Accepted in Electronics Letters, 2016

Performance analysis of physical layer security over α-μ fading channel

L. Kong, H. Tran and G. Kaddoum

Recently, many works have focused on analyzing the metrics of physical layer security over different wireless channels, such as additive white Gaussian noise (AWGN), Rayleigh, Rician and Nakagami-*m* fading distributions. In order to extend the analysis to the general case, α-μ fading channel is considered, which can span the aforementioned cases. For this purpose, the physical layer security over α-μ fading channel is presented in this letter. The closed-form expressions for the probability of positive secrecy capacity and upper bound of the secrecy outage probability are derived. Their accuracies are assessed through comparison of theoretical analysis and simulations results.

Introduction: Physical layer security is a promising solution that addresses the security issue while directly operating at the physical layer from the information-theoretic viewpoint. Numerous contributions exist that analyze the secrecy performance over AWGN, Rayleigh, Rician, Nakagam-*m* and Weibull fading channels. Performance analysis in terms of secrecy capacity and outage probability has been investigated [1, 2, 3, 4]. However, to the best knowledge of the authors, there is no previous work focusing on the general case of fading channels. With regard to different values of α and μ, the α-μ fading channel can be reduced to the specific fading channel, such as Rayleigh, Nakagami-*m* and Weibull fading distributions by adjusting certain parameters. In this letter, the secrecy performance over α-μ fading channel is evaluated by the closed-form expressions for the probability of positive secrecy capacity and upper bound of secrecy outage probability. Consequently, our theoretical analysis is confirmed by simulation results.

System model and secrecy performance analysis: A three-node classic model such as the one shown in Fig. 1 is used here to illustrate a wireless network with potential eavesdropping. In the wiretap channel model, a legitimate transmitter (Alice) equipped with a directional antenna wishes to send secret messages to an intended receiver (Bob) in the presence of an eavesdropper (Eve), the link between Alice and Bob with fading coefficient h_m is called the main channel, while the one between Alice and Eve with fading coefficient h_w is named as the wiretap channel. Both channels undergo the α-μ distribution.

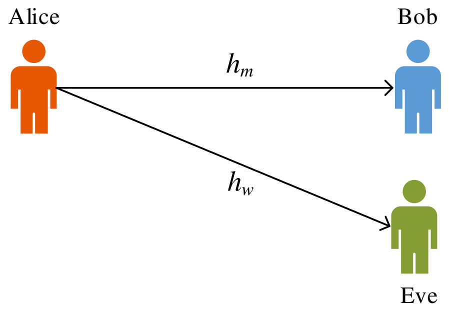

Fig. 1 *Illustration of system model with two legitimate transceivers (Alice and Bob) and one eavesdropper (Eve).*

Recalling that the probability density function (PDF) of the α-μ fading channel coefficients $h_i, (i \in \{m, w\})$ is given by [5]

$$f_{h_i}(h) = \frac{\alpha_i \mu_i^{\mu_i} h^{\alpha_i \mu_i - 1}}{\hat{h}_i^{\alpha_i \mu_i} \Gamma(\mu_i)} \exp\left(-\mu_i \frac{h^{\alpha_i}}{\hat{h}_i^{\alpha_i}}\right), \tag{1}$$

where $\hat{h}_i = \sqrt[\alpha]{E\left(h_i^{\alpha_i}\right)}$ is the $\alpha-$root mean value, $\alpha_i > 0$ is an arbitrary fading parameter, $\mu_i > 0$ is the inverse of the normalized variance of $h_i^{\alpha_i}$. The parameter μ_i is calculated by $\mu_i = E^2\left(h_i^{\alpha_i}\right)/V\left(h_i^{\alpha_i}\right)$, where $E(\cdot)$ and $V(\cdot)$ are the expectation and variance operators, respectively. $\Gamma(x) = \int_0^\infty t^{x-1}e^{-t}dt$ is the Euler's Gamma function. In particular, when changing the values of α and μ to the following cases: (i) $\alpha = 2$, $\mu = 1$; (ii) $\alpha = 2$, $\mu = m$; and (iii) $\mu = 1$, the α-μ fading model can be simplified such that it follows Rayleigh, Nakagami-*m* and Weibull distributions, respectively.

Let $g_i = |h_i|^2$ denote the instantaneous channel power gain with unit mean. The PDF of g_i is expressed as [6]

$$f_{g_i}(x) = \frac{\alpha_i x^{\frac{\alpha_i \mu_i}{2} - 1}}{2\Omega_i^{\frac{\alpha_i \mu_i}{2}} \Gamma(\mu_i)} \exp\left[-\left(\frac{x}{\Omega_i}\right)^{\frac{\alpha_i}{2}}\right], \tag{2}$$

where $\Omega_i = \frac{\Gamma(\mu_i)}{\Gamma(\mu_i + \frac{2}{\alpha_i})}$. Therefore, the received signal-to-noise ratio (SNR) at Bob and Eve receiver sides can be expressed as

$$\gamma_i = \frac{P_i g_i}{N_i} \tag{3}$$

where P_i and N_i are the transmission power and noise power, respectively. Without loss of generality, we assume N_m is equal to N_w in this paper. In addition, since we consider that Alice is equipped with a directional antenna, then the transmitted powers P_m and P_w may be different because Bob and Eve are present in different locations in the network.

According to [1, 2, 3, 4], the secrecy capacity for the given network is given as follows

$$\begin{aligned} C_s &= C_m - C_w \\ &= \begin{cases} \log_2\left(\frac{1+\gamma_m}{1+\gamma_w}\right), & if\ \gamma_m > \gamma_w \\ 0, & if\ \gamma_m \leqslant \gamma_w \end{cases} \end{aligned} \tag{4}$$

where C_m and C_w are the capacities of the main channel and the wiretap channel, respectively.

Therefore, the probability of positive secrecy capacity can be derived as follows

$$\begin{aligned} Pr(C_s > 0) &= Pr\left[\log_2\left(\frac{1+\gamma_m}{1+\gamma_w}\right) > 0\right] \\ &= Pr(\gamma_m > \gamma_w) \\ &= 1 - Pr\left(\frac{\gamma_m}{\gamma_w} < 1\right) \\ &= 1 - Pr\left(\frac{g_m}{g_w} < \frac{P_w}{P_m}\right). \end{aligned} \tag{5}$$

According to equation (16) in [7], equation (5) is derived as

$$Pr(C_s > 0) = 1 - F_\gamma(1) \tag{6}$$

where $F_\gamma(x)$ is the cumulative distribution function (CDF) of x, which is given as

$$\begin{aligned} &F_\gamma(x) = Pr\left(\frac{g_m}{g_w} < \frac{P_w}{P_m} \cdot x\right) = \left(\frac{P_w \Omega_w}{P_m \Omega_m}\right)^{\frac{\alpha \mu_m}{2}} \frac{x^{\frac{\alpha \mu_m}{2}}}{\mu_m \beta(\mu_m, \mu_w)} \\ &\times {}_2F_1\left(\mu_m + \mu_w, \mu_m; 1 + \mu_m; -\left(\frac{P_w \Omega_w}{P_m \Omega_m}\right)^{\frac{\alpha}{2}} x^{\frac{\alpha}{2}}\right), \end{aligned} \tag{7}$$

herein ${}_2F_1(.,;.;.)$ denotes the Gaussian hypergeometric function and $\beta(.,.)$ is the Beta function.

The outage probability of the secrecy capacity is defined as the probability that the secrecy capacity C_s falls below the target secrecy rate R_s, i.e.

$$\begin{aligned} P_{out}(C_s \leqslant R_s) &= Pr\left[\log_2\left(\frac{1+\gamma_m}{1+\gamma_w}\right) \leqslant R_s\right] \\ &= Pr\left[\gamma_m \leqslant 2^{R_s}(1+\gamma_w) - 1\right] \\ &= Pr(\gamma_m \leqslant \gamma_{th} + \gamma_{th}\gamma_w - 1), \end{aligned} \tag{8}$$

where $\gamma_{th} = 2^{R_s}$. Due to the complex form of the PDF of α-μ fading distribution, it is difficult to obtain a closed-form expression for (8). However, when the target data rate R_s approaches zero, we can obtain the upper bound of the outage probability by substituting equation (7) into equation (8), to get the following relationship

$$\begin{aligned} P_{out}\left(C_s \leqslant R_s\right) &= Pr\left(\gamma_m \leqslant \gamma_{th} + \gamma_{th}\gamma_w - 1\right) \\ &\leqslant Pr\left(\gamma_m \leqslant \gamma_{th}\gamma_w\right) \\ &\leqslant Pr\left(\frac{\gamma_m}{\gamma_w} \leqslant \gamma_{th}\right) \\ &\leqslant Pr\left(\frac{g_m}{g_w} \leqslant \frac{P_w}{P_m} \cdot \gamma_{th}\right) \\ &\leqslant F_\gamma\left(\gamma_{th}\right). \end{aligned} \tag{9}$$

Numerical Analysis: Fig. 2 shows the simulation and analysis results of the probability of positive secrecy capacity versus the transmission power P_m over α-μ fading channel for selected power values of eavesdropper P_w provided that $\alpha = 2$ and $\mu_m = \mu_w = 1$ (Rayleigh fading). One can observe that the analytical and simulation results are in perfect match for any given set of parameters. In addition, for the case of fixed values of P_w, the larger P_m the higher the probability of positive secrecy capacity. In Fig. 3, the probability of positive secrecy capacity in terms of different values of α and μ for fixed $P_w = 10$ dB is illustrated. Here, a similar conclusion is obtained to that of Fig. 2.

Similarly, Fig. 4 and Fig. 5 show the simulation and analysis results of the upper bound of the outage probability of physical layer security over α-μ fading channel with regard to two cases: (i) fixed $\alpha = 2$, $\mu_m = \mu_w = 1$ while varying P_w; (ii) fixed P_w while changing the values of α and μ. Here, we fix the target data rate as $R_s = 0.01$ bps. We can easily draw the same conclusion about the accuracy of our derived expression for the upper bound of outage probability, i.e. analytical derivations are verified by the simulation results.

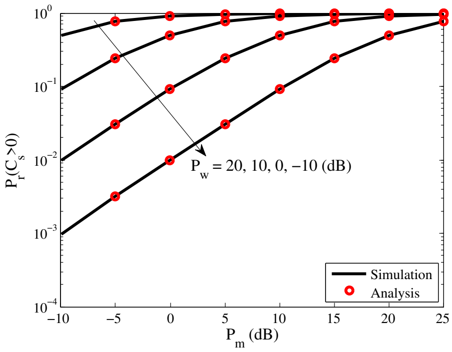

Fig. 2 *The probability of positive secrecy capacity versus P_m for selected values of P_w values with fixed values of $\alpha = 2$ and $\mu_m = \mu_w = 1$.*

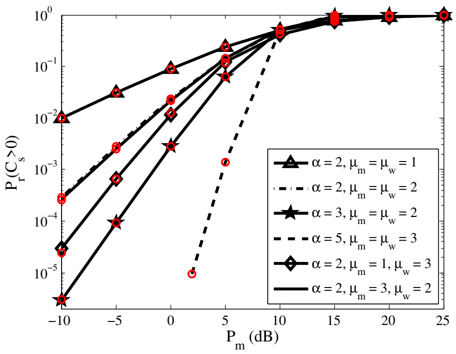

Fig. 3 *The probability of positive secrecy capacity versus P_m for different values of α and μ_i and a fixed value of $P_w = 10$ dB. The solid and circle (o) lines correspond to the simulation and analysis results, respectively.*

Conclusion: In this letter, we derive closed-form expressions for the probability of positive secrecy capacity and upper bound of outage probability for physical layer security over α-μ fading channels. For verification and correctness measures, the derived closed-form expressions are validated by simulation results.

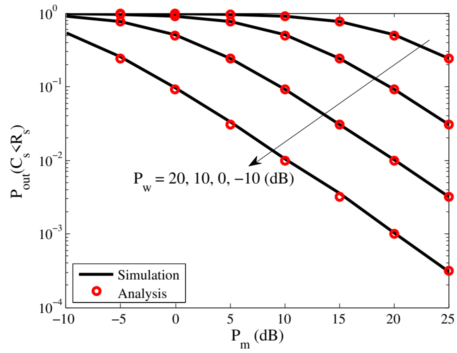

Fig. 4 *The upper bound of secrecy outage probability versus P_m for selected values of P_w with fixed values of $\alpha = 2$ and $\mu_m = \mu_w = 1$.*

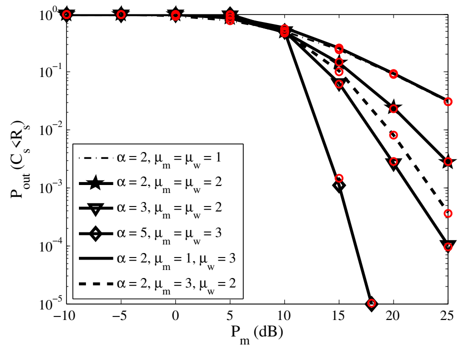

Fig. 5 *The upper bound of secrecy outage probability versus P_m for different values of α and μ_i and a fixed value of $P_w = 10$ dB. The solid and circle (o) lines correspond to simulation and analysis results, respectively.*

Acknowledgment: This work has been supported by the ETS's research chair of physical layer security in wireless networks.

L. Kong, H. Tran and G. Kaddoum (*Department of Electrical Engineering, University of Quebec, ETS, Montreal, Quebec, Canada*)

E-mail: long.kong.1@ens.etsmtl.ca

References

1 Bloch, M.; Barros, J.; Rodrigues, M.R.D.; McLaughlin, S.W.: 'Wireless Information-Theoretic Security', *IEEE Trans. Information Theory*, 2008, **54**, (6), pp. 2515-2534

2 Liu, X.: 'Probability of strictly positive secrecy capacity of the Rician-Rician fading channel', *IEEE Wireless Commun. Lett.*, 2013, **2**, (1), pp. 50-53

3 Sarkar, M.Z.I.; Ratnarajah, T.; Sellathurai, M.: 'Secrecy capacity of Nakagami-m fading wireless channels in the presence of multiple eavesdroppers', *2009 Conference Record of the Forty-Third Asilomar Conference on Signals, Systems and Computers*, Pacific Grove, CA, USA, 2009, pp.829-833

4 Liu X.: 'Probability of strictly positive secrecy capacity of the Weibull fading channel', *IEEE Global Communications Conference (GLOBECOM)*, 2013, Atlanta, GA, USA, pp.659-664

5 Yacoub, M.D.: 'The α-μ Distribution: a physical fading model for the stacy distribution', *IEEE Trans. Vehicular Technology*, 2007, **56**, (1), pp. 27-34

6 Youngpil S.; Hyundong S.; Wonha K.: 'Asymptotic SEP for M-PSK Signals over α-μ Fading Channels', *IEEE Commun. Lett.*, 2008, **12**, (9), pp.675-677

7 Tran H.; Duong, T.Q.; Zepernick, H.: 'On the performance of spectrum sharing systems over α-μ fading channel for non-identical μ parameter', *8th International Symposium on Wireless Communication Systems (ISWCS)*, 2011, Aachen, Germany, pp.477-481