KICS The Korean Institute of Communications and Information Sciences

Available online at www.sciencedirect.com
ScienceDirect

ICT Express 9 (2023) 177–181

www.elsevier.com/locate/icte

Secrecy Performance of $\alpha - \kappa - \mu$ Shadowed Fading Channel

A.S.M. Badrudduza*, S.H. Islam, M.K. Kundu, I.S. Ansari

Department of ETE, Rajshahi University of Engineering & Technology, Rajshahi, Bangladesh
Department of EEE, Rajshahi University of Engineering & Technology, Rajshahi, Bangladesh
Department of ECE, Rajshahi University of Engineering & Technology, Rajshahi, Bangladesh
James Watt School of Engineering, University of Glasgow, Glasgow G12 8QQ, United Kingdom

Received 13 July 2021; received in revised form 3 September 2021; accepted 15 September 2021
Available online 1 October 2021

Abstract

In this paper, the physical layer security aspects of a wireless framework over $\alpha - \kappa - \mu$ shadowed (AKMS) fading channel are examined by acquiring closed-form novel expressions of average secrecy capacity, secure outage probability (SOP), and strictly positive secrecy capacity. The lower bound of SOP is derived along with the asymptotic expression of SOP at the high signal-to-noise ratio regime in order to achieve secrecy diversity gain. Capitalizing on these expressions, the consequences due to the simultaneous occurrence of fading and shadowing are quantified. Finally, Monte-Carlo simulations are demonstrated to assess the correctness of the expressions.

Keywords: Physical layer security; Secrecy capacity; Shadowing; Secure outage probability

1. Introduction

Multipath fading and shadowing are two common effects in practical wireless scenarios that are liable for the degradation of propagated wireless signals. In particular, shadowing characterizes long-term variation of the signals whereas multipath fading arises due to the interference between multiple delayed versions of the transmitted signal. It is noteworthy that in realistic wireless applications, both parameters affect the secrecy performance remarkably.

In recent times, the authors are showing their intense interest in the physical layer security (PLS) issue that utilizes the time-varying property of fading channels to enhance the information security [1–6] rather than utilizing the classical cryptography approaches. Secrecy performance over Generalized-K (GK) fading channel was analyzed in [1] in terms of average secrecy capacity (ASC), secure outage probability (SOP), and strictly positive secrecy capacity (SPSC). In [2], authors exhibited superiority of $\alpha - \mu$ fading channel by stating that the secrecy performance over GK fading channel can be easily approximated via $\alpha - \mu$ fading channel. As generalized channels exhibit precedence over multipath fading channels, security over $\kappa - \mu$ and $\kappa - \mu$ shadowed fading channel was analyzed in [3,4] showing some classical models as special cases. The natural generalization of $\alpha - \mu$ and $\kappa - \mu$ fading channels was performed in [5] by modeling a secure scenario over $\alpha - \kappa - \mu$ and $\alpha - \eta - \mu$ fading channels which are further generalized by $\alpha - \eta - \kappa - \mu$ fading channel in [6]. The authors examined the secrecy characteristics and showed that for high average signal-to-noise ratio (SNR) of main and eavesdropper channels, an ASC ceiling is attained.

The aforecited works in [1–3,5,6] exhibit the impact of fading during the analysis of PLS. The impact of shadowing in PLS was presented only in [4]. But practical scenarios experience fading and shadowing simultaneously, hence the research gaps in these existing works are addressed in this paper via tackling the impact of both (fading and shadowing) on secrecy performance over $\alpha - \kappa - \mu$ shadowed (AKMS) fading model. In brief, the contributions are:

- The existing models in [1–5] can be obtained as a special case of the proposed model in this work. Moreover, this model unifies the performance evaluation of all classical multipath models such as Nakagami-m, Rician, Nakagami-q, Weibull, etc. [7, Table I].

* Corresponding author at: Department of ETE, Rajshahi University of Engineering & Technology, Rajshahi, Bangladesh.
E-mail addresses: asmb.kanon@gmail.com (A.S.M. Badrudduza), 1501060@student.ruet.ac.bd (S.H. Islam), milton.kundu@ece.ruet.ac.bd (M.K. Kundu), imran.ansari@glasgow.ac.uk (I.S. Ansari).

Peer review under responsibility of The Korean Institute of Communications and Information Sciences (KICS).

https://doi.org/10.1016/j.icte.2021.09.009

- Secrecy performance evaluation is accomplished by deducing analytical expressions for SPSC, SOP, and ASC in closed-form. Additionally, asymptotic outage characteristics at high SNR regime are also demonstrated. The correctness of the deduced expressions is analyzed via Monte-Carlo simulations.

The rest of this paper is structured as follows: System model is illustrated in Section 2 whereas the channel modeling is performed in Section 3. The formulation of the performance metrics is introduced in Section 4. Numerical results are demonstrated in Section 5 and finally, the conclusions are discussed in Section 6.

2. System model

In the proposed model, a source, $\mathcal{T}$, transmits sensitive messages to an authorized receiver, $\mathcal{H}$, via main ($\mathcal{T}-\mathcal{H}$) link. A passive eavesdropper, $\mathcal{K}$, also exists in that network that is trying to overhear the secret transmission between $\mathcal{T}$ and $\mathcal{H}$ via the eavesdropper ($\mathcal{T}-\mathcal{K}$) link. All nodes are assumed to have a single antenna. Assuming $\mathcal{T}-\mathcal{H}$ and $\mathcal{T}-\mathcal{K}$ links experience severe fading and shadowing concurrently, those are modeled as independently and identically distributed AKMS fading channels. The channel gain between $\mathcal{T}$ and $\mathcal{H}$ is denoted as $f_{th} \in \mathbb{C}^{1\times1}$. Similarly, the channel coefficient for $\mathcal{T}-\mathcal{K}$ link is denoted as $l_{tk} \in \mathbb{C}^{1\times1}$. Considering P_t, P_h, and P_k represent transmit power from $\mathcal{T}$, noise power at $\mathcal{H}$, and noise power at $\mathcal{K}$, respectively, the instantaneous SNRs of $\mathcal{T}-\mathcal{H}$ and $\mathcal{T}-\mathcal{K}$ links are given by $\gamma_h = \frac{P_t}{P_h}\|f_{th}\|^2$ and $\gamma_k = \frac{P_t}{P_k}\|l_{tk}\|^2$, respectively. The information in $\mathcal{T}-\mathcal{H}$ link is secure if $\mathcal{T}$ transmits messages at secrecy rate i.e. a rate at which eavesdroppers are incapable of wiretapping [8]. All the system parameters are summarized in Table 1.

Table 1
Notations and their descriptions.

Notations	Descriptions
α_i, κ_i, μ_i, m_i	Non-negative real shape parameters
${}_1F_1(.)$	Confluent hypergeometric function
${}_2F_1(.)$	Gauss hypergeometric function
$\Gamma(.)$	Gamma operator
$\gamma(.,.)$	Lower incomplete gamma function
$\mathcal{R}_t$	Target secrecy rate

3. Channel model

The PDF of instantaneous SNR is given by [7, Eq. (2)]

$$f_i(\gamma) = a_i \gamma^{\tilde{\alpha}_i\mu_i-1} e^{-b_i\gamma^{\tilde{\alpha}_i}} {}_1F_1(m_i, \mu_i; d_i\gamma^{\tilde{\alpha}_i}), \tag{1}$$

where $i \in (h,k)$, $\tilde{\alpha}_i = \frac{\alpha_i}{2}$, $a_i = \frac{{m_i}^{m_i}\alpha_i}{2c_i{}^{\mu_i}\Gamma(\mu_i)(\mu_i\kappa_i+m_i)^{m_i}\overline{\gamma}_i^{\tilde{\alpha}_i\mu_i}}$, $b_i = \frac{1}{c_i\overline{\gamma}_i^{\tilde{\alpha}_i}}$, $d_i = \frac{\mu_i\kappa_i}{c_i(\mu_i\kappa_i+m_i)\overline{\gamma}_i^{\tilde{\alpha}_i}}$, $\overline{\gamma}_i$ represents the average SNR of the channels, and $c_i = \left(\frac{(\mu_i\kappa_i+m_i)^{m_i}\Gamma(\mu_i)}{m_i^{m_i}\Gamma(\mu_i+\tilde{\alpha}_i^{-1}){}_2F_1(m_i,\mu_i+\tilde{\alpha}_i^{-1};\mu_i;\frac{\mu_i\kappa_i}{\mu_i\kappa_i+m_i})}\right)^{\tilde{\alpha}_i}$. Utilizing [9, Eq. (9.14.1)], (1) is simplified as

$$f_i(\gamma) = a_i \sum_{j_i=0}^{\infty} \frac{\mathcal{A}_i d_i^{j_i}}{j_i!} \gamma^{\tilde{\alpha}_i(\mu_i+j_i)-1} e^{-b_i\gamma^{\tilde{\alpha}_i}}, \tag{2}$$

where $\mathcal{A}_i = \frac{\Gamma(\mu_i)\Gamma(m_i+j_i)}{\Gamma(m_i)\Gamma(\mu_i+j_i)}$. Integrating (2) with respect to γ by making use of [9, Eqs. (3.381.8) and (8.352.6)], lower incomplete gamma function can be modified and the CDF of γ can be derived as

$$F_i(\gamma) = 1 - \frac{a_i}{\tilde{\alpha}_i} \sum_{j_i=0}^{\infty} \mathcal{B}_i e^{-b_i\gamma^{\tilde{\alpha}_i}} \sum_{l_i=0}^{\mu_i+j_i-1} \frac{{b_i}^{l_i}\gamma^{\tilde{\alpha}_i l_i}}{l_i!}, \tag{3}$$

where $\mathcal{B}_i = \frac{\mathcal{A}_i {d_i}^{j_i}(\mu_i+j_i-1)!}{{b_i}^{\mu_i+j_i}\, j_i!}$.

4. Performance metrics

4.1. Average Secrecy Capacity (ASC) performance

ASC can be expressed as [1],

$$\overline{C_s} = \Im_1 + \Im_2 - \Im_3, \tag{4}$$

where the expressions of $\Im_1$, $\Im_2$, and $\Im_3$ are derived in the Appendix.

4.2. Secrecy Outage Probability (SOP) performance

The SOP refers to the probability that $\mathcal{S}_c$ falls below $\mathcal{R}_t$ [10]. Mathematically, the lower bound of SOP is given by

$$SOP_L = \int_0^{\infty} F_h(\varphi\gamma_k) f_k(\gamma_k) d\gamma_k. \tag{5}$$

4.2.1. Exact analysis

By substituting (1) and (3) into (5), the exact expression of lower bound of the SOP is derived as

$$SOP_{L,e} = 1 - \frac{a_h a_k}{\tilde{\alpha}^2} \sum_{j_h=0}^{\infty} \sum_{l_h=0}^{\mu_h+j_h-1} \frac{\mathcal{B}_h \varphi^{\tilde{\alpha} l_h}}{b_h^{-l_h} l_h!} \times \sum_{j_k=0}^{\infty} \frac{\mathcal{A}_k d_k^{j_k}(\mu_k+j_k+l_h-1)!}{j_k!(b_k+b_h\varphi^{\tilde{\alpha}})^{\mu_k+j_k+l_h}}. \tag{6}$$

4.2.2. Asymptotic analysis

In order to achieve more insights of various system parameters on the system's outage behavior, SOP analysis at high SNR regime are shown. The asymptotic expression for lower bound of the SOP is obtained as

$$SOP_{L,a} = \frac{a'_h a'_k}{\tilde{\alpha}^2\mu_h} \varphi^{\alpha\mu_h} \sum_{j_k=0}^{\infty} \frac{\mathcal{A}_k (d'_k)^{j_k}}{j_k!} \left(\frac{\overline{\gamma}_k}{\overline{\gamma}_h}\right)^{\alpha\mu_h} \times \frac{(\mu_h+\mu_k+j_k-1)!}{(b'_k)^{\mu_h+\mu_k+j_k}}. \tag{7}$$

The proof is shown in Appendix B. From (7), it is observed that diversity gain of the system is $\mathcal{G} = \tilde{\alpha}\mu_h$. In asymptotic analysis, $\overline{\gamma}_k \to \infty$ case has been ignored as it indicates a successful wiretapping probability. Hence, the diversity gain is zero for that particular case.

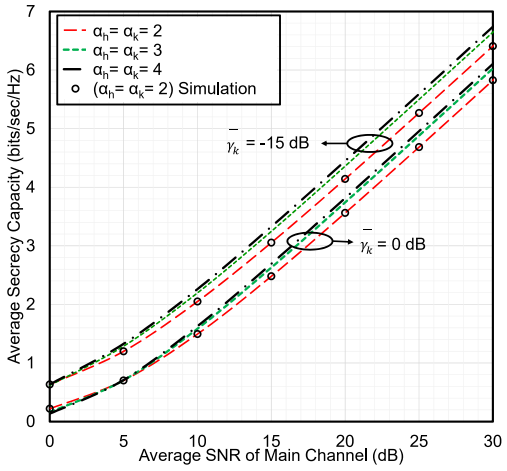

Fig. 1. The ASC versus $\overline{\gamma}_h$ for selected values of α where $m_h = m_k = 100$, $\kappa_h = \kappa_k = 1$, and $\mu_h = \mu_k = 1$.

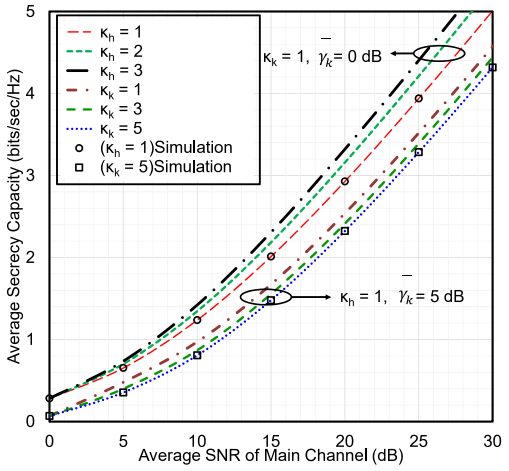

Fig. 2. The ASC versus $\overline{\gamma}_h$ for selected values of κ_h and κ_k where $m_h = m_k = 100$, $\alpha_h = \alpha_k = 1$ and $\mu_h = \mu_k = 1$.

4.3. Strictly Positive Secrecy Capacity (SPSC) performance

The SPSC, which points to the probability of existence of a non-negative secrecy capacity, is a fundamental benchmark in secure communications, mathematically can be expressed as [1]

$$SPSC = \Pr\{\mathcal{S}_c > 0\} = 1 - SOP_L|_{\mathcal{R}_t=0}. \quad (8)$$

Substituting $\mathcal{R}_t = 0$ into (6), we can obtain the expression of SPSC.

4.4. Novelty of this work

The AKMS model can be used to represent various other classical channels depending on the values of the shape parameters [7, Table I]. Assuming $\alpha_i = \alpha$, $\kappa_i = 0$, and $\mu_i = \mu$, the ASC results utilizing (4) perfectly matches with the results of [2]. For $\alpha_i = 2$, $\kappa_i = \kappa$, $\mu_i = \mu$, and $m_i \to \infty$, the SOP and SPSC results obtained via (6) and (8) completely agree with the corresponding results in [3]. Likewise, the results presented in (6) can be shown to match with [4, Eq. (6)] for $\alpha_i = 2$, $\kappa_i = \kappa$, $\mu_i = \mu$, and $m_i = m$. Furthermore, setting $\alpha_i = \alpha$, $\mu_i = 2\mu$, $m_i = \mu$, $\alpha_i = \alpha$, $\kappa_i = \kappa$, $\mu_i = \mu$, and $m_i \to \infty$, (6) can be reduced to [5, Eq. (9)] and [5, Eq. (11)], respectively.

5. Numerical results

In this section, the numerical outcomes utilizing the performance metrics of (4), (6), (7), and (8) are represented and further authenticated via Monte-Carlo simulations by generating an AKMS random variable in MATLAB and averaging 10^6 channel realizations for obtaining each value of $\mathcal{S}_c$. As the infinite series converges quickly after few terms, all of them are truncated after the first twenty terms with an accuracy factor of 10^{-4}.

The effects of α_i and κ_i on the ASC are depicted in Figs. 1 and 2 by plotting ASC against $\overline{\gamma}_h$. It is noted that an increase in α and κ_h cause a remarkable improvement

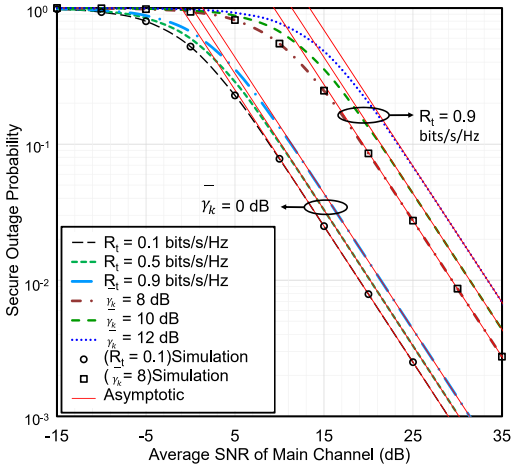

Fig. 3. The SOP versus $\overline{\gamma}_h$ for selected values of R_s and $\overline{\gamma}_k$ where $\alpha = 2$, $m_h = m_k = 15$, $\kappa_h = \kappa_k = 1$, and $\mu_h = \mu_k = 1$.

of ASC whereas the ASC performance is degraded with κ_k. The reason for this result is that the increase of α and κ_h improves the $\mathcal{T}-\mathcal{H}$ link but with the increase of κ_k the $\mathcal{T}-\mathcal{K}$ link is improved. A comparison between the numerical and simulation results discloses that the simulation results are as good as the numerical results that point to the authorizations of the deduced mathematical expressions.

The SOP is depicted against $\overline{\gamma}_h$ in Figs. 3 and 4 to observe how $\overline{\gamma}_k$, $\mathcal{R}_t$ and m_i influence the secure outage characteristics. It is observed from Fig. 3 that the SOP gradually increases with both $\overline{\gamma}_k$ and $\mathcal{R}_t$. This is because an increase in $\mathcal{R}_t$ increases the probability of dropping $\mathcal{S}_c$ below $\mathcal{R}_t$. On the other hand, an increased $\overline{\gamma}_k$ indicates an enhanced capability of successful wiretapping by the eavesdroppers. In Fig. 4, two cases are considered to demonstrate the effects of shadowing parameters over $\mathcal{T}-\mathcal{H}$ and $\mathcal{T}-\mathcal{K}$ links separately. It is noted that an increase in m_h enhances the outage performance. On the contrary, the outage performance is degraded with m_k. Actually, these results reveal that the overall shadowing of the $\mathcal{T}-\mathcal{H}$ and $\mathcal{T}-\mathcal{K}$ links decreases as the corresponding

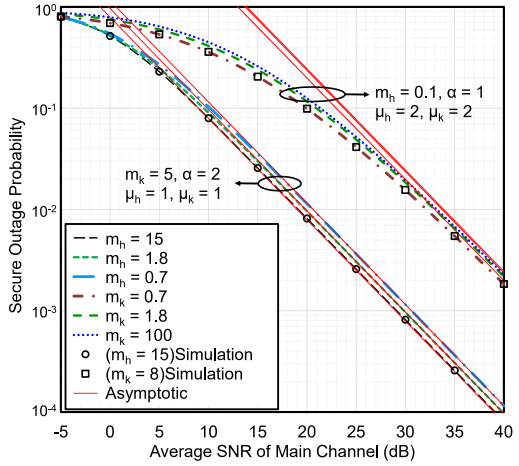

Fig. 4. The SOP versus $\overline{\gamma}_h$ for selected values of m_h and m_k where $\kappa_h = \kappa_k = 1$, $\mathcal{R}_t = 0.5$ bits/s/Hz and $\overline{\gamma}_k = 0$ dB.

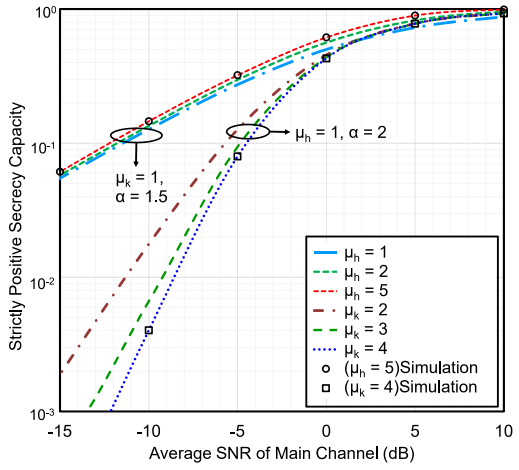

Fig. 5. The SPSC versus $\overline{\gamma}_h$ for selected values of μ_h and μ_k where $m_h = m_k = 15$, $\kappa_h = \kappa_k = 1$ and $\overline{\gamma}_k = 0$ dB.

shadowing parameters increase from 0 to ∞. Moreover, it is noted that at a high SNR regime, the asymptotic curves exactly approach the exact SOP curves.

In Fig. 5, the impacts of μ_h and μ_k are demonstrated in terms of SPSC. As an increase in μ_h and μ_k reduces the fading of the corresponding channels, it is clearly observed from the figure that the SPSC improves significantly with μ_h and deteriorates with μ_k.

6. Conclusion

This paper focuses on the assessment of the secrecy performance of a wireless network over AKMS fading channel wherein a single eavesdropper is trying to overhear and decode the transmitted secret messages. This investigation includes examining the impacts of all system parameters on the secrecy performance via deriving expressions of three secrecy parameters i.e. SPSC, ASC, and SOP. Utilizing these closed-form expressions some numerical outcomes were presented and further authenticated via Monte-Carlo simulations to demonstrate that analytical and simulation results are in close agreement with each other. Additionally, to evaluate diversity gain, asymptotic SOP analyses were derived. It is observed that diversity gain is dependent on $\tilde{\alpha}$ and μ_h, but completely independent of the shadowing parameters of $\mathcal{T}-\mathcal{H}$ and $\mathcal{T}-\mathcal{K}$ links. Finally, it can be concluded that the secrecy performance is significantly affected by the fading and shadowing parameters, particularly of the main link rather than the eavesdropper link.

CRediT authorship contribution statement

A.S.M. Badrudduza: Study conception and design, Writing – original draft. **S.H. Islam:** Data collection, Analysis and interpretation of results, Writing – original draft. **M.K. Kundu:** Data collection, Analysis and interpretation of results. **I.S. Ansari:** Study conception and design.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgment

All authors reviewed the results and approved the final version of the manuscript.

Appendix. Proof of ASC

The identity in [11, Eq. 11] is utilized for representing the exponential and logarithmic components in terms of Meijer's G function. Utilizing [11, Eq. 21], the term $\Im_1$ is expressed as

$$\Im_1 = \int_0^{\infty} ln(1+\gamma_h) f_h(\gamma_h) F_k(\gamma_h) d\gamma_h = \sum_{j_h=0}^{\infty} \frac{\sqrt{2} a_h \mathcal{A}_h d_h^{j_h}}{\alpha (2\pi)^{\alpha-.5} j_h!} \left(I_1 - \sum_{j_k=0}^{\infty} \sum_{l_k=0}^{\mu_k+j_k-1} \frac{\mathcal{B}_k b_k^{l_k}}{a_k^{-1} \tilde{\alpha} l_k!} I_2 \right), \quad \text{(A.1)}$$

where $I_1 = G_{2\alpha,2+2\alpha}^{2+2\alpha,\alpha}\left[\frac{b_h^2}{4} \middle| \begin{matrix} x_1, x_2 \\ x_5, x_1, x_1 \end{matrix}\right]$, $I_2 = G_{2\alpha,2+2\alpha}^{2+2\alpha,\alpha}\left[\frac{(b_h+b_k)^2}{4} \middle| \begin{matrix} x_3, x_4 \\ x_5, x_3, x_3 \end{matrix}\right]$, $x_1 = \Delta(\alpha, -\tilde{\alpha}(\mu_h + j_h))$, $x_2 = \Delta(\alpha, 1-\tilde{\alpha}(\mu_h + j_h))$, $x_3 = \Delta(\alpha, -\tilde{\alpha}(\mu_h + j_h + l_k))$, $x_4 = \Delta(\alpha, 1-\tilde{\alpha}(\mu_h + j_h + l_k))$, $x_5 = \Delta(2, 0)$, $\Delta(x, a) = \frac{a}{x}, \frac{a+1}{x}, ..., \frac{a+x-1}{x}$, and $G_{p,q}^{m,n}\left[x \middle| \begin{matrix} \alpha_1, ..., \alpha_p \\ \beta_1, ..., \beta_q \end{matrix}\right]$ signifies the Meijer's G function. Here, an assumption of $\tilde{\alpha}_h = \tilde{\alpha}_k = \tilde{\alpha}$ is taken into consideration during the ASC analysis for the ease of mathematical calculations. Similarly, $\Im_2$ is expressed as

$$\Im_2 = \int_0^{\infty} ln(1+\gamma_k) f_k(\gamma_k) F_h(\gamma_k) d\gamma_k = \sum_{j_k=0}^{\infty} \frac{\sqrt{2} a_k \mathcal{A}_k d_k^{j_k}}{\alpha (2\pi)^{\alpha-.5} j_k!} \left(I_3 - \sum_{j_h=0}^{\infty} \sum_{l_h=0}^{\mu_h+j_h-1} \frac{\mathcal{B}_h b_h^{l_h}}{a_h^{-1} \tilde{\alpha} l_h!} I_4 \right), \quad \text{(A.2)}$$

where $I_3 = G_{2\alpha,2+2\alpha}^{2+2\alpha,\alpha}\left[\frac{b_k^2}{4} \middle| \begin{matrix} z_1, z_2 \\ x_5, z_1, z_1 \end{matrix}\right]$, $I_4 = G_{2\alpha,2+2\alpha}^{2+2\alpha,\alpha}\left[\frac{(b_h+b_k)^2}{4} \middle| \begin{matrix} z_3, z_4 \\ x_5, z_3, z_3 \end{matrix}\right]$, $z_1 = \Delta(\alpha, -\tilde{\alpha}(\mu_k + j_k))$, $z_2 = \Delta(\alpha, 1-$

$\tilde{\alpha}(\mu_k + j_k))$, $z_3 = \triangle(\alpha, -\tilde{\alpha}(\mu_k + j_k + l_h))$, and $z_4 = \triangle(\alpha, 1 - \tilde{\alpha}(\mu_k + j_k + l_h))$. Again, $\Im_3$ is expressed in a similar way as

$$\Im_3 = \int_0^\infty ln(1+\gamma_k) f_k(\gamma_k) d\gamma_k$$
$$= \sum_{j_k=0}^{\infty} \frac{\sqrt{2} a_k \mathcal{A}_k d_k^{j_k}}{\alpha (2\pi)^{\alpha-.5} j_k!} G_{2\alpha,2+2\alpha}^{2+2\alpha,\alpha} \left[\frac{b_k^2}{4} \middle| \begin{matrix} z_1, z_2 \\ x_5, z_1, z_1 \end{matrix} \right]. \quad \text{(A.3)}$$

Appendix B. Proof of asymptotic SOP

We assume $\overline{\gamma}_h \to \infty$ with fixed $\overline{\gamma}_k$ for which the dominating term in (3) corresponds to $j = 0$. Utilizing the approximation, $\Upsilon(s, x) \approx x^s/s$ as $x \to 0$, (3) can be expressed as

$$F_i(\gamma) = \frac{a_i}{\tilde{\alpha}_i \mu_i} \gamma^{\tilde{\alpha}_i \mu_i}. \quad \text{(B.1)}$$

By substituting (1) and (B.1) into (5), the asymptotic expression for lower bound of the SOP is obtained as shown in (7) where $a'_k = \frac{{m_k}^{m_k} \alpha_k}{2{c_k}^{\mu_k} \Gamma(\mu_k)(\mu_k \kappa_k + m_k)^{m_k}}$, $b'_k = \frac{1}{c_k}$, $d'_k = \frac{\mu_k \kappa_k}{c_k(\mu_k \kappa_k + m_k)}$, $a'_h = \frac{{m_h}^{m_h} \alpha_h}{2{c_h}^{\mu_h} \Gamma(\mu_h)(\mu_h \kappa_h + m_h)^{m_h}}$.

References

[1] H. Lei, H. Zhang, I.S. Ansari, C. Gao, Y. Guo, G. Pan, K.A. Qaraqe, Performance analysis of physical layer security over GENERALIZED-K fading channels using a mixture Gamma distribution, IEEE Commun. Lett. 20 (2) (2015) 408–411.

[2] H. Lei, I.S. Ansari, G. Pan, B. Alomair, M.-S. Alouini, Secrecy capacity analysis over $\alpha - \mu$ fading channels, IEEE Commun. Lett. 21 (6) (2017) 1445–1448.

[3] N. Bhargav, S.L. Cotton, D.E. Simmons, Secrecy capacity analysis over $\kappa - \mu$ fading channels: Theory and applications, IEEE Trans. Commun. 64 (7) (2016) 3011–3024.

[4] M. Srinivasan, S. Kalyani, Secrecy capacity of $\kappa - \mu$ shadowed fading channels, IEEE Commun. Lett. 22 (8) (2018) 1728–1731.

[5] J.M. Moualeu, D.B. da Costa, W. Hamouda, U.S. Dias, R.A.A. de Souza, Physical layer security over α-κ-μ and α-η-μ fading channels, IEEE Trans. Veh. Technol. 68 (1) (2019).

[6] S. Jia, J. Zhang, H. Zhao, Y. Xu, Performance analysis of physical layer security over α - η - κ - μ fading channels, China Commun. 15 (11) (2018) 138–148.

[7] N.A. Sarker, A.S.M. Badrudduza, S.M.R. Islam, S.H. Islam, M.K. Kundu, I.S. Ansari, K.-s. Kwak, On the intercept probability and secure outage analysis of mixed $(\alpha - \kappa - \mu)$-shadowed and Málaga turbulent models, IEEE Access 9 (2021) 133849–133860.

[8] A.D. Wyner, The wire-tap channel, Bell Syst. Tech. J. 54 (8) (1975) 1355–1387.

[9] I.S. Gradshteyn, I.M. Ryzhik, Table of Integrals, Series, and Products, Academic Press, 2014.

[10] A.S.M. Badrudduza, M.Z.I. Sarkar, M.K. Kundu, Enhancing security in multicasting through correlated Nakagami-m fading channels with opportunistic relaying, Phys. Commun. 43 (2020) 101177.

[11] V.S. Adamchik, O.I. Marichev, The algorithm for calculating integrals of hypergeometric type functions and its realization in REDUCE system, in: Proceedings of the International Symposium on Symbolic and Algebraic Computation, 1990, pp. 212–224.