Physical-Layer Security over Generalized SIMO Multipath Fading Channels

Jules M. Moualeu[1], Daniel B. da Costa[2], Paschalis C. Sofotasios[3,4], Walaa Hamouda[5], Ugo S. Dias[6], and Sami Muhaidat[3,7]

[1]School of Electrical and Information Engineering, University of the Witwatersrand, Johannesburg, South Africa
e-mail: jules.moualeu@wits.ac.za
[2]Department of Computer Engineering, Federal University of Ceará, Sobral, CE, Brazil
e-mail: danielbcosta@ieee.org
[3]Department of Electrical and Computer Engineering, Khalifa University of Science and Technology, Abu Dhabi, UAE
{paschalis.sofotasios; sami.muhaidat} @ku.ac.ae
[4]Department of Electronics and Communications Engineering, Tampere University of Technology, Tampere, Finland
e-mail: paschalis.sofotasios@tut.fi
[5]Department of Electrical and Computer Engineering, Concordia University, Montreal, Canada
e-mail: hamouda@ece.concordia.ca
[6]Department of Electrical Engineering, University of Brasilia, Brasilia, DF, Brazil
e-mail: ugodias@ieee.org
[7]Institute for Communication Systems, University of Surrey, GU2 7XH, Guildford, UK
e-mail: sami.muhaidat@surrey.ac.uk

***Abstract*—The present work investigates the physical layer security of wireless communication systems over non-homogeneous fading environments, which are typically encountered in realistic wireless transmission scenarios in the context of conventional and emerging communication systems. The is carried out in the context of a single-input multiple-output system that consists of a single-antenna transmitter, a multi-antenna legitimate receiver, and a multi-antenna active eavesdropper. To this end, novel exact analytic expressions are derived for the corresponding average secrecy capacity, which are corroborated by respective results from computer simulations that verify their validity. Capitalizing on the offered results, the physical layer security is quantified in terms of different parameters. This leads to the development of useful insights on the impact of non-homogeneous fading environment and the number of employed antennas on the achieved physical layer security levels of the considered set up.**

I. Introduction

Physical layer (PHY) security has received a great deal of attention in the past few years since it can address the issues of privacy and security in wireless communication networks, without necessarily relying on encryption techniques. Owing to this fact, several reported contributions have investigated the secrecy performance over small-scale fading channels [1], [2] and large-scale fading channels [3]. However, the aforementioned fading conditions do not typically encompass various fading types that are experienced in practical communication scenarios. This also concerns the effects of non-homogeneous fading environments, which although they are encountered in realistic communication scenarios, they are typically neglected for the sake of complexity reduction. As a result, several simplistic assumptions have led to results that are largely inaccurate, which is a critical issue in the context of secure communications since the reliability of modeling effects is of paramount importance. To this end, recent emphasis on generalized fading distributions that do not necessarily assume homogeneous fading environments has recently generated a considerable interest in analyses relating to PHY security, which constitutes a critical topic of interest in emerging communication technologies (see, for instance, [4]–[9] and references therein). Specifically, the authors in [4] derived analytic expressions for the lower bound of the secrecy outage probability (SOP) and the probability of strictly positive secrecy capacity (SPSC) over generalized Gamma fading channels. Likewise, the secrecy performance analysis over generalized-K fading channels was investigated in [5], while the effects of κ-μ and α-μ fading conditions were investigated in [6] and in [7], respectively. Considering a different configuration from the above analyses, the authors in [8] and [9] the PHY security problem over single-input multiple-output (SIMO) generalized-K and κ–μ fading channels, respectively.

It is recalled that another type of versatile fading model is the η-μ fading distribution [10]. This model has been shown to provide accurate characterization of the small-scale variations of the fading signal under non-line-of-sight conditions and includes Rayleigh, Nakagami-m and Hoyt distributions as special cases. More importantly, unlike simplistic fading models, it accounts for non-homogeneous fading environments, which are encountered in practical wireless propagation both in

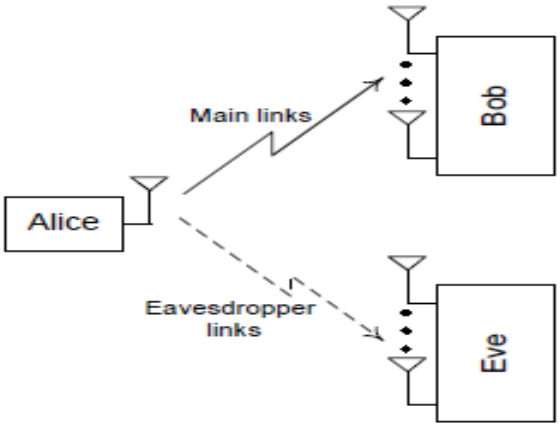

Fig. 1: System model.

conventional and in emerging communications. Based on this and its wide applicability and versatility [10], its consideration in the context of PHY security arises as an interesting issue to be investigated. Nevertheless, despite the interesting and useful properties of this model, the secrecy analysis under such fading conditions has not, to the nest of the authors' knowledge, been investigated in the open technical literature.

Motivated by the above, the present work investigates the physical layer security of SIMO systems under η-μ fading conditions. To this end, we derive a novel analytic expression for the average secrecy capacity (ASC) of the considered setup. This expression is given in terms of an infinite series, which is fully convergent and involves simple elementary and special functions. Also, a small number of terms is required for its truncation, ensuring a sufficiently low truncation error. To this end, a simple closed-form upper bound for the truncation error of the involved infinite series is derived in order to allow accurate determination of the number of truncation terms required to achieve target accuracies. The derived analytic expressions are subsequently employed to quantify the ASC under the considered fading conditions. The validity of the offered results is verified through extensive comparisons with respective results from computer simulations. It is shown that the number of antennas are critical to the level of achieved security as it improves the performance when they increase at the legitimate user and they degrade it as their number increases at the eavesdropper. Also, the effects of non-homogeneous fading have a non-negligible effect on the ASC since the achieved levels vary considerably from the standard Rayleigh fading conditions. However, the effect of fading conditions in ASC is, as expected, smaller when the number of antennas at the legitimate and at eavesdropper's links is not small.

The remainder of the paper is organized as follows: In Section II, the system and channel models are described, while Section III focuses on the analysis of the ASC, in which an exact analytical expression is derived. A closed-form upper bound for the truncation error of the infinite series of in the derived ASC is obtained in Section IV, followed by some numerical results and insightful discussions in Section V. Finally, concluding remarks are provided in Section VI.

II. System and Channel Models

Let a SIMO wiretap channel in which the transmitter (Alice) sends confidential messages to the legitimate receiver (Bob), while the eavesdropper (Eve) overhears the transmission through the eavesdropper channel, as shown in Fig. 1. In this context, it is assumed that Alice is equipped with a single antenna whereas Bob and Eve are equipped with multiple antennas, L_B, and L_E, respectively. Also, both the legitimate (Alice-Bob) channel and the eavesdropper (Alice-Eve) channel undergo independent and identically distributed (i.i.d.) quasi-static η-μ fading[1] conditions with arbitrary values of fading parameters. An active eavesdropping scenario is considered, in which the channel state information (CSI) of both the main and wiretap links are known at Alice. A maximal-ratio combining (MRC) scheme is employed at the receiver sides in an effort to exploit antenna diversity and to maximize the probability of secure transmission at Bob or secure eavesdropping at Eve.

With the help of [11, Eq. (8.445.1)] and [12], the probability density function (PDF) of the signal-to-noise ratio (SNR) γ_i, $i \in \{B, E\}$[2], at the receiver's combiner output can be expressed as

$$f_{\gamma_i}(x) = \sum_{k=0}^{\infty} \frac{2\sqrt{\pi} h_i^{L_i\mu_i} H_i^{2k} \mu_i^{2L_i\mu_i+2k} x^{2L_i\mu_i+2k-1}}{k!\Gamma(L_i\mu_i)\Gamma\left(L_i\mu_i+k+\frac{1}{2}\right)\bar{\gamma}_i^{2L_i\mu_i+2k}} e^{-\frac{2\mu_i h_i x}{\bar{\gamma}_i}} \tag{1}$$

where $\Gamma(\cdot)$ is the Gamma function, $\mu_i > 0$ represents the number of multipath clusters and $\bar{\gamma}_i = \mathbb{E}\{\gamma_i\}$ denotes the average SNR, with $\mathbb{E}\{\cdot\}$ symbolizing expectation. Moreover, h_i and H_i are functions of η_i and can be given in two different formats: (a) In *Format 1*, $h_i = (2 + \eta_i^{-1} + \eta_i)/4$ and $H_i = (\eta_i^{-1} - \eta_i)/4$, with $0 < \eta_i < \infty$ denoting the power ratio of the in-phase and quadrature components of the fading signal within each cluster; and (b) In *Format 2*, $h_i = 1/(1-\eta_i^2)$ and $H_i = \eta_i/(1-\eta_i^2)$, with $-1 < \eta_i < 1$ denoting the correlation coefficient between the scattered-wave in-phase and quadrature components in each multipath cluster. As shown in [10], *Format 1* can be directly mapped to *Format 2* through a bilinear transformation; owing to this and without a loss of generality, the present analysis considers only the *Format 1* of the η-μ distribution. From (1), the corresponding cumulative distribution function (CDF) is given by

$$F_{\gamma_i}(x) = \frac{\sqrt{\pi}}{\Gamma(L_i\mu_i)} \sum_{j=0}^{\infty} \frac{H_i^{2j} 2^{-2L_i\mu_i-2k+1}}{j!\Gamma\left(L_i\mu_i+j+\frac{1}{2}\right) h_i^{L_i\mu_i+2j}} \times \gamma_{\text{inc}}\left(2L_i\mu_i+2j, \frac{2\mu_i h_i x}{\bar{\gamma}_i}\right), \tag{2}$$

[1]The physical model of the η-μ fading distribution considers that the signals are composed of clusters of multipath waves propagating in a non-homogeneous environment. Within any one cluster, the phases of the scattered waves are random and have similar delay times with delay-time spreads of different clusters being relatively large. Also, the in-phase and quadrature components of fading signals within each cluster are assumed to be independent from each other and to have different powers [10].

[2]Henceforth, the subscript B is associated to Bob, while the subscript E is linked to Eve.

where $\gamma_{\text{inc}}(\alpha, x)$ stands for the lower incomplete Gamma function[3] [11, Eq. (8.350.1)].

III. Average Secrecy Capacity Analysis

In this section, the scenario wherein the CSI of the eavesdropper channel is available at Alice is considered. This scenario is applicable to wireless networks where Eve is active and Alice has access to her CSI [13]. In this case, a fundamental performance metric used to evaluate the secrecy performance is the ASC, which is defined as the instantaneous secrecy capacity C_S averaged over the instantaneous SNRs γ_B and γ_E, where $C_S = \max\{C_B - C_E, 0\}$ with $C_B = \log_2(1+\gamma_B)$ and $C_E = \log_2(1+\gamma_E)$ denoting the capacities of the main and eavesdropper channels, respectively. To this effect, the ASC can be mathematically formulated as

$$\begin{aligned}\bar{C}_S &= \int_0^\infty \int_0^\infty C_S f_{\gamma_B}(\gamma_B) f_{\gamma_E}(\gamma_E) \mathrm{d}\gamma_B \mathrm{d}\gamma_E \\ &= \underbrace{\frac{1}{\ln(2)} \int_0^\infty \ln(1+\gamma_B) f_{\gamma_B}(\gamma_B) F_{\gamma_E}(\gamma_B) \mathrm{d}\gamma_B}_{\mathcal{J}_1} \\ &\quad + \underbrace{\frac{1}{\ln(2)} \int_0^\infty \ln(1+\gamma_E) f_{\gamma_E}(\gamma_E) F_{\gamma_B}(\gamma_E) \mathrm{d}\gamma_E}_{\mathcal{J}_2} \\ &\quad - \underbrace{\frac{1}{\ln(2)} \int_0^\infty \ln(1+\gamma_E) f_{\gamma_E}(\gamma_E) \mathrm{d}\gamma_E}_{\mathcal{J}_3}. \end{aligned} \tag{3}$$

In what follows, the ASC is derived by deriving analytic expressions for the $\mathcal{J}_1$, $\mathcal{J}_2$ and $\mathcal{J}_3$ terms. Starting with $\mathcal{J}_1$, by substituting appropriately (1) and (2) into (3), one obtains

$$\begin{aligned}\mathcal{J}_1 &= \frac{2\pi h_B^{L_B\mu_B}}{\ln(2)\Gamma(L_B\mu_B)\Gamma(L_E\mu_E)} \sum_{k=0}^{\infty}\sum_{j=0}^{\infty} \frac{H_B^{2k} H_E^{2j} \bar{\gamma}_B^{-2L_B\mu_B-2k}}{k! j! h_E^{L_E\mu_E+2j}} \\ &\quad \times \frac{\mu_B^{2L_B\mu_B+2k}}{2^{2L_E\mu_E+2j-1}\Gamma(L_B\mu_B+k+0.5)\Gamma(L_E\mu_E+2j+0.5)} \\ &\quad \times \int_0^\infty \ln(1+\gamma_B) \gamma_B^{2L_B\mu_B+2k-1} e^{-\frac{2\mu_B h_B}{\bar{\gamma}_B}\gamma_B} \\ &\quad \times \gamma_{\text{inc}}\left(2L_E\mu_E + 2j, \frac{2\mu_E h_E \gamma_B}{\bar{\gamma}_E}\right) \mathrm{d}\gamma_B. \end{aligned} \tag{4}$$

By denoting the integral in (4) as $\mathcal{I}_1$, making use of [11, Eq. (8.352.4)], and carrying out after some algebraic manipulations, the $\mathcal{I}_1$ integral can be equivalently represented as

$$\begin{aligned}\mathcal{I}_1 &= (2L_E\mu_E + 2j - 1)! \left(\int_0^\infty \ln(1+\gamma_B) \gamma_B^{2L_B\mu_B+2k-1} \right. \\ &\quad \times e^{-\frac{2\mu_B h_B}{\bar{\gamma}_B}\gamma_B} \mathrm{d}\gamma_B - \sum_{n=0}^{2L_E\mu_E+2j-1} \frac{1}{n!} \left(\frac{2\mu_E h_E}{\bar{\gamma}_E}\right)^n \\ &\quad \left. \times \int_0^\infty \ln(1+\gamma_B) \gamma_B^{2L_B\mu_B+2k+n-1} e^{-\left(\frac{2\mu_B h_B}{\bar{\gamma}_B} + \frac{2\mu_E h_E}{\bar{\gamma}_E}\right)\gamma_B} \mathrm{d}\gamma_B \right) \end{aligned} \tag{5}$$

[3]The subscript "inc" is used here to differentiate the instantaneous SNR γ_i and the lower incomplete Gamma function $\gamma_{\text{inc}}(\cdot,\cdot)$.

It is noticed that both integrals in (5) have the form: $\int_0^\infty \ln(1+x) x^a e^{-bx} \mathrm{d}x$, where $a > 0$ and $b > 0$. Based on this and using [14, Eq. (78)], the first integral of (5), denoted by $\mathcal{I}_{11}$, can be derived as

$$\begin{aligned}\mathcal{I}_{11} &= (2L_B\mu_B + 2k - 1)! e^{\frac{2\mu_B h_B}{\bar{\gamma}_B}} \sum_{m=1}^{2L_B\mu_B+2k} \left(\frac{\bar{\gamma}_B}{2\mu_B h_B}\right)^m \\ &\quad \times \Gamma\left(-2L_B\mu_B - 2k + m, \frac{2\mu_B h_B}{\bar{\gamma}_B}\right). \end{aligned} \tag{6}$$

Similarly, the second integral in (5) can be derived so that $\mathcal{I}_1$ can further be expressed as

$$\begin{aligned}\mathcal{I}_1 &= (2L_E\mu_E + 2j - 1)! \left[(2L_B\mu_B + 2k - 1)! e^{\frac{2\mu_B h_B}{\bar{\gamma}_B}} \right. \\ &\quad \times \sum_{m=1}^{2L_B\mu_B+2k} \left(\frac{\bar{\gamma}_B}{2\mu_B h_B}\right)^m \Gamma\left(-2L_B\mu_B - 2k + m, \frac{2\mu_B h_B}{\bar{\gamma}_B}\right) \\ &\quad - \sum_{n=0}^{2L_E\mu_E+2j-1} \sum_{\iota=1}^{2L_B\mu_B+2k+n} \frac{(2L_B\mu_B + 2k + n - 1)!}{n!} \\ &\quad \times \left(\frac{2\mu_E h_E}{\bar{\gamma}_E}\right)^n \left(\frac{2\mu_B h_B}{\bar{\gamma}_B} + \frac{2\mu_E h_E}{\bar{\gamma}_E}\right)^{-\iota} e^{\frac{2\mu_B h_B}{\bar{\gamma}_B} + \frac{2\mu_E h_E}{\bar{\gamma}_E}} \\ &\quad \left. \times \Gamma\left(-2L_B\mu_B - 2k - n + \iota, \frac{2\mu_B h_B}{\bar{\gamma}_B} + \frac{2\mu_E h_E}{\bar{\gamma}_E}\right) \right]. \end{aligned} \tag{7}$$

Then, by replacing (7) into (4), an analytical expression for $\mathcal{J}_1$ can be obtained as (8), shown at the top of the next page, where $\Gamma(\cdot,\cdot)$ denotes the upper incomplete Gamma function [11, Eq. (8.350.2)]. Similarly, an expression for $\mathcal{J}_2$ can also be attained from (8) after replacing L_B by L_E, μ_B by μ_E, H_B by H_E, h_B by h_E, and $\bar{\gamma}_B$ by $\bar{\gamma}_E$, and vice-versa.

Next, by substituting appropriately (1) into the expression of $\mathcal{J}_3$ in (3), and using [14, Eq. (78)] along with some algebraic manipulations, $\mathcal{J}_3$ can be derived as

$$\begin{aligned}\mathcal{J}_3 &= \frac{2\sqrt{\pi} h_E^{L_E\mu_E}}{\ln(2)\Gamma(L_E\mu_E)} \sum_{k=0}^{\infty} \frac{H_E^{2k} \mu_E^{2L_E\mu_E+2k} \Gamma(2L_E\mu_E + 2k)}{k! \Gamma(L_E\mu_E + k + 0.5)} \\ &\quad \times e^{\frac{2\mu_E h_E}{\bar{\gamma}_E}} \sum_{m=1}^{2L_E\mu_E+2k} \frac{\Gamma\left(-2L_E\mu_E - 2k + m, \frac{2\mu_E h_E}{\bar{\gamma}_E}\right)}{(2\mu_E h_E)^m \bar{\gamma}_E^{2L_E\mu_E+2k-m}}. \end{aligned} \tag{9}$$

Therefore, by substituting (8)-(9) into (3) leads to the corresponding analytic expression for the $\bar{C}_S$.

It is evident that the derived analytic expression for the $\bar{C}_S$ is expressed in terms of an infinite series representation. However, this is not practically an issue since this series is fully convergent and it requires few terms to achieve sufficient levels of accuracy. In fact, fairly accurate results can be obtained by truncating the series after 50 terms, which yields a relative error of less than 0.002%. Also, the algebraic representation of the derived series is tractable since it consists of well-known elementary and special functions, which render it convenient to handle both analytically and numerically.

IV. A Closed-Form Upper Bound Expression for the Truncation Error of the Derived ASC

As already mentioned, the derived expression for the ASC is given in terms of infinite series. Depending on the value of

$$\mathcal{J}_1 = \frac{2\pi h_B^{L_B\mu_B}}{\ln(2)\Gamma(L_B\mu_B)\Gamma(L_E\mu_E)} \sum_{k=0}^{\infty}\sum_{j=0}^{\infty} \frac{H_B^{2k} H_E^{2j} \mu_B^{2L_B\mu_B+2k}(2L_E\mu_E+2j-1)!}{k!j!2^{2L_E\mu_E+2j-1} h_E^{L_E\mu_E+2j}\Gamma(L_B\mu_B+k+0.5)\Gamma(L_E\mu_E+j+0.5)}$$
$$\times \Bigg[(2L_B\mu_B+2k-1)!e^{\frac{2\mu_B h_B}{\bar{\gamma}_B}} \sum_{m=1}^{2L_B\mu_B+2k} \left(\frac{\bar{\gamma}_B}{2\mu_B h_B}\right)^m \Gamma\left(-2L_B\mu_B-2k+m, \frac{2\mu_B h_B}{\bar{\gamma}_B}\right) - \sum_{n=0}^{2L_E\mu_E+2j-1} \sum_{\iota=1}^{2L_B\mu_B+2k+n} \frac{1}{n!}$$
$$\times\Gamma(2L_B\mu_B+2k+n) \left(\frac{2\mu_E h_E}{\bar{\gamma}_E}\right)^n \left(\frac{2\mu_B h_B}{\bar{\gamma}_B}+\frac{2\mu_E h_E}{\bar{\gamma}_E}\right)^{-\iota} \frac{e^{\frac{2\mu_B h_B}{\bar{\gamma}_B}}}{e^{-\frac{2\mu_E h_E}{\bar{\gamma}_E}}} \Gamma\left(-2L_B\mu_B-2k-n+\iota, \frac{2\mu_B h_B}{\bar{\gamma}_B}+\frac{2\mu_E h_E}{\bar{\gamma}_E}\right)\Bigg]. \quad (8)$$

the involved parameters, this series requires different number of terms to ensure acceptable truncation that leads to accurate results. So, even though the involved series achieves a sufficient accuracy for a relatively low number of terms, deriving a tight closed-form upper bound for the exact truncation error of this series will allow the determination of the exact accuracy for a specific number of terms at a given scenario. Based on this, we derive a tight and tractable closed-form upper bound for the truncation error of the derived series representation in (3). In this case, the truncation error of (3) can be bounded by deriving closed-form bounds for $\mathcal{J}_1$, $\mathcal{J}_2$ and $\mathcal{J}_3$.

To this end, the truncation of $\mathcal{J}_1$ after $p-1$ terms results to the truncation error s in (10), at the top of the next page. It is evident that (10) can be upper bounded by (11). To this effect, we use the Pochhammer symbol identities in [15] and after some algebraic manipulations, the resulting expression with the two infinite series can be expressed in terms of the hypergeometric function [11], which yields a closed-form upper bound for $\mathcal{J}_1$. By following the same methodology, it follows that the upper bound of $\mathcal{J}_2$ can be also obtained in closed-form. The aforementioned two representations can be expressed in a more compact form as in (12), at the top of the next page, where the superscript "Tr" denotes *truncate*.

Similarly, a closed-form upper bound for the truncation error of $\mathcal{J}_3$ can be derived as

$$\mathcal{J}_3^{\mathrm{Tr}} < \frac{\mu_E^{2L\mu_E}\Gamma(2L\mu_E)\,{}_1F_0(L\mu_E;;(2\mu_E H_E)^2)}{\Gamma\left(L\mu_E+\frac{1}{2}\right)\bar{\gamma}^{2L\mu_E+2p}e^{-\frac{2\mu_E h_E}{\bar{\gamma}_E}}} \times \sum_{m=1}^{2L\mu_E+2p} \frac{\bar{\gamma}^m}{(2\mu_E h_E)^m}\Gamma\left(-2L\mu_E-2p+m, \frac{2\mu_E h_E}{\bar{\gamma}}\right). \quad (13)$$

The derived bound is tight and can be readily computed in popular software packages that include the involved elementary and special functions as built-in functions. Thus, the accuracy of the derived series can be determined with high degree of accuracy at any given case.

V. Numerical Results and Discussions

In this section, representative numerical examples are plotted along with Monte Carlo simulations to assess the accuracy of the derived mathematical results. Without loss of generality, it is assumed that $R_S = 1$bit/s/Hz throughout the paper. To this effect, Fig. 2 shows the ASC for various number of antennas at Bob and Eve, and by setting $\eta_B = 1.6$, $\eta_E = 0.7$, $\mu_B = 2.5$, $\mu_E = 0.5$, and $\bar{\gamma}_E = 10$ dB. It can be seen that our proposed mathematical analysis is in good agreement with the respective results from the Monte-Carlo simulations in all considered scenarios, which verifies the validity of the derivations. It is also observed that when the number of antennas at Eve increases, the ASC decreases. This makes sense since a high number of antennas at Eve yields some antenna diversity and therefore a secure eavesdropping which can be detrimental to the security performance of the system.

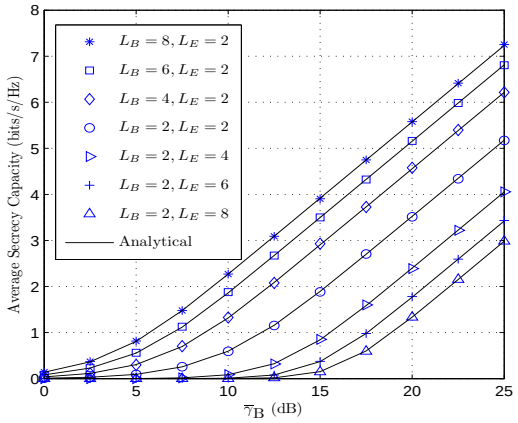

Fig. 2: Exact average secrecy capacity versus $\bar{\gamma}_B$ for various antenna settings ($\eta_B = 1.6$, $\eta_E = 0.7$, $\mu_B = 2.5$, $\mu_E = 0.5$, and $\bar{\gamma}_E = 10$ dB). The symbols represent the simulated ASC.

In the same context, Fig. 3 demonstrates the ASC for different combinations of the fading parameters, and by setting $L_B = 4$, $L_E = 4$, and $\bar{\gamma}_E = 10$ dB. It is evident that the fading parameters have effects on the security performance of the underlying system. Again, a perfect agreement between the analytical and simulation results is observed.

Fig. 4 illustrates the ASC performance for various values of $\bar{\gamma}_E$ and number of antennas L_B. Firstly, it is clear that the simulations and analytical derivations are in agreement in all considered scenarios. Secondly, as the channel quality of the wiretap channel degrades, the ASC performance improves since the eavesdropper is less likely to intercept the message intended for Bob. Thirdly, as the number of antennas at the

$$\mathcal{J}_1 = \sum_{k=p}^{\infty}\sum_{j=p}^{\infty} \frac{H_B^{2k} H_E^{2j} \mu_B^{2k} (2L_E\mu_E + 2j - 1)!}{k! j! 2^{2j} h_E^{2j} \Gamma(L_B\mu_B + k + \frac{1}{2}) \Gamma(L_E\mu_E + j + \frac{1}{2})} \left[(2L_B\mu_B + 2k - 1)! e^{\frac{2\mu_B h_B}{\bar{\gamma}_B}} \sum_{m=1}^{2L_B\mu_B + 2k} \left(\frac{\bar{\gamma}_B}{2\mu_B h_B} \right)^m \right.$$
$$\times \Gamma\left(-2L_B\mu_B - 2k + m, \frac{2\mu_B h_B}{\bar{\gamma}_B} \right) - \sum_{n=0}^{2L_E\mu_E + 2j - 1} \sum_{i=1}^{2L_B\mu_B + 2k + n} \frac{\Gamma(2L_B\mu_B + 2k + n)}{n!} \left(\frac{2\mu_E h_E}{\bar{\gamma}_E} \right)^n$$
$$\left. \times \left(\frac{2\mu_B h_B}{\bar{\gamma}_B} + \frac{2\mu_E h_E}{\bar{\gamma}_E} \right)^{-i} e^{\frac{2\mu_B h_B}{\bar{\gamma}_B} + \frac{2\mu_E h_E}{\bar{\gamma}_E}} \Gamma\left(-2L_B\mu_B - 2k - n + i, \frac{2\mu_B h_B}{\bar{\gamma}_B} + \frac{2\mu_E h_E}{\bar{\gamma}_E} \right) \right]. \tag{10}$$

$$\mathcal{J}_1 < \sum_{k=0}^{\infty} \frac{H_B^{2k} \mu_B^{2k}}{k! \Gamma(L_B\mu_B + k + \frac{1}{2})} \sum_{j=0}^{\infty} \frac{H_E^{2j} (2L_E\mu_E + 2j - 1)!}{j! 2^{2j} h_E^{2j} \Gamma(L_E\mu_E + j + \frac{1}{2})} \times \left[(2L_B\mu_B + 2p - 1)! e^{\frac{2\mu_B h_B}{\bar{\gamma}_B}} \sum_{m=1}^{2L_B\mu_B + 2p} \left(\frac{\bar{\gamma}_B}{2\mu_B h_B} \right)^m \right.$$
$$\times \Gamma\left(-2L_B\mu_B - 2p + m, \frac{2\mu_B h_B}{\bar{\gamma}_B} \right) - \sum_{n=0}^{2L_E\mu_E + 2j - 1} \times \sum_{i=1}^{2L_B\mu_B + 2p + n} \frac{\Gamma(2L_B\mu_B + 2p + n)}{n!} \left(\frac{2\mu_E h_E}{\bar{\gamma}_E} \right)^n$$
$$\left. \times \left(\frac{2\mu_B h_B}{\bar{\gamma}_B} + \frac{2\mu_E h_E}{\bar{\gamma}_E} \right)^{-i} e^{\frac{2\mu_B h_B}{\bar{\gamma}_B} + \frac{2\mu_E h_E}{\bar{\gamma}_E}} \Gamma\left(-2L_B\mu_B - 2p - n + i, \frac{2\mu_B h_B}{\bar{\gamma}_B} + \frac{2\mu_E h_E}{\bar{\gamma}_E} \right) \right]. \tag{11}$$

$$\left\{ \begin{matrix} \mathcal{J}_1 \\ \mathcal{J}_2 \end{matrix} \right\}^{\text{Tr k = j = p}} < \frac{\Gamma\left(2 \left\{ \begin{matrix} L_E\mu_E \\ L_B\mu_B \end{matrix} \right\} \right)}{\Gamma\left(L_B\mu_B + \frac{1}{2} \right) \Gamma\left(L_E\mu_E + \frac{1}{2} \right)} {}_0F_1\left(; \left\{ \begin{matrix} L_B\mu_B \\ L_E\mu_E \end{matrix} \right\} + \frac{1}{2}; \left\{ \begin{matrix} H_B^2\mu_B^2 \\ H_E^2\mu_E^2 \end{matrix} \right\} \right) {}_1F_0\left(\left\{ \begin{matrix} L_E\mu_E \\ L_B\mu_B \end{matrix} \right\}; ; \left\{ \begin{matrix} H_E^2/h_E^2 \\ H_B^2/h_B^2 \end{matrix} \right\} \right)$$
$$\times \left[\left(2 \left\{ \begin{matrix} L_B\mu_B \\ L_E\mu_E \end{matrix} \right\} + 2p - 1 \right)! e^{\left\{ \begin{matrix} 2\mu_B h_B/\bar{\gamma}_B \\ 2\mu_E h_E/\bar{\gamma}_E \end{matrix} \right\}} \sum_{m=1}^{2\left\{ \begin{matrix} L_B\mu_B \\ L_E\mu_E \end{matrix} \right\} + 2p} \left(\left\{ \begin{matrix} \bar{\gamma}_B/(2\mu_B h_B) \\ \bar{\gamma}_E/(2\mu_E h_E) \end{matrix} \right\} \right)^m \Gamma\left(-2 \left\{ \begin{matrix} L_B\mu_B \\ L_E\mu_E \end{matrix} \right\} - 2p + m, 2 \left\{ \begin{matrix} \mu_B h_B/\bar{\gamma}_B \\ \mu_E h_E/\bar{\gamma}_E \end{matrix} \right\} \right) \right. \tag{12}$$
$$- \sum_{n=0}^{2\left\{ \begin{matrix} L_E\mu_E \\ L_B\mu_B \end{matrix} \right\} + 2j - 1} \sum_{i=1}^{2\left\{ \begin{matrix} L_B\mu_B \\ L_E\mu_E \end{matrix} \right\} + 2p + n} \frac{\Gamma(2 \left\{ \begin{matrix} L_B\mu_B \\ L_E\mu_E \end{matrix} \right\} + 2p + n)}{n!} \left(\frac{2\mu_E h_E}{\bar{\gamma}_E} \right)^n \left(\frac{2\mu_B h_B}{\bar{\gamma}_B} + \frac{2\mu_E h_E}{\bar{\gamma}_E} \right)^{-i} e^{\frac{2\mu_B h_B}{\bar{\gamma}_B} + \frac{2\mu_E h_E}{\bar{\gamma}_E}}$$
$$\left. \times \Gamma\left(-2 \left\{ \begin{matrix} L_B\mu_B \\ L_E\mu_E \end{matrix} \right\} - 2p - n + i, \frac{2\mu_B h_B}{\bar{\gamma}_B} + \frac{2\mu_E h_E}{\bar{\gamma}_E} \right) \right]$$

intended receiver increases, the ASC performance improves since the probability of secure transmission is increased.

Finally, Table I shows the ASC for different values of η_B, η_E, μ_B, μ_E and other parameter values. The best and worst scenarios are considered, namely: (a) severe η_B and μ_B with favorable η_E and μ_E; and (b) favorable η_B and μ_B with severe η_E and μ_E. Without loss of generality, the following parameters are used: $\bar{\gamma}_B = \{15\text{dB}, 25\text{dB}\}$ and $\eta_\iota = 4, \mu_\iota = 2$ (severe), $\eta_\iota = 1, \mu_\iota = 5$ (light or favorable). In addition, $\bar{\gamma}_E = 0\text{dB}$ is considered. First, it is noted that the ASC performance is affected by the different values of the fading parameters η_ι and μ_ι. For example in *Format 1*, it can be noted that for various number of antennas or main link SNR values, the ASC under severe η_B, μ_B and light η_E, μ_E outperforms the one with favorable η_B, μ_B and severe η_E, μ_E. Furthermore, as the number of antennas L_B and L_E increases, the ASC improves regardless of the scenario and the values of the main link SNR (e.g. 15dB, 25dB). More importantly, it is noticed that for any number of antennas, the ASC in scenario (b) outperforms the one in scenario (a). It is also worth to mention that the performance difference between the two scenarios increases with the number of antennas between the corresponding values of the main link SNR.

Therefore, it is evident that accurate characterization and modeling of fading conditions is crucial in the realistic quantification of the ASC. Future work will consider the use of different fading conditions in the two links as well as different radio frequency impairments which are expected to play considerable role in the achievable ASC. Also, investigations in the context of orthogonal and non-orthogonal multiple access schemes are expected to provide meaningful insights that will be particularly useful in the design and deployment of future communication systems.

VI. Conclusions

In this paper, we have studied the secrecy performance of a wireless communication system over generalized η-μ fading channels. The derived analytical expression for the ASC

TABLE I: Effects of η_B, μ_B and η_E, μ_E on the ASC for various system parameters.

Formats	System Parameters		$\bar{\gamma}_B$ (dB)	ASC (bits/s/Hz)
Format 1	severe η_B–μ_B, light η_E–μ_E	$L_B = 1,\ L_E = 1$	15	3.81980
			25	7.08452
		$L_B = 2,\ L_E = 2$	15	4.31824
			25	7.61596
		$L_B = 3,\ L_E = 3$	15	4.51655
			25	7.82320
	light η_B–μ_B, severe η_E–μ_E	$L_B = 1,\ L_E = 1$	15	4.01385
			25	7.29112
		$L_B = 2,\ L_E = 2$	15	4.43691
			25	7.73743
		$L_B = 3,\ L_E = 3$	15	4.60384
			25	7.91168

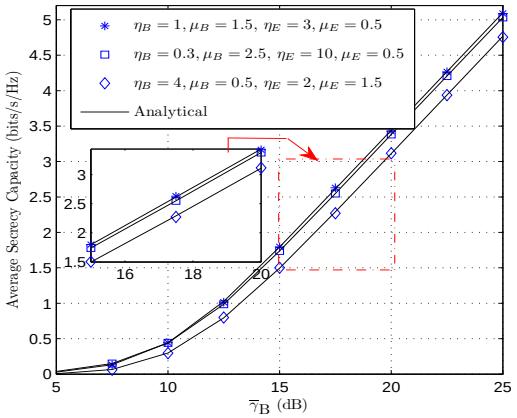

Fig. 3: Exact average secrecy capacity versus $\bar{\gamma}_B$ for various fading parameter settings ($L_B = 4$, $L_E = 4$, and $\bar{\gamma}_E = 10$ dB). The symbols represent the simulated ASC.

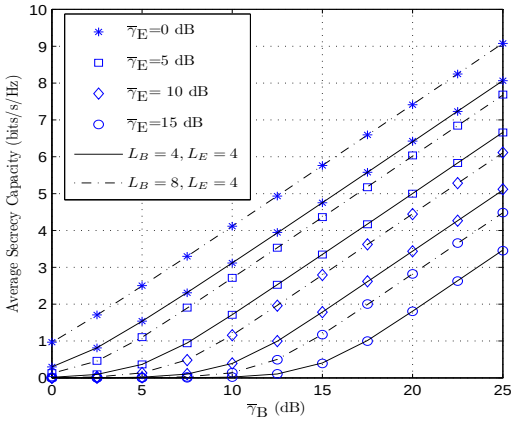

Fig. 4: Exact average secrecy capacity versus $\bar{\gamma}_B$ for $\eta_B = 2.5$, $\mu_B = 3.5$, and $\eta_E = 0.85$, $\mu_E = 0.5$. The symbols represent the simulated ASC and the solid and dash lines represent the analytical ASC.

has been validated through Monte-Carlo simulations. Also, a tractable closed-form upper bound for truncation error of the exact ASC is derived since the aforementioned expression is given in terms of double series representation. Finally, some valuable insights of the effects of the fading parameter on the security performance are provided.

REFERENCES

[1] X. Liu, "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.

[2] M. Kamel, W. Hamouda and A. Youssef, "Physical layer security in ultra-dense networks," *IEEE Wireless Commun. Lett.*, vol. 6, no. 5, pp. 690−693. Oct. 2017

[3] X. Liu, "Outage probability of secrecy capacity over correlated lognormal fading channels," *IEEE Commun. Lett.*, vol. 17, no. 2, pp. 289–292, Feb. 2013.

[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. 1257–1260, Jul. 2015.

[5] H. Lei, H. Zhang, I. S. Ansari, C. Gao, Y. Guo, G. Pan, and K. A. Qaraqe,, "Performance analysis of physical layer security over generalized-K fading channels using a mixture Gamma distribution," *IEEE Commun. Lett.*, vol. 20, no. 2, pp. 408–411, Feb. 2016.

[6] N. Bhargav, S. L. Cotton, and D. E. Simmons, "Secrecy capacity analysis over κ-μ fading channels: theory and applications,," *IEEE Trans. Commun.*, vol. 64, no. 7, pp. 3011–3024, Jul. 2016.

[7] H. Lei, I. S. Ansari, G. Pan, B. Alomair, and M.S. Alouini, "Secrecy capacity analysis over κ-μ fading channels," *IEEE Commun. Lett.*, vol. 21, no. 6, pp. 1445–1448, Jun. 2017.

[8] 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.

[9] J. M. Moualeu and W. Hamouda, "On the secrecy performance analysis of SIMO systems over κ-μ fading channels," *IEEE Commun. Lett.*, vol. 21, no. 11, pp. 2544–2547, Nov. 2017.

[10] M. D. Yacoub, "The η-μ distribution and the κ-μ distribution," *IEEE Antennas Propag. Mag.*, vol. 49, no. 1, pp. 68–81, Feb. 2007.

[11] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*, 7th ed., San Diego, CA: Academic, 2007.

[12] K. Peppas, F. Lazarakis, A. Alexandridis, and K. Dangakis, "Error performance of digital modulation schemes with MRC diversity reception over η-μ fading channels," *IEEE Trans. Wireless Commun.*, vol. 8, no. 10, pp. 4974–4980, Oct. 2009.

[13] L. Wang, M. Elkashlan, J. Huang, R. Schober, and R. Mallik, "Secure transmission with antenna selection in MIMO Nakagami-m fading channels," *IEEE Trans. Wireless Commun.*, vol. 13, no. 11, pp. 6054–6067, Nov. 2014.

[14] M.-S. Alouini and A. Goldsmith, "Capacity of Rayleigh fading channels under different adapative transmission and diversity-combining techniques," *IEEE Trans. Veh. Technol.*, vol. 48, no. 4, pp. 1165–1181, Jul. 1999.

[15] P. C. Sofotasios, T. A. Tsiftsis, Yu. A. Brychkov, S. Freear, M. Valkama, and G. K. Karagiannidis, "Analytic expressions and bounds for special functions and applications in communication theory," *IEEE Trans. Inf. Theory*, vol. 60, no. 12, pp. 7798–7823, Dec. 2014.