Unified Framework for Secrecy Characteristics with Mixture of Gaussian (MoG) Distribution

Long Kong, Symeon Chatzinotas, *Senior Member, IEEE*, and Björn Ottersten, *Fellow, IEEE*

***Abstract*—The mixture of Gaussian (MoG) distribution was proposed to model the wireless channels by implementing the completely unsupervised expectation-maximization (EM) learning algorithm. With the high convenience for density estimation applications, the focus of this letter is supposed to investigate the secrecy metrics, including secrecy outage probability (SOP), the lower bound of SOP, the probability of non-zero secrecy capacity (PNZ), and the average secrecy capacity (ASC) from the information-theoretic perspective. The above-mentioned metrics are derived with simple and unified closed-form expressions. The effectiveness of our obtained analytical expressions are successfully examined and compared with Monte-Carlo simulations. One can conclude that this letter provides a simple but effective closed-form secrecy analysis solution exploiting the MoG distribution.**

***Index Terms*—Physical layer security (PLS), mixture of Gaussian distribution**

I. Introduction

PHYSICAL layer security (PLS) is favored as a promising solution for guaranteeing secure communication. The absence of secret keys makes it outperform the conventional cryptography technique from the information-theoretic viewpoint. In recent decades, plenty of works have studied the PLS over various fading channels, e.g., Rayleigh [1], Rician (Nakagami-n) [2], Hoyt (Nakagami-q) [3], $\alpha-\mu$ [4]–[6], cascaded $\alpha-\mu$ [7], $\kappa-\mu$ [8], Lognormal [9], Fisher-Snedecor $\mathcal{F}$ [10], generalized-$\mathcal{K}$ [11], extended generalized-$\mathcal{K}$ (EGK) [12], $\alpha-\eta-\kappa-\mu$ [13], Málaga [14], etc.

To this end, we were motivated to seek a more general and flexible model, which can encompass or generalize most of the well-known fading channel models to a large extent. The mixture gamma (MG) distribution and the Fox's H-function distribution were proved to be two promising candidates to address the aforementioned concern. The MG distribution was proposed by Atapattu *et al*. in [15] to model the signal-to-noise ratio (SNR) of wireless channels. This distribution can highly accurately characterize the SNRs of composite fading channels. The application of using the MG distribution to characterize the physical layer security is effectively verified in [3], where the secrecy outage probability (SOP), the probability of non-zero secrecy capacity (PNZ), and average secrecy capacity (ASC) are derived with closed-form expressions in terms of the Fox's H-function. In parallel, the feasibility of utilizing the Fox's H-function distribution was explored in [12], which provides a unified secrecy analysis framework, and the analytical results therein indicates that simple transformation of the fading channel characteristics in the manner of Fox's H-function distribution can largely encompass the existing works [1], [5]–[7], [10].

As discussed earlier, both the MG and Fox's H-function distributions are useful and beneficial, but limited to the scenario that all the channel characteristics, i.e., the probability density functions (PDFs) and cumulative distribution functions (CDFs) of fading channel models are known. To the authors' best knowledge, no work has ever considered the scenario that the PDFs and CDFs are not exactly known. A possible answer to such a concern is the mixture of Gaussian (MoG) distribution. Selim *et al.* in [16] proposed the MoG distribution to model the wireless channels, while unsupervised expectation-maximization (EM) learning algorithm was utilized to estimate the parameters of the MoG distribution. The findings of [16] shows that the MoG distribution is especially advantageous to approximate any arbitrarily shaped non-Gaussian density, and can accurately model both composite and noncomposite channels in a very simple expression. Motivated by [16], the main contributions of this paper are twofold.

(1) Providing a simple but effective information-theoretic secrecy analysis solution under the condition of unknown fading channel characteristics. Specifically, highly accurate closed-form SOP, PNZ, and ASC expressions are derived with the aid of the MoG distribution;
(2) Validating the tightness of our obtained results with Monte-Carlo simulations. The accuracy indicator, i.e., analytical error, further confirms our obtained results.

II. System model

Consider the Alice-Bob-Eve classic wiretap model, it is assumed that the instantaneous received SNRs $\gamma_i=\bar{\gamma}_i h_i^2, i\in\{B,E\}$ at Bob and Eve, where $\bar{\gamma}_i$ is the average received SNR, h_i is the channel coefficient and modeled as the MoG distributed random variables (RVs). The PDF and CDF of γ_i are respectively given by [16, Eqs. (23) and (45)]:

$$f_i(\gamma)=\sum_{l=1}^{C_i}\frac{w_l}{\sqrt{8\pi\bar{\gamma}_i\gamma\eta_l}}\exp\left(-\left(\sqrt{\gamma/\bar{\gamma}_i}-\mu_l\right)^2/2\eta_l^2\right), \quad (1a)$$

$$F_i(\gamma)=\sum_{l=1}^{C_i}w_l\Phi\left((\sqrt{\gamma/\bar{\gamma}_i}-\mu_l)/\eta_l\right) \quad (1b)$$

$$\overset{(a)}{=}\sum_{l=1}^{C_i}\frac{w_l}{2}\left[1+\mathrm{erf}\left((\sqrt{\gamma/\bar{\gamma}_i}-\mu_l)/\sqrt{2}\eta_l\right)\right], \quad (1c)$$

This work has been supported by the Luxembourg National Research Fund (FNR) projects, titled Exploiting Interference for Physical Layer Security in 5G Networks (CIPHY), and Energy and CompLexity EffiCienT mIllimeter-wave Large-Array Communications (ECLECTIC).

L. Kong, S. Chatzinotas, and B. Ottersten are with the Interdisciplinary Centre for Security Reliability and Trust (SnT), University of Luxembourg, L-1855 Luxembourg (email: {long.kong, symeon.chatzinotas, bjorn.ottersten}@uni.lu)

where C_i represents the number of Gaussian components[1]. $w_l > 0$, μ_l and η_l are the lth weight, mean, and variance with the constraint of $\sum_l^{C_i} w_l = 1$, which can be evaluated using the unsupervised EM learning algorithm. $\bar{\gamma}_i$ is the average SNR at the receiver. $\text{erf}(x)$ and $\Phi(x)$ are the error function and the CDF of the standard normal distribution. Step (a) is developed for the sake of simplifying the following derivations.

According to [1], for one realization of (γ_B, γ_E) pair, the instantaneous secrecy capacity over quasi-static wiretap fading channels is defined as

$$C_s(\gamma_B, \gamma_E) = \left[\log_2(1+\gamma_B) - \log_2(1+\gamma_E)\right]^+, \quad (2)$$

where $[x]^+ \triangleq \max(x, 0)$.

III. Secrecy Characterization

A. SOP Characterization

Secure communication can be guaranteed only when the secrecy rate R_t is lower than the instantaneous secrecy capacity. The SOP is a pivotal and crucial secrecy indicator, and widely used to characterize the probability that perfect secrecy is compromised.

Theorem 1. *The SOP is given by*

$$\begin{aligned}\mathcal{P}_{out} = \sum_{k=1}^{C_E}\sum_{l=1}^{C_B} w_k w_l \Bigg[&\frac{2}{3}\Phi\left(\frac{\sqrt{(R_s\bar{\gamma}_E\mu_k^2+\mathcal{W})/\bar{\gamma}_B}-\mu_l}{\eta_l}\right)\\ &+\frac{1}{6}\Phi\left((\sqrt{(R_s\bar{\gamma}_E(\mu_k+\sqrt{3}\eta_k)^2+\mathcal{W})/\bar{\gamma}_B}-\mu_l)/\eta_l\right)\\ &+\frac{1}{6}\Phi\left((\sqrt{(R_s\bar{\gamma}_E(\mu_k-\sqrt{3}\eta_k)^2+\mathcal{W})/\bar{\gamma}_B}-\mu_l)/\eta_l\right)\Bigg].\end{aligned} \quad (3)$$

Proof. For a given target secrecy rate R_t, the SOP is mathematically defined as $\mathcal{P}_{out} = Pr\left(C_s \le R_t\right)$ [6], and further developed as follows

$$\mathcal{P}_{out} = \int_0^\infty F_B\left(R_s\gamma + \mathcal{W}\right) f_E(\gamma) d\gamma, \quad (4)$$

where $R_s = 2^{R_t}, \mathcal{W} = 2^{R_t} - 1$. Next, plugging (1a) and (1b) into (4), we get

$$\begin{aligned}\mathcal{P}_{out} &= \sum_{k=1}^{C_E}\sum_{l=1}^{C_B} w_k w_l \int_0^\infty \Phi\left((\sqrt{\left(R_s\gamma+\mathcal{W}\right)/\bar{\gamma}_B}-\mu_l)/\eta_l\right)\\ &\quad\times\frac{1}{\sqrt{8\pi\bar{\gamma}_E\gamma\eta_k}}\exp\left(-\left(\sqrt{\gamma/\bar{\gamma}_E}-\mu_k\right)^2/2\eta_k^2\right)d\gamma\\ &\overset{(b)}{=}\sum_{k=1}^{C_E}\sum_{l=1}^{C_B} w_k w_l \int_0^\infty \Phi\left(\frac{\sqrt{\left(R_s\bar{\gamma}_E y^2+\mathcal{W}\right)/\bar{\gamma}_B}-\mu_l}{\eta_l}\right)\\ &\quad\times\frac{1}{\sqrt{2\pi}\eta_k}\exp\left(-((y-\mu_k)^2)/2\eta_k^2\right)d\gamma,\end{aligned} \quad (5)$$

step (b) is developed by applying the interchange of variables $y = \sqrt{\frac{\gamma}{\bar{\gamma}_E}}$. Since y is a normally distributed RV, i.e., $y \sim \mathcal{N}(\mu_k, \eta_k)$, subsequently applying the result given in [9, Eq. (4)], the proof for $\mathcal{P}_{out}$ is achieved. ∎

The difficulty of deriving the exact closed-form SOP expression, the lower bound of the SOP $\mathcal{P}_{out}^L$ is thereafter widely used to provide an asymptotic behavior of SOP for two scenarios: (i) $R_t \to 0$; and (ii) both γ_B and γ_E operate at high SNR regimes. As such, $\mathcal{P}_{out}^L$ is developed as

$$\mathcal{P}_{out}^L = \int_0^\infty F_B(R_s\gamma) f_E(\gamma) d\gamma, \quad (6)$$

next, substituting (1a) and (1c) into (6), and subsequently making the change of variables $y = \sqrt{\frac{\gamma}{\bar{\gamma}_E}}$, yields

$$\mathcal{P}_{out}^L = \sum_{k=1}^{C_E}\sum_{l=1}^{C_B}\frac{w_k w_l}{2}(1+\mathcal{U}), \quad (7)$$

where

$$\mathcal{U} = \int_0^\infty \frac{\exp\left(-\frac{(y-\mu_k)^2}{2\eta_k^2}\right)}{\sqrt{2\pi}\eta_k}\text{erf}\left(\frac{\sqrt{R_s\bar{\gamma}_E/\bar{\gamma}_B}y-\mu_l}{\eta_l}\right)dy.$$

Next, applying [17, Eq. (3.462.1)] on $\mathcal{U}$ and after some mathematical manipulations, $\mathcal{P}_{out}^L$ is eventually derived as

$$\mathcal{P}_{out}^L = \sum_{k=1}^{C_E}\sum_{l=1}^{C_B}\frac{w_k w_l}{2}\left(1+\text{erf}\left[\frac{\sqrt{\frac{R_s\bar{\gamma}_E}{\bar{\gamma}_B}}\mu_k-\mu_l}{\sqrt{2\eta_l^2+2\eta_k^2\frac{R_s\bar{\gamma}_E}{\bar{\gamma}_B}}}\right]\right). \quad (8)$$

For the simplicity of following notations, let $\rho = \frac{\bar{\gamma}_B}{\bar{\gamma}_E}$.

B. PNZ Characterization

The PNZ is regarded as another important secrecy metric to measure the existence of the positive secrecy capacity with a probability $\mathcal{P}_{nz}$, mathematically speaking, it means that positive secrecy capacity can be achieved when $\gamma_B > \gamma_E$.

Theorem 2. *The PNZ is given by*

$$\mathcal{P}_{nz} = \sum_{k=1}^{C_E}\sum_{l=1}^{C_B}\frac{w_k w_l}{2}\left(1+erf\left[\frac{\sqrt{\rho}\mu_l-\mu_k}{\sqrt{2(\eta_k^2+\rho\eta_l^2)}}\right]\right), \quad (9a)$$

$$\mathcal{P}_{nz} = \sum_{k=1}^{C_E}\sum_{l=1}^{C_B} w_k w_l \Phi\left(\frac{\sqrt{\rho}\mu_l-\mu_k}{\sqrt{2(\eta_k^2+\rho\eta_l^2)}}\right). \quad (9b)$$

Apparently, $\mathcal{P}_{nz}$ does not vary with the change of ρ.

Proof. Revisiting the definition of $\mathcal{P}_{nz}$ [12], i.e., $\mathcal{P}_{nz} = \int_0^\infty F_E(\gamma) f_B(\gamma) d\gamma$, then following the same procedure as the proof of $\mathcal{P}_{out}^L$, the proof is finished. (9b) is obtained by using $\Phi(x) = \frac{1}{2}\left(1+erf(\frac{x}{\sqrt{2}})\right)$. ∎

C. ASC Characterization

The ASC is another secrecy metric that quantifies the maximum achievable secrecy rate.

Theorem 3. *The ASC is given by (10), shown at the top of next page, where* $\mathcal{G}_B(x, \bar{\gamma}_B, \mu, \eta, \rho) = \log_2(1+\bar{\gamma}_B x^2)\Phi\left(\frac{\sqrt{\rho}x-\mu}{\eta}\right)$ *and* $\mathcal{G}_E(x, \bar{\gamma}_E, \mu, \eta, \rho) = \log_2(1+\bar{\gamma}_E x^2)\Phi\left(\frac{x/\sqrt{\rho}-\mu}{\eta}\right)$.

[1]The number of components C_i is selected automatically using the Bayesian information criterion (BIC) method given in [16, Section III-C], whereas the corresponding parameters for the mixture are evaluated using the EM algorithm.

$$\bar{C}_s = \sum_{k=1}^{C_E}\sum_{l=1}^{C_B} w_l w_k \left[\frac{2}{3}\mathcal{G}_B(\mu_l,\bar{\gamma}_B,\mu_k,\eta_k,\rho) + \frac{1}{6}\mathcal{G}_B(\mu_l+\sqrt{3}\eta_l,\bar{\gamma}_B,\mu_k,\eta_k,\rho) + \frac{1}{6}\mathcal{G}_B(\mu_l-\sqrt{3}\eta_l,\bar{\gamma}_B,\mu_k,\eta_k,\rho)\right.$$
$$\left. + \frac{2}{3}\mathcal{G}_E\left(\mu_k,\bar{\gamma}_E,\mu_l,\eta_l,\frac{1}{\rho}\right) + \frac{1}{6}\mathcal{G}_E\left(\mu_k+\sqrt{3}\eta_k,\bar{\gamma}_E,\mu_l,\eta_l,\frac{1}{\rho}\right) + \frac{1}{6}\mathcal{G}_E\left(\mu_k-\sqrt{3}\eta_k,\bar{\gamma}_E,\mu_l,\eta_l,\frac{1}{\rho}\right)\right] \quad (10)$$
$$+ \sum_{k=1}^{C_E} w_k \left[\frac{2}{3}\log_2(1+\bar{\gamma}_E\mu_k^2) + \frac{1}{6}\log_2\left(1+\bar{\gamma}_E(\mu_k+\sqrt{3}\eta_k)^2\right) + \frac{1}{6}\log_2\left(1+\bar{\gamma}_E(\mu_k-\sqrt{3}\eta_k)^2\right)\right].$$

Proof. By averaging (2) over γ_B and γ_E, the ASC is mathematically expressed as [12, Eq. (6)], $\bar{C}_s = \mathcal{I}_1 + \mathcal{I}_2 - \mathcal{I}_3$, where $\mathcal{I}_1 = \int_0^\infty \log_2(1+\gamma_B) f_B(\gamma_B) F_E(\gamma_B) d\gamma_B$, $\mathcal{I}_2 = \int_0^\infty \log_2(1+\gamma_E) f_E(\gamma_E) F_B(\gamma_E) d\gamma_E$, $\mathcal{I}_3 = \int_0^\infty \log_2(1+\gamma_E) f_E(\gamma_E) d\gamma_E$. Next, substituting (1a) and (1b) into $\mathcal{I}_1$, yields

$$\mathcal{I}_1 = \sum_{l=1}^{C_B}\sum_{k=1}^{C_E} w_l w_k \int_0^\infty \frac{\log_2(1+\gamma)}{\sqrt{8\pi\bar{\gamma}_B\gamma\eta_l}} \Phi\left(\frac{\sqrt{\gamma/\bar{\gamma}_E}-\mu_k}{\eta_k}\right) \times \exp\left(-\left(\sqrt{\gamma/\bar{\gamma}_B}-\mu_l\right)^2/2\eta_l^2\right) d\gamma. \quad (11)$$

Subsequently, performing the change of variables $y = \sqrt{\gamma/\bar{\gamma}_B}$, we have

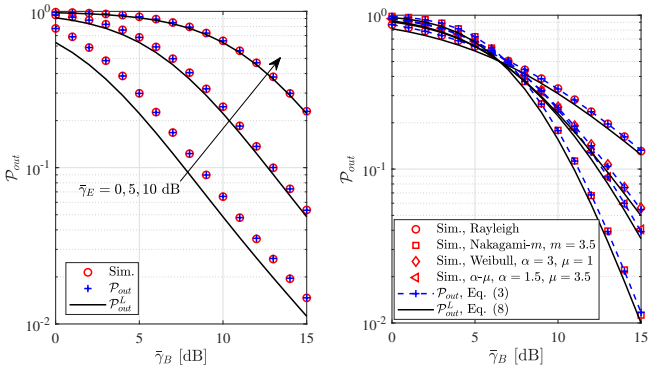
$$\mathcal{I}_1 = \sum_{l=1}^{C_B}\sum_{k=1}^{C_E} w_l w_k \int_0^\infty \frac{1}{\sqrt{2\pi}\eta_l} \exp\left(-\frac{(y-\mu_l)^2}{2\eta_l^2}\right) \times \log_2\left(1+\bar{\gamma}_B y^2\right) \Phi\left((\sqrt{\bar{\gamma}_B/\bar{\gamma}_E}y-\mu_k)/\eta_k\right) dy$$
$$\overset{(c)}{=} \sum_{l=1}^{C_B}\sum_{k=1}^{C_E} w_l w_k \left(\frac{2}{3}\mathcal{G}_B(\mu_l,\bar{\gamma}_B,\mu_k,\eta_k,\rho) + \frac{1}{6}\mathcal{G}_B(\mu_l+\sqrt{3}\eta_l,\bar{\gamma}_B,\mu_k,\eta_k,\rho) + \frac{1}{6}\mathcal{G}_B(\mu_l-\sqrt{3}\eta_l,\bar{\gamma}_B,\mu_k,\eta_k,\rho)\right), \quad (12)$$

step (c) is developed by using [9, Eq. (4)]. Similarly, $\mathcal{I}_2$ and $\mathcal{I}_3$ can be obtained. After some simple mathematical manipulations, the proof of $\bar{C}_s$ is finished. ■

IV. Numerical Results and Discussions

In this section, the accuracy of our derived analytical results is validated by performing the Monte-Carlo simulations over $\kappa-\mu$ fading channels. Assuming that the main channel and wiretap channel undergo the same fading conditions, herein $\kappa = 3$, $\mu = 1$, where the estimated parameters for the MoG distribution are adopted the ones from [16, Table. IV]. In order to encompass more fading models, we also plotted the SOP over Rayleigh, Nakagami-m, Weibull, and $\alpha-\mu$[2] fading channels in Fig. 1. (b). The SOP, PNZ, and ASC are respectively plotted and compared in Figs. 1-4 with Monte-Carlo simulations. Apparently, one can observe that there exist excellent agreements between our analytical and simulated results.

[2]The approximation parameters used to estimate $\alpha-\mu$ distribution in the manner of MoG distribution are obtained by using the method given in [18, Appendix B].



(a) $\kappa-\mu$ (b) $\alpha-\mu$

Fig. 1: $\mathcal{P}_{out}$ against $\bar{\gamma}_B$ when $R_t = 0.5$ over (a) $\kappa-\mu$ fading channels; and (b) Rayleigh, Nakagami-m, Weibull, and $\alpha-\mu$ fading channels [6] with $\bar{\gamma}_E = 5$dB.

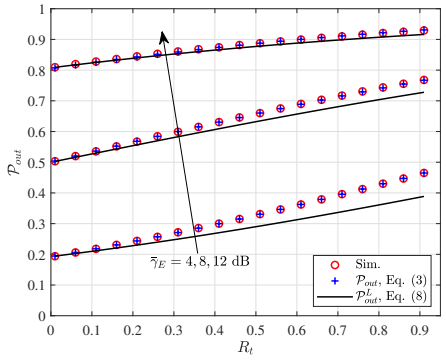


Fig. 2: $\mathcal{P}_{out}$ against R_t over $\kappa-\mu$ fading channels when $\bar{\gamma}_B = 8$ dB.

A. Numerical Results

Figs. 1 and 2 plot the SOP, $\mathcal{P}_{out}$, and the lower bound of SOP, $\mathcal{P}^L_{out}$. The increase of $\bar{\gamma}_E$ means an increasingly improving quality of the received SNR at Eve, it physically says secure communication gradually confronts high risks. Besides, the lower bound of SOP gradually shows a tight approximation to the exact SOP when (i) R_t goes to 0, i.e., observing from (4) and (6), as $R_t \to 0$, it means $\mathcal{W} \to 0$, resulting in diminishing the gap between $\mathcal{P}^L_{out}$ and $\mathcal{P}_{out}$. Practically speaking, Alice adopts no transmission rate; and (ii) $\bar{\gamma}_E$ locates at the high SNR regime, i.e., it can be physically interpreted that Eve is close to Alice.

Fig. 3 depicts the PNZ, as shown in (9a). In continuation

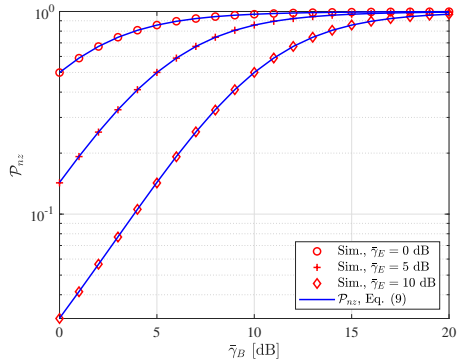


Fig. 3: $\mathcal{P}_{nz}$ versus $\bar{\gamma}_B$ over $\kappa - \mu$ fading channels.

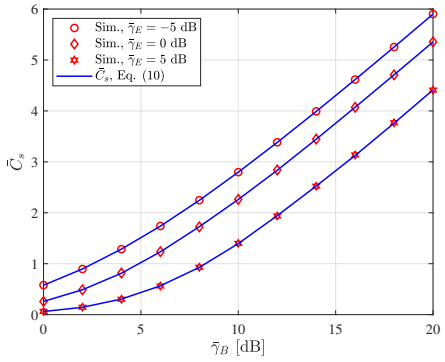


Fig. 4: $\bar{C}_s$ versus $\bar{\gamma}_B$ over $\kappa - \mu$ fading channels.

with $\mathcal{P}_{out}$, higher $\bar{\gamma}_E$ values leads to lower $\mathcal{P}_{nz}$ performance, it means Eve is largely capable of wiretapping the legitimate link. Fig. 4 shows that the analytical ASC, as in (10), demonstrates an increasing tendency with regard to ρ. Larger ρ illustrates bigger gap between $\bar{\gamma}_B$ and $\bar{\gamma}_E$, and thereafter resulting in higher $\bar{C}_s$.

Conclusively speaking, inspired by [8], [16], the MoG distribution is feasible and applicable in cellular device-to-device, vehicle-to-vehicle and on-body communications.

B. Accuracy Analysis

Observed from Figs. 1-4, our analytical results present an excellent match with Monte-Carlo simulations. For the purpose of illustrating the tightness of the analytical results, a useful measure, namely *analytical error*, is used as the accuracy indicator [9]

$$\text{analytical error} = 1 - \frac{\text{analytical results}}{\text{simulation results}} \times 100\%. \quad (13)$$

As shown in Table I, the analytical errors for the PNZ and ASC are considerable small, within $\pm 1\%$. The analytical error for the SOP gradually increases as ρ increases, but within $\pm 3\%$. Conclusively speaking, our derivations are highly accurate.

V. Conclusion

In this letter, the feasibility of the MoG distribution on the PLS analysis was explored. The secrecy metrics, including $\mathcal{P}_{out}$, $\mathcal{P}_{out}^{L}$, $\mathcal{P}_{NZ}$, and $\bar{C}_s$, are respectively derived with simple and closed-form expressions. The accuracy of our analytical results are further successfully validated by performing Monte-Carlo simulations. This letter offers a unified and effective framework when analyzing physical layer security over fading channels. The MoG approach is beneficial when the main channel and wiretap channel confront different type of fading conditions, e.g., mixture of composite and non-composite fading channels.

TABLE I: Analytical error against ρ (dB) when $\bar{\gamma}_E = 0$ dB

ρ	0	4	8	12	16
$\mathcal{P}_{out}$	0.03%	-0.25%	-0.14%	0.45%	-2.40%
$\mathcal{P}_{nz}$	0.09%	-0.09%	-0.03%	-0.03%	0.01%
$\bar{C}_s$	0.63%	-0.41%	0.27%	-0.21%	-0.008%

References

[1] 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.

[2] Y. Ai, L. Kong, and M. Cheffena, "Secrecy outage analysis of double shadowed rician channels," *Electron. Lett.*, vol. 55, no. 13, pp. 765–767, 2019.

[3] L. Kong and G. Kaddoum, "Secrecy characteristics with assistance of mixture gamma distribution," *IEEE Wireless Commun. Lett.*, vol. 8, no. 4, pp. 1086–1089, Aug. 2019.

[4] 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.

[5] 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.

[6] 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.

[7] 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.

[8] 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.

[9] 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.

[10] L. Kong and G. Kaddoum, "On physical layer security over the Fisher-Snedecor $\mathcal{F}$ wiretap fading channels," *IEEE Access*, vol. 6, no. 1, pp. 39 466–39 472, Dec. 2018.

[11] H. Lei, C. Gao, I. S. Ansari, Y. Guo, G. Pan, and K. A. Qaraqe, "On physical-layer security over SIMO generalized-K fading channels," *IEEE Trans. Veh. Technol.*, vol. 65, no. 9, pp. 7780–7785, Sep. 2016.

[12] L. Kong, G. Kaddoum, and H. Chergui, "On physical layer security over Fox's H-function wiretap fading channels," *IEEE Trans. Veh. Technol.*, vol. 68, no. 7, pp. 6608–6621, Jul. 2019.

[13] A. Mathur, Y. Ai, M. R. Bhatnagar, M. Cheffena, and T. Ohtsuki, "On physical layer security of α-η-κ-μ fading channels," *IEEE Commun. Lett.*, vol. 22, no. 10, pp. 2168–2171, Oct. 2018.

[14] J. Wang, C. Liu, J. Wang, J. Dai, M. Lin, and M. Chen, "Secrecy outage probability analysis over Malaga-Malaga fading channels," in *IEEE ICC*, May 2018, pp. 1–6.

[15] S. Atapattu, C. Tellambura, and H. Jiang, "A mixture gamma distribution to model the SNR of wireless channels," *IEEE Trans. Wireless Commun.*, vol. 10, no. 12, pp. 4193–4203, Dec. 2011.

[16] B. Selim, O. Alhussein, S. Muhaidat, G. K. Karagiannidis, and J. Liang, "Modeling and analysis of wireless channels via the mixture of gaussian distribution," *IEEE Trans. Veh. Technol.*, vol. 65, no. 10, pp. 8309–8321, Oct. 2016.

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

[18] O. Alhussein, "Performance analysis of wireless fading channels: A unified approach," Master's thesis, Dept. Applied Sciences, School of Engineering Science, Simon Fraser University, BC, Canada, 2015.