May 2015, pp. 1–6.

[5] W. Liu, Z. Ding, T. Ratnarajah, and J. Xue, "On ergodic secrecy capacity of random wireless networks with protected zones," *IEEE Trans. Veh. Technol.*, vol. 65, no. 8, pp. 6146–6158, Aug. 2016.

[6] M. Benammar and P. Piantanida, "Secrecy capacity region of some classes of wiretap broadcast channels," *IEEE Trans. Inf. Theory*, vol. 61, no. 10, pp. 5564–5582, Oct. 2015.

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

[8] H. Lei, H. Zhang, I. S. Ansari, C. Gao, Y. Guo, G. Pan, and K. A. Qaraqe, "Performance analysis of physical layer security over generalized-K fading channels using a mixture gamma distribution," *IEEE Commun. Lett.*, vol. 20, no. 2, pp. 408–411, Feb. 2016.

[9] H. Lei, C. Gao, Y. Guo, and G. Pan, "On physical layer security over generalized gamma fading channels," *IEEE Commun. Lett.*, vol. 19, no. 7, pp. 1257–1260, Jul. 2015.

[10] N. Bhargav, S. L. Cotton, and D. E. Simmons, "Secrecy capacity analysis over κ-μ fading channels: Theory and applications," *IEEE Trans. Commun.*, vol. 64, no. 7, pp. 3011–3024, Jul. 2016.

[11] N. Bhargav and S. L. Cotton, "Secrecy capacity analysis for $\alpha-\mu/\kappa-\mu$ and $\kappa-\mu/\alpha-\mu$ fading scenarios," in *Proc. IEEE 27th Annu. Int. Symp. Pers., Indoor, Mobile Radio Commun. (PIMRC)*, Sep. 2016, pp. 1–6.

[12] X. Liu, "Probability of strictly positive secrecy capacity of the rician-rician fading channel," *IEEE Wireless Commun. Lett.*, vol. 2, no. 1, pp. 50–53, Feb. 2013.

[13] A.-A. A. Boulogeorgos, D. S. Karas, and G. K. Karagiannidis, "How much does I/Q imbalance affect secrecy capacity?" *IEEE Commun. Lett.*, vol. 20, no. 7, pp. 1305–1308, Jul. 2016.

[14] G. Pan, C. Tang, X. Zhang, T. Li, Y. Weng, and Y. Chen, "Physical-layer security over Non-Small-Scale fading channels," *IEEE Trans. Veh. Technol.*, vol. 65, no. 3, pp. 1326–1339, Mar. 2016.

[15] P. Wang, G. Yu, and Z. Zhang, "On the secrecy capacity of fading wireless channel with multiple eavesdroppers," in *Proc. IEEE Int. Symp. Inf. Theory*, Jun. 2007, pp. 1301–1305.

[16] M. Z. I. Sarkar, T. Ratnarajah, and M. Sellathurai, "Secrecy capacity of Nakagami-m fading wireless channels in the presence of multiple eavesdroppers," in *Proc. Conf. Rec. 43rd Asilomar Conf. Signals, Syst. Comput.*, Nov. 2009, pp. 829–833.

[17] Y. Chen, W. Li, and H. Shu, "Wireless physical-layer security with multiple receivers and eavesdroppers: Outage probability and average secrecy capacity," in *Proc. IEEE 26th Annu. Int. Symp. Pers., Indoor, Mobile Radio Commun. (PIMRC)*, Aug. 2015, pp. 662–667.

[18] R. Zhao, Y. Huang, W. Wang, and V. K. N. Lau, "Ergodic secrecy capacity of dual-hop multiple-antenna AF relaying systems," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2015, pp. 1–6.

[19] E. Nosrati, X. Wang, and A. Khabbazibasmenj, "Secrecy capacity enhancement in two-hop DF relaying systems in the presence of eavesdropper," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2015, pp. 7365–7369.

[20] A. Jindal, C. Kundu, and R. Bose, "Secrecy outage of dual-hop AF relay system with relay selection without Eavesdropper's CSI," *IEEE Commun. Lett.*, vol. 18, no. 10, pp. 1759–1762, Oct. 2014.

[21] C. Wang and H.-M. Wang, "On the secrecy throughput maximization for MISO cognitive radio network in slow fading channels," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 11, pp. 1814–1827, Nov. 2014.

[22] W. Wang, K. C. Teh, and K. H. Li, "Relay selection for secure successive AF relaying networks with untrusted nodes," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 11, pp. 2466–2476, Nov. 2016.

[23] A. Pandey and S. Yadav, "Physical layer security in cooperative amplify-and-forward relay networks over mixed Nakagami-m and double Nakagami-m fading channels: Performance evaluation and optimisation," *IET Commun.*, vol. 14, no. 1, pp. 95–104, 2020.

[24] J. Zhang and G. Pan, "Secrecy outage analysis with Kth best relay selection in dual-hop inter-vehicle communication systems," *AEU-Int. J. Electron. Commun.*, vol. 71, pp. 139–144, Jan. 2017.

[25] Y. Ai, M. Cheffena, A. Mathur, and H. Lei, "On physical layer security of double Rayleigh fading channels for vehicular communications," *IEEE Wireless Commun. Lett.*, vol. 7, no. 6, pp. 1038–1041, Dec. 2018.

[26] H. Ilhan, M. Uysal, and I. Altunbas, "Cooperative diversity for intervehicular communication: Performance analysis and optimization," *IEEE Trans. Veh. Technol.*, vol. 58, no. 7, pp. 3301–3310, Sep. 2009.

[27] F. Tian, X. Chen, S. Liu, X. Yuan, D. Li, X. Zhang, and Z. Yang, "Secrecy rate optimization in wireless multi-hop full duplex networks," *IEEE Access*, vol. 6, pp. 5695–5704, 2018.

[28] J.-H. Lee, "Full-duplex relay for enhancing physical layer security in multi-hop relaying systems," *IEEE Commun. Lett.*, vol. 19, no. 4, pp. 525–528, Apr. 2015.

[29] D.-D. Tran, N.-S. Vo, T.-L. Vo, and D.-B. Ha, "Physical layer secrecy performance of multi-hop decode-and-forward relay networks with multiple eavesdroppers," in *Proc. IEEE 29th Int. Conf. Adv. Inf. Netw. Appl. Workshops*, Mar. 2015, pp. 430–435.

[30] T. T. Phu, T. H. Dang, T. D. Tran, and M. Voznak, "Analysis of probability of non-zero secrecy capacity for multi-hop networks in presence of hardware impairments over Nakagami-m fading channels," *App. Wireless Commun.*, vol. 25, no. 4, pp. 774–782, Dec. 2016.

[31] L. Fan, R. Zhao, F.-K. Gong, N. Yang, and G. K. Karagiannidis, "Secure multiple amplify-and-forward relaying over correlated fading channels," *IEEE Trans. Commun.*, vol. 65, no. 7, pp. 2811–2820, Jul. 2017.

[32] S. Ghose, R. Bose, and C. Kundu, "Secrecy performance of dual-hop decode-and-forward relay system with diversity combining at the eavesdropper," *IET Commun.*, vol. 10, no. 8, pp. 904–914, May 2016.

[33] H. Suzuki, "A statistical model of urban multipath propagation," *IEEE Trans. Commun.*, vol. 25, no. 7, pp. 673–680, Jul. 1977.

[34] F. Hansen and F. I. Meno, "Mobile fading—Rayleigh and lognormal superimposed," *IEEE Trans. Veh. Technol.*, vol. 26, no. 4, pp. 332–335, Nov. 1977.

[35] M.-J. Ho and G. L. Stuber, "Co-channel interference of microcellular systems on shadowed Nakagami fading channels," in *Proc. IEEE 43rd Veh. Technol. Conf.*, May 1993, pp. 568–571.

[36] C. Loo, "A statistical model for a land mobile satellite link," *IEEE Trans. Veh. Technol.*, vol. 34, no. 3, pp. 122–127, Aug. 1985.

[37] G. E. Corazza and F. Vatalaro, "A statistical model for land mobile satellite channels and its application to nongeostationary orbit systems," *IEEE Trans. Veh. Technol.*, vol. 43, no. 3, pp. 738–742, Aug. 1994.
[38] S.-H. Hwang, K.-J. Kim, J.-Y. Ahn, and K.-C. Whang, "A channel model for nongeostationary orbiting satellite system," in *Proc. IEEE 47th Veh. Technol. Conf. Technol. Motion*, May 1997, pp. 41–45.
[39] A. Abdi, W. C. Lau, M. Alouini, and M. Kaveh, "A new simple model for land mobile satellite channels: First- and second-order statistics," *IEEE Trans. Wireless Commun.*, vol. 2, no. 3, pp. 519–528, May 2003.
[40] S. K. Yoo, S. Cotton, P. Sofotasios, M. Matthaiou, M. Valkama, and G. Karagiannidis, "The Fisher–Snedecor $\mathcal{F}$ distribution: A simple and accurate composite fading model," *IEEE Commun. Lett.*, vol. 21, no. 7, pp. 1661–1664, Jul. 2017.
[41] R. I. Ansari, C. Chrysostomou, S. A. Hassan, M. Guizani, S. Mumtaz, J. Rodriguez, and J. J. P. C. Rodrigues, "5G D2D networks: Techniques, challenges, and future prospects," *IEEE Syst. J.*, vol. 12, no. 4, pp. 3970–3984, Dec. 2018.
[42] S. L. Cotton and W. G. Scanlon, "An experimental investigation into the influence of user state and environment on fading characteristics in wireless body area networks at 2.45 GHz," *IEEE Trans. Wireless Commun.*, vol. 8, no. 1, pp. 6–12, Jan. 2009.
[43] D. W. Matolak and J. Frolik, "Worse-than-Rayleigh fading: Experimental results and theoretical models," *IEEE Commun. Mag.*, vol. 49, no. 4, pp. 140–146, Apr. 2011.
[44] L. Kong and G. Kaddoum, "On physical layer security over the Fisher–Snedecor $\mathcal{F}$ wiretap fading channels," *IEEE Access*, vol. 6, pp. 39466–39472, 2018.
[45] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.
[46] S. K. Yoo, P. C. Sofotasios, S. L. Cotton, S. Muhaidat, O. S. Badarneh, and G. K. Karagiannidis, "Entropy and energy detection-based spectrum sensing over $\mathcal{F}$-composite fading channels," *IEEE Trans. Commun.*, vol. 67, no. 7, pp. 4641–4653, Jul. 2019.
[47] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*, 7th ed. New York, NY, USA: Academic, 2007.
[48] A. P. Prudnikov, Y. A. Brychkov, and O. I. Marichev, *Integrals, Series: More Special Functions*, vol. 3. New York, NY, USA: Gordon & Breach Sci. Publ., 1990.
[49] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, Jun. 2008.
[50] C. García-Corrales, F. J. Cañete, and J. F. Paris, "Capacity of κ-μ shadowed fading channels," *Int. J. Antennas Propag.*, vol. 2014, Jul. 2014, Art. no. 975109.
[51] I. S. Ansari, S. Al-Ahmadi, F. Yilmaz, M. Alouini, and H. Yanikomeroglu, "A new formula for the BER of binary modulations with dual-branch selection over generalized-K composite fading channels," *IEEE Trans. Commun.*, vol. 59, no. 10, pp. 2654–2658, Oct. 2011.
[52] H. Chergui, M. Benjillali, and S. Saoudi, "Performance analysis of project-and-forward relaying in mixed MIMO-pinhole and Rayleigh dual-hop channel," *IEEE Commun. Lett.*, vol. 20, no. 3, pp. 610–613, Mar. 2016.
[53] T. H. Nguyen and S. B. Yakubovich, *The Double Mellin-Barnes Type Integrals and Their Applications to Convolution Theory*, 1st ed. Singapore: World Scientific, 1992.
[54] *Wolfram Research, MeijeG*. Accessed: Oct. 26, 2020. [Online]. Available: http://functions.wolfram.com/HypergeometricFunctions/MeijerG/21/ShowAll.html

OSAMAH S. BADARNEH (Member, IEEE) received the Ph.D. degree in electrical engineering from the University of Quebec–École de Technologie Supérieure (ETS), Canada, in 2009. He has been an Adjunct Professor with the Department of Electrical Engineering, University of Quebec-ETS, since 2013. From 2012 to 2018, he was an Associate Professor with the Department of Electrical Engineering, University of Tabuk. He worked as an Assistant Professor at the Department of Telecommunication Engineering, Yarmouk University, from 2010 to 2012. He is currently a Professor with the Department of Electrical and Communications Engineering, German Jordanian University. His research interest includes wireless communications and networking.

PASCHALIS C. SOFOTASIOS (Senior Member, IEEE) was born in Volos, Greece, in 1978. He received the M.Eng. degree from Newcastle University, U.K., in 2004, the M.Sc. degree from the University of Surrey, U.K., in 2006, and the Ph.D. degree from the University of Leeds, U.K., in 2011. He has held academic positions at the University of Leeds; the University of California at Los Angeles, Los Angeles, CA, USA; the Tampere University of Technology, Finland; the Aristotle University of Thessaloniki, Greece; and Khalifa University, United Arab Emirates, where he is currently an Assistant Professor with the Department of Electrical Engineering and Computer Science. His M.Sc. degree was funded by a scholarship from U.K.-EPSRC and his Ph.D. degree was sponsored by U.K.-EPSRC and Pace plc. His research interests include digital and optical wireless communications and topics relating to special functions and statistics. He received the Exemplary Reviewer Award from the IEEE Communications Letters, in 2012, and the IEEE Transactions on Communications, in 2015 and 2016, and the Best Paper Award at ICUFN 2013. He serves as an Editor for the IEEE Communications Letters. He serves as a Regular Reviewer for several international journals and has been a member of the technical program committee of numerous IEEE conferences.

SAMI MUHAIDAT (Senior Member, IEEE) received the Ph.D. degree in electrical and computer engineering from the University of Waterloo, Waterloo, ON, in 2006. From 2007 to 2008, he was an NSERC Postdoctoral Fellow with the Department of Electrical and Computer Engineering, University of Toronto, Canada. From 2008 to 2012, he was an Assistant Professor with the School of Engineering Science, Simon Fraser University, BC, Canada. He is currently a Professor with Khalifa University. His research interests include wireless communications, 5G and beyond, optical communications, the IoT with emphasis on battery-less devices, and machine learning. He is an Area Editor of IEEE Transactions on Communications. He has served as a Senior Editor for IEEE Communications Letters, an Editor for IEEE Transactions on Communications, and an Associate Editor for IEEE Transactions on Vehicular Technology.

SIMON L. COTTON (Senior Member, IEEE) received the B.Eng. degree in electronics and software from Ulster University, Ulster, U.K., in 2004, and the Ph.D. degree in electrical and electronic engineering from Queen's University Belfast, Belfast, U.K., in 2007. From 2007 to 2011, he was a Research Fellow, a Senior Research Fellow, from 2011 to 2012, a Lecturer (an Assistant Professor), from 2012 to 2015, and a Reader (Associate Professor), from 2015 to 2019 with Queen's University Belfast. He is currently a Full Professor and the Director of the Centre for Wireless Innovation (CWI), Queen's University Belfast. He has authored or coauthored over 145 publications in major IEEE/IET journals and refereed international conferences, two book chapters, and two patents. His research interests include cellular device-to-device, vehicular, and body-centric communications. His other research interests include radio channel characterization and modeling and the simulation of wireless channels. He was awarded the H. A. Wheeler Prize, in July 2010, by the IEEE Antennas and Propagation Society for the Best Applications Journal Paper in the IEEE Transactions on Antennas and Propagation, in 2009. In July 2011, he was awarded the Sir George Macfarlane Award from the U.K. Royal Academy of Engineering in recognition of his technical and scientific attainment since graduating from his first degree in engineering.

KHALED M. RABIE (Senior Member, IEEE) received the Ph.D. degree in electrical and electronic engineering from The University of Manchester, U.K., in 2015. He is currently an Assistant Professor with the Department of Engineering, Manchester Metropolitan University (MMU), U.K. He has worked as a part of several large-scale industrial projects and has published more than 130 journal articles and conference papers (mostly IEEE). His primary research interest includes the next-generation wireless communication systems. He is a Fellow of the U.K. Higher Education Academy (FHEA). He received numerous awards over the past few years in recognition of his research contributions, including the Best Student Paper Award at the IEEE ISPLC, TX, USA, in 2015, the MMU Outstanding Knowledge Exchange Project Award of 2016, and IEEE ACCESS Editor of the month award for August 2019. He serves regularly on the Technical Program Committee (TPC) of several major IEEE conferences, such as GLOBECOM, ICC, and VTC. He serves as an Editor for IEEE COMMUNICATIONS LETTERS, an Associate Editor for IEEE ACCESS, an Area Editor for *Physical Communication* (Elsevier), and an Executive Editor for the *Transactions on Emerging Telecommunications Technologies* (Wiley).

NAOFAL ALDHAHIR (Fellow, IEEE) received the Ph.D. degree from Stanford University. He was a Principal Member of Technical Staff at the GE Research and AT&T Shannon Laboratory, from 1994 to 2003. He is currently an Erik Jonsson Distinguished Professor with the ECE Department and the Associate Head of UT-Dallas. He is a co-inventor of 43 issued patents, coauthor of about 450 articles, and co-recipient of four IEEE best paper awards. He received the 2019 IEEE SPCE Technical Recognition Award. He has served as the Editor-in-Chief of IEEE TRANSACTIONS ON COMMUNICATIONS, from January 2016 to December 2019.