Performance Analysis of Physical Layer Security Over Generalized-K Fading Channels Using a Mixture Gamma Distribution

Hongjiang Lei, Huan Zhang, Imran Shafique Ansari, *Member, IEEE*, Chao Gao, Yongcai Guo, Gaofeng Pan, *Member, IEEE*, and Khalid A. Qaraqe, *Senior Member, IEEE*

***Abstract*—In this letter, the secrecy performance of the classic Wyner's wiretap model over generalized-K fading channels is studied. The closed-form expressions for the average secrecy capacity, secure outage probability, and the probability of strictly positive secrecy capacity are derived. The new expressions provide a unified form, which can handle several of the well-known composite fading environments as special or limiting cases. Monte-Carlo simulations are performed to verify the proposed analysis models.**

***Index Terms*—Physical layer security, generalized-K fading, average secrecy capacity, probability of strictly positive secrecy capacity, secure outage probability.**

I. Introduction

PHYSICAL layer security has recently attracted considerable attention since these approaches can prevent eavesdropping without the data encryption in upper layer. There is an ever increasing interest of exploring the physical layer secrecy performance in digital communications over fading channels. Pan *et. al.* investigated the security performance over non-small scale fading channels in [1]. The security performance over generalized Gamma channels was studied in [2].

Manuscript received September 14, 2015; accepted November 27, 2015. Date of publication December 1, 2015; date of current version February 12, 2016. This work was supported in part by the National Natural Science Foundation of China (NSFC) under Grant 61471076 and Grant 61401372, in part by the Program for Changjiang Scholars and Innovative Research Team in University under Grant IRT1299, in part by the Natural Science Foundation Project of CQ CSTC under Grant cstc2012jjA40040 and Grant cstc2013jcyjA40040, in part by the special fund of Chongqing Key Laboratory (CSTC) and Research Fund for the Doctoral Program of Higher Education of China under Grant 20130182120017, in part by the Fundamental Research Funds for the Central Universities under Grant XDJK2015B023, and parts of this publication were made possible by PDRA (PostDoctoral Research Award) under Grant PDRA1-1227-13029 from the Qatar National Research Fund (QNRF) (a member of Qatar Foundation (QF)). The associate editor coordinating the review of this paper and approving it for publication was Y. Zou. *(Corresponding author: Chao Gao.)*

H. Lei and H. Zhang are with Chongqing Key Laboratory of Mobile Communications Technology, Chongqing University of Posts and Telecommunications, Chongqing 400065, China, and also with the Key Laboratory of Optoelectronics Technology and System, Ministry of Education, Chongqing University, Chongqing 400044, China (e-mail: leihj@cqupt.edu.cn).

I. S. Ansari and K. A. Qaraqe are with the Department of Electrical and Computer Engineering (ECEN), Texas A&M University at Qatar (TAMUQ), Doha, Qatar (e-mail: imran.ansari@qatar.tamu.edu; khalid.qaraqe@qatar.tamu.edu).

C. Gao and Y. Guo are with the Key Laboratory of Optoelectronic Technology and Systems of the Education Ministry of China, Chongqing University, Chongqing 400044, China (e-mail: chaogaocqu@126.com; ycguo@cqu.edu.cn).

G. Pan is with the School of Electronic and Information Engineering, Southwest University, Chongqing, 400715, China (e-mail: gfpan@swu.edu.cn).

Digital Object Identifier 10.1109/LCOMM.2015.2504580

Zou *et. al.* proposed several diversity techniques for improving wireless security against eavesdropping attacks in [3]. Several optimal relay selection schemes were proposed to improve the physical-layer security in wireless cooperative networks and cognitive radio networks in [4] and [5], respectively.

Generalized-K (GK) distribution [6] is one of the relatively new tractable models used to describe the statistical behavior of path loss, shadowing, and small-scale fading effects as compared to the other composite channel models [7]. It is quite a general model since K-distribution [8] is included as its special case and it accurately approximates many other fading models, such as Rayleigh-Lognormal and Nakagami-Lognormal distribution [9]. In recent years, the system performance over GK fading channels has been analyzed extensively, such as outage probability (OP) [7], ergodic capacity (EC) [10], and average bit error probability (ABEP) or average symbol error rate (ASER) [11]. The existing works on GK fading channels are limited to analyzing common end-to-end communication performance.

So far, there have been very few works related to the physical layer security over GK fading channels, especially on the classic Wyner's model [12]. In this letter, the security performance over GK channels was analyzed and the closed-form expressions are derived for the average secrecy capacity (ASC), secure outage probability (SOP), and the strictly positive secrecy capacity (SPSC) for the classic Wyner's wiretap model over GK fading channels. The new expressions provide a unified form, which can handle several of the well-known composite fading environments as special or limiting cases.

II. System Model

In this letter, the classic Wyner's wiretap model [12] is considered, where the source S sends confidential messages to the legitimate destination D over the main channel while the eavesdropper E attempts to decode these messages from its received signal through the eavesdropper channel. It is assumed that the main and eavesdropper channels experience independent GK fading.

The probability density function (PDF) of the signal-to-noise ratio (SNR) over GK channel is expressed as [13]

$$f_i(\gamma) = \frac{2\Xi_i^{\frac{k_i+m_i}{2}}\gamma^{\frac{k_i+m_i-2}{2}}}{\Gamma(m_i)\Gamma(k_i)} K_{k_i-m_i}\left(2(\Xi_i\gamma)^{\frac{1}{2}}\right), i \in \{D, E\}, \tag{1}$$

where m_i ($i \in \{D, E\}$) and k_i ($i \in \{D, E\}$) are the fading parameters of the main and eavesdropper channels, respectively, $K_v(\cdot)$ is the modified Bessel function of order v, as defined in Eq. (8.407.1) of [14], $\Xi_i = \frac{k_i m_i}{\bar{\gamma}_i}$ ($i \in \{D, E\}$), $\bar{\gamma}_i$ ($i \in \{D, E\}$) is the average SNR of the main and eavesdropper channels, respectively.

The modified Bessel function in Eq. (1) makes it complex to further analyze the performance, especially performance analysis pertaining to security issues. In order to reduce the complexity, the Mixture Gamma (MG) distribution was proposed to model the SNR over GK channels in [15]. As mentioned [15], the MG distribution has attractive properties such that an accurate approximation is possible for a variety of composite fadings by utilizing mathematically tractable expressions.

The PDF of γ_i ($i \in \{D, E\}$) in the form of the MG distribution is expressed by [15]

$$f_i(\gamma) = \sum_{j=1}^{L} \alpha_{i,j} \gamma^{m_i - 1} e^{-\varsigma_{i,j}\gamma}, i \in \{D, E\}, \tag{2}$$

where $\alpha_{i,j} = \frac{\theta_{i,j}}{\sum_{v=1}^{L} (\theta_{i,v} \Gamma(m_i) \varsigma_{i,v}{}^{-m_i})}$ ($i \in \{D, E\}$), $\varsigma_{i,j} = \frac{\Xi_i}{t_j}$ ($i \in \{D, E\}$), $\theta_{i,j} = \frac{\Xi_i{}^{m_i} \omega_j t_j{}^{k_i - m_i - 1}}{\Gamma(m_i)\Gamma(k_i)}$ ($i \in \{D, E\}$), ω_j ($i \in \{D, E\}$) and t_j ($i \in \{D, E\}$) are the weight factor and the abscissas for the Gaussian-Laguerre integration [16], L is the number of terms, $\Gamma(z) = \int_0^\infty t^{z-1} e^{-t} dt$ is the well-known Gamma function, as defined in Eq. (8.310.1) of [14].

Making use of Eq. (2), the cumulative distribution function (CDF) of γ_i ($i \in \{D, E\}$) is obtained as

$$F_i(\gamma) = \sum_{j=1}^{L} \alpha_{i,j} \varsigma_{i,j}{}^{-m_i} \Upsilon\left(m_i, \varsigma_{i,j}\gamma\right), i \in \{D, E\}, \tag{3}$$

where $\Upsilon(\alpha, x) = \int_0^x e^{-t} t^{\alpha - 1} dt$ is the lower incomplete Gamma function, as defined by Eq. (8.350.1) of [14]. It is assumed that m_i ($i \in \{D, E\}$) are integers. Making use of Eq. (8.352.6) of [14], Eq. (3) can be expressed as

$$F_i(\gamma) = A_i - (m_i - 1)! \sum_{j=1}^{L} \sum_{p=0}^{m_i - 1} \left(\frac{\alpha_{i,j} \varsigma_{i,j}{}^{-m_i + p} \gamma^p}{p! e^{\varsigma_{i,j}\gamma}}\right), \quad i \in \{D, E\}, \tag{4}$$

where $A_i = (m_i - 1)! \sum_{j=1}^{L} \alpha_{i,j} \varsigma_{i,j}{}^{-m_i}$ ($i \in \{D, E\}$).

III. ASC Analysis

In this section, we assume that the full channel state information (CSI) of both the main and eavesdropper channels is available at S, which is called active eavesdropping [17]. In such a scenario, S can adapt the achievable secrecy rate R_s such that $R_s \le C_s$ [17]. In this section, the maximum achievable secrecy rate $R_s = C_s$ is focused on, which is characterized as [18]

$$C_s = [\ln(1 + \gamma_D) - \ln(1 + \gamma_E)]^+, \tag{5}$$

where $\ln(1 + \gamma_D)$ and $\ln(1 + \gamma_E)$ are the capacity of the main and eavesdropper channels, respectively. $[x]^+ = \max\{x, 0\}$. Since both the main and eavesdropper channels experience independent fading, thus ASC can be given by

$$\begin{aligned} \bar{C}_s &= E\left[C_s(\gamma_D, \gamma_E)\right] \\ &= \int_0^\infty \int_0^\infty C_s(\gamma_D, \gamma_E) f(\gamma_D, \gamma_E) d\gamma_D d\gamma_E \\ &= I_1 + I_2 - I_3, \end{aligned} \tag{6}$$

where $f(\gamma_D, \gamma_E) = f_D(\gamma_D) f_E(\gamma_E)$ is the joint pdf of γ_D and γ_E, and

$$I_1 = \int_0^\infty \ln(1 + \gamma_D) f_D(\gamma_D) F_E(\gamma_D) d\gamma_D, \tag{7}$$

$$I_2 = \int_0^\infty \ln(1 + \gamma_E) f_E(\gamma_E) F_D(\gamma_E) d\gamma_E, \tag{8}$$

$$I_3 = \int_0^\infty \ln(1 + \gamma_E) f_E(\gamma_E) d\gamma_E. \tag{9}$$

Subitituting Eqs. (2) and (4) into Eq. (7), I_1 becomes

$$\begin{aligned} I_1 = {} & A_E \sum_{s=1}^{L} \alpha_{D,s} \int_0^\infty {\gamma_D}^{m_D - 1} \ln(1 + \gamma_D) e^{-\varsigma_{D,s}\gamma_D} d\gamma_D \\ & - (m_E - 1) \sum_{s=1}^{L} \sum_{t=1}^{L} \sum_{p=0}^{m_E - 1} \left(B_1 \int_0^\infty \ln(1 + \gamma_D) {\gamma_D}^{m_D + p - 1} \right. \\ & \left. \times e^{-(\varsigma_{D,s} + \varsigma_{E,t})\gamma_D} d\gamma_D\right), \end{aligned} \tag{10}$$

where $B_1 = \left(\alpha_{D,s} \alpha_{E,t} \varsigma_{E,t}{}^{-m_E + p}\right) / p!$. Making use of Eq. (78) of [19], I_1 is obtained as

$$\begin{aligned} I_1 = {} & A_E \sum_{s=1}^{L} \alpha_{D,s} (m_D - 1)! e^{\varsigma_{D,s}} \sum_{n=1}^{m_D} \frac{\Gamma\left(n - m_D, \varsigma_{D,s}\right)}{\varsigma_{D,s}{}^n} \\ & - (m_E - 1)! \sum_{s=1}^{L} \sum_{t=1}^{L} \sum_{p=0}^{m_E - 1} \left(B_1 (m_D + p - 1)! \right. \\ & \left. \times e^{\varsigma_{D,s} + \varsigma_{E,t}} \sum_{k=1}^{m_D + p} \frac{\Gamma\left(k - m_D - p, \varsigma_{D,s} + \varsigma_{E,t}\right)}{\left(\varsigma_{D,s} + \varsigma_{E,t}\right)^k}\right), \end{aligned} \tag{11}$$

where $\Gamma(\alpha, x) = \int_x^\infty e^{-t} t^{\alpha - 1} dt$ is the upper incomplete Gamma function, as defined by Eq. (8.350.2) of [14].

Similarly, one can solve the integral of I_2 as

$$\begin{aligned} I_2 = {} & A_D \sum_{t=1}^{L} \alpha_{E,t} (m_E - 1)! e^{\varsigma_{E,t}} \sum_{n=1}^{m_E} \frac{\Gamma\left(n - m_E, \varsigma_{E,t}\right)}{\varsigma_{E,t}{}^n} \\ & - (m_D - 1)! \sum_{t=1}^{L} \sum_{j=1}^{L} \sum_{p=0}^{m_D - 1} \left(B_2 (m_E + p - 1)! \right. \\ & \left. \times e^{\varsigma_{D,j} + \varsigma_{E,t}} \sum_{k=1}^{m_E + p} \frac{\Gamma\left(k - m_E - p, \varsigma_{D,j} + \varsigma_{E,t}\right)}{\left(\varsigma_{D,j} + \varsigma_{E,t}\right)^k}\right), \end{aligned} \tag{12}$$

where $B_2 = \alpha_{E,t} \alpha_{D,j} \varsigma_{D,j}{}^{-m_D + p} / p!$.

Subitituting Eq. (2) into Eq. (9) and making use of Eq. (78) of [19], I_3 is obtained as

$$\begin{aligned} I_3 &= \int_0^\infty \ln(1+\gamma_E)\, f_E(\gamma_E)\, d\gamma_E \\ &= \sum_{t=1}^{L} \alpha_{E,t} \int_0^\infty \ln(1+\gamma_E)\, {\gamma_E}^{m_E-1} e^{-\varsigma_{E,t}\gamma_E} d\gamma_E \\ &= \sum_{t=1}^{L} \alpha_{E,t}\, (m_E-1)! e^{\varsigma_{E,t}} \sum_{k=1}^{m_E} \frac{\Gamma\left(k-m_E, \varsigma_{E,t}\right)}{{\varsigma_{E,t}}^{k}}. \end{aligned} \tag{13}$$

Substituting Eqs. (11), (12), and (13) into Eq. (6), the closed-form expression for the ASC is obtained.

IV. SOP Analysis

When S has no information about the eavesdroppers channel, S has no choice but to encode the confidential data into codewords of a constant rate R_s [17]. If $R_s \le C_s$, perfect secrecy can be achieved. Otherwise, information theoretic security is compromised. Such scenarios are called passive eavesdropping, and SOP is a useful performance metrics to evaluate the security performance, which can be expressed as [18]

$$\begin{aligned} SOP &= P\{C_s(\gamma_D, \gamma_E) < R_s\} \\ &= P\{\gamma_D < \Theta\gamma_E + \Theta - 1\} \\ &= \int_0^\infty F_D(\Theta\gamma_E + \Theta - 1)\, f_E(\gamma_E)\, d\gamma_E, \end{aligned} \tag{14}$$

where R_s ($R_s \ge 0$) is the target secrecy capacity threshold, and $\Theta = e^{R_s} \ge 1$. Subitituting Eqs. (2) and (4) into Eq. (14), SOP is expressed as

$$\begin{aligned} SOP &= \int_0^\infty F_D(\Theta\gamma_E + \Theta - 1)\, f_E(\gamma_E)\, d\gamma_E \\ &= A_D - (m_D-1)! \sum_{s=1}^{L}\sum_{t=1}^{L}\sum_{p=0}^{m_D-1} \Bigg(B_3 e^{-\varsigma_{D,s}(\Theta-1)} \\ &\quad \times \int_0^\infty {\gamma_E}^{m_E-1} e^{-(\Theta\varsigma_{D,s}+\varsigma_{E,t})\gamma_E} (\Theta\gamma_E + \Theta - 1)^p d\gamma_E \Bigg), \end{aligned} \tag{15}$$

where $B_3 = \left(\alpha_{D,t}\alpha_{E,s}{\varsigma_{D,t}}^{-m_D+p}\right) / p!$. Basing on binomial formula, as defined in Eq. (1.111) of [14], and utilizing Eq. (3.326.2) of [14], the SOP is obtained as

$$\begin{aligned} SOP = A_D - (m_D-1)! \sum_{s=1}^{L}\sum_{t=1}^{L}\sum_{p=0}^{m_D-1} \Bigg(B_3 e^{-\varsigma_{D,s}(\Theta-1)} \\ \times \sum_{q=0}^{p} \binom{p}{q} \frac{\Theta^q (\Theta-1)^{p-q} \Gamma(m_E+q)}{\left(\varsigma_{E,t} + \Theta\varsigma_{D,s}\right)^{m_E+q}} \Bigg), \end{aligned} \tag{16}$$

where $\binom{k}{l} = \frac{k!}{l!(k-l)!}$ is the binomial coefficient.

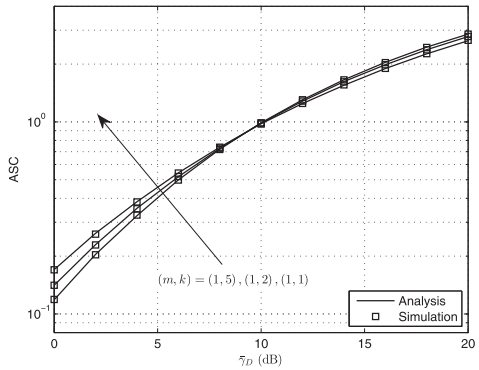

Fig. 1. ASC for generalized-K channels versus $\bar{\gamma}_D$.

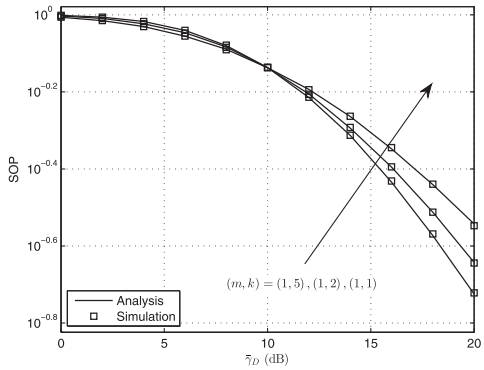

Fig. 2. SOP for generalized-K channels versus $\bar{\gamma}_D$.

V. SPSC Analysis

The SPSC [1], which means the probability of existence of secrecy capacity, is a fundamental benchmark in secure communications, can be obtained by

$$\begin{aligned} SPSC &= \Pr\{C_s(\gamma_D, \gamma_E) > 0\} \\ &= 1 - SOP\,|R_s = 0\,. \end{aligned} \tag{17}$$

Subtituting $R_s = 0$ into Eq. (17), the $SPSC$ is obtained as

$$SPSC = 1 - A_D + \sum_{s=1}^{L}\sum_{t=1}^{L}\sum_{p=0}^{m_D-1} \frac{B_3\,(m_D-1)!\Gamma(m_E+p)}{\left(\varsigma_{D,s}+\varsigma_{E,t}\right)^{m_E+p}}. \tag{18}$$

VI. Numerical results

In this section, numerical results and Monte-carlo simulations are presented to validate the analytical deviations. The main parameters used in simulations and analysis are set as $L = 5$, $m_D = m_E = m$, $k_D = k_E = k$ and $R_s = 2$ bit/s/Hz. The curves for various (m, k) and $\bar{\gamma}_E$ are plotted for comparison purposes while varying $\bar{\gamma}_D$.

In Figs. 1–6, simulation and analytical results are compared for ASC, SOP, and SPSC over GK channels. It is clear that analysis results match very well with simulation curves in all figures. Further, it can be observed that the all the security performance improves while increasing $\bar{\gamma}_D$, which is the average SNR of the main channel.

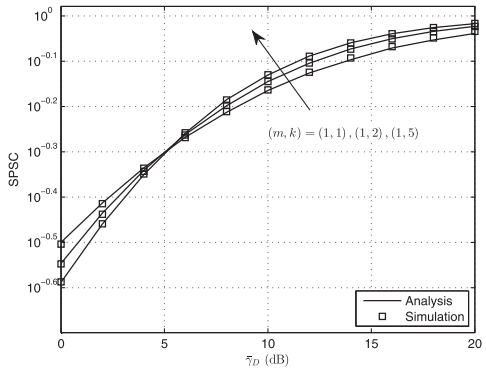

Fig. 3. SPSC over generalized-K channels versus $\bar{\gamma}_D$.

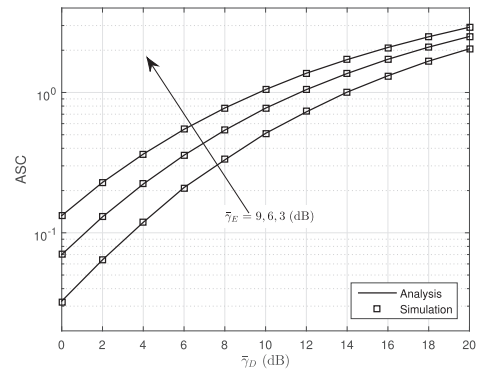

Fig. 4. ASC over generalized-K channels versus $\bar{\gamma}_D$.

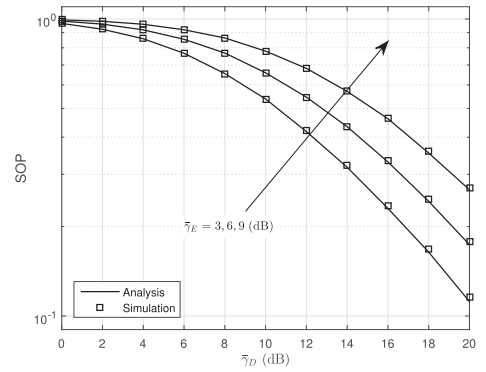

Fig. 5. SOP over generalized-K channels versus $\bar{\gamma}_D$.

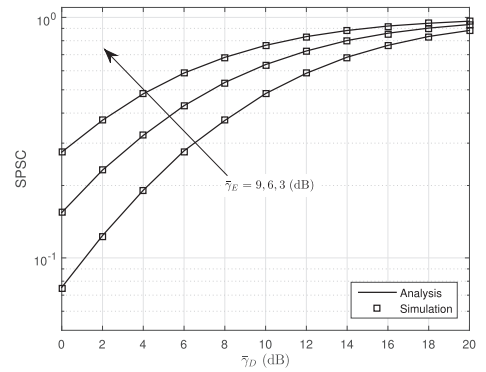

Fig. 6. SPSC over generalized-K channels versus $\bar{\gamma}_D$.

From Figs. 1, 2, and 3, one can find that the ASC, SOP, and SPSC degrades while decreasing k, which is the fading factor of GK channels. From Figs. 4, 5, and 6, it can be observed that the all the security performance improves while decreasing $\bar{\gamma}_E$, which is the average SNR of the eavesdropper channel.

VII. Conclusion

In this letter, the physical layer security is analyzed for the classic Wyner's model over independent GK channels. The closed-form expressions for the ASC, SOP, and SPSC, have been derived, which were validated through simulations.

References

[1] 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.*, 2015, doi: 10.1109/TVT.2015.2412140, to be published.

[2] 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.

[3] Y. Zou, J. Zhu, X. Wang, and V. Leung, "Improving physical-layer security in wireless communications using diversity techniques," *IEEE Netw.*, vol. 29, no. 1, pp. 42–48, Jan. 2015.

[4] Y. Zou, X. Wang, and W. Shen, "Optimal relay selection for physical-layer security in cooperative wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 10, pp. 2099–2111, Oct. 2013.

[5] Y. Zou, B. Champagne, W.-P. Zhu, and L. Hanzo, "Relay-selection improves the security-reliability trade-off in cognitive radio systems," *IEEE Trans. Commun.*, vol. 63, no. 1, pp. 215–228, Jan. 2015.

[6] P. M. Shankar, "Error rates in generalized shadowed fading channels," *Wireless Pers. Commun.*, vol. 28, no. 3, pp. 233–238, Feb. 2004.

[7] J. Cao, L.-L. Yang, and Z. Zhong, "Performance analysis of multihop wireless links over generalized-K fading channels," *IEEE Trans. Veh. Technol.*, vol. 61, no. 4, pp. 1590–1598, May 2012.

[8] A. Abdi and M. Kaveh, "K distribution: An appropriate substitute for Rayleigh-lognormal distribution in fading-shadowing wireless channels," *Electron. Lett.*, vol. 34, no. 9, pp. 851–852, Apr. 1998.

[9] G. L. Stüber, *Principles of Mobile Communication*, New York, NY, USA: Springer, 2011.

[10] J. Jung, S. Lee, H. Park, and I. Lee, "Capacity and error probability analysis of diversity reception schemes over generalized-K fading channels using a mixture Gamma distribution," *IEEE Trans. Wireless Commun.*, vol. 13, no. 9, pp. 4721–4730, Sep. 2014.

[11] I. S. Ansari, S. Al-Ahmadi, F. Yilmaz, M. S. Alouini, and H. Yanikomeroglu, "A new formula for the BER of binary modulations with dual-branch selection over generalized-K composite fading channels," *IEEE Trans. Commun.*, vol. 59, no. 10, pp. 2654–2658, Oct. 2011.

[12] A. D. Wyner, "The wire-tap channel," *Bell Sys. Technol. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[13] P. S. Bithas, N. C. Sagias, P. T. Mathiopoulos, G. K. Karagiannidis, and A. A. Rontogiannis, "On the performance analysis of digital communications over generalized-K fading channels," *IEEE Commun. Lett.*, vol. 10, no. 5, pp. 353–355, Jan. 2006.

[14] I. Gradshteyn and I. Ryzhik, *Table of Integrals, Series and Products*, 7th ed. San Diego, CA, USA: Academic, 2007.

[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] M. Abramowitz and I. A. Stegun, *Handbook of Mathematical Functions With Formulas, Graphs, and Mathematical Tables*, 9th ed. New York, NY, USA: Dover, 1972.

[17] L. Wang, M. Elkashlan, J. Huang, R. Schober, and R. Mallik, "Secure transmission with antenna selection in MIMO Nakagami-m fading channels," *IEEE Trans. Wireless Commun.*, vol. 13, no. 11, pp. 6054–6067, Nov. 2014.

[18] M. Bloch, J. Barros, M. R. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, Jun. 2008.

[19] M.-S. Alouini and A. J. Goldsmith, "Capacity of Rayleigh fading channels under different adaptive transmission and diversity-combining techniques," *IEEE Trans. Veh. Technol.*, vol. 48, no. 4, pp. 1165–1181, Jul. 1999.