Cascaded κ-μ Fading Channels with Colluding Eavesdroppers: Physical-Layer Security Analysis

Deemah H. Tashman and Walaa Hamouda
Department of Electrical and Computer Engineering Concordia University, Montreal, Canada
Email: {d_tashma, hamouda}@ece.concordia.ca

***Abstract*—This paper studies the physical-layer security (PLS) of a system model consisting of a transmitter, a receiver, and multiple eavesdroppers. Cascaded general fading channel, which is the κ-μ distribution is assumed at the main and the wiretap links of the network. The impacts of the cascade level, the number of eavesdroppers attempting to overhear the confidential information, and the wiretap channel's parameters on the system's secrecy are investigated. Two of the main secrecy metrics are used to evaluate the secrecy level of the system, which are the secrecy outage probability (OP_{sec}) and the probability of non-zero secrecy capacity (P_{nsc}). Exact and asymptotic form expressions for (OP_{sec}) and (P_{nsc}) are derived. Asymptotic analysis is performed to gain a clear vision about the impact of some key parameters over the secrecy. The results show that the fading channel cascade level has a significant effect on the system's secrecy. Also, the results show that the system is less protected when increasing the number of eavesdroppers or when improving the wiretap channel's conditions. Analytical results are validated using Monte-Carlo simulations.**

***Index Terms*—Cascaded general fading channels, physical-layer security, probability of non-zero secrecy capacity, secrecy outage probability.**

I. Introduction

NETWORK security is expected to be an important factor in the 5G since it is supposed to support a huge number of connections [1], [2]. Up until now, the methods used to enhance the secrecy of the networks have been heavily dependent on the cryptography approach implemented in the upper layers of the network. However, security methods based on encryption approaches have several drawbacks especially for 5G communications. For instance, the added software and hardware complexity of these approaches to the network since high processing power is needed [3]. Therefore, physical-layer security (PLS) has become a very interesting alternative for investigating and improving the security of the exchange of confidential information between legitimate ends in 5G [4]. As PLS does not depend on encryption and decryption techniques, there is no need for the exchange of security keys. PLS methods exploits wireless media characteristics between legitimate ends, such as fading [4]. PLS was first addressed by Shannon [5] and further explored later by Wyner [6] and it clearly shows that security of the data is guaranteed if the channel between legitimate users has better conditions than the channel exists between the transmitter and the attackers [7].

General fading distributions, such as κ-μ fading have been verified via field measurement campaigns to better fit the experimental data compared to other known distributions, such as Rician and Nakagami-m [8]. κ-μ distribution suits the line-of-sight (LOS) applications and it is defined by two physical parameters, which are κ and μ. $\kappa > 0$ is defined as the ratio between the total power of the dominant components and the power of the scattered waves, while $\mu > 0$ represents the number of the multipath clusters. κ-μ fading channel is known for its flexibility as it includes some of the well-known channels as special cases, such as Rician, Rayleigh, Nakagami-m, and the one-sided Gaussian distributions [8].

Cascaded fading channels have gained interest as they can be used to model the channel for various communication systems, such as mobile-to-mobile (M2M) communications, multi-hop cooperative communications, and radio frequency identification pinhole channels [3]. For example, double Rayleigh fading channels have been used to model the propagation through keyhole channels in multiple-input-multiple-output (MIMO) systems [9], M2M communications and vehicular communications [10], [11]. Cascaded fading channels exist when the transmitter and the receiver are in rich scattering areas. Cascaded fading channels are also called multiplicative channels as the channel gain at the receiver end is generated by the multiplication of a high number of rays reflected from the scatters between the transmitter and the receiver [12].

Recently, PLS has been extensively used with different fading channel models. In [13] and [14], PLS was studied for generalised-k and for Weibull fading channels, respectively. PLS for Rician fading channels was studied in [15]. Lately, PLS was studied for some systems where cascaded fading channels are employed. PLS for cascaded Nakagami-m fading channels was studied in [3] and [16]. Cascaded α-μ fading channel was used in [10] to study the system's secrecy. Secrecy was also investigated for cascaded Rayleigh fading channels in [17]. PLS was studied over cascaded κ-μ fading channels over the main link only in [18].

To the best of the authors knowledge, no work has considered studying PLS for a network where cascaded κ-μ fading channels are assumed at the main and the wiretap links with multiple eavesdroppers. Hence, we focus on studying the PLS for a three-node wiretap system; a transmitter, a receiver and several colluding eavesdroppers (or a single eavesdropper with multiple numbers of antennas). Colluding eavesdroppers each equipped with a single antenna can be replaced by a single eavesdropper with multiple antennas since colluding eavesdroppers perform joint processing over the intercepted information [19]. The eavesdropper receiver is assumed to use

978-1-7281-6535-6/20/$31.00 ©2020 IEEE

maximal-ratio combining (MRC) over the received signals to enhance the received signal-to-noise-ratio (SNR). The channels are modeled as cascaded κ-μ fading channels. Two major PLS metrics are used in this paper, which are the secrecy outage probability (OP_{sec}) and the probability of non-zero secrecy capacity (P_{nsc}). Exact and asymptotic expressions for (OP_{sec}) and (P_{nsc}) are derived. The effect of the cascade level of the channels over these metrics is studied. Moreover, the effect of the number of eavesdroppers and the wiretap channel's conditions over the secrecy of the system are also considered.

The paper is organized as follows; section II represents the system model and the PLS analysis over the cascaded κ-μ fading channels. Section III includes the analytical and simulation results. Conclusions are given in section IV.

II. Physical-Layer Security Analysis

In this section, PLS is investigated for a three-node network. Assume we have a transmitter (Alice) trying to communicate with a receiver (Bob) over the main channel (the one between Alice and Bob). Multiple colluding eavesdroppers may be considered as a single eavesdropper (E) equipped with multi-antennas. E is trying to overhear the confidential information sent from Alice through the wiretap channel (the one between Alice and E). The main and the wiretap channels are assumed to follow the cascaded κ-μ fading distribution (see Fig. 1). The received signal at the legitimate receiver (Bob) is given by

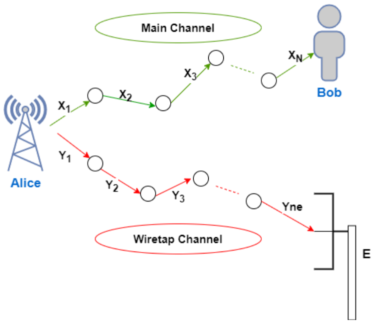

Fig. 1. The system model.

$$y_m = \sqrt{P} Z_N x + w_m, \tag{1}$$

where P is the transmit power. x is the transmitted symbol at Alice and w_m is the AWGN at the receiver with zero mean and variance N_0. Z_N is the channel gain for the main link, which is defined by $Z_N = \prod_{i=1}^{N} X_i$. X_i is a set of independent κ-μ random variables (RVs) with the parameters κ_i and μ_i $(i \in \{1, 2, \cdots, N\})$. Hence, Z_N follows cascaded $\kappa-\mu$ fading with the following probability density function (PDF) [18]

$$\begin{aligned} f_{Z_N}(z) \;=\; & \sum_{v_1=0}^{\infty} \sum_{v_2=0}^{\infty} \cdots \sum_{v_N=0}^{\infty} a_1 z^{2\mu_1 + 2v_1 - 1} \\ & \times \; G_{N\ 0}^{0\ N} \left(\begin{matrix} \epsilon \\ - \end{matrix} \middle| \frac{1}{z^2 \prod_{i=1}^{N} \mu_i (1+\kappa_i)} \right), \end{aligned} \tag{2}$$

where $G_{p\ q}^{m\ n}\left(\begin{smallmatrix} a_r \\ b_s \end{smallmatrix} \middle| z\right)$ is the Meijer G-function defined in [20, Eq. 9-301], $\epsilon = \mu_1 - \mu_2 + v_1 - v_2 + 1, \cdots, \mu_1 - \mu_N + v_1 - v_N + 1, 1$, and

$$\begin{aligned} a_1 = 2 \prod_{i=1}^{N} & \left[\frac{\left[\mu_i (1+\kappa_i)\right]^{\mu_1 - \mu_i + v_1 - v_i} \mu_i (1+\kappa_i)^{\frac{\mu_i + 1}{2}}}{\kappa_i^{\frac{\mu_i - 1}{2}} \exp(\kappa_i \mu_i) \Gamma(v_i + \mu_i)} \right] \\ \times \prod_{i=1}^{N} & \left[\frac{\left[2\mu_i \sqrt{\kappa_i (1+\kappa_i)}\right]^{2v_i + \mu_i - 1}}{(v_i)! 2^{2v_i + \mu_i - 1}} \right]. \end{aligned}$$

The cumulative distribution function (CDF) of the RV Z_N is given by [18]

$$\begin{aligned} F_{Z_N}(z) = & \sum_{v_1=0}^{\infty} \sum_{v_2=0}^{\infty} \cdots \sum_{v_N=0}^{\infty} \frac{a_1}{2} z^{2(\mu_1 + v_1)} \\ & \times G_{1\ N+1}^{N\ 1} \left(\begin{matrix} 1-\mu_1-v_1 \\ \rho \end{matrix} \middle| z^2 \prod_{i=1}^{N} \mu_i (1+\kappa_i) \right), \end{aligned} \tag{3}$$

where $\rho = -\mu_1 + \mu_2 - v_1 + v_2, \cdots, -\mu_1 + \mu_N - v_1 + v_N, 0, -\mu_1 - v_1$. The intercepted message at E is given by

$$y_{E,k} = \sqrt{P} Z_{E,k} x + w_{E,k}, \tag{4}$$

where $w_{E,k}$ is the AWGN at the k^{th} antenna of E with zero mean and variance N_0. $Z_{E,k}$ is the channel gain for the wiretap link, which is the one between Alice and the k^{th} antenna of E for $k = 1, 2, \cdots, K$. K is the number of eavesdroppers (number of antennas at E). $Z_{E,k}$ is defined by $Z_{E,k} = \prod_{j=1}^{n_e} Y_j^{(k)}$. $Y_j^{(k)}$ is a set of independent κ-μ RVs with the parameters $\kappa_{ej}^{(k)}$ and $\mu_{ej}^{(k)}$ $(j \in \{1, 2, \cdots, n_e\})$ for the k^{th} link. Hence, $Z_{E,k}$ follows the cascaded $\kappa-\mu$ fading distribution with the following PDF

$$\begin{aligned} f_{Z_{E,k}}(z_e) = & \sum_{r_1^{(k)}=0}^{\infty} \sum_{r_2^{(k)}=0}^{\infty} \cdots \sum_{r_{n_e}^{(k)}=0}^{\infty} a_2^{(k)} z_e^{2\mu_{e1}^{(k)} + 2r_1^{(k)} - 1} \\ & \times G_{n_e^{(k)}\ 0}^{0\ n_e^{(k)}} \left(\begin{matrix} \beta_e^{(k)} \\ - \end{matrix} \middle| \frac{1}{z_e^2 \prod_{j=1}^{n_e^{(k)}} \mu_{ej}^{(k)} \left(1+\kappa_{ej}^{(k)}\right)} \right), \end{aligned} \tag{5}$$

where $\beta_e^{(k)} = \mu_{e1}^{(k)} - \mu_{e2}^{(k)} + r_1^{(k)} - r_2^{(k)} + 1, \cdots, \mu_{e1}^{(k)} - \mu_{en_e}^{(k)} + r_1^{(k)} - r_{n_e}^{(k)} + 1, 1$ and

$$a_2^{(k)} = 2 \prod_{j=1}^{n_e^{(k)}} \left[\frac{\left[\mu_{ej}^{(k)} \left(1+\kappa_{ej}^{(k)}\right)\right]^{\mu_{e1}^{(k)} - \mu_{ej}^{(k)} + r_1^{(k)} - r_j^{(k)}} \mu_{ej}^{(k)}}{{\kappa_{ej}^{(k)}}^{\frac{\mu_{ej}^{(k)}-1}{2}} \exp\left(\kappa_{ej}^{(k)} \mu_{ej}^{(k)}\right) \Gamma\left(r_j^{(k)} + \mu_{ej}^{(k)}\right)} \right]$$
$$\times \prod_{j=1}^{n_e^{(k)}} \left[\frac{\left[2\mu_{ej}^{(k)} \sqrt{\kappa_{ej}^{(k)} \left(1+\kappa_{ej}^{(k)}\right)}\right]^{2r_j^{(k)} + \mu_{ej}^{(k)} - 1}}{(r_j^{(k)})! 2^{2r_j^{(k)} + \mu_{ej}^{(k)} - 1}} \right]$$
$$\times \prod_{j=1}^{n_e^{(k)}} \left[\left(1+\kappa_{ej}^{(k)}\right)^{\frac{\mu_{ej}^{(k)}+1}{2}} \right].$$

The CDF of the RV $Z_{E,k}$ is given by

$$F_{Z_{E,k}}(z_e) = \sum_{r_1^{(k)}=0}^{\infty} \sum_{r_2^{(k)}=0}^{\infty} \cdots \sum_{r_{n_e}^{(k)}=0}^{\infty} \frac{a_2^{(k)}}{2} z_e^{2\left(\mu_{e1}^{(k)} + r_1^{(k)}\right)}$$
$$\times G_{1,\, n_e^{(k)}+1}^{n_e^{(k)},\, 1} \left(\left. \begin{matrix} 1-\mu_{e1}^{(k)} - r_1^{(k)} \\ s^{(k)} \end{matrix} \right| z_e^2 \prod_{j=1}^{n_e^{(k)}} \mu_{ej}^{(k)} \left(1+\kappa_{ej}^{(k)}\right) \right), \tag{6}$$

where $s^{(k)} = -\mu_{e1}^{(k)} + \mu_{e2}^{(k)} - r_1^{(k)} + r_2^{(k)}, \cdots, -\mu_{e1}^{(k)} + \mu_{en_e}^{(k)} - r_1^{(k)} + r_{n_e}^{(k)}, 0, -\mu_{e1} - r_1^{(k)}$. The SNR at Bob is given by $\gamma_B = |Z_N|^2 \frac{P}{N_\circ}$ with the following PDF and CDF

$$f_{\gamma_B}(\gamma) = \sum_{v_1=0}^{\infty} \sum_{v_2=0}^{\infty} \cdots \sum_{v_N=0}^{\infty} \frac{a_1}{2} \left(\frac{\prod_{i=1}^{N} E\left[X_i^2\right]}{\bar{\gamma_B}} \right)^{\mu_1+v_1}$$
$$\times G_{N,\,0}^{0,\,N} \left(\left. \begin{matrix} \epsilon \\ - \end{matrix} \right| \frac{\bar{\gamma_B}}{\gamma \prod_{i=1}^{N} E\left[X_i^2\right] \mu_i (1+\kappa_i)} \right)$$
$$\times \gamma^{\mu_1+v_1-1}, \tag{7}$$

$$F_{\gamma_B}(\gamma) = \sum_{v_1=0}^{\infty} \sum_{v_2=0}^{\infty} \cdots \sum_{v_N=0}^{\infty} \frac{a_1}{2} \left(\gamma \frac{\prod_{i=1}^{N} E\left[X_i^2\right]}{\bar{\gamma_B}} \right)^{\mu_1+v_1}$$
$$\times G_{1,\,N+1}^{N,\,1} \left(\left. \begin{matrix} 1-\mu_1-v_1 \\ \rho \end{matrix} \right| \frac{\gamma \prod_{i=1}^{N} E\left[X_i^2\right] \mu_i (1+\kappa_i)}{\bar{\gamma_B}} \right), \tag{8}$$

where $\bar{\gamma_B}$ is the average received SNR at Bob. The eavesdropper (E) employs MRC over the received signals. Hence, the received SNR at E is given by $\gamma_E = \sum_{i=1}^{K} \gamma_{E,i} = \sum_{i=1}^{K} |Z_{E,i}|^2 \frac{P}{N_0}$. Using [21] and (5), the PDF of γ_E is given by

$$f_{\gamma_E}(\gamma_e) = \sum_{r_1=0}^{\infty} \sum_{r_2=0}^{\infty} \cdots \sum_{r_{n_e}=0}^{\infty} \frac{c_{x,e}}{2} \left(\frac{\prod_{j=1}^{n_e} E\left[X_j^2\right]}{\bar{\gamma_E} K} \right)^{\mu_{e1}K + r_1}$$
$$\times G_{n_e,\,0}^{0,\,n_e} \left(\left. \begin{matrix} \beta_e' \\ - \end{matrix} \right| \frac{\bar{\gamma_E} K}{\gamma_e \prod_{j=1}^{n_e} E\left[X_j^2\right] \mu_{ej} K_j (1+\kappa_{ej})} \right)$$
$$\times \gamma_e^{\mu_{e1}K + r_1 - 1}, \tag{9}$$

where $\bar{\gamma_E}$ is the average received SNR at E, $\beta_e' = \mu_{e1}K - \mu_{e2}K + r_1 - r_2 + 1, \cdots, \mu_{e1}K - \mu_{en_e}K + r_1 - r_{ne} + 1, 1$, and

$$c_{x,e} = 2 \prod_{j=1}^{n_e} \left[\frac{\left[2\mu_{ej} K_j \sqrt{\kappa_{ej}(1+\kappa_{ej})}\right]^{2r_j + \mu_{ej}K_j - 1}}{(r_j)! 2^{2r_j + \mu_{ej}K_j - 1}} \right]$$
$$\times \prod_{j=1}^{n_e} \left[\frac{\left[\mu_{ej} K_j (1+\kappa_{ej})\right]^{\mu_{e1}K - \mu_{ej}K_j + r_1 - r_j}}{\kappa_{ej}^{\frac{\mu_{ej}K_j - 1}{2}} \exp\left(\kappa_{ej} \mu_{ej} K_j\right)} \right]$$
$$\times \prod_{j=1}^{n_e} \left[\frac{\mu_{ej} K_j (1+\kappa_{ej})^{\frac{\mu_{ej}K_j+1}{2}}}{\Gamma\left(r_j + \mu_{ej} K_j\right)} \right].$$

To prove the accuracy of (9), the pdf is plotted along with Monte-Carlo simulation in Fig. 2. Using (9) and [22, Eq. (26)], the CDF of γ_E can be given by

$$F_{\gamma_E}(\gamma_e) = \sum_{r_1=0}^{\infty} \sum_{r_2=0}^{\infty} \cdots \sum_{r_{n_e}=0}^{\infty} \frac{c_{x,e}}{2} G_{1,\,n_e+1}^{n_e,\,1} \left(\left. \begin{matrix} \epsilon' \\ \eta_e' \end{matrix} \right| \frac{A\gamma_e}{\bar{\gamma_E} K} \right)$$
$$\times \left(\gamma_e \frac{\prod_{j=1}^{n_e} E\left[X_j^2\right]}{\bar{\gamma_E} K} \right)^{\mu_{e1}K + r_1}, \tag{10}$$

where $\epsilon' = 1 - \mu_{e1}K - r_1$, $\eta_e' = -\mu_{e1}K + \mu_{e2}K - r_1 + r_2, \cdots, -\mu_{e1}K + \mu_{e'n_e}K - r_1 + r_{n_e}, 0, -\mu_{e1}K - r_1$, and $A = \prod_{j=1}^{n_e} E\left[X_j^2\right] \mu_{ej} K_j (1+\kappa_{ej})$.

A. Secrecy Outage Probability

In this section, the secrecy outage probability (OP_{sec}), which is an important secrecy measurement metric for passive eavesdropping is studied. The secrecy capacity can be expressed as

$$C_s = \begin{cases} C_m - C_e, & \text{if } \gamma_B > \gamma_E \\ 0, & \text{if } \gamma_B \leq \gamma_E \end{cases}, \tag{11}$$

where C_m and C_e are the capacities of the main and the wiretap channels, respectively. OP_{sec} is expressed as

$$\begin{aligned} OP_{sec} &= P_r\left(C_s < C_{th}\right) \\ &= \int_0^{\infty} f_{\gamma_E}(\gamma_e) F_{\gamma_B}\left(2^{C_{th}}(1+\gamma_e) - 1\right) d\gamma_e, \end{aligned} \tag{12}$$

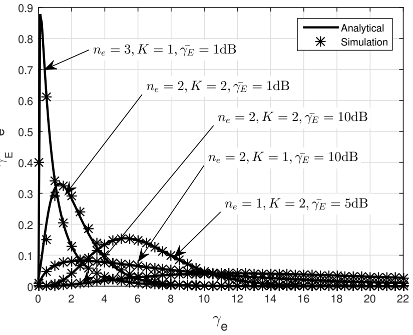

Fig. 2. The PDF of the received SNR at the eavesdropper (γ_E) for multiple values of cascade level of the wiretap channel (n_e) and multiple number of antennas at E (K). $\kappa_e = 1$ and $\mu_e = 2$.

where C_{th} is a predefined secrecy rate. A lower bound for OP_{sec} can be found instead (OP_{sec}^{L}). This is because further calculations for the OP_{sec} with the presence of the argument of the CDF in (12) is complicated. OP_{sec}^{L} is given by [23]

$$OP_{sec}^{L}=\int_{0}^{\infty} f_{\gamma_E}\left(\gamma_e\right) F_{\gamma_B}\left(2^{C_{th}}\gamma_e\right) d\gamma_e\cdot \tag{13}$$

Using (8) and (9) and with the help of [24, Eq. (2.3.31)] and [20, Eq. (7.813-1)] yields

$$\begin{aligned} OP_{sec}^{L}=&\sum_{v_1=0}^{\infty}\sum_{v_2=0}^{\infty}\cdots\sum_{v_N=0}^{\infty}\sum_{r_1=0}^{\infty}\sum_{r_2=0}^{\infty}\cdots\sum_{r_{n_e}=0}^{\infty} c_a \\ &\times G\,{}^{N\ \ n_e+1}_{n_e+1\ N+1}\left({}^{\xi}_{\rho}\middle|D\right), \end{aligned}\tag{14}$$

where $\xi=1-\mu_1-v_1, 1-\mu_1-v_1-\mu_{e2}K-r_2,\cdots,$ $1-\mu_1-v_1-\mu_{en_e}K-r_{n_e}, 1-\mu_{e1}K-r_1-\mu_1-v_1,$ $D=\frac{2^{C_{th}}\bar{\gamma_E}K\prod_{i=1}^{N}E\left[X_i^2\right]\mu_i(1+\kappa_i)}{\bar{\gamma_B}\prod_{j=1}^{n_e}E[X_j^2]\mu_{ej}K_j(1+\kappa_{ej})}$, and

$$\begin{aligned} c_a=&\frac{a_1c_{x,e}}{4}2^{C_{th}(\mu_1+v_1)}\left(\frac{\prod_{i=1}^{N}E\left[X_i^2\right]}{\bar{\gamma_B}}\right)^{\mu_1+v_1} \\ &\times\left(\frac{\prod_{j=1}^{n_e}E[X_j^2]\mu_{ej}K\left(1+\kappa_{ej}\right)}{\bar{\gamma_E}K}\right)^{-\mu_{e1}K-r_1-\mu_1-v_1} \\ &\times\left(\frac{\prod_{j=1}^{n_e}E[X_j^2]}{\bar{\gamma_E}K}\right)^{\mu_{e1}K+r_1}. \end{aligned}$$

B. Asymptotic Secrecy Outage Probability

In this section, the asymptotic OP_{sec}^{L} is evaluated when $\bar{\gamma_E}\rightarrow\infty$. Rewriting (14) with the help of [25, Eq. (2.2.1)] and [25, Eq. (3.11.3)] yields

$$\begin{aligned} OP_{sec}^{L}=&\sum_{v_1=0}^{\infty}\sum_{v_2=0}^{\infty}\cdots\sum_{v_N=0}^{\infty}\sum_{r_1=0}^{\infty}\sum_{r_2=0}^{\infty}\cdots\sum_{r_{n_e}=0}^{\infty} c_ac_b \\ &\times H\,{}^{N\ \ n_e+1}_{n_e+1\ N+1}\left({}^{\epsilon_d}_{\eta_d}\middle|D\right), \end{aligned}\tag{15}$$

where $H\,{}^{m\ n}_{p\ q}\left({}^{a}_{b}\middle|\cdot\right)$ is the H-function defined in [25, Eq. 3.11.1], $\epsilon_d=\{1,1\},\{1-\mu_{e2}K-r_2,1\},\cdots,\{1-\mu_{en_e}K-r_{n_e},1\},$ $\{1-\mu_{e1}K-r_1,1\}, \eta_d=\{\mu_2+v_2,1\},\cdots,\{\mu_N+v_N,1\},$ $\{\mu_1+v_1,1\},\{0,1\}$, and $c_b=\left(\frac{\bar{\gamma_B}\prod_{j=1}^{n_e}E[X_j^2]\mu_{ej}K_j(1+\kappa_{ej})}{2^{C_{th}}K\prod_{i=1}^{N}E\left[X_i^2\right]\mu_i(1+\kappa_i)}\right)^{\mu_1+v_1}\cdot$ Furthermore, the H-function can be rewritten again using its integral representation. Hence, (15) can be given by

$$\begin{aligned} OP_{sec}^{L}=&\sum_{v_1=0}^{\infty}\sum_{v_2=0}^{\infty}\cdots\sum_{v_N=0}^{\infty}\sum_{r_1=0}^{\infty}\sum_{r_2=0}^{\infty}\cdots\sum_{r_{n_e}=0}^{\infty}\frac{c_ac_b}{2\pi i} \\ &\times\int_C\frac{\Gamma[s]\prod_{i=1}^{N}\Gamma[\mu_i+v_i-s]}{\Gamma[1+s]}\prod_{j=1}^{n_e}\Gamma[\mu_{ej}K+r_j+s]D^s ds\cdot \end{aligned}\tag{16}$$

To find the asymptotic expression for OP_{sec}^{L}, the residue method can be used [26]. Hence, as $\bar{\gamma_E}\rightarrow\infty$, D $\rightarrow\infty$ and the asymptotic expression of OP_{sec}^{L} can be expressed as

$$\begin{aligned} OP_{sec}^{L}\approx&\sum_{v_1=0}^{\infty}\sum_{v_2=0}^{\infty}\cdots\sum_{v_N=0}^{\infty}\sum_{r_1=0}^{\infty}\sum_{r_2=0}^{\infty}\cdots\sum_{r_{n_e}=0}^{\infty}\frac{c_ac_b}{2\pi i} \\ &\times\text{Res}\left\{g(s),0\right\} \\ \approx&\sum_{v_1=0}^{\infty}\sum_{v_2=0}^{\infty}\cdots\sum_{v_N=0}^{\infty}\sum_{r_1=0}^{\infty}\sum_{r_2=0}^{\infty}\cdots\sum_{r_{n_e}=0}^{\infty} c_ac_b \\ &\times\prod_{i=1}^{N}\Gamma[\mu_i+v_i]\prod_{j=1}^{n_e}\Gamma[\mu_{ej}K+r_j], \end{aligned}\tag{17}$$

where $g(s)$ is given by

$$g(s)=D^s\frac{\Gamma[s]\prod_{i=1}^{N}\Gamma[\mu_i+v_i-s]\prod_{j=1}^{n_e}\Gamma[\mu_{ej}K+r_j+s]}{\Gamma[1+s]}\cdot$$

One can notice from (17) that the diversity order is zero, which means that the secrecy cannot be achieved at all when the wiretap channel's conditions are highly improved ($\bar{\gamma_E}\rightarrow\infty$) and E will be able to overhear the confidential information.

C. Probability of Non-zero Secrecy Capacity

Another secrecy metric commonly used is the probability of non-zero secrecy capacity, which can be expressed as

$$P_{nsc}=P_r\left(C_s>0\right)=P_r\left(\gamma_B>\gamma_E\right)=F_{\frac{\gamma_E}{\gamma_B}}\left(1\right)\cdot \tag{18}$$

To find the probability of non-zero secrecy capacity, some mathematical manipulations are needed to be performed over equations (7) and (9) as

$$\begin{aligned} f_{\gamma_B}\left(\gamma\right)=&\sum_{v_1=0}^{\infty}\sum_{v_2=0}^{\infty}\cdots\sum_{v_N=0}^{\infty}\frac{a_1\prod_{i=1}^{N}E\left[X_i^2\right]}{2\bar{\gamma_B}\left(\prod_{i=1}^{N}\mu_i\left(1+\kappa_i\right)\right)^{\mu_1+v_1-1}} \\ &\times H\,{}^{N\ \ 0}_{0\ \ N}\left({}^{-}_{\lambda}\middle|\frac{\gamma\prod_{i=1}^{N}E\left[X_i^2\right]\mu_i\left(1+\kappa_i\right)}{\bar{\gamma_B}}\right), \end{aligned}\tag{19}$$

where $\lambda=\{\mu_2+v_2-1,1\},\cdots,\{\mu_N+v_N-1,1\},$ $\{\mu_1+v_1-1,1\}$, and

$$\begin{aligned} f_{\gamma_E}\left(\gamma_e\right)=&\sum_{r_1=0}^{\infty}\sum_{r_2=0}^{\infty}\cdots\sum_{r_{n_e}=0}^{\infty}\frac{c_{x,e}\prod_{j=1}^{n_e}E[X_j^2]}{2\bar{\gamma_E}K} \\ &\times\frac{1}{\left(\prod_{j=1}^{n_e}\mu_{ej}K_j\left(1+\kappa_{ej}\right)\right)^{\mu_{e1}K+r_1-1}} \\ &\times H\,{}^{n_e\ \ 0}_{0\ \ n_e}\left({}^{-}_{P}\middle|\frac{\gamma_e\prod_{j=1}^{n_e}E[X_j^2]\mu_{ej}K_j\left(1+\kappa_{ej}\right)}{\bar{\gamma_E}K}\right), \end{aligned}\tag{20}$$

where $P = \{\mu_{e2}K + r_2 - 1, 1\}, \cdots, \{\mu_{en_e}K + r_{n_e} - 1, 1\}$, $\{\mu_{e1}K + r_1 - 1, 1\}$. Using (19) and (20), $f_{\frac{\gamma_E}{\gamma_B}}(\gamma)$ can be expressed as

$$f_{\frac{\gamma_E}{\gamma_B}}(y) = \sum_{r_1=0}^{\infty}\sum_{r_2=0}^{\infty}\cdots\sum_{r_{n_e}=0}^{\infty}\sum_{v_1=0}^{\infty}\sum_{v_2=0}^{\infty}\cdots\sum_{v_N=0}^{\infty} c_{x,e}a_1 \times \frac{\prod_{j=1}^{n_e} E[X_j^2]}{2\bar{\gamma_E}K\left(\prod_{j=1}^{n_e}\mu_{ej}K_j\left(1+\kappa_{ej}\right)\right)^{\mu_{e1}K+r_1-1}} \times \frac{\bar{\gamma_B}}{2\prod_{i=1}^{N}E[X_i^2]\left(\prod_{i=1}^{N}\mu_i\left(1+\kappa_i\right)\right)^{\mu_1+v_1+1}} \times H^{n_e\ N}_{N\ n_e}\left(\begin{matrix}\delta\\ P\end{matrix}\middle| \frac{\bar{\gamma_B}\prod_{j=1}^{n_e}E[X_j^2]\mu_{ej}K_j\left(1+\kappa_{ej}\right)}{\bar{\gamma_E}K\prod_{i=1}^{N}E\left[X_i^2\right]\mu_i\left(1+\kappa_i\right)}y\right), \quad (21)$$

where $\delta = \{-\mu_2 - v_2, 1\}, \cdots, \{-\mu_N - v_N, 1\}$, $\{-\mu_1 - v_1, 1\}$. Using (21) and [27], P_{nsc} can be found as

$$P_{nsc} = 1 - \sum_{r_1=0}^{\infty}\sum_{r_2=0}^{\infty}\cdots\sum_{r_{n_e}=0}^{\infty}\sum_{v_1=0}^{\infty}\sum_{v_2=0}^{\infty}\cdots\sum_{v_N=0}^{\infty} c_{x,e}a_1 \times \frac{\prod_{j=1}^{n_e} E[X_j^2]}{4\prod_{i=1}^{N}E[X_i^2]\left(\prod_{j=1}^{n_e}\mu_{ej}K_j\left(1+\kappa_{ej}\right)\right)^{\mu_{e1}K+r_1}} \times \frac{1}{\left(\prod_{i=1}^{N}\mu_i\left(1+\kappa_i\right)\right)^{\mu_1+v_1}} \times H^{n_e+1\ N}_{N+1\ n_e+1}\left(\begin{matrix}\psi\\ \psi'\end{matrix}\middle| \frac{\bar{\gamma_B}\prod_{j=1}^{n_e}E[X_j^2]\mu_{ej}K_j\left(1+\kappa_{ej}\right)}{\bar{\gamma_E}K\prod_{i=1}^{N}E\left[X_i^2\right]\mu_i\left(1+\kappa_i\right)}\right), \quad (22)$$

where $\psi = \{-\mu_2 - v_2 + 1, 1\}, \cdots, \{-\mu_N - v_N + 1, 1\}$, $\{-\mu_1 - v_1 + 1, 1\}, \{1, 1\}$ and $\psi' = \{0, 1\}, \{\mu_{e2}K + r_2, 1\}, \cdots, \{\mu_{en_e}K + r_{n_e}, 1\}$, $\{\mu_{e1}K + r_1, 1\}$.

D. Asymptotic Probability of Non-Zero Secrecy Capacity

The asymptotic P_{nsc} is evaluated when $\bar{\gamma_E} \to \infty$ to notice the effect of improving the wiretap channel's conditions over the secrecy. Following the same procedure utilized to find the asymptotic secrecy outage probability, the asymptotic probability of non-zero secrecy capacity can be expressed as

$$P_{nsc} \approx 1 - \sum_{v_1=0}^{\infty}\sum_{v_2=0}^{\infty}\cdots\sum_{v_N=0}^{\infty}\sum_{r_1=0}^{\infty}\sum_{r_2=0}^{\infty}\cdots\sum_{r_{n_e}=0}^{\infty} c_{x,e}a_1c_c \times \prod_{i=1}^{N}\Gamma[\mu_i + v_i]\prod_{j=1}^{n_e}\Gamma[\mu_{ej}K + r_j], \quad (23)$$

where $c_c = \frac{\prod_{j=1}^{n_e}E[X_j^2]}{4\prod_{i=1}^{N}E[X_i^2]\left(\prod_{j=1}^{n_e}\mu_{ej}K_j(1+\kappa_{ej})\right)^{\mu_{e1}K+r_1}}$ $\times \frac{1}{\left(\prod_{i=1}^{N}\mu_i(1+\kappa_i)\right)^{\mu_1+v_1}}$.
Equation (23) proves that no secrecy can be achieved when the average received SNR at E is very high and the wiretap channel's conditions are extremely good in terms of the average received SNR. This is possible if the eavesdropper is very close to the transmitter, which makes the eavesdropper strongly capable of successfully decoding the intercepted information.

III. Numerical Results

In this section, results for the derived equations are presented along with the simulation. The analytical curves are plotted by truncating the infinite series expansion indices $(v$ and $r)$ to the first 20 terms. A perfect match of the simulation results with the analytical ones can be observed.

Fig. 3 shows the effect of the cascaded level for the main and the wiretap channels $(N$ and $n_e)$ over the secrecy outage probability (OP_{sec}^{L}). The channels fading parameters are: $\kappa = 0$ and $\mu = 1$, which represents the Rayleigh channel as a special case. Other channels can be obtained by varying the values of κ and μ. The significant impact over the secrecy of the transmitted information can be noted by varying the cascade level (number of keyholes) as more severe fading appears when the number of scatters increases. Moreover, the effect of changing the value of the average received SNR at the eavesdropper $(\bar{\gamma_E})$ over the security is presented. By improving the eavesdropper's channel, better signal reception at E can be achieved, which degrades the secrecy of the system as the eavesdropper becomes capable of decoding the information correctly. Improving the wiretap channel may occur when the eavesdropper is getting closer to the transmitter. In addition, the asymptotic secrecy outage probability can be observed from the figure when the value of $\bar{\gamma_E}$ is very high. That is a zero slope (zero diversity order) can be seen and a value of 1 can be achieved for the secrecy outage probability. Hence, the secrecy of this system with such parameters cannot be achieved regardless of the value of the average received SNR at Bob $(\bar{\gamma_B})$ and the information will be intercepted by the eavesdropper. Furthermore, increasing the average received SNR at Bob $(\bar{\gamma_B})$ helps to reduce the secrecy outage probability regardless of the change in the cascade level.

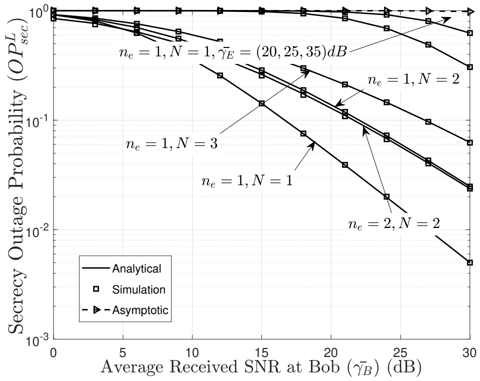

Fig. 3. The lower bound of the secrecy outage probability (OP_{sec}^{L}) for two antennas at the eavesdropper $(K = 2)$. For the main channel: $\kappa = 0, \mu = 1$ and for the wiretap channel: $\kappa_e = 0, \mu_e = 1$ (Rayleigh). $C_{th} = 1$ and $\bar{\gamma_E} = 1$ dB.

Fig. 4 reveals the effect of changing the number of antennas of the eavesdropper (E) over the secrecy. It can be noticed that

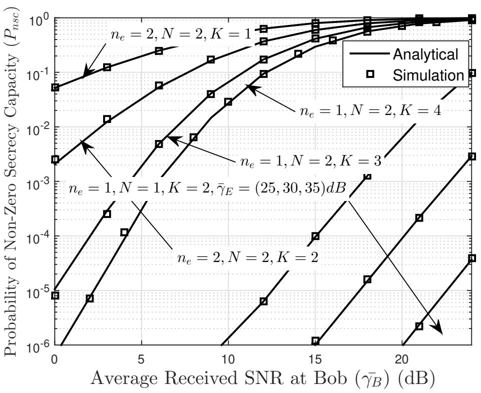

Fig. 4. The probability of non-zero secrecy capacity (P_{nsc}) for different number of antennas at the eavesdropper (K). For the main channel: $\kappa = 1, \mu = 2$ and for the wiretap channel: $\kappa_e = 1, \mu_e = 2$. $\bar{\gamma_E} = 10$ dB.

increasing the number of antennas at E increases the chance for E to successfully intercepts and decodes the confidential information between Alice and Bob. That is the eavesdropper becomes more powerful with increasing the number of antennas as the receiver employs the MRC technique. Furthermore, increasing the average received SNR at Bob ($\bar{\gamma_B}$) helps to reduce the effect of increasing the number of passive eavesdroppers (K) and increases the chance to achieve a positive secrecy capacity. In addition, the effect of the average received SNR at E ($\bar{\gamma_E}$) over the probability of non-zero secrecy capacity is studied. Higher values for $\bar{\gamma_E}$ implies better channel conditions in the wiretap link and degradation in the security. Improving the wiretap channel's conditions in terms of the average received SNR ($\bar{\gamma_E}$) will eventually cause a very low value for the probability of non-zero secrecy capacity, which represents the asymptotic situation. That is the information will be intercepted by the eavesdropper easily and decoded successfully.

IV. Conclusion

In this paper, we studied the secrecy of a system model consisting of a transmitter, a receiver, and a multi-antenna eavesdropper trying to intercept the confidential information sent to the legitimate receiver. The main and wiretap links fading distributions are assumed to be cascaded κ-μ. Exact and asymptotic expressions for two of the main secrecy metrics formulas were derived, which are the secrecy outage probability and the probability of non-zero secrecy capacity. The results show that the cascade level (number of scatters) at both links have a noticeable effect over the secrecy performance. Moreover, a clear degradation in the secrecy can be observed for an increase in the number of antennas at E or in the value of the average received SNR at E. Analytical results were successfully verified by Monte-Carlo simulation.

References

[1] F. Pan, Y. Jiang, H. Wen, R. Liao, and A. Xu, "Physical Layer Security Assisted 5G Network Security," in *2017 IEEE 86th Veh. Technol. Conf. (VTC-Fall)*, Toronto, ON, Canada, Sep. 2017, pp. 1–5.

[2] Y. Wu, A. Khisti, C. Xiao, G. Caire, 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, April 2018.

[3] S. Ö. Ata, "Secrecy performance analysis over cascaded fading channels," *IET Commun.*, vol. 13, no. 2, pp. 259–264, Jan. 2019.

[4] F. Jameel, S. Wyne, G. Kaddoum, and T. Q. Duong, "A Comprehensive Survey on Cooperative Relaying and Jamming Strategies for Physical Layer Security," *IEEE Commun. Surv. Tutorials*, vol. 21, no. 3, pp. 2734–2771, thirdquarter 2019.

[5] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, no. 4, pp. 656–715, 1949.

[6] L. H. Ozarow and A. D. Wyner, "Wire-tap channel II," *AT&T Bell Lab. Tech. J.*, vol. 63, no. 10, pp. 2135–2157, 1984.

[7] D. H. Tashman and W. Hamouda, "An Overview and Future Directions on Physical-Layer Security for Cognitive Radio Networks," *IEEE Network*, pp. 1–7, 2020.

[8] M. D. Yacoub, "The $\kappa-\mu$ distribution and the $\eta-\mu$ distribution," *IEEE Antennas Propag. Mag.*, vol. 49, no. 1, pp. 68–81, Feb. 2007.

[9] K. Peppas, F. Lazarakis, A. Alexandridis, and K. Dangakis, "Cascaded generalised-K fading channel," *IET commun.*, vol. 4, no. 1, pp. 116–124, Jan. 2010.

[10] L. Kong, G. Kaddoum, and D. B. da Costa, "Cascaded $\alpha-\mu$ Fading Channels: Reliability and Security Analysis," *IEEE Access*, vol. 6, pp. 41 978–41 992, May 2018.

[11] D. H. Tashman and W. Hamouda, "Physical-Layer Security for Cognitive Radio Networks over Cascaded Rayleigh Fading Channels," in *GLOBECOM 2020 - 2020 IEEE Global Commun. Conf.*, Taipei, Taiwan, 2020, pp. 1–6.

[12] I. Ghareeb and D. Tashman, "Statistical analysis of cascaded Rician fading channels," *Int. J. Electron. Lett.*, vol. 8, no. 1, pp. 46–59, 2020.

[13] H. Lei, C. Gao, I. S. Ansari, Y. Guo, G. Pan, and K. A. Qaraqe, "On Physical-Layer Security Over SIMO Generalized-K Fading Channels," *IEEE Trans. Veh. Technol.*, vol. 65, no. 9, pp. 7780–7785, Sep. 2016.

[14] X. Liu, "Probability of strictly positive secrecy capacity of the Weibull fading channel," in *2013 IEEE Global Commun. Conf. (GLOBECOM)*, Atlanta, GA, USA, Dec. 2013, pp. 659–664.

[15] ——, "Probability of Strictly Positive Secrecy Capacity of the Rician-Rician Fading Channel," *IEEE Wireless Commun. Lett.*, vol. 2, no. 1, pp. 50–53, Feb. 2013.

[16] R. Singh and M. Rawat, "Unified Analysis of Secrecy Capacity Over N∗Nakagami Cascaded Fading Channel," in *2018 18th Int. Symp. Commun. Inf. Technol. (ISCIT)*, Sep. 2018, pp. 422–427.

[17] S. Ö. Ata, "Physical layer security over cascaded Rayleigh fading channels," in *2018 26th Signal Process. Commun. Appl. Conf. (SIU)*, Izmir, Turkey, May 2018, pp. 1–4.

[18] D. Tashman, W. A. Hamouda, and I. Dayoub, "Secrecy Analysis over Cascaded κ-μ Fading Channels with Multiple Eavesdroppers," *IEEE Trans. Veh. Technol.*, pp. 1–1, 2020.

[19] S. Jia, J. Zhang, H. Zhao, and R. Zhang, "Relay Selection for Improved Security in Cognitive Relay Networks With Jamming," *IEEE Wireless Commun. Lett.*, vol. 6, no. 5, pp. 662–665, Oct. 2017.

[20] I. S. Gradshteyn and I. M. Ryzhik, *Table of integrals, series, and products*. Academic press, 2007.

[21] M. Milisic, M. Hamza, and M. Hadzialic, "Outage and symbol error probability performance of L-branch maximal-ratio combiner for generalized κ-μ fading," in *2008 50th Int. Symp. ELMAR*, vol. 1, Zadar, Croatia, Sep. 2008, pp. 231–236.

[22] V. Adamchik and O. Marichev, *The algorithm for calculating integrals of hypergeometric type functions and its realization in REDUCE system*, 1990.

[23] J. M. Moualeu and W. Hamouda, "On the Secrecy Performance Analysis of SIMO Systems Over $\kappa-\mu$ Fading Channels," *IEEE Commun. Lett.*, vol. 21, no. 11, pp. 2544–2547, Nov. 2017.

[24] J. Proakis and M. Salehi, *Digital Communications, 5th ed. New York*. McGraw-Hill, 2008.

[25] A. M. Mathai, *A handbook of generalized special functions for statistical and physical sciences*. Oxford University Press, USA, 1993.

[26] H. Chergui, M. Benjillali, and S. Saoudi, "Performance Analysis of Project-and-Forward Relaying in Mixed MIMO-Pinhole and Rayleigh Dual-Hop Channel," *IEEE Commun. Lett.*, vol. 20, no. 3, pp. 610–613, March 2016.

[27] C. D. Bodenschatz, "Finding an H-function distribution for the sum of independent H-function variates ," Ph.D. dissertation 1992.