2022 57th International Scientific Conference on Information, Communication and Energy Systems and Technologies (ICEST) | 978-1-6654-8500-5/22/$31.00 ©2022 IEEE | DOI: 10.1109/ICEST55168.2022.9828605

Secrecy outage probability and intercept probability analysis over α-F fading channels

Jelena A. Anastasov[1], Aleksandra S. Panajotović[1], Nikola M. Sekulović[2], Dejan N. Milić[1] and Daniela M. Milović[1]

Abstract – **In this paper, we investigated the secrecy performance of traditional Wyner's wiretap model over α-F fading channels. The expressions for evaluating the secrecy outage probability and the probability of intercept are derived. Due to high generality of assumed fading model which includes other models as special or limiting cases, presented analysis is quite general. Based on obtained analytical results, the impact of fading depth and shadowing severity of main/wiretap channel on the physical layer security metrics is studied. The results showed that secrecy transmission can be enhanced by proper exploiting propagation characteristics of authorized/unauthorized wireless channels.**

Keywords – **Shadowed fading channel, Physical layer security, Intercept probability, Secrecy outage probability.**

I. Introduction

Due to the inherent broadcast nature of wireless transmission, privacy and security problems in communication among legitimate nodes is of high importance [1], [2]. In general, various cryptographic protocols can be utilized by the upper layers, in comparison to physical layer, to enhance secrecy data transmission. Since an eavesdropper, as authorized or unauthorized user, usually owns unlimited computing power and can easily break down confidential keys, the encryption method requires to be strengthened.

Physical layer security (PLS) approach is an alternative in securing wireless transmission [2], [3]. The main concept of PLS refers to the information-theoretic perspective. From this point of view, PLS approach is based on the exploitation of the legitimate/illegitimate channel characteristics in order to achieve secure communications. Numerous PLS works are established to develop high secrecy rates for typical wiretap channel consisting of a source, a destination and an eavesdropper [4]-[10]. The security system enhancement over generalized Gamma, i.e. α-μ fading channels is presented in [4], [5]. The secrecy capacity for classic Wyner's wiretap model over non-small scale fading channels is investigated in [6]. The average secrecy capacity, the secrecy outage probability (SOP) and the probability of strictly positive secrecy capacity over generalized K (GK) fading channels is determined in [7]. In [8], [9], the PLS metric is analyzed over shadowed/fading channels that also encompasses the nonlinearity of propagation medium. Different secrecy metrics over Fisher-Snedecor (F) fading channels are derived in [10].

In this paper, we analyze the PLS of basic wiretap model over α-F fading channels. Novel expressions for evaluating SOP and the intercept probability (IP) are derived. These expressions are general and can be simplified for Gamma, Weibull, Nakagami-m, Rayleigh, α-μ, one-sided Gaussian and F fading scenarios. The impact of various channel parameters as well as the average SNRs over main/wiretap channel on the PLS is demonstrated.

II. System and Channel Model

We assume a presence of an eavesdropper (E) that attempts to intercept transmission of confidential signal from the source (S) to the specified destination node (D) [11] (Fig.1). All nodes are equipped by a single antenna.

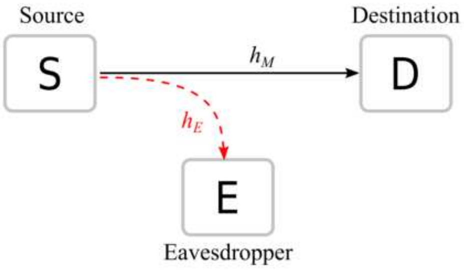

Fig. 1. System model

Specifically, S transmits secret message by emitting signal $s(t)$, with $E[|s(t)|^2]=1$, and the signal received by D is

$$x_M(t)=\sqrt{P}h_M s(t)+n_M(t), \tag{1}$$

with P being the emitting power from S, h_M being a fading coefficient of the main channel, i.e. the channel between the S and D, and $n_M(t)$ denoting additive white Gaussian noise (AWGN). The illegitimate node is also in the area of coverage trying to overhear the signal from S, and thus the received signal at node E can be defined as

$$x_E(t)=\sqrt{P}h_E s(t)+n_E(t), \tag{2}$$

[1]Jelena A. Anastasov, Aleksandra S. Panajotović, Dejan N. Milić and Daniela M. Milović are with the University of Niš, Faculty of Electronic Engineering, Aleksandra Medvedeva 14, 18000 Nis, Serbia, E-mails: {jelena.anastasov, aleksandra.panajotovic, dejan.milic, daniela.milovic}@elfak.ni.ac.rs.

[2]Nikola M. Sekulović is with the College of Applied Technical Sciences, Aleksandra Medvedeva 18, 18000 Nis, Serbia, E-mails: nikola.sekulovic@akademijanis.edu.rs.

978-1-6654-8500-5/22/$31.00 ©2022 IEEE

with h_E denoting a fading coefficient of the wiretap channel, i.e. the channel between the S and E, and $n_E(t)$ denoting AWGN. The channel state information of both channels is available at S.

Let express the received signal-to-noise-ratios (SNRs) from the main or wiretap link as

$$\gamma_* = \frac{|h_*|^2 P}{\sigma_*^2}, \tag{3}$$

where the subscript, *, denotes either main (M), either eavesdropper's (E) channel index and σ_*^2 denotes a variance of zero-mean AWGN.

Following the assumption that the main and wiretap channel are corrupted by α-F fading, the probability density function (PDF) of the instantaneous SNR, over both channels, has the following form [12, Eq.(3)]

$$p_{\gamma_*}(\gamma) = \frac{\alpha_*}{2\mathrm{B}(\mu_*, m_{s_*})}\left(\frac{(m_{s_*}-1)\bar{\gamma}_*^{\frac{\alpha_*}{2}}}{\mu_*\lambda_*^{\frac{\alpha_*}{2}}}\right)^{m_{s*}} \gamma^{\frac{\alpha_*\mu_*}{2}-1} \times\left(\gamma^{\frac{\alpha_*}{2}} + \frac{(m_{s_*}-1)\bar{\gamma}_*^{\frac{\alpha_*}{2}}}{\mu_*\lambda_*^{\frac{\alpha_*}{2}}}\right)^{-(\mu_*+m_{s*})}, \tag{4}$$

where B(·,·) denotes the Beta function [13], $\bar{\gamma}_*$ is the average SNR; m_{s_*} is the shadowing severity parameter, $m_{s_*} > 1$, μ_* is the fading depth parameter, $\mu_* \geq 0.5$, α_* is the non-linearity of the propagation medium, $\alpha_* > 0$, and λ_* is defined as

$$\lambda_* = \left(\frac{m_{s_*}-1}{\mu_*}\right)^{\frac{2}{\alpha_*}} \frac{\Gamma\left(\mu_* + \frac{2}{\alpha_*}\right)\Gamma\left(m_{s_*} - \frac{2}{\alpha_*}\right)}{\Gamma(\mu_*)\Gamma(m_{s_*})}, \; m_{s_*} > \frac{2}{\alpha_*}. \tag{5}$$

Utilizing the specific values of Meijer's G function relying on [14, Eq. (07.34.03.0271.01)] and additionally the form of the argument simplification [14, Eq. (07.34.16.0001.01)], the previous analytical expression of the PDF can be rewritten as

$$p_{\gamma_*}(\gamma) = \frac{\alpha_*}{2\Gamma(\mu_*)\Gamma(m_{s_*})\gamma} G_{1,1}^{1,1}\left(\frac{\gamma^{\frac{\alpha_*}{2}}}{a_*\bar{\gamma}_*^{\frac{\alpha_*}{2}}}\middle| \begin{matrix} 1-m_{s_*} \\ \mu_* \end{matrix}\right), \tag{6}$$

with $a_* = \frac{(m_{s_*}-1)}{\mu_*\lambda_*^{\frac{\alpha_*}{2}}}$ and $G_{p,q}^{m,n}(\cdot)$ denoting univariate Meijer's G function [13, Eq. (9.301)].

The cumulative distribution function (CDF) of the instantaneous SNR can be evaluated, according to its definition and relying to [15, Eq. (26)], as

$$F_{\gamma_*}(\gamma) = \frac{1}{\Gamma(\mu_*)\Gamma(m_{s_*})} G_{2,2}^{1,2}\left(\frac{\gamma^{\frac{\alpha_*}{2}}}{a_*\bar{\gamma}_*^{\frac{\alpha_*}{2}}}\middle| \begin{matrix} 1-m_{s_*}, 1 \\ \mu_* \;\;\;, 0 \end{matrix}\right). \tag{7}$$

The α-F fading model [12] is a composite fading model that defines the multipath fading and shadowing phenomena over wireless propagation channel as well as medium non-linearity. Other well-known fading models can be reported from this model as special or limiting case, such as F (Nakagami-m, Rayleigh, one-sided Gaussian), or α-μ model. Thus, the analysis that follows has high level of generality.

III. Secrecy Performance

Referring the Shannon capacity formula [16], one can evaluate the instantaneous channel capacity of the main channel as well as over the wiretap channel as

$$R_* = \log_2(1+\gamma_*). \tag{8}$$

The secrecy capacity over S-D link is a difference between the main and wiretap channel capacities

$$C_s = R_M - R_E = \log_2\left(\frac{1+\gamma_M}{1+\gamma_E}\right). \tag{9}$$

In the scenario with passive eavesdropping, the SOP is very often measured as a benchmark to indicate the security of the authorized. From the information-theoretical concept, the SOP is defined as a secrecy outage event when secrecy capacity falls below the target secrecy rate, R_t. Thus, the SOP can be exactly defined as [10]

$$P_{out}^{EX} = \Pr[C_s < R_t] = \Pr[\gamma_M \leq R_s\gamma_E + R_s - 1], \tag{10}$$

where $\gamma_0 = R_s\gamma_E + R_s - 1$ and $R_s = 2^{R_t}$. In the analysis that follows, we have determined the lower bounded version of SOP as [10]

$$\begin{aligned} P_{out}^{L} &= \Pr[\gamma_M \leq R_s\gamma_E] \leq P_{out} = \\ &= \int_0^\infty \int_0^{R_s\gamma_E} p_M(\gamma_M)\, p_E(\gamma_E)\, d\gamma_E d\gamma_M \\ &= \int_0^\infty F_M(R_s\gamma_E)\, p_E(\gamma_E)\, d\gamma_E. \end{aligned} \tag{11}$$

By substituting (7) and (6) with appropriate subscripts and arguments in (11), and with the help of [14, Eq. (07.34.21.0012.01)], by making the change of variables, $\gamma_E^{\alpha_E/2} = t$, the P_{out}^{L} integral is solved in the following form

$$P_{out}^{L}=\frac{\alpha_M}{2\Gamma\left(m_{s_E}\right)\Gamma\left(m_{s_M}\right)\Gamma\left(\mu_E\right)\Gamma\left(\mu_M\right)}$$
$$\times H_{3,3}^{2,3}\Bigg(\Bigg(R_s^{\frac{\alpha_M\alpha_E}{2}}\frac{a_E^{\alpha_M}}{a_M^{\alpha_E}\rho^{\frac{\alpha_M\alpha_E}{2}}}\left|\begin{matrix}\left(1-m_{s_M},1\right),(1,1),\left(1-\mu_E,\frac{\alpha_M}{\alpha_E}\right)\\ \left(\mu_M,1\right),\left(1+m_{s_E},\frac{\alpha_M}{\alpha_E}\right),(0,1)\end{matrix}\right.\Bigg), \quad (12)$$

where $\rho=\overline{\gamma}_M/\overline{\gamma}_E$ defines the average main-to-eavesdropper's channel power ratio (MER), and $H_{p,q}^{m,n}(\cdot)$ denoting Fox H function [17, Eq. (1.2)].

The IP is also a fundamental metric in determining system PLS. It is a probability that the secrecy capacity becomes non-positive, namely

$$P_{\text{int}}=\Pr\left[\gamma_M<\gamma_E\right]=\int_0^{\infty}F_M\left(\gamma_E\right)p_E\left(\gamma_E\right)d\gamma_E. \quad (13)$$

Again, by substituting (7) and (6) into previous formula and recalling [14, Eq. (07.34.21.0012.01)], we have derived the IP expression in the following form

$$P_{\text{int}}=\frac{\alpha_M}{2\Gamma\left(m_{s_E}\right)\Gamma\left(m_{s_M}\right)\Gamma\left(\mu_E\right)\Gamma\left(\mu_M\right)}$$
$$\times H_{3,3}^{2,3}\left(\frac{a_E^{\alpha_M}}{a_M^{\alpha_E}\rho^{\frac{\alpha_M\alpha_E}{2}}}\left|\begin{matrix}\left(1-m_{s_M},1\right),(1,1),\left(1-\mu_E,\frac{\alpha_M}{\alpha_E}\right)\\ \left(\mu_M,1\right),\left(1+m_{s_E},\frac{\alpha_M}{\alpha_E}\right),(0,1)\end{matrix}\right.\right). \quad (14)$$

IV. Numerical results

In this section, numerical results of the SOP and IP are presented to illustrate the proposed mathematical analysis carried out in the paper. Numerical results are obtained using Mathematica and figures are drawn in Origin software package. The Fox's H functions are evaluated with the help of program given in [18, Appendix].

Figure 2 plots the SOP as a function of the received average SNR of the main link, $\overline{\gamma}_M$, for several average SNR values of wiretap link, $\overline{\gamma}_E$, and its shape shadowing parameter, m_{S_E}. It can be seen that higher values of SNR of the main link provide better system performance. On the other hand, increasing of SNR which characterize wiretap link leads to performance deterioration. In the regime of high SNRs of the main link, increasing of shadowing parameter which characterize eavesdropper's channel results in lower SOP.

Figure 3 shows the SOP in terms of $\overline{\gamma}_E$ for different values of $\overline{\gamma}_M$ and m_{S_M}. This figure also confirms that the lower SNRs of wiretap link and higher SNR values of the main link provide better secrecy system performance. Increasing of m_{S_M} means that the main link suffers from the lower shadowing resulting in lower SOP, i.e. more secure transmission.

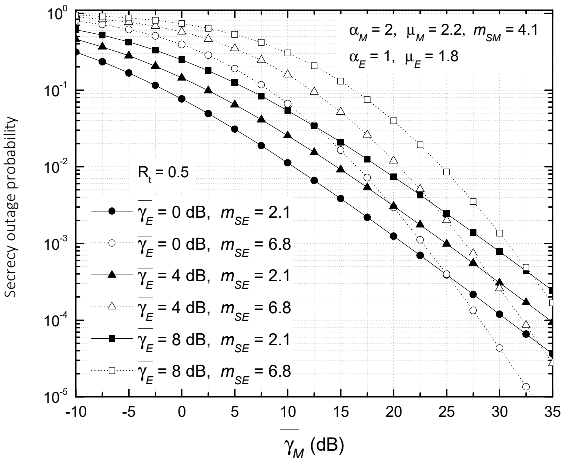

Fig. 2. SOP versus $\overline{\gamma}_M$ for different $\overline{\gamma}_E$ and m_{S_E}

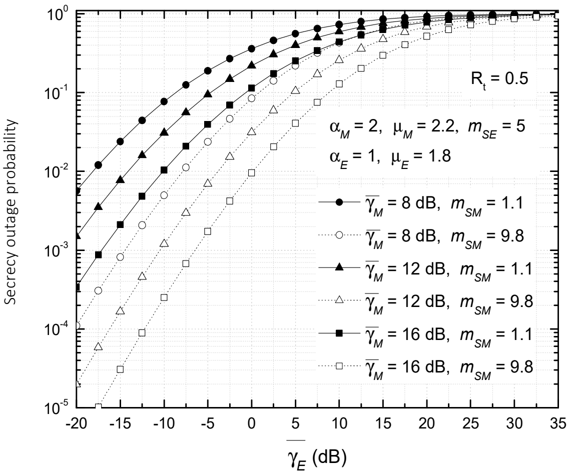

Fig. 3. SOP versus $\overline{\gamma}_E$ for different $\overline{\gamma}_M$ and m_{S_M}

Figure 4 illustrates the IP versus MER for different m_{S_M} and m_{S_E}. It can be seen that the IP decreases with an increase of m_{S_M}. The IP of 10^{-3} can be achieved for MER values of about 22.5 dB, 17.5 dB, and 16.3 dB for m_{S_M} = 1.5, 5 and 50, respectively. In addition, we can note that moving from moderate shadowing (m_{S_M} = 5) toward heavy shadowing (m_{S_M} = 1.5), 5 dB is needed to keep the same security. However, moving from light shadowing (m_{S_M} = 50) toward moderate shadowing, only about 1.2 dB is needed. In the case of power domination of signal over main channel (high MER), the IP performance is better for a less severe shadowing over wiretap channel. For a lower values of MER, the IP increases which is in agreement with Fig. 2.

The influence of parameters α_M, α_E, μ_M and μ_E is depicted in Fig. 5. In the cases when average SNR from the main link dominates over the average SNR from the wiretap link, which presents real scenario, increasing of the consider channel parameters leads to a security benefits.

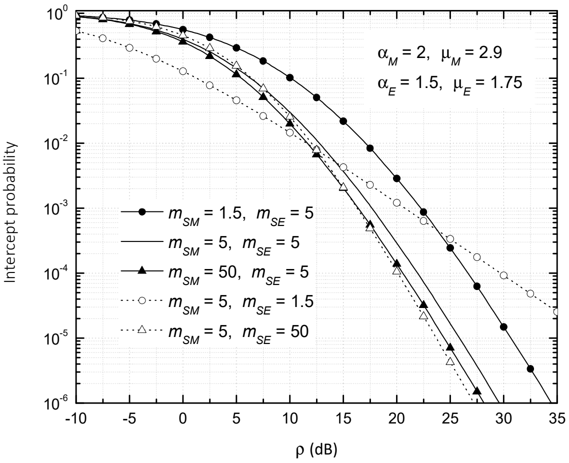

Fig. 4. IP versus ρ for different m_{S_M} and m_{S_E}

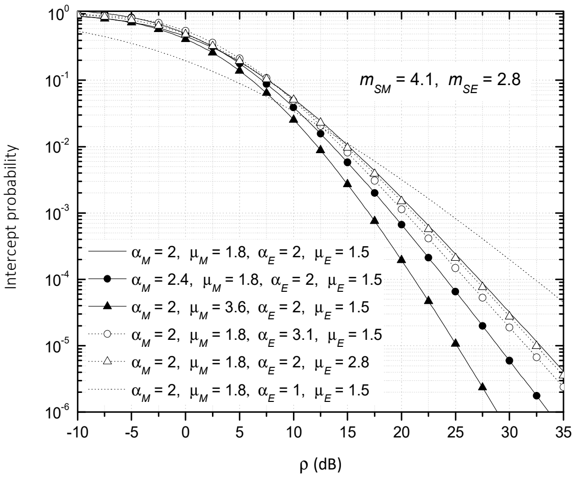

Fig. 5. IP versus ρ for different α_M , α_E , μ_M and μ_E

V. Conclusion

In the paper, a detail analysis of secrecy outage probability and the intercept probability for PLS over composite α-F fading channels is carried out. Obtained results showed that favorable channel conditions over main channel could upgrade the secure transmission. Lighter shadowing conditions over wiretap channel decreases the secrecy outage probability only in the regime of high SNRs of the main link. Also, less severe wiretap shadowing referrers to lower values of intercept probability and thus to the improvement of the system's secrecy. The advantage of proposed analysis is that it can be utilized for simplified fading scenarios which are special cases of α-F model.

Acknowledgement

This work has been supported by the Ministry of Education, Science and Technological Development of the Republic of Serbia.

References

[1] R. Liu, W. Trappe, *Securing Wireless Communications at the Physical Layer*, New York, Springer, 2009.

[2] Y. Zou, J. Zhu, X. Wang and L. Hanzo, "A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends", Proc. IEEE, vol. 104, no. 9, pp. 1727–1765, 2016.

[3] Y. Wu, A. Khisti, C. Xiao, G. Caire, K.K. Wong and X. Gao, "A Survey of Physical Layer Security Techniques for 5G Wireless Networks and Challenges Ahead", IEEE J. Sel. Areas Commun., vol. 36, no. 4, pp. 679–695, 2018.

[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. 1257-1261, 2015.

[5] L. Kong, H. Tran, and G. Kaddoum, "Performance Analysis of Physical Layer Security over α − μ Fading Channel", Electron. Lett., vol. 52, no. 1, pp. 45–47, 2016.

[6] G. Pan , C. Tang, X. Zhang, T. Li, Y. Weng and Y. Chen, "Physical-Layer Security Over Non-Small-Scale Fading", IEEE Trans. Veh. Technol., vol.65, no.3, pp. 1326 – 1339, 2016.

[7] H. Lei, I. S. Ansari, C. Gao, Y. Guo, G. Pan, and K. A. Qaraqe, "Physical Layer Security over Generalised-K Fading Channels", IET Commun., vol. 10, no. 16, pp. 2233–2237, 2016.

[8] J. M. Moualeu, D. B. da Costa, W. Hamouda, U. S. Dias and R. A. A. de Souza, "Physical Layer Security Over α-k-μ and α-η-μ Fading Channels", IEEE Trans. Veh. Technol., vol. 68, no. 1, pp. 1025-1029, 2019.

[9] J. Sun, X. Li, M. Huang, Y. Ding, J. Jin and G. Pan, "Performance Analysis of Physical Layer Security over k-μ Shadowed Fading Channels", IET Commun., vol. 12, no. 8, pp. 970-975, 2018.

[10] L. Kong and G. Kaddoum, "On Physical Layer Security over the Fisher-Snedecor F Wiretap Fading Channels". IEEE Access vol. 6, pp. 39466–39472, 2018.

[11] A.D. Wyner, "The Wire-tap Channel", Bell Syst. Tech. J., vol. 54, no. 8, pp. 1355–1387, 1975.

[12] O. S. Badarneh, "The *α-F* Composite Fading Distribution: Statistical Characterization and Applications", IEEE Trans. Veh. Technol., vol. 69, no. 8, pp. 8097-8106, 2020.

[13] I. S. Gradshteyn, I. M. Ryzhik, *Tables of Integrals, Series, and Products*, fifth edition, New York, Academic Press, 1994.

[14] The wolfram functions site, URL: ⟨http://functions.wolfram.com⟩.

[15] V. S. Adamchik, O. I. Marichev, "The Algorithm for Calculating Integrals of Hypergeometric Type Functions and Its Realization in Reduce System", ISSAC'90, Conference Proceedings, Tokyo, Japan, pp. 212-224, Tokyo, Japan, 1990.

[16] M. Bloch, J. Barros, M. Rodrigues, and S. McLaughlin, "Wireless Information-Theoretic Security", IEEE Trans. Inf. Theory, vol. 54, no. 6, pp. 2515-2534, 2008.

[17] A.M. Mathai, R.K. Saxena and H.J. Haubold, "The H-Function: Theory and Applications", first edition, Springer Science, New York, 2009.

[18] J.A. Anastasov, N. M. Zdravkovic, G.T. Djordjevic, "Outage Capacity Evaluation of Extended Generalized-K Fading Channel in the Presence of Random Blockage", J. Franklin Inst., vol. 352, no. 10, pp. 4610–4623, 2015.