Secrecy Performance Analysis over Double Nakagami-m Fading Channels

Serdar Özgür Ata
Informatics and Information Security Research Center, TÜBİTAK/BİLGEM, Kocaeli, Turkey
Email: serdar.ata@tubitak.gov.tr

***Abstract*—Next-generation wireless communication systems with high user mobility inherit cascaded fading channel models, where the fading effects are more severe than classical channel models including Rayleigh and Nakagami-m. In this study, physical layer secrecy/security performance analysis has been investigated over double Nakagami-m fading channels. While analytic results are derived, the closed-form expression of the probability of positive secrecy capacity is obtained, then the exact secrecy outage probability is obtained in the closed-form. Furthermore, computer simulations are given to verify the analytic results.**

***Keywords*—Physical layer security, positive secrecy capacity, secrecy outage probability, cascaded fading channels.**

I. Introduction

In order to cope with the security threats in mobile wireless systems, several physical layer security techniques have been proposed and investigated in the literature. Among these methods, exploiting the time-varying nature of wireless communication channels have been drawing attention in recent years [1]. Early works on the physical layer security over Gaussian wiretap channels show that the positive secrecy capacity (SC) exists if the legal user has a better channel quality than the illegal user while SC becomes zero if conversely [2], [3]. Later, basic secrecy performance metrics such as average secrecy capacity (ASC), secrecy outage probability (SOP), and the probability of positive secrecy capacity (PPSC) are defined and investigated for several fading-channel models [4], [5].

In a variety of wireless communication scenarios such as vehicle-to-vehicle communication channels, keyhole channels, and multi-hop amplify-and-forward relaying channels, it is observed that short-term fading can be modeled in a multiplicative form [6]–[8]. This type of channels is named as cascaded fading channels where the fading effects are worse than Rayleigh/Nakagami fading in classical cellular communications [9]. In the studies on cascaded fading channels, it has been shown that the double-Rayleigh fading channel model is appropriate for keyhole effect problems in [10]. It is also shown that the fading effect in vehicle-to-vehicle communication systems can be modeled as double-Rayleigh [11]. Subsequently, the double-Nakagami-m fading channel model is investigated in [12] and [13]. As the double-fading channel models are insufficient to model multi-hop relay communication systems, generalized cascaded channel models have been studied in [14] and [15], presenting cascaded Rayleigh and cascaded Nakagami-m channel models, respectively. Additionally, cascaded Generalized-K channel and cascaded Weibull channel models are examined in [16] and [17].

ISBN 978-1-5386-4695-3

Secrecy performance analysis of classical fading channels has already been investigated extensively in the literature. The ASC and SOP analysis are presented for both correlated and uncorrelated log-normal fading channels in [18]. In [19], the problem of broadcasting confidential messages among multiple legal users are investigated for Rayleigh fading channels, and SC analysis is performed in case of transmitting a single common message, while the sum-SC analysis is done in case of transmitting multiple independent messages. The SOP analysis of the correlated Rayleigh fading channels are studied in [20] and [21]. The SOP, ergodic-SC and PPSC analysis for Nakagami-m fading channels are examined in [22] considering multiple illegal users. On the other hand, analytical models of SOP and PPSC are derived under Nakagami-m fading channels for cognitive radio applications in [23]. Furthermore, the secrecy characteristics of the Generalized-K and Gamma fading channels are investigated in [24] and [25]. [26] addresses Rician fading channels with SC and PPSC analyses, and presents an analytical expression of the PPSC. The PPSC and SOP expressions for Weibull channels are derived in the form of single integrals in [27] and [28]. Moreover, an analytical expression of the PPSC and a lower bound for the SOP is obtained for $\kappa - \mu$ fading channels in [29]. An upper bound for the PPSC in α-μ fading channels is derived in [30], [31].

Although there are several studies analyzing the secrecy performance of the classical channel models, information-theoretic secrecy analysis has not been performed for cascaded channel models yet. In this paper, we study the secrecy performance analysis of the wireless communication systems over double Nakagami-m fading channels. As the novel contribution of this paper, we derived the closed-form expressions of the PPSC and SOP. Finally, the analytic results are verified by comparing with the computer simulations.

The outline of this paper is as follows. The system model is explained in Section II. The analytical expressions of the probability of positive secrecy capacity and the secrecy outage probability are derived in Section III and Section IV, respectively. The simulations and numerical results are presented in Section V. Finally, the paper is concluded in Section VI.

II. System Model

We examine the physical layer security performance of a three-node wiretap communication system pictured in Fig. 1. The illegal user E is observing the information conveyed by the message of the source S sending to the legal user L. In the system the fading channels from S to L, and S to E are assumed to be independent and modeled as double Nakagami-m fading channels. Therefore, the channel fading coefficient

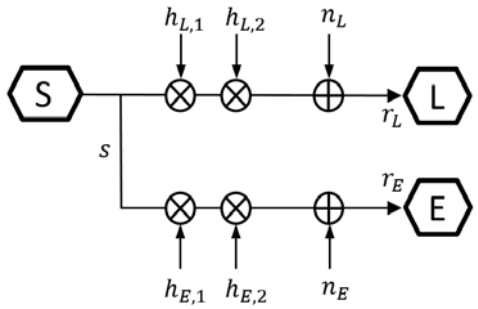

Fig. 1: Cascaded wiretap channel model.

between the nodes S and X, $X \in \{L,\ E\}$, denoted by h_X is expressed as

$$h_X = h_X^1 h_X^2. \tag{1}$$

where the fading parameters h_X^1 ve h_X^2 are independent and identically Nakagami-m distributed random variables with the distribution parameter of m_X^i and average power of $\Omega_X^i = E[(h_X^i)^2]$, $i = 1,\ 2$. Here $E[.]$ represents the expected value operator. Then the probability density function (pdf) of the channel fading coefficient h_X is given as

$$\begin{aligned} f_{h_X}(h) &= \frac{4h^{m_X^1+m_X^2-1}}{\Gamma(m_X^1)\Gamma(m_X^2)}\beta_X^{(m_X^1+m_X^2)/2} \\ &\quad \times K_{m_{X,1}-m_{X,2}}\left(2h\sqrt{\beta_X}\right) \end{aligned} \tag{2}$$

where $\beta_X = \prod_{i=1}^{2} m_X^i/\Omega_X^i$ [13]. In the proposed system, the additive noise at the nodes L and E are modeled as Gaussian random variables having zero-mean and two-sided power spectral density of $N_0/2$. The power of the signal s sent from the source node S is assumed to be P. Therefore the received signal by X is expressed as

$$r_X = h_X\sqrt{P}s + n_X, \tag{3}$$

where n_X represents the additive noise. Thus, the instantaneous signal-to-noise ratio (SNR) at X becomes

$$\gamma_X = Ph_X^2/N_0, \tag{4}$$

and by using (2), the pdf of γ_X is obtained as

$$\begin{aligned} f_{\gamma_X}(\gamma) &= f_h(\gamma)|dh/d\gamma_X| \\ &= \frac{2\gamma^{\left(m_X^1+m_X^2-2\right)/2}}{\Gamma(m_X^1)\Gamma(m_X^2)}\beta_X^{(m_X^1+m_X^2)/2} \\ &\quad \times K_{m_X^1-m_X^2}\left(2\sqrt{\gamma\beta_X}\right). \end{aligned} \tag{5}$$

The cumulative distribution function (CDF) of γ_X $F_{\gamma_X}(\gamma) = \int_0^\gamma f_{\gamma_X}(\gamma)d\gamma$ is derived by using [33, Eq.(03.04.21.0008.1)]

$$\begin{aligned} F_{\gamma_X}(\gamma) &= \pi \csc\left(\pi\left(m_X^2 - m_X^1\right)\right) \\ &\quad \times \left[\frac{\gamma^{m_X^1}}{\Gamma(m_X^2)}{}_1\tilde{F}_2\left(m_X^1; 1+m_X^1-m_X^2, 1+m_X^1; \gamma\beta_X\right)\right. \\ &\quad \left. -\frac{\gamma^{m_X^2}}{\Gamma(m_X^1)}{}_1\tilde{F}_2\left(m_X^2; 1-m_X^1+m_X^2, 1+m_X^2; \gamma\beta_X\right)\right] \end{aligned} \tag{6}$$

where ${}_1\tilde{F}_2(;,;)$ is the regularized hypergeometric function [33, Eq.(07.32.02.0001.01)].

III. Probability of Positive Secrecy Capacity

In the system model, if L and E nodes are assumed to be active, thus all of the nodes already have the channel state information (CSI) of the channels in between the nodes S, L and E. This scenario is reasonable for the case in which E is a relay in the network, and therefore it's also a legal user in this perspective. When S has the CSI of all channels, then it can transmit the messages with the secrecy capacity R_s, satisfying $R_s < C_s$ to provide the information-theoretic secrecy. Here C_s is the instantaneous secrecy capacity and expressed as

$$C_s \triangleq \max\left[\log_2(1+\gamma_L) - \log_2(1+\gamma_E), 0\right] \tag{7}$$

in terms of the channel capacities of L and E [5]. At this end, an important performance metric, the PPSC is defined as the probability of always having a positive SC in the system and expressed as [5]

$$P_{PSC} = P(C_s > 0). \tag{8}$$

Using (7), (5) and (6), this probability may be written as

$$\begin{aligned} P_{PSC} &= P(\log_2(1+\gamma_L) - \log_2(1+\gamma_E) > 0) \\ &= P\left(\gamma_L > \gamma_E\right) \\ &= 1 - \int_0^\infty F_{\gamma_L}(\gamma) f_{\gamma_E}(\gamma)d\gamma \\ &= 1 - \frac{\pi\csc\left(\pi\left(m_L^2 - m_L^1\right)\right)}{\Gamma(m_L^1)\Gamma(m_L^2)}\frac{2\beta_E^{(m_E^1+m_E^2)/2}}{\Gamma(m_E^1)\Gamma(m_E^2)} \\ &\quad \times (I_1 - I_2) \end{aligned} \tag{9}$$

where I_i is defined as

$$\begin{aligned} I_i \triangleq \int_0^\infty &\Gamma(m_L^i)\gamma^{\left(2m_L^i+m_E^1+m_E^2-2\right)/2}K_{m_E^1-m_E^2}\left(2\sqrt{\gamma\beta_E}\right) \\ &\times {}_1\tilde{F}_2\left(m_L^i; 1-m_L^j+m_L^i, 1+m_L^i; \gamma\beta_L\right)d\gamma \end{aligned} \tag{10}$$

for $i, j \in \{1, 2\}, i \neq j$. This integral is solved by using [33, Eq.(07.32.26.0001.01)] and [32, Eq.(7.542)] as follows

$$\begin{aligned} I_i &= \frac{1}{4}\left(\frac{1}{2\beta_E}\right)^{2m_L^i+m_E^1+m_E^2-1} \\ &\quad \times\Gamma(\frac{2m_L^i+2m_E^1-1}{2})\Gamma(\frac{2m_L^i+2m_E^2-1}{2}) \\ &\quad \times {}_3\tilde{F}_2\left(m_L^i; \frac{2m_L^i+2m_E^1-1}{2}, \frac{2m_L^i+2m_E^2-1}{2},\right. \\ &\qquad \left. 1-m_L^j+m_L^i, 1+m_L^i; -\beta_L/\beta_E\right), \end{aligned} \tag{11}$$

and substituting (11) in (9), the closed-form expression of the PPSC is obtained.

IV. Secrecy Outage Probability

If E is a passive node, and therefore there is no available CSI to S about the channel between S and E, S should transmit at a constant secrecy capacity R_s satisfying $C_s > R_s$ to achieve full secrecy. On the other hand, if $C_s < R_s$, then information-theoretic secrecy can not be achieved [3]. For such systems, SOP is defined as the probability of SC falling below a given threshold value and expressed as

$$P_{SO} = P(C_s < R_s) \tag{12}$$

as a performance metric for the physical layer security [5]. Let $c \triangleq 2^{R_s} > 1$, and $d \triangleq c - 1$, and using (5), (6), and (7) this probability is defined as

$$\begin{aligned} P_{SO} &= P\left(\log_2\left(1+\gamma_L\right) - \log_2\left(1+\gamma_E\right) < R_s\right) \\ &= P\left(\gamma_L < c\gamma_E + d\right) \\ &= \int_0^\infty F_{\gamma_L}\left(c\gamma + d\right) f_{\gamma_E}(\gamma) d\gamma \\ &= \left(\prod_{i=1}^{2} \Gamma(m_{L,i})\Gamma(m_{E,i})\right)^{-1} (J_1 - J_2) \end{aligned} \tag{13}$$

where

$$\begin{aligned} J_i \triangleq \int_0^\infty & \pi \csc\left(\pi\left(m_L^2 - m_L^1\right)\right) \Gamma(m_L^i) \left(c\gamma + d\right)^{m_L^i} \\ & \times {}_1\tilde{F}_2\left(m_L^i; 1 - m_L^j + m_L^i, 1 + m_L^i; \left(c\gamma + d\right)\beta_L\right) \\ & \times 2\beta_E^{\left(m_E^1 + m_E^2\right)/2} \gamma^{\left(m_E^1 + m_E^2 - 2\right)/2} K_{m_E^1 - m_E^2}\left(2\sqrt{\gamma\beta_E}\right) d\gamma. \end{aligned} \tag{14}$$

By applying $x = c\beta_L\gamma$ transformation, J_i can be written as

$$\begin{aligned} J_i = \int_0^\infty & \beta_L^{-m_L^i} S_i\left(x + a\right) \\ & \times 2\left(xb\right)^{\left(m_E^1 + m_E^2\right)/2} x^{-1} K_{m_E^1 - m_E^2}\left(2\sqrt{xb}\right) dx \end{aligned} \tag{15}$$

where $a \triangleq d\beta_L$, $b \triangleq \beta_E / \left(c\beta_L\right)$, and

$$\begin{aligned} S_i(z) = & \pi \csc\left(\pi\left(m_L^2 - m_L^1\right)\right) \Gamma(m_L^i) z^{m_L^i} \\ & \times {}_1\tilde{F}_2\left(m_L^i; 1 - m_L^j + m_L^i, 1 + m_L^i; z\right). \end{aligned} \tag{16}$$

At this end, with the help of [33, Eq.(07.34.03.0727.01)] and [33, Eq.(07.34.03.0805.01)], it may be written that

$$\begin{aligned} J_1 - J_2 = \int_0^\infty & x^{-1} G_{1,3}^{2,1}\left[x + a \middle| \begin{matrix} 1 \\ m_L^1,\, m_L^2,\, 0 \end{matrix}\right] \\ & \times G_{0,2}^{2,0}\left[bx \middle| \begin{matrix} m_E^1,\, m_E^2 \end{matrix}\right] dx \end{aligned} \tag{17}$$

where $G_{p,q}^{m,n}[.|.]$ is the Meijer's-G function [32, Eq.(9.301)]. By using the integral property of the Meijer's G function, [33, Eq.(07.34.03.0456.01)], (17) can be solved and P_{SO} is obtained as

$$\begin{aligned} P_{SO}(R_s) = & \sum_{k=0}^{\infty} \frac{\left((1 - 2^{R_s})\beta_L\right)^k}{k! \prod_{i=1}^{2} \Gamma(m_{L,i})\Gamma(m_{E,i})} \\ & \times G_{4,4}^{3,3}\left[\frac{\beta_E}{2^{R_s}\beta_L} \middle| \begin{matrix} 1,\, k - m_L^1 + 1,\, k - m_L^2 + 1,\, k+1 \\ m_E^1,\, m_E^2,\, k,\, k+1 \end{matrix}\right] \end{aligned} \tag{18}$$

in the closed-form.

V. Simulations and Numerical Results

In this section, simulation results verifying the theoretical derivations are presented. The average power values of the fading coefficients of $S-E$ and $S-L$ channels are assumed to be $\Omega_L^i = \Omega_E^i = 1$, $i \in \{1, 2\}$ in the numerical calculations and simulations, and S transmits at unity power, i.e., $P = 1$.

The PPSC performance of the double Nakagami-m channel is given in Fig. 2 for three different average SNR values of the $S-E$ channel, $\bar{\gamma}_E$, as 4 dB, 8 dB, and 12 dB. Fading parameters of the $S-L$ channel are chosen as $m_L^1 = 2$, $m_L^2 = 1.5$ while these parameters for the $S-E$ channel are set as $m_E^1 = 2$, $m_E^2 = 3$. The secrecy performance of the system improves and PPSC increases as $\bar{\gamma}_E$ decreases.

In Fig. 3, the SOP performance over Nakagami-m and double Nakagami-m fading channels is compared. The threshold value of the channel capacity is set as $R_s = 1.5$ bit/Hz/sn, and the average SNR value of the $S-E$ channel $\bar{\gamma}_E$ is chosen as 4 dB and 8 dB. Fading parameter values of the channels are chosen as $m_L^1 = 2.5$ and $m_E^1 = 1.5$ for Nakagami-m channels, and $m_L^1 = m_E^1 = 2.5$ and $m_E^2 = m_E^2 = 1.5$ for double Nakagami-m channels. The figure shows that, the SOP performance over double Nakagami-m channel is worsen compared to Nakagami-m channel. For example, the SOP value of 10^{-2} is achieved at $\bar{\gamma}_L = 20$ dB for Nakagami-m channel, whereas the same SOP value is obtained when $\bar{\gamma}_L$ =24 dB in double Nakagami-m channels, for $\bar{\gamma}_E = 4$ dB.

As seen from Fig. 2 and Fig. 3, the simulation and analytic results are perfectly matched.

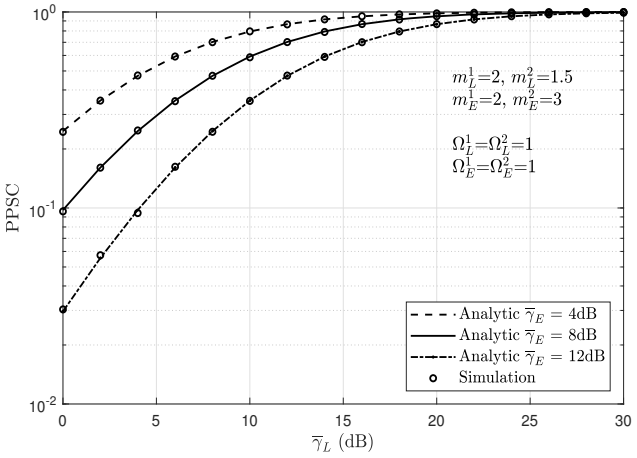

Fig. 2: Probability of positive secrecy capacity over double Nakagami-m channels.

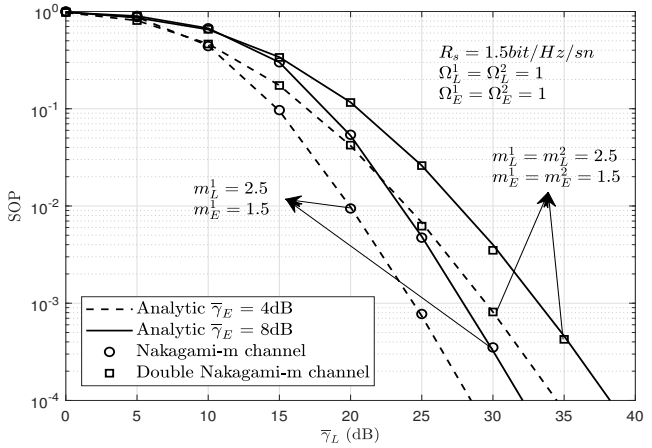

Fig. 3: Comparison of the secrecy outage probability over Nakagami-m and double Nakagami-m fading channels.

VI. Conclusions

In this paper, secrecy performance analysis over cascaded fading channels are investigated. The cascaded fading channel models provide an accurate fading model for the wireless communication scenarios such as mobile-to-mobile communications, keyhole channels, and multi-hop relaying systems. The analytic results are derived for the double Nakagami-m fading channels and the novel results on the physical layer security performance in cascaded wiretap communication channels are presented. While analytic results are evaluated, first the closed-form expression of the probability of positive secrecy capacity is obtained, then the exact secrecy outage probability is obtained in the closed-form. The analytical results are verified by computer simulations. Obtained results show that the increasing average SNR of the illegal user's channels decreases the secrecy performance. In addition, it is shown that the cascading nature of the channel degrades the secrecy performance of the wireless communication systems.

References

[1] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, M. Di Renzo, "Safeguarding 5G Wireless Communication Networks Using Physical Layer Security," IEEE Commun. Mag., pp. 20-27, 2015.

[2] A. D. Wyner, "The wire-tap channel," Bell Syst. Tech. J., 54, pp. 1355–1367, 1975.

[3] I. Csiszar, J. Körner, "Broadcast channels with confidential messages," IEEE Trans. Inf. Theory, 24, pp. 339–348, 1978.

[4] J. Barros, M. R. D. Rodrigues, "Secrecy capacity of wireless channels," IEEE Int. Symp. Inf. Theory, pp. 356–360, 2006,

[5] M.Bloch, J. Barros, M.R.D. Rodrigues, S.W. McLaughlin, "Wireless information-theoretic security," IEEE Trans. Inf. Theory, 54, pp. 2515-2534, 2008.

[6] A.F. Molisch, F. Tufvesson, J. Karedal, C.F. Mecklenbrauker, "A survey on vehicle-to-vehicle propagation channels," IEEE Trans. Wireless Commun., 16, pp. 12-22, 2009.

[7] S.Sanayei, A.Hedayat, A.Nosratinia, "Space time codes in keyhole channels: Analysis and design," IEEE Trans. Wireless Commun., 6, pp. 2006–2011, 2007.

[8] C.S.Patel, G.L. Stuber, T.G. Pratt, "Statistical properties of amplify and forward relay fading channels," IEEE Trans. Vehicular Tech., 55, pp. 1–9, 2006.

[9] D.W. Matolak, J. Frolik, "Worse-than-Rayleigh fading: Experimental results and theoretical models," IEEE Trans. Antennas Propag., pp. 140–146, 2011.

[10] D. Chizhik, G.J. Foschini, R.A. Valenzuela, "Keyholes, correlations, and capacities of multi-element transmit and receive antennas," IEEE Trans. Wireless Commun., 1, pp. 361–368, 2002.

[11] G. Wu, S. Talwar, K. Johnsson, N. Himayat, K.D. Johnson, "M2M: from Mobile to Embedded Internet," IEEE Commun. Mag., 49, pp. 36-43, 2011.

[12] B. Talha, M.Patzold, "Channel models for mobile-to-mobile cooperative communication systems," IEEE Vehicular Tech. Mag., pp. 33-43, 2011.

[13] H. Shin, J.H. Lee, "Performance analysis of space-time block codes over keyhole Nakagami-m fading channels," IEEE Trans. Vehicular Tech., 53, pp. 351–362, 2004.

[14] J. Salo, H. El-Sallabi, P. Vainikainen, "The distribution of the product of independent Rayleigh random variables," IEEE Trans. Antennas Propag., 54, pp. 639–643, 2006.

[15] G.K. Karagiannikis, N.C. Sagias, P.T. Mathiopoulos, "N*Nakagami: A novel stochastic model for cascaded fading channels," IEEE Trans. Commun., 55, pp. 1453–1458, 2007.

[16] I. Trigui, A. Laourine, S. Affes, A. Tephen, "On the performance of cascaded generalized K fading channels," IEEE Globecom, pp. 1-6, 2009.

[17] N. Sagias, G. Tombras, "On the cascaded Weibull fading channel model," Journal of the Franklin Inst., 344, pp. 1–11, 2007.

[18] G. Pan, C. Tang, X. Zhang, T. Li, Y. Weng, Y. Chen, "Physical layer security over non-small scale fading channels," IEEE Trans. Vehicular Tech., 65, pp. 1326–39, 2016.

[19] A. Khisti, A. Tchamkerten, G. Wornell, "Secure broadcasting over fading channels," IEEE Trans. Inf. Theory, 54, pp. 2453–2469, 2008.

[20] J. Zhu, X. Jiang, O. Takahashi, N. Shiratori, "Secrecy capacity of correlated Rayleigh fading channels," 18th Asia-Pacific Conf. on Commun., pp. 333-337, 2012.

[21] X. Sun, J. Wang, W. Xu, C. Zhao, Performance of secure communications over correlated fading channels, IEEE Signal Proc. Letters, 19, pp. 479–482, 2012.

[22] M. Zahurul I. Sarkar, T. Ratnarajah, M. Sellathurai, "Secrecy capacity of Nakagami-m fading wireless channels in the presence of multiple eavesdroppers," 43rd ASILOMAR Conf. Sig. Sys. and Comp., pp. 829-833, 2009.

[23] C. Tang, G. Pan, T. Li, "Secrecy outage analysis of underlay cognitive radio unit over Nakagami-m fading channels," IEEE Wireless Commun. Letters, 3, pp. 609-612, 2014.

[24] H. Lei, H. Zhang, I.S. Ansari, C. Gao, Y. Guo, G. Pan, K. Qaraqe, "Performance analysis of physical layer security over generalized-K fading channels using a mixture Gamma distribution," IEEE. Commun. Letters, 20, pp. 408-411, 2016.

[25] H. Lei, C. Gao, Y. Guo, G. Pan, "On physical layer security over generalized Gamma fading channels," IEEE. Commun. Letters, 19, pp. 1257-1260, 2015.

[26] X. Liu, "Probability of strictly positive secrecy capacity of the Rician fading channel," IEEE Wireless Commun. Letters, 2, pp. 50–53, 2013.

[27] X. Liu, "Average secrecy capacity of the Weibull fading channel," 13th IEEE Consum. Commun. Networking Conf., 2016.

[28] X. Liu, Probability of strictly positive secrecy capacity of the Weibull fading channel, IEEE GLOBECOM, pp. 659–664, 2013.

[29] N. Bhargav, S.L. Cotton, D.E. Simmons, "Secrecy capacity analysis over κ-μ fading channels: Theory and applications," IEEE Trans. Commun., 64, pp.3011-3024, 2016.

[30] L. Kong, H. Tran, G. Kaddoum, "Performance analysis of physical layer security over α-μ fading channels," IET Elec. Lett., 52, pp. 45-47, 2016.

[31] H. Lei, I.S. Ansari, G. Pan, B. Alomair, M.-S. Alouini, "Secrecy capacity analysis over α-μ fading channels," IEEE Commun. Letters, 2017.

[32] I.S. Gradshteyn, I.M. Ryzhik, Table of Integrals, Series, and Products, 7th ed., Elsevier Inc., 2007.

[33] Wolfram Research, Inc. The Wolfram functions site. [Online]. http://functions.wolfram.com