# Intercept Probability Analysis over the Cascaded Fisher-Snedecor $\mathcal{F}$ Fading Wiretap Channels

Long Kong[†], Yun Ai[⋆], Jiguang He[‡], Nandana Rajatheva[‡], and Georges Kaddoum[†]

[†]Department of Electrical Engineering, École de technologie supérieure (ÉTS), Université du Québec, Montreal, Canada
[⋆]Faculty of Engineering, Norwegian University of Science and Technology, Gjøvik, Norway
[‡]Center for Wireless Communications (CWC), University of Oulu, Oulu, Finland
Email: long.kong.1@ens.etsmtl.ca, yun.ai@ntnu.no, {jiguang.he,nandana.rajatheva}@oulu.fi, georges.kaddoum@etsmtl.ca

***Abstract*—In this paper, we have investigated the physical layer security over cascaded Fisher-Snedecor $\mathcal{F}$ fading channels in the presence of randomly distributed eavesdroppers. To characterize the eavesdroppers' intercept capability, both the conceptual $k$-th nearest and best eavesdroppers are introduced. The probability density function (PDF) of the $k$-th nearest and best eavesdropper is characterized. The probability of interception, $\mathcal{P}_{int}$, is correspondingly regarded as the secrecy metric, and is further derived with closed-form expressions in terms of Fox's $H$-function. For the purposes of providing more insights, the asymptotic behavior of the intercept probability is also provided. To explore the effects of the eavesdroppers' density and the channel fading conditions on the secrecy performance, we have performed the Monte-Carlo simulation and compared our analytical results with the simulated ones. One can find that our analytical results are successfully verified by the simulation results.**

***Index Terms*—Physical layer security, cascaded Fisher-Snedecor $\mathcal{F}$, Fox's $H$-function, Poisson point process**

## I. Introduction

Information-theoretic security, i.e., physical layer security (PLS), has attracted plenty of attentions [1], since the seminal work was established by Shannon and Wyner. On the basis of the classic Wyner's wiretap channel model, many work related to the secrecy performance analysis over various fading channels, including the Gaussian fading channels [2], Rayleigh [3], Rician [4], [5], Nakagami-$m$ [6], Weibull [7], genralized-$\mathcal{K}$ [8], $\alpha-\mu$ [9]–[13], $\kappa-\mu$ [14], $\alpha$-$\eta$-$\kappa$-$\mu$ [15], Fisher-Snedor $\mathcal{F}$ [16], and Fox's $H$-function fading channel [17], etc., were done. Apart from the aforementioned fading model, other models, including the composite fading model and cascaded fading model, are also widely used to characterize some wireless communication scenarios. In particular, the cascaded fading model demonstrates feasibility and applicability in modeling the multi-hop cooperative communications [11], [18], mobile-to-mobile (M2M) communication [19], [20], and radio-frequency identification (RFID) pinhole channels [21], etc.

More recently, the Fisher-Snedecor $\mathcal{F}$ fading channel was proposed by [22], and the Fisher-Snedecor $\mathcal{F}$ is widely used in the device-to-device (D2D) communications due to its good accuracy as well as its simple mathematical form compared with the generalized $\mathcal{K}$ fading channel. Later on, the authors [18] characterized the $N*$Fisher-Snedecor $\mathcal{F}$ distribution, where the probability density function (PDF) and cumulative distribution function (CDF) of the $N*$Fisher-Snedecor $\mathcal{F}$ distribution are derived and given in terms of the Meijer's $G$-function.

Despite the large amount of research dedicated to the research on PLS over various fading channels [2]–[11], [14]–[17], the PLS analysis with focus on cascaded fading channels has been rare in open literature, except our previous work [23]. In [23], the secrecy performance metrics such as average secrecy capacity (ASC) and secrecy outage probability (SOP) of communication systems over the cascaded $\alpha-\mu$ fading channels have been derived in terms of the Fox's $H$-function. Moreover, novel expressions for the the cascaded $\alpha-\mu$ statistical distributions, including the PDF and CDF, were provided in a general and unified form in [23], which facilitates the performance analysis cascaded $\alpha-\mu$ fading channels. The distribution expressions provided in [23] are advantageous since they are derived under the assumption that the fading of each hop is independently but not identically distributed, and also they are not limited to the number of $N$.

To the best of our knowledge, no work in the open literature has ever investigated the PLS over cascaded Fisher-Snedecor $\mathcal{F}$ fading channels. In this work, we study the secrecy performance of communication systems over the cascaded Fisher-Snedecor $\mathcal{F}$ fading in the presence of randomly distributed eavesdroppers. The locations of all eavesdroppers are modeled by the homogeneous Poisson point process (HPPP). The intercept capabilities of all eavesdroppers are mathematically described either by the distance from the source node, i.e., the $k$-th nearest eavesdropper, or by the overall quality of the received signal-to-noise ratio (SNR) at eavesdroppers, i.e., the $k$-th best eavesdropper. The SNR of the $k$-th best eavesdropper accounts for both the large and small scale fading effects [12]. The intercept probability is derived with regards to the $k$-th nearest and best eavesdropper, respectively. Afterwards, Monte Carlo simulations are presented to show the accuracy of our analytical results.

The rest of this paper is structured as follows: Section II presents the system model and formulates the secrecy problem. Subsequently, the intercept probability is derived in Section III and numerically discussed in Section IV. Finally, concluding remarks are given in Section V.

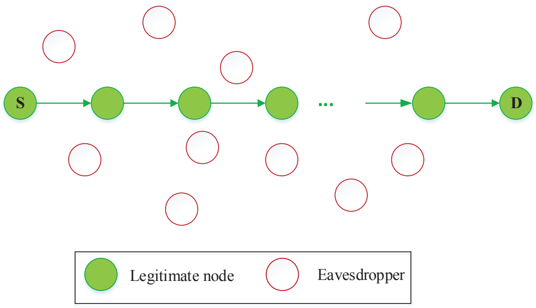

Fig. 1. System model

*Mathematical Functions and Notations*: $[x]^+ = \max(0, x)$, $\Gamma(x)$ is the Gamma function. $H_{p,q}^{m,n}[.]$ is the univariate Fox's $H$-function [24, Eq. (1.2)]. $G_{p,q}^{m,n}[.]$ is the univariate Meijer's $G$-function [25, Eq. (9.301)].

## II. System Model and Problem Formulation

### A. System model

As shown in Fig. 1, we consider a digital communication system, where a source (S) intends to send confidential messages to a destination (D) via multiple amplify-and-forward relays in the presence of randomly distributed eavesdroppers. The locations of all eavesdroppers are characterized by the HPPP distribution with density $\theta_e$. We further assume the following assumptions for the analysis: (i) S is located at the origin; (ii) all eavesdroppers are randomly distributed in an unbounded Euclidean space of dimension $d$; (iii) all users are equipped with single antenna; and (iv) each communication link experiences the Fisher-Snedecor $\mathcal{F}$ fading channels.

The instantaneous received SNR at D is

$$\gamma_D = \prod_{i=1}^{N} \bar{\gamma}_D g_i, \tag{1}$$

where $\bar{\gamma}_D$ is the average power at the receiver side, $g_i = |h_i|^2$, and $h_i$ is the fading coefficient, which follows independent and non-identically Fisher-Snedecor $\mathcal{F}$ distribution with parameters $(m_i, m_{i,s})$. By using the results given in [18], the PDF and CDF of the received instantaneous SNR at D are respectively given by

$$f_D(\gamma) = \kappa_D G_{N,N}^{N,N}\left[\varrho_D\gamma \middle| \begin{matrix} (-m_{i,s})_{i=1:N} \\ (m_i-1)_{i=1:N} \end{matrix}\right], \quad \gamma > 0, \tag{2a}$$

$$F_D(\gamma) = \frac{\kappa_D}{\varrho_D} G_{N+1,N+1}^{N,N+1}\left[\varrho_D\gamma \middle| \begin{matrix} (1-m_{i,s})_{i=1:N}, 1 \\ (m_i)_{i=1:N}, 0 \end{matrix}\right], \tag{2b}$$

where $\kappa_D = \frac{\prod_{i=1}^{N}\mathcal{C}_i}{\bar{\gamma}_D}, \mathcal{C}_i = \frac{\lambda_i}{\Gamma(m_i)\Gamma(m_{i,s})}, \lambda_i = \frac{m_i}{m_{i,s}}$, and $\varrho_D = \frac{\prod_{i=1}^{N}\lambda_i}{\bar{\gamma}_D}$. As shown in Fig. 2, the PDF of $\gamma_D$ is plotted to show the correctness of (2a).

The received SNR at a random eavesdropper is given as

$$\gamma_E = \frac{\bar{\gamma}_E g_e}{r_e^{\alpha}}. \tag{3}$$

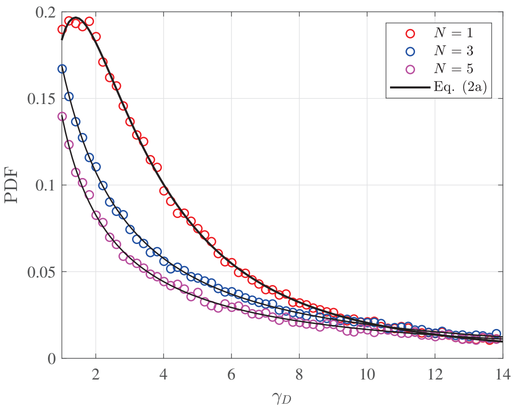

Fig. 2. The PDF of $\gamma_D$ for selected values of $N$ when $m_D = 3$, $m_{D,s} = 2$, $\bar{\gamma}_D = 5$ dB.

Similarly, $\bar{\gamma}_E$ is the average power at the receiver side. $g_e = |h_e|^2$, and $h_e$ is the Fisher-Snedecor $\mathcal{F}$ distributed fading coefficient with parameter $(m_e, m_{e,s})$. $r_e$ is the distance of a randomly distributed eavesdropper from the source, $\alpha$ is the path-loss exponent.

In order to better characterize the eavesdroppers' intercepting capability, two ordering schemes, i.e., either according to the distance or the quality of the received SNR (namely, the $k$-th nearest and best eavesdropper) are considered.

### B. User Association

*1) The $k$-th nearest eavesdropper:* The $k$-th nearest eavesdropper is ordered by the distance from the source to the considered eavesdropper. In other words, all the randomly distributed eavesdroppers are in the descending order, i.e., $|r_1| < |r_2| < |r_3| < \cdots$.

**Theorem 1.** *Inspired by [12, Lemma 1], the PDF of the instantaneous SNR of $k$-th nearest eavesdropper is given by*

$$f_N(\gamma) = \frac{\mathcal{C}_E/\bar{\gamma}_E}{\Gamma(k)A_e^{\frac{1}{\delta}}} H_{2,1}^{1,2}\left[\frac{\lambda_E\gamma}{\bar{\gamma}_E A_e^{\frac{1}{\delta}}} \middle| \begin{matrix} (-m_{e,s}, 1), (1-k-\frac{1}{\delta}, \frac{1}{\delta}) \\ (m_e - 1, 1) \end{matrix}\right], \tag{4}$$

*where $A_e = \pi\theta_e$, $\lambda_E = \frac{m_E}{m_{E,s}}$, $\mathcal{C}_E = \frac{\lambda_E}{\Gamma(m_E)\Gamma(m_{E,s})}$, and $\delta = \frac{d}{\alpha}$.*

*Proof.* Substituting the PDF of $r_e^{\alpha}$ [6, Eq. (5)],

$$f_{r_e^{\alpha}}(y) = \exp(-A_e y^{\delta})\frac{\delta(A_e y^{\delta})^k}{y\Gamma(k)}, \tag{5}$$

and the PDF of $g_e$ [16]

$$f_{g_e}(\gamma) = \mathcal{C}_E G_{1,1}^{1,1}\left[\lambda_E\gamma \middle| \begin{matrix} -m_{e,s} \\ m_e - 1 \end{matrix}\right] \tag{6}$$

into

$$f_N(\gamma) = \int_0^{\infty} \frac{y}{\bar{\gamma}_E} f_{g_e}\left(\frac{y\gamma}{\bar{\gamma}_E}\right) f_{r_e^{\alpha}}(y)dy, \tag{7}$$

and using [26, Eq.(8.3.2.21)]

$$G_{p,q}^{m,n}\left[x \middle| \begin{matrix} (a_p) \\ (b_q) \end{matrix}\right] = H_{p,q}^{m,n}\left[x \middle| \begin{matrix} (a_p, 1) \\ (b_q, 1) \end{matrix}\right], \tag{8}$$

we have

$$f_N(\gamma) \overset{(a)}{=} \frac{A_e^k \mathcal{C}_E}{\bar{\gamma}_E \Gamma(k)} \int_0^\infty y^{k\delta} H_{0,1}^{1,0}\left[ A_e^{\frac{1}{\delta}} \gamma \middle| \begin{matrix} - \\ (0, \frac{1}{\delta}) \end{matrix} \right] \\ \times H_{1,1}^{1,1}\left[ \frac{\lambda_E \gamma}{\bar{\gamma}_E} y \middle| \begin{matrix} (-m_{e,s}, 1) \\ (m_e - 1, 1) \end{matrix} \right] dy, \tag{9}$$

where step $(a)$ is developed by re-expressing the exponential function in terms of the Fox's $H$-function [24, Eq.(1.125)], and then using the Mellin transform of the product of two Fox's $H$-function [26, Eq. (2.25.1.1)], the proof is accomplished. ■

*2) The $k$-th best eavesdropper:* Different from the $k$-th nearest user, the $k$-th best user is ordered according to the quality of the received SNR at the eavesdroppers, i.e., $\gamma_{E,1} > \gamma_{E,2} > \gamma_{E,3} \cdots$. Obviously, the eavesdropper with smaller index is more capable of successfully intercepting the legitimate links.

For the notational simplicity, all the $k$-th nearest and best eavesdropper are denoted as $\gamma_{N,k}$ and $\gamma_{B,k}$, respectively.

**Theorem 2.** *Similarly, by employing the results from [12], [27], the PDF of the instantaneous SNR for the $k$-th best eavesdropper is given by*

$$f_B(\gamma) = \exp\left( -A_b \left( \frac{\bar{\gamma}_E}{\gamma} \right) \right) \frac{\delta \left( A_b \left( \frac{\bar{\gamma}_E}{\gamma} \right)^\delta \right)^k}{\gamma \Gamma(k)} \\ \overset{(b)}{=} \frac{1}{\bar{\gamma}_E \Gamma(k) A_b^{\frac{1}{\delta}}} H_{1,0}^{0,1}\left[ \frac{\gamma}{\bar{\gamma}_E A_b^{\frac{1}{\delta}}} \middle| \begin{matrix} (1 - k - \frac{1}{\delta}, \frac{1}{\delta}) \\ - \end{matrix} \right], \tag{10}$$

*where $A_b = \frac{\lambda_e c_d \delta \mathcal{C}_E \Gamma(m_k + \delta) \Gamma(m_{k,s} - \delta)}{\lambda_E^{\delta+1}}$ and $c_d = \frac{\pi^{\frac{d}{2}}}{\Gamma\left(1 + \frac{d}{2}\right)}$.*

*Proof.* Applying the results given in [11, Eqs. (11-12)], and following the same methodology as in [11], we have the proof achieved with ease. Step $(b)$ is further developed with the help of [24, Eqs. (1.58-1.60)] to simplify the following intercept probability analysis. ■

As shown in Fig. 3, we have demonstrated that our analytical PDFs of the $k$-th nearest and best eavesdropper are in perfect match with Monte Carlo simulations.

### C. Problem Formulation

The instantaneous secrecy capacity of such a system configuration under the assumption that eavesdroppers do not collude is given by

$$C_{s,k} = [\log_2(1 + \gamma_D) - \log_2(1 + \gamma_l)]^+, \quad l \in \{N, B\}. \tag{11}$$

The probability of interception indicates the capability of the eavesdroppers of decoding and intercepting the legitimate transmitted messages from S. Mathematically, it is expressed as follows [11, Eq. (16)]

$$\mathcal{P}_{int,l} = Pr(C_{s,k} < 0) = \mathcal{P}(\gamma_D < \gamma_l) = \int_0^\infty F_l(\gamma) f_D(\gamma) d\gamma. \tag{12}$$

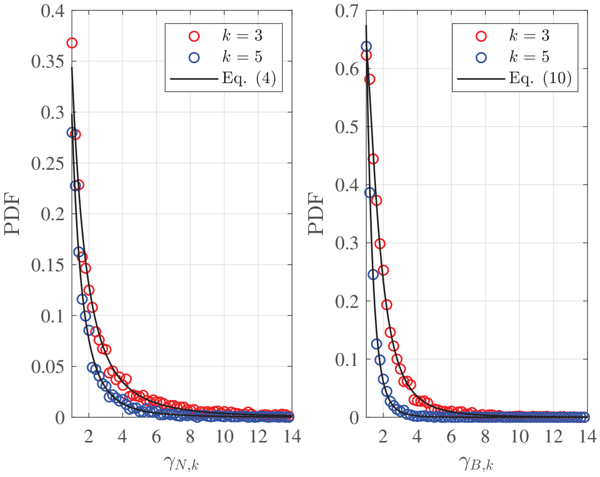

Fig. 3. The PDFs of $\gamma_{N,k}$ and $\gamma_{B,k}$ for the $k$-th nearest and best eavesdropper when $m_e = 2$, $m_{e,s} = 3$, $\bar{\gamma}_E = 0$ dB, $d = \alpha = 2$, and $\theta_e = 0.75$.

## III. Secrecy Performance Characterization

In this section, we aim at deriving the $\mathcal{P}_{int,l}$ under the two ordering schemes. In addition, the asymptotic behavior of the intercept probability is also demonstrated herein.

### A. The $k$-th nearest eavesdropper

*1) Exact Analysis:* In the presence of the $k$-th nearest eavesdropper, the intercept probability over the cascaded Fisher-Snedecor $\mathcal{F}$ fading channels is given by (13), shown at the top of next page.

*Proof.* Plugging (2b) and (4) into

$$\mathcal{P}_{int,N} = \int_0^\infty F_D(\gamma) f_N(\gamma) d\gamma, \tag{14}$$

and then using [26, Eqs. (8.3.2.21) and (2.25.1.1)], the proof is achieved. ■

*2) Asymptotic Analysis:*

**Remark 1.** *Observing (13), $\mathcal{P}_{int,N}$ is given in terms of $\delta = \frac{d}{\alpha}$. When $\delta = 1$, i.e., $\alpha = 2$ and $d = 2$. Physically speaking, it is the situation that all the users are scattered in the 2 dimensional space with a special pass-loss exponent. Subsequently, using [26, Eq. (8.3.2.21)], the intercept probability is given by (15) in Meijer's G-function*[1]*, shown at the top of next page.*

**Remark 2.** *Again, observing from (13), the $\mathcal{P}_{int,N}$ is the function of $\varrho_D = \frac{\prod_{i=1}^N \lambda_i}{\bar{\gamma}_D}$ and $\bar{\gamma}_E$. As the ratio $\frac{\bar{\gamma}_E}{\bar{\gamma}_D}$ goes to 0, applying the asymptotic expansion of the Meijer's G-function [28, Eq. (07.34.06.006.01)], we have the following asymptotic $\mathcal{P}_{int,N}$ given in (16), shown at the top of next page. For the simplicity of notations, let $m_{N+1} = m_{e,s}, m_{N+2} = k, m_{N+1,s} = 0, m_{N+2,s} = m_e$.*

[1] It is noted that the implementation of univariate Meijer's $G$-function is available at mathematical packages, such as Mathematica (MeijerG$[a_1, \cdots, a_n, a_{n+1}, \cdots, a_p, b_1, \ldots, b_m, b_{m+1}, \cdots, b_q, z]$), and MATLAB (meijerG$(a, b, c, d, z)$).

$$\mathcal{P}_{int,N} = \frac{\kappa_D \mathcal{C}_E}{\varrho_D \lambda_E \Gamma(k)} H^{N+2,N+2}_{N+2,N+3}\left[ \frac{\varrho_D \bar{\gamma}_E A_e^{\frac{1}{\delta}}}{\lambda_E} \middle| \begin{array}{c} (1-m_{i,s},1)_{i=1:N}, (1,1), (1-m_e,1) \\ (m_i,1)_{i=1:N}, (m_{e,s},1), \left(k, \frac{1}{\delta}\right), (0,1) \end{array} \right]. \tag{13}$$

$$\mathcal{P}_{int,N} = \frac{\kappa_D \mathcal{C}_E}{\varrho_D \lambda_E \Gamma(k)} G^{N+2,N+2}_{N+2,N+3}\left[ \frac{\varrho_D \bar{\gamma}_E A_e}{\lambda_E} \middle| \begin{array}{c} (1-m_{i,s})_{i=1:N}, 1, 1-m_e \\ (m_i)_{i=1:N}, m_{e,s}, k, 0 \end{array} \right]. \tag{15}$$

$$\mathcal{P}_{int,N} = \sum_{i=1}^{N+2} \frac{\kappa_D \mathcal{C}_E}{\varrho_D \lambda_E \Gamma(k)} \frac{\prod\limits_{j=1, j\neq i}^{N+2} \Gamma(m_j - m_i) \prod\limits_{j=1}^{N+2} \Gamma(m_{j,s} + m_i)}{\Gamma(1+m_i)} \left( \frac{\varrho_D \bar{\gamma}_E A_e}{\lambda_E} \right)^{m_i}. \tag{16}$$

### *B. The $k$-th best eavesdropper*

*1) Exact Analysis:* The intercept probability for the $k$-th best eavesdropper over the cascaded Fisher-Snedecor $\mathcal{F}$ fading channels is given by (17), shown at the top of next page.

*Proof.* Plugging (2b) and (10) into

$$\mathcal{P}_{int,B} = \int_0^\infty F_D(\gamma) f_B(\gamma) d\gamma, \tag{18}$$

and then using the Mellin transform of the the product of two Fox's $H$-functions, the proof is finished. ■

*2) Asymptotic Analysis:* The asymptotic analysis of $\mathcal{P}_{int,B}$ can be similarly achieved by following Remarks. 1 and 2.

## IV. Numerical Results and Discussion

In this section, the intercept probability in terms of the $k$-th eavesdropper obtained via Monte-Carlo simulations is compared with our analytical results. The Fox's $H$-function is computed by using the approach proposed in [29], this approach is widely used in the open literature to implement the Fox's $H$-function. For simplicity, all the simulation parameters are set to follow the identical Fisher-Snedecor $\mathcal{F}$ distribution, i.e., $m_1 = \cdots = m_N = m_D$ and $m_{1,s} = \cdots = m_{N,s} = m_{D,s}$. The markers denote the Monte-Carlo simulations, the dashed and dotted lines represent the exact analytical results for $\mathcal{P}_{int,N}$ and $\mathcal{P}_{int,B}$, respectively.

Fig. 4 plots the analytical $\mathcal{P}_{int,N}$ and $\mathcal{P}_{int,B}$ against the $k$-th nearest and best eavesdropper for selected values of $N$. One can observe that (i) our analytical expressions for the $\mathcal{P}_{int,N}$ and $\mathcal{P}_{int,B}$ given in Section III are in perfect agreements with the Monte-Carlo simulations; (ii) the larger values of $N$ results in a higher intercept probability, in other words, the larger value of $N$ is more beneficial for the eavesdropper to be capable of wiretapping the legitimate links; and (iii) for selected $N$, the $k$-th best eavesdropper always behaves better than the $k$-th nearest one.

Likewise, in Fig. 5, the impact of the eavesdroppers' density $\theta_e$ on the successfully intercept probability is explored. One can conclude that the $k$-th best eavesdropper is more powerful in intercepting confidential messages compared to the $k$-th nearest one. In addition, the higher density $\theta_e$ contributes more to the successful intercept probability.

Finally, Fig. 6 illustrates the $\mathcal{P}_{int,N}$ and $\mathcal{P}_{int,B}$ for selected values of $\bar{\gamma}_D$. Again, it can be seen that for selected $\bar{\gamma}_D$, the $k$-th best eavesdropper has a higher intercept probability than the $k$-th best one.

## V. Concluding remarks

In this paper, we investigated the PLS of a digital communication link, characterized by the cascaded Fisher-Snedecor $\mathcal{F}$ fading channels. Randomly distributed eavesdroppers are considered and are termed as the $k$-th nearest and best eavesdroppers. The intercept probability are correspondingly derived with closed-form expressions in terms of the Fox's $H$-function. Numerical results and discussions are conducted to show that (i) larger values of $N$ leads to a higher intercept probability; (ii) a higher eavesdropper density $\theta_e$ means a higher intercept probability; and (iii) more importantly, the $k$-th best eavesdropper always outperforms the $k$-th nearest eavesdropper.

## References

[1] J. M. Hamamreh, H. M. Furqan, and H. Arslan, "Classifications and applications of physical layer security techniques for confidentiality: A comprehensive survey," *IEEE Commun. Surveys Tutorials*, pp. 1–1, 2018.

[2] S. Leung-Yan-Cheong and M. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 24, no. 4, pp. 451–456, Jul. 1978.

[3] 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.

[4] 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.

[5] Y. Ai, L. Kong, and M. Cheffena, "Secrecy outage analysis of double shadowed Rician channels," *Electron. Lett.*, 2019.

[6] W. Liu, S. Vuppala, G. Abreu, and T. Ratnarajah, "Secrecy outage in correlated Nakagami-$m$ fading channels," in *Proc. IEEE PIMRC*, Washington, DC, USA, Sept. 2014, pp. 145–149.

[7] X. Liu, "Probability of strictly positive secrecy capacity of the Weibull fading channel," in *2013 IEEE GLOBECOM*, Dec. 2013, pp. 659–664.

[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] L. Kong, H. Tran, and G. Kaddoum, "Performance analysis of physical layer security over $\alpha - \mu$ fading channel," *Electron. Lett.*, vol. 52, pp. 45–47, Jan. 2016.

[10] L. Kong, G. Kaddoum, and Z. Rezki, "Highly accurate and asymptotic analysis on the SOP over SIMO $\alpha-\mu$ fading channels," *IEEE Commun. Lett.*, vol. 22, no. 10, pp. 2088–2091, Oct. 2018.

[11] L. Kong, G. Kaddoum, and S. Vuppala, "On secrecy analysis for D2D networks over $\alpha - \mu$ fading channels with randomly distributed eavesdroppers," in *Proc. ICC Workshops*, May 2018, pp. 1–6.

[12] L. Kong, S. Vuppala, and G. Kaddoum, "Secrecy analysis of random MIMO wireless networks over $\alpha - \mu$ fading channels," *IEEE Trans. Veh. Technol.*, vol. 67, no. 12, pp. 11 654–11 666, Dec. 2018.

$$\mathcal{P}_{int,B} = \frac{\kappa_D}{\rho_D \Gamma(k)} H^{N+1,N+1}_{N+1,N+2}\left[\varrho_D \bar{\gamma}_E A_b^{\frac{1}{\delta}} \middle| \begin{array}{c}(1-m_{i,s},1)_{i=1:N},(1,1)\\ (m_i,1)_{i=1:N},\left(k,\frac{1}{\delta}\right),(0,1)\end{array}\right]. \tag{17}$$

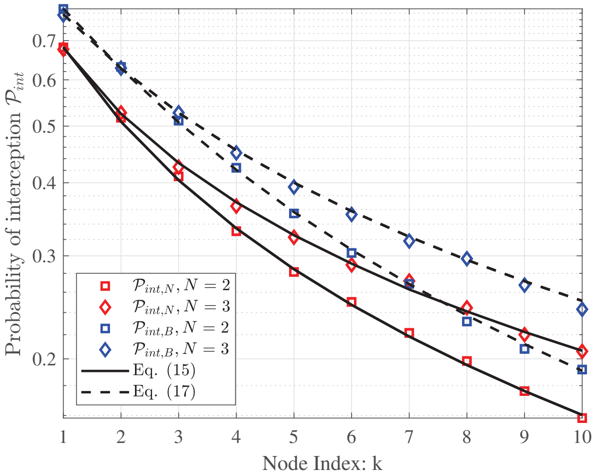

Fig. 4. $\mathcal{P}_{int,N}$ and $\mathcal{P}_{int,B}$ versus the $k$-th nearest and best eavesdropper for selected values of $N$, when $m_D = m_E = 2$, $m_{D,s} = m_{E,s} = 3$, $\theta_e = 1.5$, $\bar{\gamma}_D = 5$ dB, $\alpha = 2$, $d = 2$, and $\bar{\gamma}_E = 0$ dB.

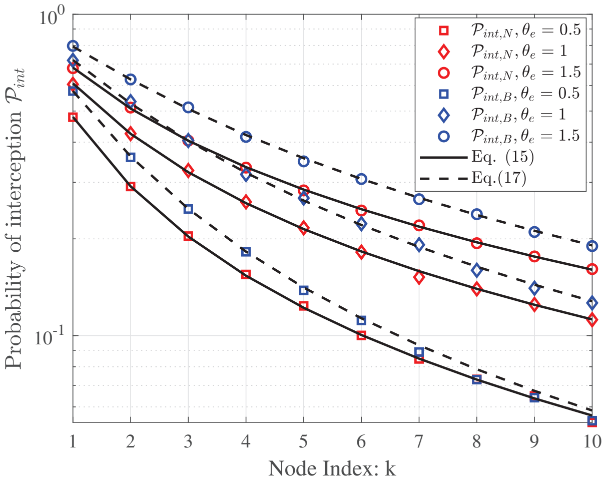

Fig. 5. $\mathcal{P}_{int,N}$ and $\mathcal{P}_{int,B}$ versus the $k$-th nearest and best eavesdropper for selected $\theta_E$, when $m_D = m_E = 2$, $m_{D,s} = m_{E,s} = 3$, $N = 2$, $\bar{\gamma}_D = 5$ dB, $\alpha = 2$, $d = 2$, and $\bar{\gamma}_E = 0$ dB.

[13] A. Mathur, Y. Ai, M. Cheffena, and G. Kaddoum, "Secrecy performance of correlated $\alpha - \mu$ fading channels," *IEEE Commun. Lett.*, pp. 1–1, 2019.

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

[15] A. Mathur, Y. Ai, M. R. Bhatnagar, M. Cheffena, and T. Ohtsuki, "On physical layer security of $\alpha$-$\eta$-$\kappa$-$\mu$ fading channels," *IEEE Commun. Lett.*, vol. 22, no. 10, pp. 2168–2171, Oct. 2018.

[16] 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, 2018.

[17] L. Kong, G. Kaddoum, and H. Chergui, "On physical layer security over Fox's H-function wiretap fading channels," pp. 1–1, 2019.

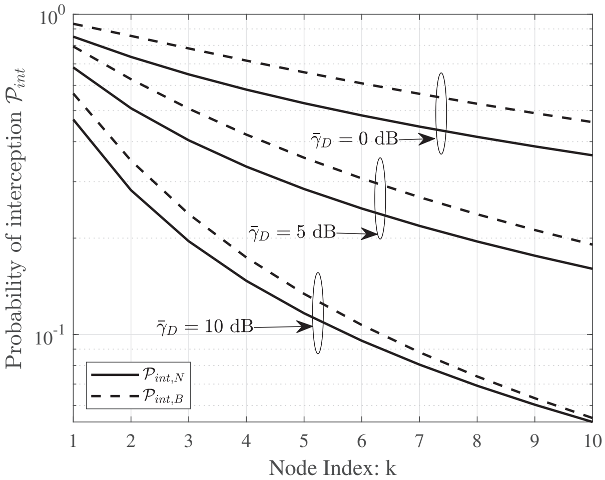

Fig. 6. $\mathcal{P}_{int,N}$ and $\mathcal{P}_{int,B}$ versus the $k$-th nearest and best eavesdropper for selected $\bar{\gamma}_D$, when $m_D = m_E = 2$, $m_{D,s} = m_{E,s} = 3$, $N = 2$, $\theta_e = 1.5$, $\alpha = 2$, $d = 2$, and $\bar{\gamma}_E = 0$ dB.

[18] O. S. Badarneh, S. Muhaidat, P. C. Sofotasios, S. L. Cotton, K. Rabie, and D. B. da Costa, "The N*Fisher-Snedecor $\mathcal{F}$ cascaded fading model," in *Proc. WiMob*, Limassol, Cyprus, Oct 2018, pp. 1–7.

[19] A. A. A. Boulogeorgos, P. C. Sofotasios, B. Selim, S. Muhaidat, G. K. Karagiannidis, and M. Valkama, "Effects of RF impairments in communications over cascaded fading channels," *IEEE Trans. Veh. Technol.*, vol. 65, no. 11, pp. 8878–8894, Nov. 2016.

[20] 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.

[21] A. Bekkali, S. Zou, A. Kadri, M. Crisp, and R. V. Penty, "Performance analysis of passive UHF RFID systems under cascaded fading channels and interference effects," *IEEE Trans. Wireless Commun.*, vol. 14, no. 3, pp. 1421–1433, Mar. 2015.

[22] S. K. Yoo, S. L. Cotton, P. C. Sofotasios, M. Matthaiou, M. Valkama, and G. K. 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.

[23] L. Kong, G. Kaddoum, and D. B. da Costa, "Cascaded $\alpha - \mu$ fading channels: Reliability and security analysis," *IEEE Access*, vol. 6, pp. 41 978–41 992, 2018.

[24] A. M. Mathai, R. K. Saxena, and H. J. Haubold, *The H-function: theory and applications*. Springer Science & Business Media, 2009.

[25] I. S. Gradshteyn and I. M. Ryzhik, *Table of integrals, series, and products*. Academic press, 2014.

[26] A. P. Prudnikov, Y. A. Brychkov, and O. I. Marichev, *Integrals and Series: More special functions*. Gordon and Breach Science Publishers, 1990, vol. 3.

[27] L. Kong and G. Kaddoum, "Secrecy characteristics with assistance of mixture gamma distribution," *IEEE Wireless Commun. Lett.*, pp. 1–1, 2019.

[28] W. R. Inc. (2007) The wolfram functions site. [Online]. Available: http://functions.wolfram.com/

[29] K. P. Peppas, "A new formula for the average bit error probability of dual-hop amplify-and-forward relaying systems over generalized shadowed fading channels," *IEEE Wireless Commun. Lett.*, vol. 1, no. 2, pp. 85–88, Apr. 2012.