Secure Outage Probability in the Presence of Two Eavesdroppers and Composite Fading

Yoo, S. K., Sofotasios, P. C., Cotton, S. L., Zhang, L., Song, J. S. & Ansari, I. S.

Original citation & hyperlink:
Yoo, SK, Sofotasios, PC, Cotton, SL, Zhang, L, Song, JS & Ansari, IS 2022, Secure Outage Probability in the Presence of Two Eavesdroppers and Composite Fading. in 2022 Global Information Infrastructure and Networking Symposium, GIIS 2022. 2022 Global Information Infrastructure and Networking Symposium, GIIS 2022, Institute of Electrical and Electronics Engineers Inc., pp. 85-88, 2022 Global Information Infrastructure and Networking Symposium, GIIS 2022, Argostoli, Greece, 26/09/22.
https://dx.doi.org/10.1109/GIIS56506.2022.9936943

DOI 10.1109/GIIS56506.2022.993694B
ISBN 9781665490955

Publisher: IEEE

Secure Outage Probability in the Presence of Two Eavesdroppers and Composite Fading

Seong Ki Yoo[1], Paschalis C. Sofotasios[2,3], Simon L. Cotton[4], Lei Zhang[4], Jae Seung Song[5], Imran S. Ansari[6]
[1]Centre for Future Transport and Cities, Coventry University, CV1 2TE, Coventry, UK
[2]Centre for Cyber-Physical Systems, EECS Department, Khalifa University, 127 788, Abu Dhabi, UAE
[3]Department of Electrical Engineering, Tampere University, 33101, Tampere, Finland
[4]Centre for Wireless Innovation, ECIT Institute, Queen's University Belfast, BT3 9DT, Belfast, UK
[5]Software Engineering and Security Lab., Sejong University, Seoul, South Korea
[6]James Watt School of Engineering, University of Glasgow, G12 8QQ, Glasgow, UK

***Abstract*—We investigate the secure outage probability (SOP) in the presence of two eavesdroppers over $\mathcal{F}$ composite fading channels. The derived analytic results are relatively simple and their validity is justified through comparisons with respective simulation results. Subsequently, they are used to quantify the impact of the involved parameters on the achievable secure communication in the considered set up.**

I. Introduction

Device-to-device (D2D) communications provide direct connection between wireless devices and are attractive for several reasons, e.g., improvement of cell edge throughput and lower power consumption [1]. Thus, there is an increasing interest towards D2D communications as they are anticipated to be a core part of several emerging use cases. Some examples are the Internet of wearable things (IoWT) for digital healthcare applications [2] and unmanned aerial vehicle (UAV)-assisted Industrial Internet of Things (IIoT) Networks [3].

In D2D communications, user equipments (UEs) are operated in close proximity to the human body, e.g., held in a user's hand, carried in a pocket or worn on the body in the case of a smart watch. Based on this and due to the transitory behavior of humans, UEs are often mobile and operated in populated environments. Consequently, D2D communication links are fundamentlly heavily susceptible to multipath fading and shadowing caused by the user's body and/or nearby objects [4]. This can degrade significantly the quality of radio links and reduce the performance of D2D systems. Therefore, it is important to accurately characterize the combined effects of multipath fading and shadowing [5], [6] as this affects the achievable level of both quality of service and secure communications [7–9] and the references therein.

In fact, since UEs are personal devices, often operated in dense and crowded environments, the privacy and security of D2D communications are also important considerations. In D2D communications, a legitimate user communicates with the intended user (in this case forming a legitimate D2D pair) in the presence of an Eavesdropper (Eve) [10]. In this scenario, secure communication is achievable when the channel quality of a legitimate D2D pair is better than that of the wiretap D2D pair (i.e., between a legitimate user and the non-intended user, Eve). The maximum transmission rate achieved in secure communication is defined as the secrecy capacity, at which the Eve is not able to obtain any information. The notion of secrecy capacity has become an important metric in the performance analysis of wireless systems. It has been extensively studied for non-degraded channels [11], multipath fading channels [12–15], large-scale fading channels [16], [17], composite fading channels [18–22] and multi-antenna channels [23]. For example, in [12], the secrecy capacity was analyzed over κ-μ fading channels based on empirical measurements, whereas [19] addressed the secrecy outage analysis over correlated Nakagami-m / gamma composite fading conditions.

Motivated by the importance of encapsulating realistic fading behavior in the analysis of physical layer security in emerging communication scenarios, the present contribution quantifies the achievable secure outage probability over composite fading channels. More specifically, this study is addressed in the presence of two eavesdroppers and $\mathcal{F}$ composite fading channels, which has been shown extensively that they are typically encountered in realistic D2D communications scenarios, including personal and vehicular communications. To that end, we derive an analytic expression for the secure outage probability (SOP), which is expressed in closed-form and is tractable both analytically and numerically. Capitalizing on this, we analyze the behavior of the considered set up over different $\mathcal{F}$ composite fading conditions and quantify the effect of increasing numbers of Eves on the respective SOP performance. To the best of the authors' knowledge, the derived analytic results are novel and are expected to provide useful insights that will be useful in the design and deployment of D2D communication systems.

II. System and Channel Model

The physical signal model proposed for the $\mathcal{F}$ composite fading channel is similar to that for the Nakagami-m fading channel [24]. However, in contrast to the Nakagami-m signal, in an $\mathcal{F}$ composite fading channel, the root-mean-square (rms) power of the received signal is subject to random variations induced by shadowing. The $\mathcal{F}$ composite fading model has widely been used for both conventional and emerging wireless applications, e.g., optical [25], cellular [26], cognitive radio and vehicular [25] communications. Of note, the probability density function (PDF) and cumulative distribution function (CDF) of the received signal envelope (R) in $\mathcal{F}$ fading channels were first presented in [26]. Yet, in our analysis we use the modified version presented in [27].

Regarding the considered system model, we assume that a legitimate transmitter (Alice) sends a confidential message W to the corresponding legitimate receiver (Bob) in the presence of two Eves. Alice encodes a message block, $W = [W(1), W(2), ..., W(i)]$, into a codeword, $X = [X(1), X(2), ..., X(i)]$, for transmission over the channel. Bob can obtain information about the transmitted message by decoding the received signal, Y_M, while Eves are also capable of eavesdropping the transmitted message by decoding the received signal, Y_E. In this case, the received signal at Bob and at the k^{th} Eve are respectively given by [28]

$$Y_M(i) = h_M(i)X(i) + n_M(i), \tag{1}$$

$$Y_{E_k}(i) = h_{E_k}(i)X(i) + n_{E_k}(i) \tag{2}$$

where $h_M(i)$ and $h_{E_k}(i)$ denote the complex channel fading coefficients from Alice to Bob (main channel) and from Alice to the k^{th} Eve (wiretap channel), respectively. Moreover, $n_M(i)$ and $n_{E_k}(i)$ are the zero-mean circularly symmetric complex Gaussian noise random variables with unit variance of the main channel and wiretap channel, respectively. In order to simplify the analysis, we assume that both the main channel and each wiretap channel undergo $\mathcal{F}$ composite fading, where the channel gains remain constant during the transmission of entire codewords, i.e., $\forall i \in \mathbb{Z}^+$: $h_M(i) = h_M$ and $h_{E_k}(i) = h_{E_k}$. Moreover, codewords are independent from each other and have an average transmit signal power (P), i.e., $\frac{1}{N}\sum_{i=1}^{N} \mathbb{E}\{|X(i)|^2\} \le P$, whereas the average noise power in the main channel and wiretap channel are denoted by N_M and N_{E_k}. Consequently, the corresponding instantaneous signal-to-noise ratio (SNR) and average SNR at Bob are given by $\gamma_{_M} = P|h_M|^2/N_M$ and $\bar{\gamma}_{_M} = P\,\mathbb{E}\{|h_M|^2\}/N_M$, respectively. Likewise, the instantaneous SNR and average SNR at the k^{th} Eve are given by $\gamma_{_{E_k}} = P|h_{E_k}|^2/N_{E_k}$ and $\bar{\gamma}_{_{E_k}} = P\,\mathbb{E}\{|h_{E_k}|^2\}/N_{E_k}$, respectively. Also, the PDFs of γ_M and γ_{E_k} can be expressed with the corresponding parameters $\{m_{_M}, m_{s_M}, \bar{\gamma}_{_M}\}$ and $\{m_{E_k}, m_{s_{E_k}}, \bar{\gamma}_{_{E_k}}\}$, respectively, as

$$f_{\gamma_M}(\gamma_{_M}) = \frac{{m_{_M}}^{m_M}(m_{s_M}-1)^{m_{s_M}}\,\bar{\gamma}_M^{m_{s_M}}\gamma_M^{m_M-1}}{B(m_{_M}, m_{s_M})[m_{_M}\gamma_{_M} + (m_{s_M}-1)\,\bar{\gamma}_{_M}]^{m_M+m_{s_M}}}, \tag{3}$$

$$f_{\gamma_{E_k}}(\gamma_{_{E_k}}) = \frac{{m_{_{E_k}}}^{m_{E_k}}(m_{s_{E_k}}-1)^{m_{s_{E_k}}}\,\bar{\gamma}_{E_k}^{m_{s_{E_k}}}\gamma_{E_k}^{m_{E_k}-1}}{B\left(m_{_{E_k}}, m_{s_{E_k}}\right)\left[m_{_{E_k}}\gamma_{_{E_k}} + (m_{s_{E_k}}-1)\bar{\gamma}_{_{E_k}}\right]^{m_{E_k}+m_{s_{E_k}}}}. \tag{4}$$

III. Secure Outage Probability

The capacity of the main channel is given by $C_M = \log_2(1+\gamma_{_M})$ and the PDF of γ_M is given by (3). The transmitted message is secure only when C_M is greater than that of any wiretap channel. Thus, $C_E = \log_2\left(1+\gamma_{_{E_m}}\right)$ where $\gamma_{_{E_m}} = \max\left(\gamma_{_{E_1}}, \gamma_{_{E_2}}\right)$, whose PDF is given by

$$f_{\gamma_{E_m}}\left(\gamma_{_{E_m}}\right) = \sum_{i=1}^{2}\left[\prod_{j=1, j\neq i}^{2} F_{\gamma_{E_j}}\left(\gamma_{_{E_m}}\right)\right] f_{\gamma_{E_i}}\left(\gamma_{_{E_m}}\right) \tag{5}$$

where

$$F_{\gamma_{E_j}}(\gamma_{_{E_m}}) = \sum_{k_j=0}^{m_{E_j}-1}\binom{m_{_{E_j}}-1}{k_j}\frac{(-1)^{k_j}}{B\left(m_{_{E_j}}, m_{s_{E_j}}\right)(m_{s_{E_j}}+k_j)} \times\left(1-\frac{\left[(m_{s_{E_j}}-1)\,\bar{\gamma}_{_{E_j}}\right]^{m_{s_{E_j}}+k_j}}{\left[m_{_{E_j}}\gamma_{_{E_m}} + (m_{s_{E_j}}-1)\,\bar{\gamma}_{_{E_j}}\right]^{m_{s_{E_j}}+k_j}}\right) \tag{6}$$

which holds for $m_{_{E_j}} \in \mathbb{N}$, whilst $\binom{a}{b}$ is the binomial coefficient [29]. Thus, the secrecy capacity is expressed as

$$C_S(\gamma_{_M}, \gamma_{_{E_m}}) = \begin{cases}\log_2(1+\gamma_{_M}) - \log_2\left(1+\gamma_{_{E_m}}\right), & \gamma_{_M} > \gamma_{_{E_m}}\\ 0, & \gamma_{_M} \le \gamma_{_{E_m}}.\end{cases} \tag{7}$$

When Alice sends data at a secrecy rate, $\mathcal{R}_s > 0$, higher than the secrecy capacity, C_s, the target error probability can not be satisfied. This leads to an outage in the communication between Alice and Bob, namely SOP, which is defined

$$\mathcal{P}_{out}(\mathcal{R}_s) = \mathbb{P}[C_s \le \mathcal{R}_s] = 1 - \mathbb{P}[C_s > \mathcal{R}_s] \tag{8}$$

where $\mathbb{P}[C_s > \mathcal{R}_s]$ denotes the probability of successful secure transmission, which is given by

$$\mathbb{P}[C_s > \mathcal{R}_s] = \mathbb{P}\left[\log_2\left(\frac{1+\gamma_{_M}}{1+\gamma_{_E}}\right) > \mathcal{R}_s\right] \tag{9a}$$

$$= \mathbb{P}\left[\gamma_{_M} > 2^{\mathcal{R}_s}(1+\gamma_{_E}) - 1\right] \tag{9b}$$

$$= \int_0^\infty f_{\gamma_E}(\gamma_{_E})\left[\int_{2^{\mathcal{R}_s}(1+\gamma_E)-1}^{\infty} f_{\gamma_M}(\gamma_{_M})\,\mathrm{d}\gamma_{\mathrm{M}}\right]\mathrm{d}\gamma_{\mathrm{E}} \tag{9c}$$

$$= \int_0^\infty f_{\gamma_E}(\gamma_{_E})\left[1 - F_{\gamma_M}\left(2^{\mathcal{R}_s}(1+\gamma_{_E}) - 1\right)\right]\mathrm{d}\gamma_{\mathrm{E}} \tag{9d}$$

$$= 1 - \int_0^\infty f_{\gamma_E}(\gamma_{_E})\,F_{\gamma_M}\left(2^{\mathcal{R}_s}(1+\gamma_{_E}) - 1\right)\mathrm{d}\gamma_{\mathrm{E}} \tag{9e}$$

where $F_{\gamma_M}(\cdot)$ is the CDF of $\gamma_{_M}$, which for $\mathcal{F}$ fading is

$$F_{\gamma_M}(\gamma_{_M}) = \sum_{l=0}^{m_M-1}\binom{m_{_M}-1}{l}\frac{(-1)^l}{B(m_{_M}, m_{s_M})}\left\{\frac{1}{m_{s_M}+l} - \frac{(m_{s_M}-1)^{m_{s_M}+l}\,\bar{\gamma}_M^{m_{s_M}+l}}{(m_{s_M}+l)\left[m_{_M}\gamma_{_M} + (m_{s_M}-1)\,\bar{\gamma}_{_M}\right]^{m_{s_M}+l}}\right\}, m_{_M} \in \mathbb{N}. \tag{10}$$

Hence, the corresponding SOP in the presence of multiple Eves can be expressed from (8) and (9e), such that

$$\mathcal{P}_{out}(\mathcal{R}_s) = \int_0^\infty f_{\gamma_{E_m}}(\gamma_{_{E_m}})F_{\gamma_M}\left(2^{\mathcal{R}_s}\left(1+\gamma_{_{E_m}}\right) - 1\right)\mathrm{d}\gamma_{\mathrm{E_m}}. \tag{11}$$

Let us begin by studying the case of two Eves which experience independent and identically distributed (*i.i.d.*) composite fading. By substituting (5) and (10) into (11), we obtain

$$\mathcal{P}_{out}\left(\mathcal{R}_s\right) = 2\sum_{l=0}^{m_M-1}\sum_{k_1=0}^{m_E-1}\binom{m_M-1}{l}\binom{m_E-1}{k_1} \times \frac{(-1)^{l+k_1}\, {m_E}^{m_E}\left[(m_{s_E}-1)\bar{\gamma}_E\right]^{m_{s_E}}\left\{\mathcal{I}_1-\mathcal{I}_2-\mathcal{I}_3+\mathcal{I}_4\right\}}{B^2(m_E, m_{s_E})B(m_M, m_{s_M})\,(m_{s_M}+l)(m_{s_E}+k_1)} \tag{12}$$

where

$$\mathcal{I}_1 = \int_0^\infty \frac{\gamma_{E_m}^{m_E-1}}{\left[m_E\gamma_{E_m}+(m_{s_E}-1)\,\bar{\gamma}_E\right]^{m_E+m_{s_E}}}\mathrm{d}\gamma_{\mathrm{E_m}} \tag{13}$$

$$\mathcal{I}_2 = \int_0^\infty \frac{\gamma_{E_m}^{m_E-1}}{\left[m_E\gamma_{E_m}+(m_{s_E}-1)\,\bar{\gamma}_E\right]^{m_E+m_{s_E}}} \times \left[\frac{m_M\left(2^{\mathcal{R}_s}\left(1+\gamma_{E_m}\right)-1\right)}{(m_{s_M}-1)\,\bar{\gamma}_M}+1\right]^{-(m_{s_M}+l)}\mathrm{d}\gamma_{\mathrm{E_m}} \tag{14}$$

$$\mathcal{I}_3 = \int_0^\infty \frac{\gamma_{E_m}^{m_E-1}\left[(m_{s_E}-1)\bar{\gamma}_E\right]^{m_{s_E}+k_1}}{\left[m_E\gamma_{E_m}+(m_{s_E}-1)\,\bar{\gamma}_E\right]^{m_E+2\,m_{s_E}+k_1}}\mathrm{d}\gamma_{\mathrm{E_m}} \tag{15}$$

and

$$\mathcal{I}_4 = \int_0^\infty \frac{\gamma_{E_m}^{m_E-1}\left[(m_{s_E}-1)\bar{\gamma}_E\right]^{m_{s_E}+k_1}}{\left[m_E\gamma_{E_m}+(m_{s_E}-1)\,\bar{\gamma}_E\right]^{m_E+2\,m_{s_E}+k_1}} \times \left[\frac{m_M\left(2^{\mathcal{R}_s}\left(1+\gamma_{E_m}\right)-1\right)}{(m_{s_M}-1)\,\bar{\gamma}_M}+1\right]^{-(m_{s_M}+l)}\mathrm{d}\gamma_{\mathrm{E_m}}. \tag{16}$$

With the aid of [29, Eq. (3.194.3)], [29, Eq. (3.197.1)] and after some manipulations, the following expressions are obtained

$$\mathcal{I}_1 = \frac{B\left(m_E, m_{s_E}\right)}{{m_E}^{m_E}\left[(m_{s_E}-1)\,\bar{\gamma}_E\right]^{m_{s_E}}} \tag{17}$$

$$\mathcal{I}_2 = \frac{\mathcal{D}_1^{m_E}\mathcal{D}_2^{m_{s_M}+l}B\left(m_E, \mathcal{D}_3\right)}{{m_E}^{m_E}\left[(m_{s_E}-1)\,\bar{\gamma}_E\right]^{m_{s_E}}} \times {}_2F_1\Big(m_E+m_{s_E}, m_E; m_E+\mathcal{D}_3; 1-\mathcal{D}_1\Big) \tag{18}$$

$$\mathcal{I}_3 = \frac{B\left(m_E, 2\,m_{s_E}+k_1\right)}{{m_E}^{m_E}\left[(m_{s_E}-1)\,\bar{\gamma}_E\right]^{m_{s_E}}} \tag{19}$$

and

$$\mathcal{I}_4 = \frac{B\left(m_E, \mathcal{D}_4\right)\mathcal{D}_1^{m_E}\mathcal{D}_2^{m_{s_M}+l}}{{m_E}^{m_E}\left[(m_{s_E}-1)\,\bar{\gamma}_E\right]^{m_{s_E}}} \times {}_2F_1\left(m_E+2\,m_{s_E}+k_1, m_E; m_E+\mathcal{D}_4; 1-\mathcal{D}_1\right) \tag{20}$$

where $\mathcal{D}_1 = \frac{m_E\left[m_M\left(2^{\mathcal{R}_s}-1\right)+(m_{s_M}-1)\,\bar{\gamma}_M\right]}{m_M\,2^{\mathcal{R}_s}\,(m_{s_E}-1)\,\bar{\gamma}_E}$, $\mathcal{D}_2 = \frac{(m_{s_M}-1)\,\bar{\gamma}_M}{m_M\,(2^{\mathcal{R}_s}-1)+(m_{s_M}-1)\,\bar{\gamma}_M}$, $\mathcal{D}_3 = m_{s_E}+m_{s_M}+l$, $\mathcal{D}_4 = 2\,m_{s_E}+k_1+m_{s_M}+l$ and ${}_2F_1(\cdot,\cdot;\cdot;\cdot)$ denotes the Gauss hypergeometric function [29, Eq. (9.111)]. Substituting (17), (18), (19) and (20) into (12) and after some algebraic manipulations, the SOP in the presence of two Eves which experience *i.i.d* $\mathcal{F}$ composite fading can be obtained in closed-form as

$$\mathcal{P}_{out}\left(\mathcal{R}_s\right) = \sum_{l=0}^{m_M-1}\sum_{k_1=0}^{m_E-1}\binom{m_M-1}{l}\binom{m_E-1}{k_2} \times \frac{2\,(-1)^{l+k_1}}{B^2(m_E, m_{s_E})B(m_M, m_{s_M})\,(m_{s_M}+l)(m_{s_E}+k_1)} \times\Big\{B(m_E, m_{s_E})-B(m_E, 2m_{s_E}+k_1)-\mathcal{D}_1^{m_E}\mathcal{D}_2^{m_{s_M}+l}[\mathcal{Q}_1-\mathcal{Q}_2]\Big\} \tag{21}$$

where

$$\mathcal{Q}_1 = B(m_E, \mathcal{D}_3)\,{}_2F_1(m_E+m_{s_E}, m_E; m_E+\mathcal{D}_3; 1-\mathcal{D}_1) \tag{22}$$

and

$$\mathcal{Q}_2 = B(m_E, \mathcal{D}_4)\,{}_2F_1(m_E+2m_{s_E}+k_1, m_E; m_E+\mathcal{D}_4; 1-\mathcal{D}_1). \tag{23}$$

IV. Numerical Results

Fig. 1 shows the behavior of the SOP over $\mathcal{F}$ composite fading channels in the presence of a single Eve ($L = 1$) for different values of m_M, m_{s_M}, $\bar{\gamma}_M$ and $\mathcal{R}_s$ when $m_E = 2$, $m_{s_E} = 2$ and $\bar{\gamma}_E = 10$ dB. It is clear that, irrespective of the values of m_M, m_{s_M} and $\mathcal{R}_s$, the SOP decreases as $\bar{\gamma}_M$ increases. For comparison, in Fig. 1, we consider the red continuous curve as a reference, where both main channel and Eve channel experience the same fading conditions ($m_M = m_E = 2$, $m_{s_M} = m_{s_E} = 2$). When looking at the cases of ($m_E = 10$, $m_{s_E} = 2$) and ($m_E = 2$, $m_{s_E} = 10$), i.e., when the main channel conditions ($m_M = 2$, $m_{s_M} = 2$) are worse than those for the Eve channel ($m_E = 3$, $m_{s_E} = 3$), the SOP decreases compared to the reference plot. Moreover, it is obvious that as the secrecy rate ($\mathcal{R}_s$) increases, the SOP increases. Interestingly, the effect of m_E (i.e., the multipath fading parameter) on the SOP becomes less significant compared to that of m_{s_E} (i.e., the shadowing parameter). Figs. 1 also include the SOP (line with circles) over $\mathcal{F}$ composite fading channels in the presence of two Eves ($L = 2$) which experience *i.i.d* $\mathcal{F}$ composite fading. For all of the composite fading conditions, it is clear that the SOP increases as the number of Eves increases to two ($L = 2$), demonstrating the impact of an increasing number of Eves upon the SOP.

Fig. 2 illustrates the corresponding SOP in the presence of two Eves which experience independent and not identically distributed (*i.n.i.d.*) $\mathcal{F}$ composite fading when $m_M = 2$, $m_{s_M} = 2$ and $\mathcal{R}_s = 0.2$. For comparison, in Fig. 2, we consider the red continuous curve as a reference, where the both Eve channels experience the same fading conditions ($m_{E_1]} = m_{E_2]} = 2$, $m_{s_{E_1}} = m_{s_{E_2}} = 2$, $\bar{\gamma}_{E_1} = \bar{\gamma}_{E_2} = 10$ dB). When the $m_{E_2]}$, $m_{s_{E_2}}$, $\bar{\gamma}_{E_2}$ parameters increase, i.e., the second Eve channel conditions become better that those for the first Eve channel conditions ($m_{E_1]} = 2$, $m_{s_{E_1}} = 2$, $\bar{\gamma}_{E_1} = 10$), the SOP increases compared to the reference plot.

V. Conclusion

This paper addressed the physical layer security and fading characteristics of device to device communications in terms

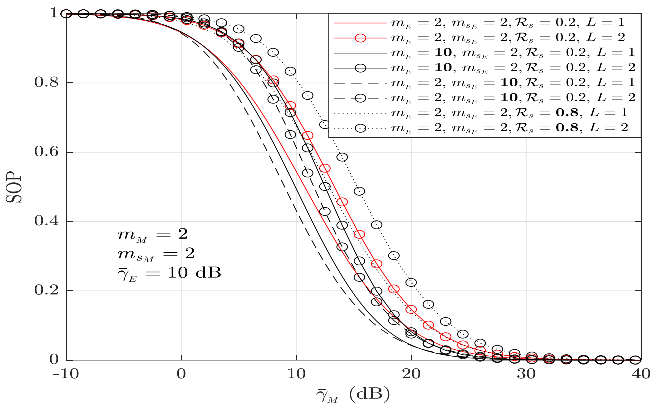

Fig. 1. SOP versus $\bar{\gamma}_M$ considering different m_E, m_{s_E}, $\mathcal{R}_s$ and L (a number of Eves) when $m_M = 2$, $m_{s_M} = 2$ and $\bar{\gamma}_E = 10$ dB.

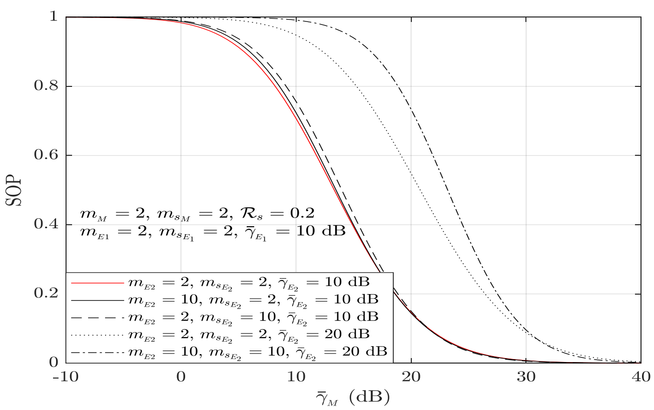

Fig. 2. SOP versus $\bar{\gamma}_M$ in the presence of *i.n.i.d.* two Eves when $m_M = 2$, $m_{s_M} = 2$ and $\mathcal{R}_s = 0.2$ dB.

of the achievable secure outage probability in the presence of two eavesdroppers and $\mathcal{F}$ composite fading channels. In this context, a novel closed-form expression was derived for the corresponding SOP which then assisted in developing useful insights into the behavior of the SOP as a function of the key parameters of $\mathcal{F}$ composite fading channels as well as the number of Eves. The derived analytic results are novel and were corroborated by results from computer simulations.

References

[1] A. Asadi, Q. Wang, and V. Mancuso, "A survey on device-to-device communication in cellular networks," *Commun. Surv. Tutor.*, vol. 16, no. 4, pp. 1801–1819, 2014.

[2] N. Pathak, A. Mukherjee, and S. Misra, "Reconfigure and reuse: Interoperable wearables for healthcare IoT," in *Proc. IEEE INFOCOM*, 2020, pp. 20–29.

[3] Z. Su, W. Feng, J. Tang, Z. Chen, Y. Fu, N. Zhao, and K.-K. Wong, "Energy efficiency optimization for D2D communications underlaying UAV-assisted industrial IoT networks with SWIPT," *IEEE Internet Things J (Early Access)*, 2022.

[4] S. K. Yoo, S. L. Cotton, Y. J. Chun, W. G. Scanlon, and G. A. Conway, "Channel characteristics of dynamic off-body communications at 60 GHz under line-of-sight (LOS) and non-LOS conditions," *IEEE Antennas and Wireless Propag. Lett.*, vol. 16, pp. 1553–1556, 2017.

[5] Z. Hussain, H. Mehdi, S. M. A. Saleem *et al.*, "Analysis of D2D communications over Gamma/Nakagami fading channels," *Eng. Technol. Appl. Sci. Res.*, vol. 8, no. 2, pp. 2693–2698, Apr. 2018.

[6] S. K. Yoo and S. L. Cotton, "Composite fading in non-line-of-sight off-body communications channels," in *Proc. EUCAP*, Mar. 2017, pp. 286–290.

[7] E. Illi, F. E. Bouanani, D. B. da Costa, P. C. Sofotasios, F. Ayoub, K. Mezher, and S. Muhaidat, "Physical layer security of a dual-hop regenerative mixed rf/uow system," *IEEE Transactions on Sustainable Computing*, vol. 6, no. 1, pp. 90–104, 2021.

[8] J. M. Moualeu, P. C. Sofotasios, D. B. da Costa, S. Muhaidat, W. Hamouda, and U. S. Dias, "Physical-layer security of simo communication systems over multipath fading conditions," *IEEE Transactions on Sustainable Computing*, vol. 6, no. 1, pp. 105–118, 2021.

[9] O. S. Badarneh, P. C. Sofotasios, S. Muhaidat, S. L. Cotton, K. M. Rabie, and N. Aldhahir, "Achievable physical-layer security over composite fading channels," *IEEE Access*, vol. 8, pp. 195 772–195 787, 2020.

[10] H. Zhang, T. Wang, L. Song, and Z. Han, "Radio resource allocation for physical-layer security in D2D underlay communications," in *Proc. IEEE ICC*, 2014, pp. 2319–2324.

[11] I. Csiszár and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, 1978.

[12] 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.

[13] 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. Asilomar Conf. Signals, Syst. Comput.*, Nov. 2009, pp. 829–833.

[14] J. Barros and M. R. Rodrigues, "Secrecy capacity of wireless channels," in *Proc. IEEE Int. Symp. Inf. Theory*, Jul. 2006, pp. 356–360.

[15] Y. Liang, H. V. Poor, and S. Shamai, "Secure communication over fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2470–2492, Jun. 2008.

[16] X. Liu, "Outage probability of secrecy capacity over correlated log-normal fading channels," *IEEE Commun. Lett.*, vol. 17, no. 2, pp. 289–292, Feb. 2013.

[17] ——, "Strictly positive secrecy capacity of log-normal fading channel with multiple eavesdroppers," in *Proc. IEEE ICC*, Jun. 2014, pp. 775–779.

[18] M. Srinivasan and S. Kalyani, "Secrecy capacity of κ-μ shadowed fading channels," *IEEE Commun. Lett.*, vol. 22, no. 8, pp. 1728–1731, Aug. 2018.

[19] G. C. Alexandropoulos and K. P. Peppas, "Secrecy outage analysis over correlated composite Nakagami-m/gamma fading channels," *IEEE Commun. Lett.*, vol. 22, no. 1, pp. 77–80, Jan. 2018.

[20] L. Kong and G. Kaddoum, "On physical layer security over the Fisher-Snedecor $\mathcal{F}$ wiretap fading channels," *IEEE Access*, vol. 6, pp. 39 466–39 472, Jul. 2018.

[21] J. Gong, H. Lee, and J. Kang, "Generalised moment generating function-based secrecy performance analysis over Fisher-Snedecor $\mathcal{F}$ composite fading channels," *Electron. Lett.*, vol. 54, no. 24, pp. 1381–1383, Dec. 2018.

[22] O. S. Badarneh *et al.*, "On the secrecy capacity of Fisher-Snedecor $\mathcal{F}$ fading channels," in *Proc. WiMob*, Oct. 2018, pp. 102–107.

[23] M. Pei, J. Wei, K.-K. Wong, and X. Wang, "Masked beamforming for multiuser MIMO wiretap channels with imperfect CSI," *IEEE Trans. Wireless Commun.*, vol. 11, no. 2, pp. 544–549, Dec. 2011.

[24] M. Nakagami, *The m-distribution — A general formula of intensity distribution of rapid fading*. Statistical methods in radio wave propagation, Elsevier, 1960.

[25] K. P. Peppas, G. C. Alexandropoulos, E. D. Xenos, and A. Maras, "The Fischer–Snedecor $\mathcal{F}$-distribution model for turbulence-induced fading in free-space optical systems," *J. Light. Technol.*, vol. 38, no. 6, pp. 1286–1295, Dec. 2019.

[26] S. K. Yoo *et al.*, "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.

[27] ——, "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.

[28] A. D. Wyner, "The wire-tap channel," *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975.

[29] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*, 7th ed. London: Academic Press, 2007.