FACTA UNIVERSITATIS
Series: **Automatic Control and Robotics** Vol. 21, Nº 2, 2022, pp. 117 - 130
https://doi.org/10.22190/FUACR220830010A

Regular Paper

PERFORMANCE OF SECURE COMMUNICATION OVER α-FISHER-SNEDECOR FADING CHANNELS

UDC (621.395.38+629.783)

Jelena Anastasov, Aleksandra Panajotović, Dejan Milić, Daniela Milović

University of Niš, Faculty of Electronic Engineering, Department of Telecommunications, Republic of Serbia

Abstract. *In this paper, we investigate the physical layer security (PLS) of the traditional Wyner's wiretap channel model. Secrecy performance analysis is performed assuming a presence of an active eavesdropper trying to overhear the confidential data transmission from the source node to the predefined destination. In what follows, we derive the lower bound of the secrecy outage probability, the strictly positive secrecy capacity as well as the average secrecy capacity, over the composite α-Fisher-Snedecor (α-F) fading environment. According to the analytical results, numerical results are also shown. The impact of the path loss component, the average signal-to-noise ratios over the main/wiretap channel as well as the impact of the fading, the non-linearity of the propagation medium and the shadowing shaping parameter on the PLS metrics is examined. The overall analysis and the obtained results have a high level of generality and also a high level of applicability since the α-F distribution was recently proposed, as the best fit distribution for the channel characterization of the device-to-device wireless communication in the future Beyond 5G networks.*

Key words: *Composite fading channel, physical layer security, device-to-device communication*

1. INTRODUCTION

The amount of wirelessly transmitted data constantly increases with rapid development of new emerging concepts and technologies such as the Internet-of-Things (IoT) and 6G [1]. Due to the open access property in wireless communications, it is of high significance to provide a secure data transmission, especially for private and sensitive data.

Received August 30, 2022 / Accepted September 27, 2022
Corresponding author: Jelena Anastasov
University of Niš, Faculty of Electronic Engineering, Department of Telecommunications, Aleksandra Medvedeva 14, 18000 Niš, Republic of Serbia
E-mail: jelena.anastasov@elfak.ni.ac.rs

Cryptography, as a built-in technique at system's upper layers, can be used to achieve this goal [2]. Cryptographic protocols promote a shared-key concept between authorized entities, which can be inconvenient in networks with massive number of devices. In addition, the eavesdroppers, as authorized or unauthorized users, usually own unlimited computing power and can easily break down confidential keys by utilizing the brute force attack method. This is why the cryptography requires to be strengthened.

The information-theoretic security has gained increased attention over the recent years by imposing the concept of secure data transmission on the physical layer [3]. The physical layer security (PLS) approach addresses the security issue by exploiting the dynamic characteristics of the propagation channel which is prone to eavesdropping [4]-[6]. In [7], Wyner had introduced the notion of the wiretap channel between the source (Alice) and an eavesdropper (Eve), who tries to intercept the intended transmission to a legitimate receiver (Bob).

Numerous PLS works are established to develop high secrecy rates for classic Wyner's wiretap channel model [8]-[17]. In all of the existing researches, the security performance is analysed using several metrics in the context of different wireless communication systems and over various fading channels. In what follows, a detailed PLS literature overview for basic wiretapped system model over fading channels, is given.

The strictly positive secrecy capacity (SPCS) has been determined in [8] over large open area with a line-of-sight between the transmitter and the receiver. The secure transmission between two nodes over α-μ fading channels, which include the non-linearity of propagation media, is analysed in [9], in terms of the average secrecy capacity (ASC). Novel analytical expressions for the SPSC and a lower bound on the secrecy outage probability (SOP) are derived over κ-μ fading channels, in [10], and further applied to performance studies of different emerging wireless applications, such as cellular device-to-device (D2D), vehicle-to-vehicle, peer-to-peer, and body centric communications. In addition, the expressions for the SPSC and a lower bound on SOP over a mixture of α-μ/κ-μ, and vice versa, fading channels are derived in [11].

The secrecy capacity for classic Wyner's wiretap model over a non-small scale fading channels, i.e. over the independent/correlated lognormal fading channels is investigated in [12]. A detailed analysis of all PLS metrics, that encompasses the interplay of both the fading and the shadowing phenomenon, over generalized-*K* fading channels, is given in [13], [14]. In [15], the SOP and the SPSC are analysed over shadowed κ-μ fading environment, with the aid of the moment matching method.

The Fisher-Snedecor (*F*) distribution was proposed in [16] to characterize the composite fading conditions over D2D communication channels at 5.8GHz, as less simple than the generalized-*K*. The SOP, the SPSC, the ASC and asymptotic ASC over *F* fading channels are investigated in [17], [18].

Recently, the author in [19] has proposed an even more general composite fading distribution, the α-Fisher-Snedecor (α-*F*) fading distribution that characterize, the nonlinearity of the propagation media, in addition to the fading and shadowing phenomena in the wireless channel. This model is pronounced as the best fit for the realistic channel measurements for D2D communications and underwater acoustic. To the best of authors' knowledge the PLS analysis over α-*F* fading has not yet been reported.

In this paper, we present the detailed PLS analysis of the basic wiretap model over α-*F* fading channels. Novel expressions for evaluating the asymptotic ASC, lower bound on the SOP and the exact SPSC are derived. These expressions are quite general and can be

simplified to Gamma, Weibull, Nakagami-*m*, exponential, α-μ, one-sided Gaussian and *F* fading scenarios. The interplay of various channels' parameters as well as the average SNRs over main/wiretap channel on the PLS is analysed.

The main contributions of this work can be summarized as:

- novel analytical forms of PLS metrics for source-destination-eavesdropper communication model, over general α-*F* fading channels, are given
- impact of the interplay of the fading depth, shadowing severity and nonlinearity parameter of the main/wiretap channel on secure transmission between the source and intended node, is examined
- in addition, the path loss component is taken into analysis
- presented results of α-*F* fading model can accommodate other existing fading scenarios, based on the estimate of α-*F* distribution parameters

The list of parameters, symbols and abbreviations throughout the paper is given in Table 1, to make easier for the reader to follow.

Table 1 List of notations, symbols, abbreviations

Notations, symbols, abbreviations	
$*$	designates: *M* for the main channel, *E* for the wiretap (eavesdropper's) channel
h_*	channel fading coefficient
γ_*	instantaneous signal-to-noise ratio (SNR)
d_*	distance from the source to the destination/eavesdropper
ξ	path loss parameter
m_{s_*}	shadowing severity factor
α_*	nonlinearity propagation factor
μ_*	fading depth parameter
$\overline{\gamma}_*$	average SNR
C_s	secrecy capacity
$\overline{C}_s$	average secrecy capacity (ASC)
ρ	average main-to-eavesdropper's channel power ratio (MER)
P_{out}^{EX}	exact secrecy outage probability (SOP)
P_{out}^{L}	lower bound of SOP
P_{nz}	strictly positive secrecy capacity (SPSC)
r	ratio between the main and wiretap link distances
$G_{p,q}^{m,n}(.)$	univariate Meijer's *G* function
$H_{p,q}^{m,n}(.)$	Fox's *H* function

2. PROBLEM FORMULATION

The system model we used in the analysis is shown in Fig.1. The source transmits the secret message by emitting signal $s(t)$, with $E[|s(t)|^2] = 1$, and therefore the signal received by the destination can be written in the following way

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

where P denotes the emitting power from the source, h_M represents a fading coefficient of the main channel i.e. the channel between the source and destination, and $n_M(t)$ denotes the additive white Gaussian noise (AWGN). The destination node is at the distance d_M from the source. The illegitimate node is also in the area of coverage, at the distance d_E from the source. The intruder tries to overhear the desired signal, and thus the receiving signal at the eavesdropper can be defined as

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

where h_E denotes a fading coefficient of the wiretap channel i.e. the channel between the source and eavesdropper, and $n_E(t)$ denotes the AWGN. The channel state information (CSI) of both channels is available at the source [3].

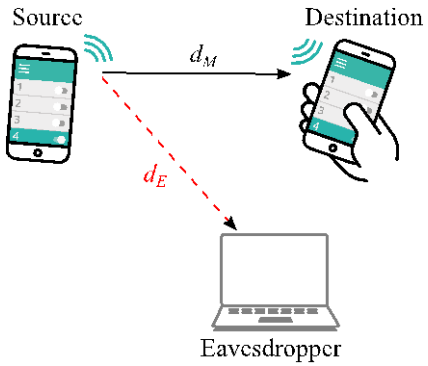

Fig. 1 System model

Let us express the instantaneous signal-to-noise-ratios (SNRs) over the main or wiretap link as

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

where the subscript, *, denotes either main (M), either eavesdropper's (E) channel index, σ_*^2 defines a variance of zero-mean AWGN and d_* denotes the distance between two nodes, while parameter ξ characterizes the path loss.

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 form [19]

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

where $\mathrm{B}(\cdot,\cdot)$ denotes the Beta function [20], $\overline{\gamma}_*$ 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 the parameter defined as

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

with $\Gamma(\cdot)$ being the Gamma function [20]. By utilizing the specific values of the Meijer's G function relying on [21, eq. (07.34.03.0271.01)] and the form of the argument simplification [21, eq. (07.34.16.0001.01)], the previous expression of the PDF can be rewritten as

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

with $a_*=\dfrac{(m_{s_*}-1)}{\mu_*\lambda_*^{\frac{\alpha_*}{2}}}$ and $G_{p,q}^{m,n}(.)$ denoting the univariate Meijer's G function [20, Eq. (9.301)]. The asymptotic PDF for the large average SNR values can be obtained with the help of [21, eq. (07.34.06.0001.01)], i.e. $\overline{\gamma}_*\to\infty$, and taking into account only the first term in summation, in the following form

$$p_{\gamma_*}^{asymp}(\gamma)=\frac{\alpha_*}{2B(\mu_*,m_{s_*})\gamma}\left(\frac{\gamma^{\frac{\alpha_*}{2}}}{a_*\overline{\gamma}_*^{\frac{\alpha_*}{2}}/d_*^{\xi}}\right)^{\mu_*}.\tag{7}$$

The cumulative distribution function (CDF) of the instantaneous SNR can be evaluated, relying on [22, Eq. (26)], as

$$F_{\gamma_*}(\gamma)=\frac{1}{\Gamma(\mu_*)\Gamma(m_{s_*})}G_{2,2}^{1,2}\left(\frac{\gamma^{\frac{\alpha_*}{2}}}{a_*\overline{\gamma}_*^{\frac{\alpha_*}{2}}/d_*^{\xi}}\middle|\begin{matrix}1-m_{s_*},1\\ \mu_*\quad,0\end{matrix}\right).\tag{8}$$

In addition, the asymptotic CDF when $\bar{\gamma}_* \to \infty$ can be defined by recalling [21, eq. (07.34.06.0001.01)], as

$$F_{\gamma_*}^{asymp}(\gamma) = \frac{1}{B(\mu_*, m_{s_*})\mu_*} \left(\frac{\mu_*}{a_* \bar{\gamma}_*^{\frac{\alpha_*}{2}} / d_*^{\xi}} \right)^{\mu_*} \gamma^{\frac{\alpha_* \mu_*}{2}}. \tag{9}$$

2. PHYSICAL LAYER SECURITY METRICS

In this Section, ASC, SOP and SPSC are analytically determined.
To evaluate the instantaneous channel capacity over the main channel as well as over the wiretap channel, we can rely on the Shannon capacity formula [3]

$$R_* = \log_2(1+\gamma_*). \tag{10}$$

The first step to establish the ASC expression is to start from secrecy capacity as defined in [4]. The secrecy capacity is characterize as a difference between the channel capacities of the main and wiretap links, i.e. mathematically

$$C_s = R_M - R_E = \log_2\left(\frac{1+\gamma_M}{1+\gamma_E}\right), \tag{11}$$

while assuming that the perfect CSIs are available at all nodes.

2.1. Analytical expression of ASC

ASC is frequently measured as a benchmark to indicate the average communication rate of the main transmission. The metric's definition can be given in the following form

$$\bar{C}_s = \iint_{\bar{D}} d\gamma_M d\gamma_E \log_2\left(\frac{1+\gamma_M}{1+\gamma_E}\right) p_M(\gamma_M) p_E(\gamma_E); \quad \bar{D} = \begin{cases} 0 \le \gamma_M < \infty \\ 0 \le \gamma_E < \gamma_M \end{cases}. \tag{12}$$

The previous formula can be rewritten as

$$\begin{aligned} \bar{C}_s &= \int_0^{\infty} d\gamma_M \, p_M(\gamma_M) \int_0^{\gamma_M} \log_2\left(\frac{1+\gamma_M}{1+\gamma_E}\right) p_E(\gamma_E) d\gamma_E \\ &= \mathrm{I}_1 + \mathrm{I}_2 - \mathrm{I}_3 \end{aligned}, \tag{13}$$

where the integrals are defined as
$\mathrm{I}_1 = \int_0^{\infty} \log_2(1+\gamma_M) p_M(\gamma_M) F_E(\gamma_M) d\gamma_M$, $\mathrm{I}_2 = \int_0^{\infty} \log_2(1+\gamma_E) p_E(\gamma_E) F_M(\gamma_E) d\gamma_E$ and $\mathrm{I}_3 = \int_0^{\infty} \log_2(1+\gamma_E) p_E(\gamma_E) d\gamma_E$. To avoid solutions of the integrals in a form of complex bivariate Meijer's *G* functions, as it was done for the wiretap Fisher-Snedecor channel scenario in [18], we have determined the simplified form of ASC. Namely, the first and the second integral are asymptotically solved in the following forms

$$\mathrm{I}_1^{\text{asymp}} = \frac{2^{\mu_M + m_{s_M} - 1} \mu_E^{\ \mu_E - 1}}{\ln(2)\Gamma(m_{s_M})\Gamma(\mu_M)(2\pi)^{\alpha_M} B(\mu_E, m_{sE})} \left(\frac{\lambda_E^{\frac{\alpha_E}{2}}}{(m_{s_E} - 1)\overline{\gamma}_E^{\frac{\alpha_E}{2}} / d_E^{\xi}} \right)^{\mu_E}$$

$$\times G_{2+2\alpha_M, 2+\alpha_M}^{2+2\alpha_M, 2+\alpha_M} \left(\left(\frac{\mu_M \lambda_M^{\frac{\alpha_M}{2}}}{(m_{s_M} - 1)\frac{\overline{\gamma}_M^{\frac{\alpha_M}{2}}}{d_M^{\xi}}} \right)^2 \middle| \begin{matrix} \frac{1 - m_{s_M}}{2}, \frac{2 - m_{s_M}}{2}; \Delta\left(\alpha_M, -\frac{\alpha_E \mu_E}{2}\right); \Delta\left(\alpha_M, -\frac{\alpha_E \mu_E}{2}\right) \\ \frac{\mu_M}{2}, \frac{\mu_M + 1}{2}; \Delta\left(\alpha_M, -\frac{\alpha_E \mu_E}{2}\right); \Delta\left(\alpha_M, -\frac{\alpha_E \mu_E}{2}\right) \end{matrix} \right) \quad (14)$$

and

$$\mathrm{I}_2^{\text{asymp}} = \frac{2^{\mu_E + m_{s_E} - 1} \mu_M^{\ \mu_M - 1}}{\ln(2)\Gamma(m_{s_E})\Gamma(\mu_E)(2\pi)^{\alpha_E} B(\mu_M, m_{sM})} \left(\frac{\lambda_M^{\frac{\alpha_M}{2}}}{(m_{s_M} - 1)\overline{\gamma}_M^{\frac{\alpha_M}{2}} / d_M^{\xi}} \right)^{\mu_M}$$

$$\times G_{2+2\alpha_E, 2+\alpha_E}^{2+2\alpha_E, 2+\alpha_E} \left(\left(\frac{\mu_E \lambda_E^{\frac{\alpha_E}{2}}}{(m_{s_E} - 1)\frac{\overline{\gamma}_E^{\frac{\alpha_E}{2}}}{d_E^{\xi}}} \right)^2 \middle| \begin{matrix} \frac{1 - m_{s_E}}{2}, \frac{2 - m_{s_E}}{2}; \Delta\left(\alpha_E, -\frac{\alpha_M \mu_M}{2}\right); \Delta\left(\alpha_E, 1 - \frac{\alpha_M \mu_M}{2}\right) \\ \frac{\mu_E}{2}, \frac{\mu_E + 1}{2}; \Delta\left(\alpha_E, -\frac{\alpha_M \mu_M}{2}\right); \Delta\left(\alpha_E, -\frac{\alpha_M \mu_M}{2}\right) \end{matrix} \right), \quad (15)$$

where $\Delta(s,t) = \frac{t}{s}, \frac{t+1}{s}, \cdots, \frac{t+s-1}{s}$ and when $\alpha_M, \alpha_E \in N^+$. The expressions (14) and (15) are obtained by substituting the asymptotic forms of CDFs in I_1 and I_2, and then recalling [21, eq.(07.34.21.0011.01)]. The third integral is solved by substituting (6) into I_3, and with the help of [23, eq. (2.24.1.1)] in the following way

$$\mathrm{I}_3 = \frac{2^{\mu_E + m_{s_E} - 1}}{\ln(2)\Gamma(m_{s_E})\Gamma(\mu_E)(2\pi)^{\alpha_E}}$$

$$\times G_{2+2\alpha_E, 2+\alpha_E}^{2+2\alpha_E, 2+\alpha_E} \left(\frac{\mu_E \lambda_E^{\frac{\alpha_E}{2}}}{(m_{s_E} - 1)\overline{\gamma}_E^{\frac{\alpha_E}{2}} / d_E^{\xi}} \middle| \begin{matrix} \frac{1 - m_{s_E}}{2}, \frac{2 - m_{s_E}}{2}; 0, \cdots, \frac{\alpha_E - 1}{\alpha_E}; \frac{1}{\alpha_E}, \cdots, \frac{\alpha_E}{\alpha_E} \\ \frac{\mu_E}{2}, \frac{\mu_E + 1}{2}; 0, \cdots, \frac{\alpha_E - 1}{\alpha_E}; 0, \cdots, \frac{\alpha_E - 1}{\alpha_E} \end{matrix} \right). \quad (16)$$

Thus, by summarizing (14), (15) and (16), the asymptotic ASC is determined.

2.2. Analytical expression of SOP

In the scenario with both the active/passive eavesdropping, SOP is very often measured to indicate conceptually the security of the authorized communication. From the information-theory point of view, SOP is a secrecy outage event when secrecy capacity falls below the target secrecy rate, R_t. Thus, SOP can be defined in the exact form, as [18]

$$P_{out}^{EX} = \Pr[C_s < R_t] = \Pr[\gamma_M \le R_s\gamma_E + R_s - 1], \tag{17}$$

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 [18]

$$\begin{aligned} P_{out}^{L} &= \Pr[\gamma_M \le R_s\gamma_E] \le P_{out} = \\ &= \int_0^{\infty}\int_0^{R_s\gamma_E} p_M(\gamma_M)\,p_E(\gamma_E)\,d\gamma_E\,d\gamma_M \\ &= \int_0^{\infty} F_M(R_s\gamma_E)\,p_E(\gamma_E)\,d\gamma_E. \end{aligned} \tag{18}$$

By substituting (8) and (6) with appropriate subscripts in (18), and with the help of [21, 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

$$\begin{aligned} P_{out}^{L} &= \frac{\alpha_M}{2\Gamma(m_{s_E})\Gamma(m_{s_M})\Gamma(\mu_E)\Gamma(\mu_M)} \\ &\times H_{3,3}^{2,3}\left(R_s^{\frac{\alpha_M\alpha_E}{2}} \frac{a_E^{\alpha_M} r}{a_M^{\alpha_E}\rho^{\frac{\alpha_M\alpha_E}{2}}} \middle| \begin{matrix} (1-m_{s_M},1),(1,1),\left(1-\mu_E,\frac{\alpha_M}{\alpha_E}\right) \\ (\mu_M,1),\left(1+m_{s_E},\frac{\alpha_M}{\alpha_E}\right),(0,1) \end{matrix} \right), \end{aligned} \tag{19}$$

where $\rho = \bar{\gamma}_M / \bar{\gamma}_E$ defines the average main-to-eavesdropper's channel power ratio (MER), r denotes the ratio between the main and wiretap link distances, $r=d_M/d_E$, and $H_{p,q}^{m,n}(.)$ is the notation of the Fox's H function [24, eq. (1.2)]. The Fox's H function is not commonly built-in function in *Mathematica* or *Matlab* software packages, but can be evaluated with the help of the program given in [25, Appendix]. Formula (19) can be rewritten in the simplified form of the Meijer's G function, when $\alpha_M, \alpha_E \in N^+$, relying on [23, eq. (8.3.2.22)]], in the following form

$$\begin{aligned} P_{out}^{L} &= \frac{\alpha_E^{\mu_M+m_{s_M}-1}\alpha_M^{\mu_E+m_{s_E}-1}}{(2\pi)^{\alpha_E+\alpha_M-2}\Gamma(m_{s_E})\Gamma(m_{s_M})\Gamma(\mu_E)\Gamma(\mu_M)} \\ &\times G_{2\alpha_E+\alpha_M,2\alpha_E+\alpha_M}^{\alpha_E+\alpha_M,2\alpha_E+\alpha_M}\left(R_s^{\frac{\alpha_M\alpha_E}{2}} \frac{a_E^{\alpha_M} r}{a_M^{\alpha_E}\rho^{\frac{\alpha_M\alpha_E}{2}}} \middle| \begin{matrix} \Delta(\alpha_E,1-m_{s_M}),\Delta(\alpha_E,1),\Delta(\alpha_M,1-\mu_E) \\ \Delta(\alpha_E,\mu_M),\Delta(\alpha_M,1-(1-m_{sE})),\Delta(\alpha_E,0) \end{matrix} \right). \end{aligned} \tag{20}$$

2.3. Analytical expression of SPSC

The existence of non-zero secrecy capacity i.e. SPSC is assured with the probability given by

$$\begin{aligned} P_{nz} &= \Pr[\gamma_M > \gamma_E] = \\ &= \int_0^{\infty} F_E(\gamma_M)\,p_M(\gamma_M)\,d\gamma_M. \end{aligned} \tag{21}$$

Thus, by substituting (8) and (6) in (21) and once more recalling [21, eq. (07.34.21.0012.01)], we have derived SPSC in the following form

$$P_{nz} = \frac{\alpha_E}{2\Gamma(m_{s_E})\Gamma(m_{s_M})\Gamma(\mu_E)\Gamma(\mu_M)} \times H_{3,3}^{2,3}\left(\frac{a_M^{\alpha_E}\rho^{\frac{\alpha_M\alpha_E}{2}}}{a_E^{\alpha_M} r} \middle| \begin{matrix} (1-m_{s_E},1),(1,1),\left(1-\mu_M,\frac{\alpha_E}{\alpha_M}\right) \\ (\mu_E,1),\left(1+m_{s_M},\frac{\alpha_M}{\alpha_E}\right),(0,1) \end{matrix} \right). \quad (22)$$

By simplifying the Fox's H function with the help of [23, eq. (8.3.2.22)]], SPSC is rewritten in the following form as

$$P_{nz} = \frac{\alpha_E}{2\Gamma(m_{s_E})\Gamma(m_{s_M})\Gamma(\mu_E)\Gamma(\mu_M)} \times G_{2\alpha_M+\alpha_E,2\alpha_M+\alpha_E}^{\alpha_M+\alpha_E,2\alpha_M+\alpha_E}\left(\frac{a_M^{\alpha_E}\rho^{\frac{\alpha_M\alpha_E}{2}}}{a_E^{\alpha_M} r} \middle| \begin{matrix} \Delta(\alpha_M,1-m_{s_E},),\Delta(\alpha_M,1),\Delta(\alpha_E,1-\mu_M) \\ \Delta(\alpha_M,\mu_E),\Delta(\alpha_E,1-(1-m_{sM})),\Delta(\alpha_M,0) \end{matrix} \right). \quad (23)$$

3. NUMERICAL RESULTS

In this section, numerical results of ASC, SOP and SPSC are presented to illustrate the carried out mathematical analysis. Numerical results are obtained using *Mathematica* and figures are drawn in *Origin* software package. In all figures, the path loss parameter is ξ=2.7, which is a commonly used value for the parameter that describes the path loss in a fading environment.

Fig. 2 illustrates ASC versus MER, ρ, for different space constellations of the destination and eavesdropper; and identically distributed (i.d.) fading links, $\alpha_M = \alpha_E = \alpha$, $m_{sM} = m_{sE} = m_s$, $\mu_M = \mu_E = \mu$. For higher values of the ratio r, i.e. when eavesdropper is closer to the source, the ASC values are lower, as expected. Also, as the fading depth, the nonlinearity as well as the shadowing severity over the propagation medium decreases (m_s, α and μ increase), ASC outperforms. In a more realistic scenario, when the destination is closer to the source in comparison to the eavesdropper's position (r=0.8), the most favorable channel conditions (α=3.4, m_s=4.8, μ=3.8) indicates lower or at least the same ASC values than less favorable channels case (α=2.4, m_s=3.8, μ=2.8). This i.d. channel feature can be utilized by the PLS approach in order to ensure a secure transmission. In this figure, the asymptotes are also obtained according to expressions (14), (15) and (16). The asymptotes show a good agreement with the exact results, especially for favorable channel conditions and favorable space constellation of nodes.

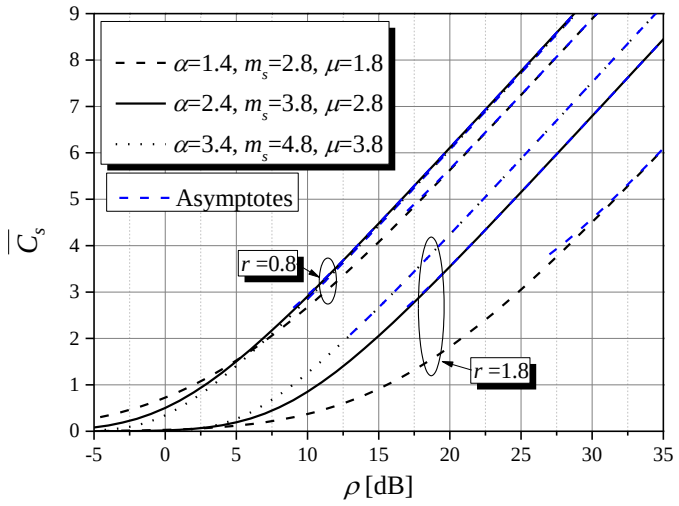

Fig. 2 The ASC vs. MER for different channel conditions and different distances of receiving nodes

SPSC in the function of the average SNR of the main channel for different average SNRs of the wiretap channel is shown in Fig. 3. One can notice that SPSC can be improved by assuring larger average SNR values of the main channels and/or lower average SNRs of the wiretap channel. The improvement is more obvious for higher nonlinearity parameter of the main channel, α_M= 5, i.e. for lower nonlinearity of the main propagation medium.

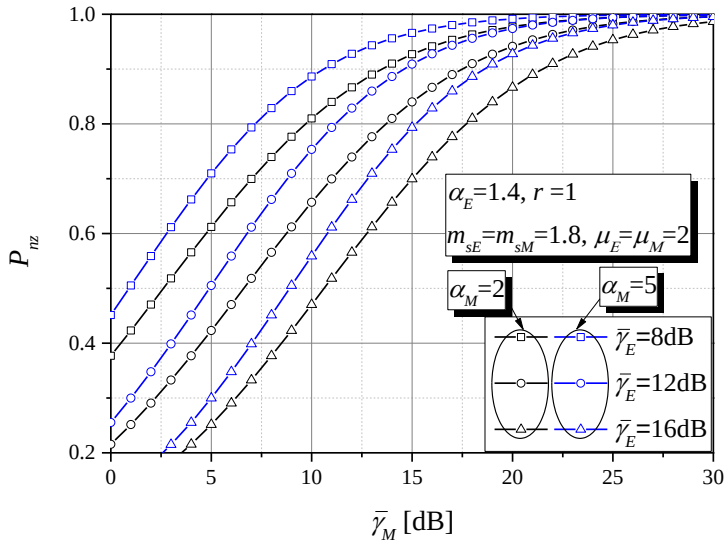

Fig. 3 SPSC vs. the average SNR values of the main channel for different nonlinearity propagation scenarios

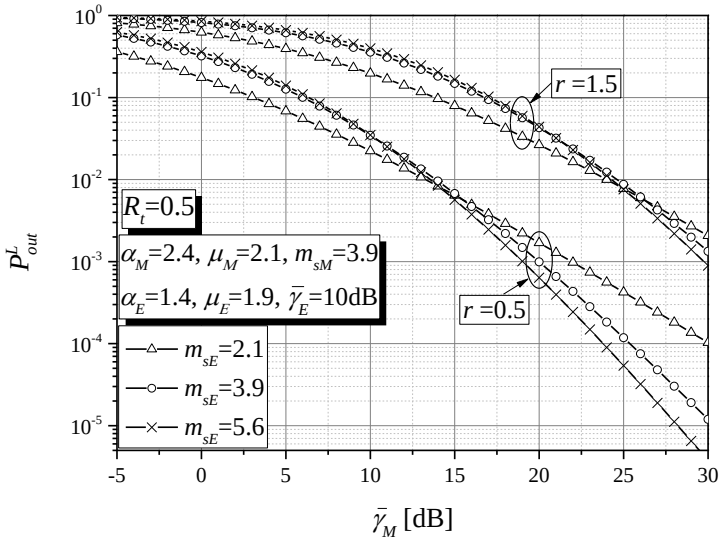

Fig. 4 Lower bound of SOP vs. the average SNR values of the main channel for different distances' ratios

The lower bound of SOP, versus the average SNRs of the main channel for different distance ratios and different fading depth scenarios over the wiretap channel, is demonstrated in Fig. 4. An interesting remark here is that up to some point the largest fading deepness over the wiretap channel assures the lowest SOP values, and then the interplay of the same fading parameter, m_{sE}, is vice versa. This is more obvious when the destination is closer to the source. For instance, when r=0.5 the value of the average SNR over the main channel is around 15dB ($\bar{\gamma}_M = 15\text{dB}$), after which the favorable fading conditions over the wiretap channel impacts beneficially the SOP metric. In addition, when r=1.5, the $\bar{\gamma}_M$ is shown to be around 25dB ($\bar{\gamma}_M = 25\text{dB}$). This result justifies the PLS principle how to deploy effectively the randomness of the wireless channels, i.e. fading to upgrade the system security issue.

ASC in the function of the average SNR over wiretap channel for different nonlinearity propagation cases is presented in Fig. 5. The largest ASC values are obtained for larger average SNRs of the main channel in the region of lower average SNR values of the wiretap channel. It can be noticed that by increasing the nonlinearity parameter α_E, the nonlinearity of the wiretap propagation medium decreases, and thus the ASC decreases i.e. deteriorates. In the case of $\alpha_M = \alpha_E$=2, the results coincide with those for F fading scenario.

In Fig. 6, SPSC versus the distance ratio r for different shadowing scenarios over the main channel and different MER regimes, is illustrated. The increase in MER leads to an increase of SPSC and even equals one for λ=19dB, when the destination node is closer to the source. The SPSC dependence on the shadowing severity over the main channel is more pronounced in the range of lower MERs. For instance, for λ=19dB the aforementioned dependence is insignificant. Further, for λ=14dB, when m_{sM} increases from m_{sM}=1.4 to m_{sM} =3.4, and r=1.2, the increase of less than a half order of magnitude of the SPSC can be noticed; and an increase of even one order of magnitude is noticeable for λ=9dB.

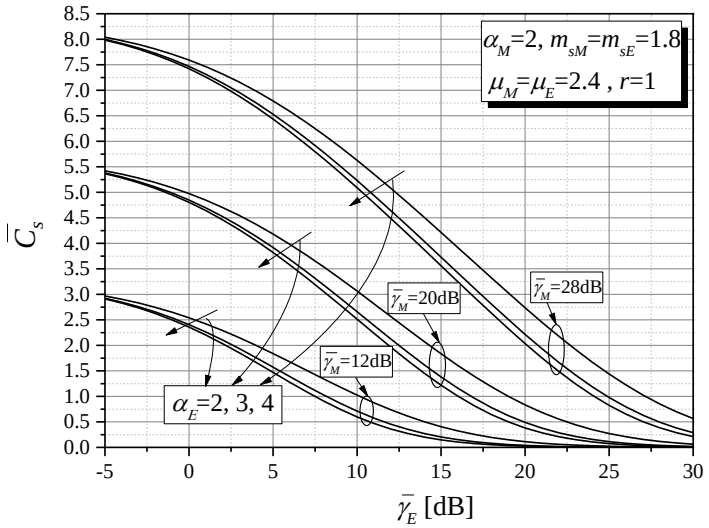

Fig. 5 ASC vs. the average SNR over the wiretap channel for different wiretap nonlinearity propagation scenarios

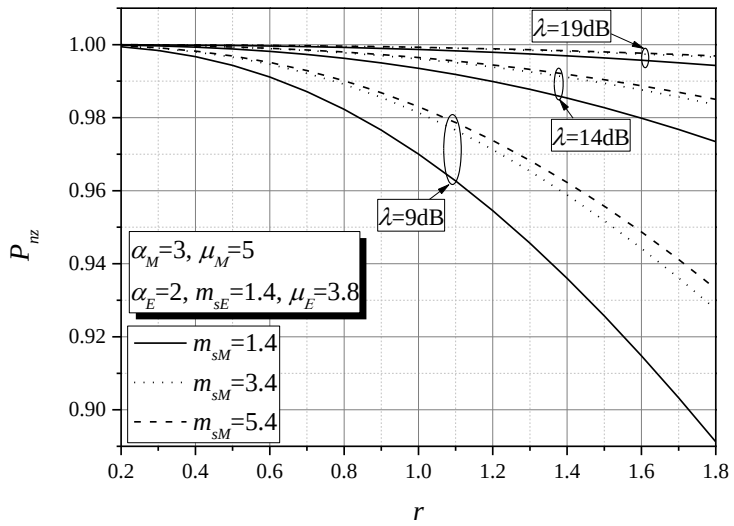

Fig. 6 SPSC vs. the distance ratio, r, for different MERs and different shadowing scenarios over the main channel

4. CONCLUSION

In the paper, the detailed analysis of basic PLS metrics over composite α-F fading channels was carried out. The obtained results showed that favorable channel conditions over main channel could upgrade the secure transmission. In addition, for i.d. fading channels, the impact of the fading depth, the propagation nonlinearity and the shadowing

severity depends on the space constellation of the system's nodes. Another concluding remark, assuming non i.d. fading channels is that the largest fading deepness over the wiretap channel assures the lowest SOP values, up to some specific value of $\bar{\gamma}_M$, and then the interplay of the same fading parameter is vice versa. This is obtained when the destination is closer to the source. Also, for the same constellation scenario, the SPSC dependence on the shadowing severity over the main channel is more pronounced in the range of lower MER values.

In overall, the obtained results can be useful in the design of securer wireless D2D communication links. Also, proposed analysis has high level of generality and can be utilized in analysis for fading scenarios which are special cases of the α-F fading model.

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

REFERENCES

[1] W. Saad, M. Bennis, and M. Chen, "A vision of 6G wireless systems: Applications, trends, technologies, and open research problems," IEEE Network, vol. 34, no. 3, pp. 134–142, May 2020., doi: 10.1109/MNET.001.1900287.

[2] B. Schneier, "Cryptographic design vulnerabilities," Computer, vol. 31, no. 9, pp. 29-33, Sept. 1998., do: 10.1109/2.708447.

[3] M. Bloch, J. Barros, M. Rodrigues, and S. McLaughlin, "Wireless Information-Theoretic Security", IEEE Transaction of Information Theory, vol. 54, no. 6, pp. 2515-2534, 2008., doi: 10.1109/TIT.2008.921908.

[4] R. Liu, W. Trappe, Securing wireless communications at the physical layer, New York, Springer, 2009.

[5] Y. Zou, J. Zhu, X. Wang and L. Hanzo, "A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends," Proceedings of the IEEE, vol. 104, no. 9, pp. 1727–1765, 2016., doi: 10.1109/JPROC.2016.2558521.

[6] 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 Journal on Selected Areas in Communications, vol. 36, no. 4, pp. 679–695, 2018. doi: 10.1109/JSAC.2018.2825560.

[7] A.D. Wyner, "The Wire-tap Channel," The Bell System Technical Journal, vol. 54, no. 8, pp. 1355–1387, 1975., doi: 10.1002/j.1538-7305.1975.tb02040.x

[8] X. Liu, "Probability of Strictly Positive Secrecy Capacity of the Rician-Rician Fading Channel," IEEE Wireless Communications Letters, vol. 2, no. 1, pp. 50-53, February 2013., doi: 10.1109/WCL.2012. 101812.120660.

[9] L. Kong, H. Tran, and G. Kaddoum, "Performance Analysis of Physical Layer Security over α − μ Fading Channel," Electronics Letters, vol. 52, no. 1, pp. 45–47, 2016., doi: 10.1049/el.2015.2160.

[10] N. Bhargav, S. L. Cotton, and D. E. Simmons, "Secrecy capacity analysis over k-μ fading channels: Theory and applications," IEEE Transactions on Communications, vol. 64, no. 7, pp. 3011–3024, Jul. 2016., doi: 10.1109/TCOMM.2016.2565580.

[11] 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 Transactions on Vehicular Technology, vol. 68, no. 1, pp. 1025-1029, 2019., doi: 10.1109/TVT.2018.2884832.

[12] G. Pan , C. Tang, X. Zhang, T. Li, Y. Weng and Y. Chen, "Physical-Layer Security Over Non-Small-Scale Fading," IEEE Transactions on Vehicular Technology, vol.65, no.3, pp. 1326 – 1339, 2016., doi: 10.1109/TVT.2015.2412140.

[13] H. Lei, I. S. Ansari, C. Gao, Y. Guo, G. Pan, and K. A. Qaraqe, "Physical Layer Security over Generalised-K Fading Channels," IET Communications, vol. 10, no. 16, pp. 2233–2237, 2016., doi: 10.1049/iet-com.2015.0384.

[14] H. Zhao, Y. Liu, A. Sultan-Salem and M. -S. Alouini, "A Simple Evaluation for the Secrecy Outage Probability Over Generalized-K Fading Channels," IEEE Communications Letters, vol. 23, no. 9, pp. 1479-1483, Sept. 2019., doi: 10.1109/LCOMM.2019.2926360.

[15] 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 Communications, vol. 12, no. 8, pp. 970-975, 2018., doi: 10.1049/iet-com.2017.1268.

[16] S. K. Yoo, S. L. Cotton, P. C. Sofotasios, M. Matthaiou, M. Valkama and G. K. Karagiannidis, "The Fisher–Snedecor F Distribution: A Simple and Accurate Composite Fading Model," IEEE Communications Letters, vol. 21, no. 7, pp. 1661-1664, July 2017., doi: 10.1109/LCOMM.2017.2687438.

[17] O. S. Badarneh, P. C. Sofotasios, S. Muhaidat, S. L. Cotton, K. Rabie, and N. Al-Dhahir, "On the secrecy capacity of Fisher-Snedecor F fading channels," in Proc. *2018 14th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, 2018., doi: 10.1109/WiMOB.2018.8589137.

[18] 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., doi: 10.1109/ACCESS.2018.2853700.

[19] O. S. Badarneh, "The α-F Composite Fading Distribution: Statistical Characterization and Applications," IEEE Transactions on Vehicular Technology, vol. 69, no. 8, pp. 8097-8106, 2020., doi: 10.1109/TVT.2020.2995665.

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

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

[22] 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.

[23] A. P. Prudnikov, Y. A. Brychkov, and O. I. Marichev, *Integral and Series: Volume 3, More Special Functions*, New York: CRC Press Inc, 1990.

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

[25] J.A. Anastasov, N. M. Zdravkovic, and G.T. Djordjevic, "Outage Capacity Evaluation of Extended Generalized-K Fading Channel in the Presence of Random Blockage," Journal of Franklin Institute, vol. 352, no. 10, pp. 4610–4623, 2015., doi:10.1016/j.jfranklin.2015.07.008.