Secrecy Capacity of a Nakagami-m Fading Channel in the Presence of Cooperative Eavesdroppers

Souad Belmoubarik, *Student Member, IEEE*, Ghassane Aniba, *Member, IEEE*, Belhaj Elgraini
Electronics and Communications Laboratory (LEC)
Mohammadia School of Engineers, Mohammed V University, Rabat, Morocco
Email: {belmoubarik,ghassane,elgraini}@emi.ac.ma

***Abstract*—Physical layer security helps enormously cryptography to improve the confidentiality of communications over wireless networks. Indeed, the secrecy capacity is used at the physical layer to ensure not only the security of communications but also to exploit efficiently the channel capacity. The principle of secrecy capacity is to characterize the maximum data transmission rate, that can be reached while the exchanged information is kept secret from a malicious entity. In this paper, we present a closed-form expression of outage probability and we specify the outage secrecy capacity of a Nakagami-m fading channel in the presence of cooperative correlated eavesdroppers performing the maximal ratio combining which helps the eavesdroppers to tap the maximum of the exchanged information between the transmitter and the legitimate receiver. Simulations results show that a raise in the number of the cooperative eavesdroppers degrades significantly the secrecy capacity of this communication system, moreover the correlation degree between the eavesdroppers has a negative impact on the communication confidentiality especially when it takes small values.**

***Index Terms*—Secrecy capacity, outage probability, cooperative Nakagami-m fading channel, constant correlation.**

I. Introduction

THE information security is one of the biggest issues in the communication theory. Messages sent by a transmitter must be decoded only by legitimate(s) receiver(s) and not by any malicious enemy. From the beginning, Shannon developed the theory of secrecy systems to strength the information security and defined the mathematical structure of secrecy systems [1]. Moreover, some recent research studies have investigated the secrecy capacity of different fading channels. Among these studies, El Gamal [2] characterized the secrecy capacity of an ergodic fading wiretap channel, for different scenarios depending on the availability of channel state information (CSI) at the transmitter. In fact, he suggested a power control approach and a data rate adaptation to enhance the secrecy capacity of such system. The work done in [3] focused on the transmission of confidential data over a single input single output (SISO) suffering from Rayleigh fading, this communication system is subject to be eavesdropped by a third party and provided the outage secrecy capacity of that wireless channel. Whereas authors in [4], determined an asymptotic secrecy capacity of a correlated log-normal fading channels performing the maximal ratio and the equal gain combining for both the legitimate receiver and the eavesdroppers. In addition to that, the secrecy capacity of multiple independent eavesdroppers have been studied in [5], where both the main channel and each eavesdropper channel undergoes the Nakagami-m fading. An other work in [6] has characterized the upper and the lower bounds of the secrecy capacity of a communication system composed by a transmitter with single antenna exchanging secret information with a legitimate receiver endowed with multiple antennas in the presence of an eavesdropper equipped with multiple antennas. This later is supposed to perform the maximal ratio combining (MRC) or the selection combining (SC) techniques in order to tap the maximum of information through a correlated Rayleigh fading channels.

In order to complement the studies done previously on the secrecy capacity for different fading channels, we consider in this paper to work on a Nakagami-m fading channel subject to multiple cooperative eavesdroppers in a constant correlation scenario. The considered communication system is a SISO where the transmitter and the legitimate receiver have perfect CSI about the main channel. The purpose of this paper is to present a closed form expression of the outage probability, as well as characterize the secrecy capacity of this communication system by the outage secrecy capacity.

The rest of this paper is organized as follows: the description of the proposed system is presented in Section II. The outage probability as well as the outage secrecy capacity are detailed in Section III. In Section IV, we discuss the performance analysis of the outage secrecy capacity of the studied communication system. Finally, a conclusion is presented in Section V.

II. System Model

We consider the following scenario, which is illustrated in Fig. 1. A transmitter Tx wants to send a confidential message W to a legitimate receiver Rx. The message is subject to a third party. This later is a cluster of L cooperative eavesdroppers trying to decode the exchanged message throughout the main channel, which is the channel between the transmitter and the legitimate receiver. Throughout this paper, we suppose that the main channel and each channel of the cooperative eavesdroppers undergoes Nakagami-m fading and their states are independent from the one of the main channel. However, we assume that the set of the eavesdroppers channels are identically distributed as well as correlated between them. In addition to that, it is supposed that the transmitter and the legitimate receiver have perfect CSI about the main channel, but no CSI about the eavesdropper channel. Besides, the

978-1-4799-7391-0/14/$31.00

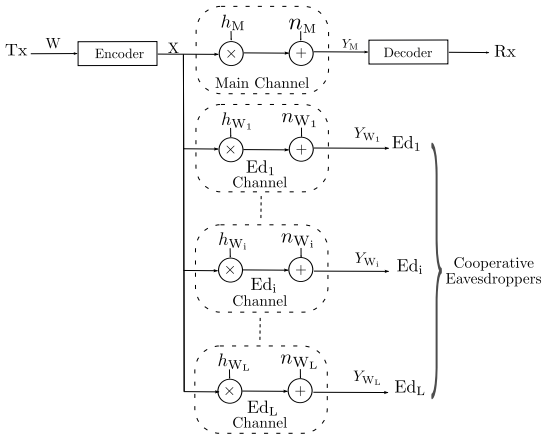


Fig. 1: The system model of the wiretap Nakagami$-m$ fading channel

cooperative eavesdroppers perform an ideal MRC at the level of an elected eavesdropper from the set in order to combine the received signals from the overall eavesdroppers branches.

The received signals at time t at the legitimate receiver and at each channel of the cooperative eavesdroppers are represented as following:

$$y_{\mathrm{M}}(t) = x(t)h_{\mathrm{M}}(t) + n_{\mathrm{M}}(t)$$

and

$$y_{\mathrm{Wi}}(t) = x(t)h_{\mathrm{W_i}}(t) + n_{\mathrm{W_i}}(t),\ i = 1, 2, ..., L$$

Where i denotes the diversity order, $h_{\mathrm{M}}(i)$ and $h_{\mathrm{W}}(i)$ are the complex channel coefficient of the main channel and the i^{th} eavesdropper channel respectively. Both the main and the eavesdroppers channels are respectively affected by $n_{\mathrm{M}}(t)$, $n_{\mathrm{Wi}}(t)$. These latter, represent additive white Gaussian noise (AWGN) with zero mean and unit variance for both channels. We consider in our model that the Nakagami-m fading is assumed to be quasi-static for both the considered channels. Thus, the gain of each channel stays constant over the coherence time, i.e. $h_{\mathrm{M}}(t)$=h_{M} and $h_{\mathrm{W_i}}(t)$=$h_{\mathrm{W_i}}$, and changes independently from one coherence time to another coherence time.

III. Secrecy Rate and Secrecy Capacity of the channel

The secrecy capacity is the maximum of achievable secrecy rate. Where, The secrecy rate is the amount of information that can be exchanged between two entities under the condition to be transmitted reliably and confidently. The capacity of the main channel and the eavesdropper are respectively given by

$$C_{\mathrm{M}} = \log\left(1 + \gamma_{\mathrm{M}}\right) \qquad \text{and} \qquad C_{\mathrm{W}} = \log\left(1 + \gamma_{\mathrm{W}}\right),$$

where,

$$\gamma_{\mathrm{M}} = |h_{\mathrm{M}}|^2 \frac{P}{N_{\mathrm{M}}} \qquad \text{and} \qquad \gamma_{\mathrm{W}} = |h_{\mathrm{W}}|^2 \frac{P}{N_{\mathrm{W}}}$$

We denote P the channel power for both the main and the eavesdropper channel. Besides, N_{M} and N_{W} are the noise power of main channel and the eavesdropper channel respectively. Then, the secrecy capacity for one realization of the proposed quasi-static Nakagami-m fading can be defined as following [3]:

$$C_{\mathrm{s}} = \begin{cases} \log(1+\gamma_{\mathrm{M}}) - \log(1+\gamma_{\mathrm{W}}) & if \quad \gamma_{\mathrm{M}} > \gamma_{\mathrm{W}} \\ 0 & if \quad \gamma_{\mathrm{M}} \leq \gamma_{\mathrm{W}} \end{cases} \tag{1}$$

A. The existence of a non-zero secrecy capacity

As mentioned previously, both the main channel and the L eavesdroppers branches experience Nakagami-m fading. The probability density function (PDF) of the channels gain $|h_{\mathrm{M}}|$ and $|h_{\mathrm{W_i}}|$ is given by

$$p(g) = \frac{2m^m g^{2m-1}}{\Gamma(m)P^m} \exp\left(-\frac{mg^2}{P}\right)$$

where P is the average received power, g is the channel gain, $\Gamma(.)$ is the Gamma function and m is the fading parameter.

Since, the signal-to-noise ratio (SNR) of both main and eavesdroppers channels are function of the channel power gain, i.e. γ_{M} or $\gamma_{\mathrm{W_i}} \sim |h|^2$. Then the power fading gain follows a Gamma distribution defined by

$$p(\gamma_{\mathrm{M}}) = \left(\frac{v}{\bar{\gamma}_{\mathrm{M}}}\right)^{v} \frac{\gamma_{\mathrm{M}}^{v-1}}{\Gamma(v)} \exp\left(-v\frac{\gamma_{\mathrm{M}}}{\bar{\gamma}_{\mathrm{M}}}\right), \quad \gamma_{\mathrm{M}} > 0$$

$$p(\gamma_{\mathrm{W_i}}) = \left(\frac{u_i}{\bar{\gamma}_{\mathrm{W_i}}}\right)^{u_i} \frac{\gamma_{\mathrm{W_i}}^{u_i-1}}{\Gamma(u_i)} \exp\left(-u_i\frac{\gamma_{\mathrm{Wi}}}{\bar{\gamma}_{\mathrm{Wi}}}\right), \quad \gamma_{\mathrm{W_i}} > 0$$

where v and u_i are the Nakagami-m fading parameters for the main channel and the i^th, $0 \leq i < L$, eavesdropper branch respectively. It is considered that all the L eavesdroppers branches are identically distributed. Furthermore we denote, $\bar{\gamma}_{\mathrm{M}}$ and $\bar{\gamma}_{\mathrm{W_i}}$ are the average of the SNR for the main channel and the i^th eavesdropper branch respectively. We assume that all eavesdroppers branches have identical fading parameter, u_i=u_j=u for $i,\ j \in$ [0, L], and identical average signal power, $\bar{\gamma}_{\mathrm{W_i}} = \bar{\gamma}_{\mathrm{W_b}}$, then the PDF of each eavesdropper branch is given by

$$p(\gamma_{\mathrm{W_i}}) = \left(\frac{u}{\bar{\gamma}_{\mathrm{W_b}}}\right)^{u} \frac{\gamma_{\mathrm{W_i}}^{u-1}}{\Gamma(u)} \exp\left(-u\frac{\gamma_{\mathrm{W_i}}}{\bar{\gamma}_{\mathrm{W_b}}}\right), \quad \gamma_{\mathrm{W_i}} > 0$$

Since the L diversity branches are correlated and will be received at one of the eavesdroppers performing an ideal MRC, then the SNR output γ_{W} at the combiner follows the distribution defined by [7]

$$p(\gamma_{\mathrm{W}}) = \frac{u^{uL} a^u b^{u(L-1)}}{\Gamma(uL)} \gamma_{\mathrm{W}}^{uL-1} \exp(-ub\gamma_{\mathrm{W}}) \; {}_1F_1(u, uL, u(b-a)\gamma_{\mathrm{W}}), \tag{2}$$

where

$$a = \frac{1}{\bar{\gamma}_{\mathrm{W_b}}(1 + (L-1)\rho)} \qquad \text{and} \qquad b = \frac{1}{\bar{\gamma}_{\mathrm{W_b}}(1-\rho)}$$

We have assumed that the different branches are close from each other, then the correlation coefficient ρ could be considered constant. In fact, i.e $\rho_{ij} = \rho$ with $0 \leq \rho < 1$.

The probability of the existence of a non-zero secrecy capacity can be expressed by

$$\begin{aligned} P(C_{\mathrm{s}} > 0) =& P(\gamma_{\mathrm{M}} > \gamma_{\mathrm{W}}) \\ =& \int_0^{\infty} \int_0^{\gamma_{\mathrm{M}}} p(\gamma_{\mathrm{M}}, \gamma_{\mathrm{W}}) \, \mathrm{d}\gamma_{\mathrm{M}} \mathrm{d}\gamma_{\mathrm{W}} \\ =& \int_0^{\infty} \int_0^{\gamma_{\mathrm{M}}} p(\gamma_{\mathrm{M}}) p(\gamma_{\mathrm{W}}) \, \mathrm{d}\gamma_{\mathrm{M}} \mathrm{d}\gamma_{\mathrm{W}} \end{aligned}$$

where the final expression of this probability is given in Eq. (3), we denote that ${}_2\mathrm{F}_1$ is the Gaussian Hypergeometric series [8].

In the case of independent cooperative eavesdroppers channels ($\rho = 0$), the expression in (3) becomes as following

$$\begin{aligned} P(C_{\mathrm{s}} > 0) = & \frac{\Gamma(v+uL)}{\Gamma(v)\Gamma(uL+1)} \frac{\left(\frac{v}{\bar{\gamma}_{\mathrm{M}}}\right)^{v} \left(\frac{u}{\bar{\gamma}_{\mathrm{We}}}\right)^{uL}}{\left(\frac{v}{\bar{\gamma}_{\mathrm{M}}} + \frac{u}{\bar{\gamma}_{\mathrm{We}}}\right)^{v+uL}} \\ & {}_2\mathrm{F}_1 \left(1, v+uL; 1+uL; \frac{1}{1+\frac{v\bar{\gamma}_{\mathrm{Wb}}}{u\bar{\gamma}_{\mathrm{M}}}}\right) \end{aligned}$$

In the case of Rayleigh fading channel eavesdropped by a single wiretapper ($v = 1$, $u = 1$, $L = 1$ and $\rho = 0$), the expression in (3) becomes equivalent to the corresponding equation presented in [3].

B. Outage Probability and Outage secrecy capacity

The secrecy rate is obtained by calculating the outage probability which refers to an outage that occurs in the communication between the legitimate nodes, when the transmitter sends data at a rate R_{s} higher than C_{s}. In such case, the target error probability can not be satisfied and that lead to an outage in the communication system.

$$P_{\mathrm{out}}(R_{\mathrm{s}}) = P(C_{\mathrm{s}} < R_{\mathrm{s}}) \tag{4}$$

Hereafter, we use (4) to calculate the probability outage of the proposed system.

$$\begin{aligned} P_{\mathrm{out}}(R_{\mathrm{s}}) = & P(C_{\mathrm{s}} < R_{\mathrm{s}} | \gamma_{\mathrm{M}} > \gamma_{\mathrm{W}}) P(\gamma_{\mathrm{M}} > \gamma_{\mathrm{W}}) \\ & + P(C_{\mathrm{s}} < R_{\mathrm{s}} | \gamma_{\mathrm{M}} \leq \gamma_{\mathrm{W}}) P(\gamma_{\mathrm{M}} \leq \gamma_{\mathrm{W}}) \end{aligned} \tag{5}$$

With,

$$P(\gamma_M \leq \gamma_{\mathrm{W}}) = 1 - P(\gamma_{\mathrm{M}} > \gamma_{\mathrm{W}}) \tag{6}$$

Based on (1) when γ_{M} is lower than γ_{W}, the secrecy capacity is equal to zero also since $R_{\mathrm{s}} > 0$, consequently we have;

$$P(C_{\mathrm{s}} < R_{\mathrm{s}} | \gamma_{\mathrm{M}} \leq \gamma_{\mathrm{W}}) = 1 \tag{7}$$

We have also,

$$\begin{aligned} & P(C_{\mathrm{s}} < R_{\mathrm{s}} | \gamma_{\mathrm{M}} > \gamma_{\mathrm{W}}) \\ & = P(\log(1+\gamma_{\mathrm{M}}) - \log(1+\gamma_{\mathrm{W}}) < R_{\mathrm{s}} | \gamma_{\mathrm{M}} > \gamma_{\mathrm{W}}) \\ & = P(\gamma_{\mathrm{M}} < 2^{R_{\mathrm{s}}}(1+\gamma_{\mathrm{W}}) - 1 | \gamma_{\mathrm{M}} > \gamma_{\mathrm{W}}) \\ & = \int_0^{\infty} \int_{\gamma_{\mathrm{W}}}^{(1+\gamma_{\mathrm{W}})2^{R_{\mathrm{s}}}-1} p(\gamma_{\mathrm{M}}, \gamma_{\mathrm{W}} | \gamma_{\mathrm{M}} > \gamma_{\mathrm{W}}) \, \mathrm{d}\gamma_{\mathrm{M}} \mathrm{d}\gamma_{\mathrm{W}} \\ & = \int_0^{\infty} \int_{\gamma_{\mathrm{W}}}^{(1+\gamma_{\mathrm{W}})2^{R_{\mathrm{s}}}-1} \frac{p(\gamma_{\mathrm{M}}, \gamma_{\mathrm{W}})}{p(\gamma_{\mathrm{M}} > \gamma_{\mathrm{W}})} \, \mathrm{d}\gamma_{\mathrm{M}} \mathrm{d}\gamma_{\mathrm{W}} \end{aligned}$$

Since the two considered main and eavesdropper channels are independents, then:

$$\begin{aligned} & P(C_s < R_s | \gamma_{\mathrm{M}} > \gamma_{\mathrm{W}}) P(\gamma_{\mathrm{M}} > \gamma_{\mathrm{W}}) \\ & = P(\gamma_{\mathrm{M}} > \gamma_{\mathrm{W}}) \int_0^{\infty} \int_{\gamma_{\mathrm{W}}}^{(1+\gamma_{\mathrm{W}})2^{R_s}-1} \frac{p(\gamma_{\mathrm{M}}) p(\gamma_{\mathrm{W}})}{p(\gamma_{\mathrm{M}} > \gamma_{\mathrm{W}})} \, \mathrm{d}\gamma_{\mathrm{M}} \mathrm{d}\gamma_{\mathrm{W}} \\ & = \int_0^{\infty} \int_{\gamma_{\mathrm{W}}}^{(1+\gamma_{\mathrm{W}})2^{R_s}-1} p(\gamma_{\mathrm{M}}) p(\gamma_{\mathrm{W}}) \, \mathrm{d}\gamma_{\mathrm{M}} \mathrm{d}\gamma_{\mathrm{W}} \\ & = \int_0^{\infty} \int_0^{(1+\gamma_{\mathrm{W}})2^{R_s}-1} p(\gamma_{\mathrm{M}}) p(\gamma_{\mathrm{W}}) \, \mathrm{d}\gamma_{\mathrm{M}} \mathrm{d}\gamma_{\mathrm{W}} \\ & - \int_0^{\infty} \int_0^{\gamma_{\mathrm{W}}} p(\gamma_{\mathrm{M}}) p(\gamma_{\mathrm{W}}) \, \mathrm{d}\gamma_{\mathrm{M}} \mathrm{d}\gamma_{\mathrm{W}} \end{aligned}$$

If we recall (5) and (7), the formula of the probability outage is given by

$$\begin{aligned} P_{\mathrm{out}}(R_{\mathrm{s}}) = & \int_0^{\infty} \int_0^{(1+\gamma_{\mathrm{W}})2^{R_{\mathrm{s}}}-1} p(\gamma_{\mathrm{M}}) p(\gamma_{\mathrm{W}}) \, \mathrm{d}\gamma_{\mathrm{M}} \mathrm{d}\gamma_{\mathrm{W}} \\ & - \int_0^{\infty} \int_0^{\gamma_{\mathrm{W}}} p(\gamma_{\mathrm{M}}) p(\gamma_{\mathrm{W}}) \, \mathrm{d}\gamma_{\mathrm{M}} \mathrm{d}\gamma_{\mathrm{W}} + 1 - P(\gamma_{\mathrm{M}} > \gamma_{\mathrm{W}}) \end{aligned}$$

From the definition of the probability $P(\gamma_{\mathrm{W}} > \gamma_{\mathrm{M}})$ and (6) we have as follows:

$$\begin{aligned} P(\gamma_{\mathrm{W}} > \gamma_{\mathrm{M}}) &= \int_0^{\infty} \int_0^{\gamma_{\mathrm{W}}} p(\gamma_{\mathrm{M}}) p(\gamma_{\mathrm{W}}) \, \mathrm{d}\gamma_{\mathrm{M}} \mathrm{d}\gamma_{\mathrm{W}} \\ &= 1 - P(\gamma_{\mathrm{M}} > \gamma_{\mathrm{W}}) \end{aligned}$$

Thus,

$$P_{\mathrm{out}}(R_{\mathrm{s}}) = \int_0^{\infty} \int_0^{(1+\gamma_{\mathrm{W}})2^{R_s}-1} p(\gamma_{\mathrm{M}}) p(\gamma_{\mathrm{W}}) \, \mathrm{d}\gamma_{\mathrm{M}} \mathrm{d}\gamma_{\mathrm{M}}$$

$$P(C_{\mathrm{s}} > 0) = \frac{u^{uL} a^{u} b^{u(L-1)}}{\Gamma(v)\Gamma(uL)} \left(\frac{v}{\bar{\gamma}_{\mathrm{M}}}\right)^{v} \sum_{k=0}^{\infty} \frac{(u)_k}{(uL)_k} \frac{(u(b-a))^k}{k!} \frac{\Gamma(v+uL+k)}{(uL+k)\left(\frac{v}{\bar{\gamma}_{\mathrm{M}}} + ub\right)^{v+uL+k}} {}_2\mathrm{F}_1 \left(1, v+uL+k; 1+k+uL; \frac{1}{1+\frac{v}{ub\bar{\gamma}_{\mathrm{M}}}}\right) \tag{3}$$

which lead to have after some calculation ,

$$P_{\text{out}} = \int_0^{\infty} \frac{a^u b^{u(L-1)}}{\Gamma(v)} \frac{u^{uL}}{\Gamma(uL)} {\gamma_{\text{W}}}^{uL-1} \exp(-ub\gamma_{\text{W}}) \\ {}_1\text{F}_1\left(u, uL, u(b-a)\gamma_{\text{W}}\right) \gamma\left(v, \frac{v}{\bar{\gamma}_{\text{M}}}(2^{R_{\text{s}}}(1+\gamma_{\text{W}})-1)\right) \text{d}\gamma_{\text{W}}$$

Then, we obtain a Laplace Transform of the product of two confluent hypergeometric function of the first kind as following,

$$\begin{aligned} P_{\text{out}} =& \frac{a^u b^{u(L-1)}}{\Gamma(v+1)} \frac{u^{uL}}{\Gamma(uL)} \left(\frac{v}{\bar{\gamma}_{\text{M}}}\right)^v \exp(-\frac{v}{\bar{\gamma}_{\text{M}}}(2^{R_{\text{s}}}-1)) \\ & \int_0^{\infty} {\gamma_{\text{W}}}^{uL-1} ((2^{R_{\text{s}}}-1) + 2^{R_{\text{s}}}\gamma_{\text{W}})^v \\ & \exp\left(-(ub + \frac{v}{\bar{\gamma}_{\text{M}}}2^{R_{\text{s}}})\gamma_{\text{W}}\right) {}_1F_1\left(u, uL, u(b-a)\gamma_{\text{W}}\right) \\ & {}_1\text{F}_1\left(1, 1+v, \frac{v}{\bar{\gamma}_{\text{M}}}(2^{R_{\text{s}}}(1+\gamma_{\text{W}})-1)\right) \text{d}\gamma_{\text{W}} \end{aligned}$$

We denote that both the fading factors v and u are reals numbers. After the decomposition of the two hypergeometric function above as well as after an extensive computations, we present in Eq. (8) the final closed-form formula of the outage probability which is given by
where U is the Tricomi confluent hypergeometric function, the Kummer's function of the second kind, [9] which is defined by

$$U(\alpha, \beta, z) = \frac{1}{\Gamma(\alpha)} \int_0^{\infty} \exp(-zt) t^{\alpha-1} (1+t)^{\beta-\alpha-1} \, \text{d}t \quad (9)$$

under the condition that $\text{Re}[\alpha] > 0$ and $\text{Re}[z] > 0$.

In the case of Rayleigh fading channel eavesdropped by a single wiretapper ($v = 1$, $u = 1$, $L = 1$ and $\rho = 0$), the expression in (8) becomes equivalent to the corresponding equation presented in [3].

As mentioned before, The secrecy capacity of the proposed communication system will be characterized by the outage secrecy capacity. Where, the outage secrecy capacity is the maximum of achievable transmission rate such that the probability outage is smaller than a target small value as described below.

$$C_{\text{out}}(\epsilon) = \max_{P_{\text{out}}(R_s) \leq \epsilon} (R_{\text{s}})$$

However, it is complicated to analytically resolve (8) to find the maximum rate R_s which corresponds to the C_{out} because of the difficulty to find the inverse function for the Tricomi function U. Therefore, we will calculate numerically the value of C_{out} in the next section.

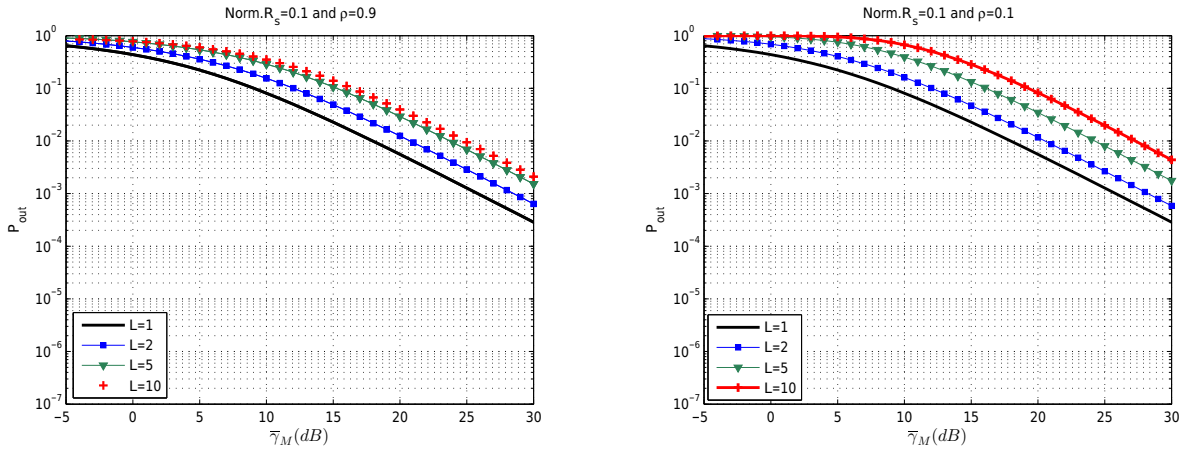
IV. Simulation and Results

In this section, we analyze the outage secrecy capacity of a SISO communication system target of a set of cooperative correlated eavesdroppers as well as the secrecy capacity of a wiretap Gaussian channel in the presence of one eavesdropper with $\bar{\gamma}_{\text{W}_\text{b}}$=5dB. Both the main channel and the branches of the correlated eavesdroppers experience Nakagami-m fading. We have simulated this communication system under some assumptions as described in the previous sections. We denote that the considered normalization in Figs 2 and 3 is done with respect to the capacity of an AWGN channel with SNR equal to each value of $\bar{\gamma}_{\text{M}}$.

Figure 2 shows the variations of the outage probability versus the main channel's SNR for selected values of u=0.5, v=1.5 and $\bar{\gamma}_{\text{W}_\text{b}} = 0$dB for both cases (a) $\rho = 0.9$ and (b) $\rho = 0.1$. In these scenarios, the outage probability decreases as the SNR of the main channel increases and as the correlation parameter increases. Besides, the outage probability increases with the number of the cooperative eavesdroppers. For the same number of eavesdroppers $L = 5$, we denote that when the correlation parameter decreases from $\rho = 0.9$ to $\rho = 0.1$, the outage probability increases by 40% for the value of $\bar{\gamma}_{\text{M}} = 8$dB. However, this percentage becomes lower when the the main channel's SNR takes high values, for example it achieves 16% for $\bar{\gamma}_{\text{M}} = 25$dB. Moreover, a considerable outage occurs as the number of the eavesdroppers raises. For instance, for $L = 10$, the P_{out} increases by 90% when the parameter $\rho = 0.9$ changes to the value $\rho = 0.1$, this percentage approximatively remains constant for all values of $\bar{\gamma}_{\text{M}}$. In order to analyze these results, the number of eavesdroppers impacts negatively the communication confidentiality. Since the eavesdroppers cluster performs the MRC technique to tap the maximum of exchanged information.

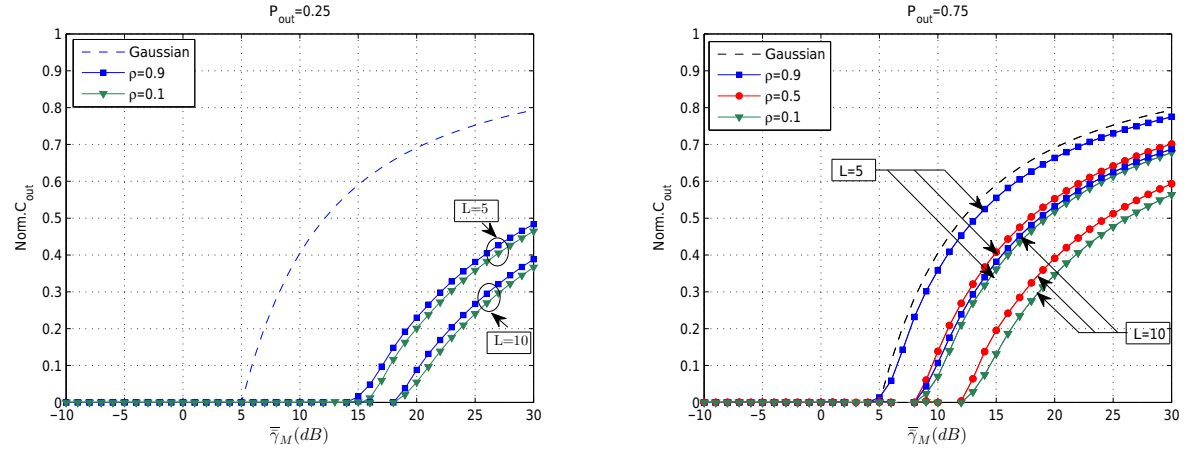
When the number of eavesdroppers is small in a low correlation scenario, an increase in the main channel SNR value reduces significantly the outage probability. However when the number of the eavesdroppers raises, the output signal $\bar{\gamma}_{\text{W}}$ is considerably high which causes an important outage probability even if $\bar{\gamma}_{\text{M}}$ increases. Furthermore, in high correlation scenario, the eavesdroppers number doesn't have a big impact on the outage probability. Then an important correlation coefficient deteriorates the quality of eavesdropper output signal and consequently its capacity which leads to a low outage probability.

$$\begin{aligned} P_{\text{out}} = & a^u b^{u(L-1)} \left(\frac{v}{\bar{\gamma}_{\text{M}}}\right)^v \left(\frac{u}{2^{R_{\text{s}}}}\right)^{uL} (2^{R_s}-1)^{v+uL} \exp(-\frac{v}{\bar{\gamma}_{\text{M}}}(2^{R_s}-1)) \sum_{l=0}^{\infty} \sum_{k=0}^{\infty} \left(\frac{v}{\bar{\gamma}_{\text{M}}}\right)^k \frac{(2^{R_s}-1)^{k+l}}{2^{R_{\text{s}}l}} \frac{(u)_l (u(b-a))^l}{\Gamma(v+k+1) l!} \\ & U\left(uL+l, v+uL+k+l+1, (2^{R_s}-1)\left(\frac{v}{\bar{\gamma}_{\text{M}}} + \frac{ub}{2^{R_s}}\right)\right) \end{aligned} \quad (8)$$



(a) (b)

Fig. 2: The outage probability for Nakagami-m fading channel versus $\bar{\gamma}_{\mathrm{M}}$ at a normalized $R_{\mathrm{s}} = 0.1$, a fixed $v = 1.5$, $u = 0.5$ and (a) $\rho = 0.9$ and (b) $\rho = 0.1$.



(a) (b)

Fig. 3: Normalized outage secrecy capacity for selected $v = 1.5$, $u = 0.5$ and (a) $P_{\mathrm{out}} = 0.25$, (b) $P_{\mathrm{out}} = 0.75$.

Figure. 3 depicts the normalized outage secrecy capacity for Nakagami-m fading channel versus $\bar{\gamma}_{\mathrm{M}}$, where we consider u=0.5, v=1.5 and $\bar{\gamma}_{\mathrm{W_b}} = 5$dB for selected values $\rho = 0.1$, $\rho = 0.5$ and $\rho = 0.9$ for both scenarios (a) $P_{\mathrm{out}} = 0.25$ and (b) $P_{\mathrm{out}} = 0.75$. Besides, it depicts the normalized secrecy capacity of a Gaussian wiretap channel in the presence of a single eavesdropper with $\bar{\gamma}_{\mathrm{W_b}} = 5$dB. It is clear that the higher $\bar{\gamma}_{\mathrm{M}}$ the higher C_{out}.

For P_{out}=0.75, the more the number of eavesdroppers increases and the less they are correlated, the more the outage secrecy capacity decreases. In fact, a raise in the number of the eavesdroppers is considered harmful for the outage secrecy capacity of the considered communication system. Furthermore for the same value of L, when ρ changes from 0.1 to 0.5 we denote that the correlation has a minor impact on the outage secrecy capacity. Whereas, it is noticed a serious change in the C_{out} when the correlation parameter takes high values like $\rho = 0.9$. In fact, for $\rho = 0.9$, the C_{out} takes important values in the case of $L = 10$ and approaches the secrecy capacity of the Gaussian channel in the case of $L = 5$. The reason behind these results is that, a high correlation between the eavesdroppers significantly degrades the output signal $\bar{\gamma}_{\mathrm{W}}$ and the capacity of the elected eavesdropper channel. Besides, the eavesdroppers number threats the confidentiality of the exchanged information between the legitimate entities. Moreover, the secrecy of the communication system takes advantage from higher correlation coefficient between the eavesdroppers channels at lower values than higher values of the main channel's SNR.

However for $P_{\mathrm{out}} = 0.25$, the outage secrecy capacity takes lower values than in the case of $P_{\mathrm{out}} = 0.75$. Moreover, the variation in the correlation parameter doesn't show a great impact on the outage secrecy capacity for the same number of eavesdroppers. For this reason we didn't depict the case of $\rho = 0.5$ to alleviate the figure. However, the presence of an important number of eavesdroppers degrades significantly

the secrecy capacity and that is due to the MRC technique performed by the elected eavesdropper. For example, for $\bar{\gamma}_{\mathrm{M}} = 20$ dB and $L = 5$, the $C_{\mathrm{out}} = 0.2011$ in the case of $\rho = 0.1$ and $C_{\mathrm{out}} = 0.2298$ in the case of $\rho = 0.9$. Whereas for $L = 10$, the $C_{\mathrm{out}} = 0.0547$ in the case of $\rho = 0.1$ and $C_{\mathrm{out}} = 0.0882$ in the case of $\rho = 0.9$. The reason behind these results is the selected value of the $P_{\mathrm{out}} = 0.25$ which requires a good SNR at the main channel, thus a change in the correlation parameter doesn't show a noticeable impact on the outage secrecy capacity, since as explained previously that the secrecy capacity of a communication system takes advantage from higher correlation between the eavesdroppers especially at low values of the main channel's SNR. However, the MRC diversity technique strengths the elected eavesdropper signal and presents an efficient role in breaking the communication security.

V. Conclusion

In this paper, we have characterized the outage secrecy capacity of a Nakagami-m fading channel target of multiple correlated eavesdroppers performing the MRC technique where the main channel's CSI is known at the legitimate transmitter and receiver. Throughout this work, we determine a closed-form expression of the outage probability and we characterize the outage secrecy capacity for the considered scenario. Our results show that, the secrecy capacity increases as the number of the eavesdroppers decreases ans as the correlation coefficient between the eavesdroppers increases. Since, an important correlation between the different eavesdroppers degrades the quality of the elected eavesdropper channel and consequently deteriorates its capacity. Then, the secrecy capacity of the considered communication system takes advantage from this important value of correlation especially at low values of the main channel's SNR. Besides, the MRC diversity technique strengths the elected eavesdropper signal which lead to a degradation in the performance of the communications system's secrecy capacity. Finally, The goal behind our work is to characterize the secrecy capacity performance in different cases depending on the number of the enemy set and also depending on the correlation degree between them.

References

[1] C. E. Shannon, "Communication theory of secrecy systems," *Bell system technical journal*, vol. 28, pp. 656–715, 1949.

[2] P. K. Gopala, L. Lifeng, and H. El Gamal, "On the secrecy capacity of fading channels," *Information Theory, IEEE Transactions on*, vol. 54, pp. 4687–4698, 2008.

[3] J. Barros and M. R. D. Rodrigues, "Secrecy capacity of wireless channels," in *Information Theory, IEEE International Symposium on*, 2006, pp. 356–360.

[4] M. Z. I. Sarkar and T. Ratnarajah, "Secrecy capacity over log-normal fading channel with diversity combining techniques," in *IEEE Wireless Communications and Networking Conference (WCNC)*, 2013, pp. 2457–2461.

[5] M. Z. I. Sarkar, T. Ratnarajah, and M. Sellathurai, "Secrecy capacity of nakagami-m fading wireless channels in the presence of multiple eavesdroppers," in *Record of the Forty-Third Asilomar Conference on, Signals, Systems and Computers*, 2009, pp. 829–833.

[6] M. Z. I. Sarkar and T. Ratnarajah, "Bounds on the secrecy capacity with diversity combining techniques," in *IEEE Wireless Communications and Networking Conference (WCNC)*, 2012, pp. 2847–2851.

[7] J. Gurland, *Distribution of the Maximum of the Arithmetic Mean of Correlated Random Variables*. Institute of Mathematical Statistics, 1995.

[8] H. M. Srivastava and P. W. Kalrsson, *Mutiple Gaussian Hypergeometric Series*. Ellis horwood, Ltd, 1985.

[9] K. B. Oldham, J. C. Myland, and J. Spanier, *An atlas of functions with Equator, the atlas function calculator*. Springer, 2009.