On The Physical Layer Security Under κ-μ Shadowed Fading Channels With Diversity Approaches

Marcia Manuela Medrado Nunes and Ugo Silva Dias

***Abstract*— This paper presents a investigation on the performance of security under κ-μ shadowed fading channels using the Wyner's classic wiretap model. A better fit was presented for the κ-μ shadowed fading channel curves in relation to other fading models, as Rayleigh and Nakagami-*m*. Results and analyses are obtained through the Secrecy Outage Probability, the Strictly Positive Secrecy Capacity and Average Secrecy Capacity curves by varying the intruder and main channel characteristics. Also, some types of diversity techniques are analysed as the Select Combining, the Maximum Ratio Combining and the MIMO with the κ-μ shadowed fading channel to obtain safer environments.**

***Keywords*— Physical Layer Security, κ-μ shadowed fading channel, Diversity Techniques, Security Metrics.**

I. Introduction

The security issue is increasingly becoming the focus of studies and improvements in wireless communications, specially the physical layer. Studies on the information exchange security have always been extensively performed for the upper layers, but currently the security provided in the physical layer has gained great importance. The need to exploit the security performance in the physical layer has become evident to successful prevent the eavesdropping. Therefore, to characterize the propagation scenario when there are intruder channels in the systems, it is needed to deepen in the security metrics study. Among these security metrics are the Strictly Positive Secrecy Capacity (SPSC), the Secrecy Outage Probability (SOP) and the Average Secrecy Capacity (ASC).

Works on this subject are being fairly raised, as the study of Strictly Positive Secrecy Capacity of log-normal fading channel with single and multiple eavesdroppers in [1] and [2], respectively. There are studies on Strictly Positive Secrecy Capacity under Rice and Weibull fading channels in [3] and [4], respectively. The Outage Probability of Secrecy Capacity over correlated log-normal was investigated in [5]. In [6], the Rayleigh fading channel was used to characterize the SPSC and the SOP in a wiretap channel model. In [7] are presented some diversity techniques to raise the security in wireless networks against wiretap attacks. Some methods of secure selection were presented with the purpose of increasing the security in the physical layer in cooperatives wireless networks and in cognitive radio networks in [8] e [9], respectively. A study of SOP and SPSC was performed in [10], using the α-μ fading channel under the Wyner's classic wiretap model.

Marcia Manuela Medrado Nunes and Ugo Silva Dias¸ Department of Electrical Engineering, University of Brasilia, Brasilia-DF, Brazil, Email: marcia.nunes@ieee.org, ugodias@ieee.org.

Until then, the references about physical layer security focus on channels as Rayleigh, Rice, Nakagami-*m* or log-Normal [11]-[17]. All these works are proposing analytical models for specific types of fading channels and don't cover the various types of fading in practical scenarios. The κ-μ shadowed distribution has been used to characterize scenarios with line of sight and shadowing [18]. It provides a general model of fading with good fit to practical data and with the advantage of generalization of fading models such as unilateral Gaussian, Rayleigh, Nakagami-*m* and Rice, all shaded. Another important aspect of this distribution is its analytical properties that allow the derivation of the probability density function and the cumulated distribution function in closed equations.

The κ-μ shadowed fading channel is more general, flexible, includes some important distributions and fits well the practical data and there are, so far, no specific studies about the SOP, the SPSC and the ASC for the physical layer security under this fading channel, specially with the use of Wyner's classic wiretap model. In addition, the use of diversity techniques such as the Select Combining (SC), the Maximum Rate Combining (MRC), and the Multiple-Input and Multiple-Output (MIMO) significantly improves the reliability of wireless transmission systems because of the diversity characteristics.

This work propose to perform a specific investigation about SOP, SPSC and ASC for the physical layer security under κ-μ shadowed fading channel in the Wyner's classic wiretap model and analyse the use of SC, MRC and MIMO as techniques of diversity in the security scenario with the metrics mentioned above.

This paper is organized as follows: the Section II presents a theoretical review about the Wyner's classic wiretap model used in this work, specifying the channels. The Section III characterize the κ-μ shadowed fading channel. The Section IV presents a theoretical review about the security metrics used, more specifically the Secrecy Outage Probability, the probability of Strictly Positive Secrecy Capacity and the Average Secrecy Capacity. The Section V presents a theoretical review of the diversity techniques that will be analysed in the work, such as the Select Combining, the Maximum Ratio Combining and the MIMO. The Section VI presents and analyses the obtained results by changing the parameters in the κ-μ shadowed fading channel for the main and intruder channels, as well as the obtained results by applying the diversity techniques in the proposed scenario. Lastly, a brief considerations conclude this paper in Section VII.

II. WYNER'S CLASSIC WIRETAP MODEL

The model defined by Wyner and discussed in [19] is based in a wireless communication model in three different nodes. The emitter, treated as S, sends the confidential messages to the receiver, treated as R and a intruder tries to decode the message from the received signal through a intruder channel, treated as E.

For the proposed scenario used in this work, it is considered that the main and intruder channels have independent fading, and also independent complex Gaussian noises with zero-mean and unitary variations. Both channels have ergodic fading blocks in which the coefficients of the channels remain constant during the period of the block, varying independently between them.

III. THE κ-μ SHADOWED DISTRIBUTION

The κ-μ shadowed distribution is obtained from a generalization of κ-μ distribution. Differently from the distribution that κ-μ shadowed is obtained, in the environment with shadowing the dominant components of all the clusters can randomly fluctuate because of shadowing, where inside each cluster, the multipath waves are assumed to have scattered waves with identical power and a dominant component with certain arbitrary power.

The probability density function of the signal-to-noise ratio (SNR) of the transmitted signal for the κ-μ shadowed distribution is given by [18]

$$f_k(\gamma) = \frac{\mu_k^{\mu_k} m_k^{m_k} (1+\kappa_k)^{\mu_k}}{\Gamma(\mu_k)\,\bar{\gamma_k}\,(\mu_k\kappa_k + m_k)^{m_k}} \left(\frac{\gamma}{\bar{\gamma_k}}\right)^{\mu_k - 1} \times \exp^{-\frac{\mu_k(1+\kappa_k)\gamma}{\bar{\gamma_k}}} \; {}_1\mathrm{F}_1\left(m_k, \mu_k; \frac{\mu_k^2 \kappa\,(1+\kappa_k)}{\mu_k\kappa_k + m_k}\right) \frac{\gamma}{\bar{\gamma_k}}, \quad (1)$$

$\kappa_k (k \in R, E) \geq 0$ is the ratio of the total power of the dominant components and the total power of the scattered waves for the main and intruder channels, respectively. $\mu_k (k \in R, E)$ is related to the number of clusters of the main and intruder channels, respectively. The shadowing is represented by $m_k (k \in R, E)$. With a larger *m*, a minor effect of shadowing under the main and intruder channels is observed. $\overline{\gamma}_k (k \in R, E)$ is the average signal-to-noise ratio for R and E and ${}_1\mathrm{F}_1$ is the Hypergeometric Confluent Gamma Function.

The cumulated distribution function of the SNR of the transmitted signal for the κ-μ shadowed distribution is given by [18]

$$F_k(\gamma) = \frac{\mu_k^{\mu_k - 1} m_k^{m_k} (1+\kappa_k)^{\mu_k}}{\Gamma(\mu_k)(\mu_k\kappa_k + m_k)^{m_k}} \left(\frac{1}{\bar{\gamma_k}}\right)^{\mu_k} \gamma_k^{\mu_k} \times \Phi_2\left(\mu_k - m_k, m_k; \mu_k + 1; -\frac{\mu_k(1+\kappa_k)\gamma_k}{\bar{\gamma_k}}, -\frac{\mu_k(1+\kappa_k)}{\bar{\gamma_k}} \frac{m_k\gamma_k}{\mu_k\kappa_k + m_k}\right), \quad (2)$$

with Φ_2 as the Bivariate Confluent Hyper geometric Function.

IV. SECURITY METRICS

Considering the wiretap channel model mentioned in the section II, with P_t as the fixed average transmission power, h_R as the complex channel gain from S to R, h_E as the complex channel gain from S to R, ω_R^2 and ω_E^2 as the Gaussian Noise variances [20] is possible to define the instantaneous SNRs of the received signals at R and E as

$$\gamma_R = P_t |h_R|^2 / \omega_R^2 \quad (3)$$

$$\gamma_E = P_t |h_E|^2 / \omega_E^2. \quad (4)$$

Given γ_R and γ_E, the secrecy capacity is defined as the maximum transmission rate that the intruder is unable to decode the information from the main channel [20]. In the based scenario, the maximum reachable rate of secrecy R_S is equal to the secrecy capacity C_S, which can be characterized as

$$C_S = [ln(1+\gamma_R) - ln(1+\gamma_E)]^+, \quad (5)$$

$ln(1+\gamma_R)$ and $ln(1+\gamma_E)$ are the capacity of the main channel and the intruder channel, respectively.

A. The Secrecy Outage Probability

The Secrecy Outage Probability is defined as the probability of the instantaneous decay of the secrecy capacity after exceeding a certain threshold. The SOP can be defined as [20] $Cth \geq 0$ is the intended secrecy capacity threshold and $\Theta = \exp(Cth) \geq 1$.

$$\begin{aligned} SOP &= P\{C_s(\gamma_R, \gamma_E) \leq C_{th}\} \\ &= P\{ln(1+\gamma_R) - ln(1+\gamma_E) \leq C_{th}\} \\ &= P\{\gamma_R \leq \Theta\gamma_E + \Theta - 1\} \\ &= \int_0^\infty \int_0^{\Theta\gamma_E + \Theta - 1} f_R(\gamma_R)\, d\gamma_R f_E(\gamma_E)\, d\gamma_E \end{aligned} \quad (6)$$

Using the κ-μ shadowed fading channel,

$$\begin{aligned} SOP = &\int_0^\infty \frac{1}{\gamma_{E_0}\Gamma(\mu_E)} \exp^{-\frac{\gamma_e(1+\kappa_E)\mu_E}{\gamma_{E_0}}} m^m \\ &\times \left(\frac{\gamma_E}{\gamma_{E_0}}\right)^{-1+\mu_E} (1+\kappa_E)^{\mu_E} \mu_E^{\mu_E} (m + \kappa_E\mu_E)^{-m} \\ &\times {}_1\mathrm{F}_1\left[m; \mu_E; \frac{\gamma_E\kappa_E(1+\kappa_E)\mu_E^2}{\gamma_{E_0}(m+\kappa_E\mu_E)}\right] \\ &\times \int_0^{-1+\theta+\gamma_E\theta} \frac{1}{\gamma_{R_0}\Gamma(\mu_R)} \exp^{-\frac{\gamma_R(1+\kappa_R)\mu_R}{\gamma_{R_0}}} m^m \\ &\times \left(\frac{\gamma_R}{\gamma_{R_0}}\right)^{-1+\mu_R} (1+\kappa_R)^{\mu_R} \mu_R^{\mu_R} (m+\kappa_R\mu_R)^{-m} \\ &\times {}_1\mathrm{F}_1\left[m; \mu_R; \frac{\gamma_R\kappa_R\mu_R^2(1+\kappa_R)\mu_R^2}{\gamma_{R_0}(m+\kappa_R\mu_R)}\right] d\gamma_R d\gamma_E. \end{aligned} \quad (7)$$

B. The Strictly Positive Secrecy Capacity

The Strictly Positive Secrecy Capacity Probability is when the SNR of the main channel has a better SNR than the

intruder channel, characterizing a secure channel at the chosen rate. This metric can be defined as [20]

$$\begin{aligned} SPSC &= P\left\{C_s\left(\gamma_R,\gamma_E\right)>0\right\} \\ &= P\left\{ln\left(1+\gamma_R\right)-ln\left(1+\gamma_E\right)>0\right\} \\ &= P\left\{\gamma_R-\gamma_E>1\right\} \\ &= P\left\{\gamma_e<\gamma_R-1\right\} \\ &= \int_0^{\infty}\int_0^{\gamma_R-1} f_R\left(\gamma_R\right)d\gamma_R f_E\left(\gamma_E\right)d\gamma_E. \end{aligned} \tag{8}$$

Using the κ-μ shadowed fading channel,

$$\begin{aligned} SPSC = &\int_0^{\infty}\frac{1}{\gamma_{R_0}\Gamma(\mu_R)}\exp^{-\frac{\gamma_R(1+\kappa_R)\mu_R}{\gamma_{R_0}}} m^m \\ &\times\left(\frac{\gamma_R}{\gamma_{R_0}}\right)^{-1+\mu_R}(1+\kappa_R)^{\mu_R}\mu_R^{\mu_R}(m+\kappa_R\mu_R)^{-m} \\ &\times {}_1\mathrm{F}_1\left[m;\mu_R;\frac{\gamma_R\kappa_R(1+\kappa_R)\mu_R^2}{\gamma_{R_0}(m+\kappa_R\mu_R)}\right] \\ &\times\int_0^{-1+\gamma_R}\frac{1}{\gamma_{E_0}\Gamma(\mu_E)}\exp^{-\frac{\gamma_E(1+\kappa_E)\mu_E}{\gamma_{E_0}}} m^m \\ &\times\left(\frac{\gamma_E}{\gamma_{E_0}}\right)^{-1+\mu_E}(1+\kappa_E)^{\mu_E}\mu_E^{\mu_E}(m+\kappa_E\mu_E)^{-m} \\ &\times {}_1\mathrm{F}_1\left[m;\mu_E;\frac{\gamma_E\kappa_E(1+\kappa_E)\mu_E^2}{\gamma_{E_0}(m+\kappa_E\mu_E)}\right]d\gamma_E d\gamma_R \end{aligned} \tag{9}$$

C. The Average Secrecy Capacity

The Average Secrecy Capacity defines the average of the maximum transmission rate reached in a secure channel and it is given by [21]

$$\begin{aligned} ASC &= \int_0^{\infty}\int_0^{\infty} C_S(\gamma_R,\gamma_E)f(\gamma_R,\gamma_E)d\gamma_R\gamma_E \\ &= \int_0^{\infty} ln(1+\gamma_R)f_R\left(\int_0^{\gamma_R} f_{E(\gamma_E)d\gamma_E}\right)d\gamma_R \\ &- \int_0^{\infty} ln(1+\gamma_E)f_E(\gamma_E)\int_{\gamma_E}^{\infty} f_R(\gamma_R)d\gamma_R d\gamma_E. \end{aligned} \tag{10}$$

Using the κ-μ shadowed fading channel,

$$\begin{aligned} ASC = &\int_0^{\infty}\left(\alpha_R\,{}_1\mathrm{F}_1\left[m;\mu_R;\beta_E\right]\right. \\ &\times\left.\left(\int_0^{\gamma_R}\frac{\alpha_E\,{}_1\mathrm{F}_1\left[m;\mu_E;\beta_R\right]}{\gamma_{E_0}\Gamma(\mu_R)}d\gamma_E\right)\log(1+\gamma_R)\right) \\ &/(\gamma_{R_0}\Gamma(\mu_R))d\gamma_R - \int_0^{\infty}\left(\alpha_E\,{}_1\mathrm{F}_1\left[m;\mu_E;\beta_R\right]\right. \\ &\times\left.\left(\int_{\gamma_E}^{\infty}\frac{\alpha_R\,{}_1\mathrm{F}_1\left[m;\mu_R;\beta_E\right]}{\gamma_{R_0}\Gamma(\mu_R)}d\gamma_R\right)\log(1+\gamma_E)\right) \\ &/(\gamma_{E_0}\Gamma(\mu_E))d\gamma_E. \end{aligned} \tag{11}$$

With

$$\begin{aligned} \alpha_R = &\exp^{-\frac{\gamma_R(1+\kappa_R)\mu_R}{\gamma_{R_0}}} m^m\left(\frac{\gamma_R}{\gamma_{R_0}}\right)^{-1+\mu_R} \\ &\times(1+\kappa_R)^{\mu_R}\mu_R^{\mu_R}(m+\kappa_R\mu_R)^{-m}, \end{aligned} \tag{12}$$

$$\begin{aligned} \alpha_E = &\exp^{-\frac{\gamma_E(1+\kappa_E)\mu_E}{\gamma_{E_0}}} m^m\left(\frac{\gamma_E}{\gamma_{E_0}}\right)^{-1+\mu_E} \\ &\times(1+\kappa_E)^{\mu_E}\mu_E^{\mu_E}(m+\kappa_E\mu_E)^{-m}, \end{aligned} \tag{13}$$

$$\beta_R = \frac{\gamma_R\kappa_R(1+\kappa_R)\mu_R^2}{\gamma_{R_0}(m+\kappa_R\mu_R)}, \tag{14}$$

$$\beta_E = \frac{\gamma_E\kappa_E(1+\kappa_E)\mu_E^2}{\gamma_{E_0}(m+\kappa_E\mu_E)}. \tag{15}$$

V. Diversity Techniques

The use of multiple transmitters and receivers as MIMO, MRC and SC enhances the reliability of wireless transmission.

For the Maximum Ratio Combining are used [22]

$$\begin{aligned} f_\gamma(\gamma) = &\frac{\tilde{\mu}^{\tilde{\mu}}\tilde{m}^{\tilde{m}}(1+\kappa)^{\tilde{\mu}}}{\Gamma(\tilde{\mu})(\tilde{\mu}\kappa+\tilde{m})^{\tilde{m}}\eta^{\tilde{\mu}}}\gamma^{\tilde{\mu}-1}\exp^{-[\frac{\tilde{\mu}(1+\kappa)}{\eta}]\gamma} \\ &\times\ {}_1\mathrm{F}_1\left(\tilde{m};\tilde{\mu};\left[\frac{\tilde{\mu}^2\kappa(1+\kappa)}{\tilde{\mu}\kappa+\tilde{m}\eta}\right]\gamma\right), \end{aligned} \tag{16}$$

with $\tilde{\mu}=N_RN_S\mu$, $\tilde{m}=N_RN_Sm$ and $\eta=N_RN_S\gamma_0$.

We can obtain the instantaneous SNR of κ-μ shadowed fading channel with MIMO characterization from the MRC PDF mentioned above.

The CDF for the instantaneous SNR after Selection Combining can be written for i.i.d. branches as

$$\begin{aligned} F_D(\gamma_{SD}) &= P(\gamma_i\le\gamma_{SD}, i=1,...,L) = \prod_{i=1}^{L}P(\gamma_i\le\gamma_{SD}) \\ &= \left(\int_{\infty}^{\gamma_{SD}} f_D(\gamma_i)d\gamma_i\right)^L. \end{aligned} \tag{17}$$

Then, it is possible to derive the PDF with the κ-μ shadowed fading channel,

$$\begin{aligned} f(\gamma_{SD}) &= \frac{d}{d\gamma_{SD}}F(\gamma_{SD}) \\ &= \frac{1}{\gamma_0\Gamma(\mu)}\exp^{-\frac{\gamma_{SD}(1+\kappa)\mu}{\gamma_0}} Lm^m\left(\frac{\gamma_{SD}}{\gamma_0}\right)^{-1+\mu} \\ &\times(1+\kappa)^{\mu}\mu^{\mu}(m+\kappa\mu)^{-m}\ {}_1\mathrm{F}_1\left[m;\mu;\gamma_{SD}\,T\right] \\ &\times\left(\int_0^{\gamma_{SD}}\frac{1}{\gamma_0\Gamma(\mu)}\exp^{-\frac{\gamma(1+\kappa)\mu}{\gamma_0}} m^m\left(\frac{\gamma}{\gamma_0}\right)^{-1+\mu}\right. \\ &\times(1+\kappa)^{\mu}\mu^{\mu}(m+\kappa\mu)^{-m} \\ &\times\left.{}_1\mathrm{F}_1\left[m;\mu;\gamma\,T\right]d\gamma\right)^{L-1}, \end{aligned} \tag{18}$$

with $T=\frac{\kappa(1+\kappa)\mu^2}{\gamma_0(m+\kappa\mu)}$, L is the number of branches and $\gamma_{SD}=max\left\{\gamma_1,\gamma_2,...,\gamma_L\right\}$.

VI. Numerical Results and Analyses

For the simulations and analyses, the threshold for the secrecy capacity ($Cth = 1$) dB was assumed. In the curves that will be presented below, K represents the relation between the average SNR of the main channel and the average SNR of the intruder, $\overline{\gamma_D} = K\overline{\gamma_E}$.

The Fig. 1 presents the ASC curve for the κ-μ shadowed fading channel varying the values of κ_D,κ_E,μ_D and μ_E. Fig.3 presents the SOP curve for the κ-μ shadowed fading channel varying the values of κ_D,κ_E,μ_D and μ_E. Fig.2 presents the SPSC curve for the κ-μ shadowed fading channel varying the values of κ_D,κ_E,μ_D and μ_E. The D and E represents the main channel and the intruder channel, respectively. In the same Figs. 1, 2 and 3 is showed the Rayleigh and Nakagami-m curves for comparisons. The value of m chosen was 2.

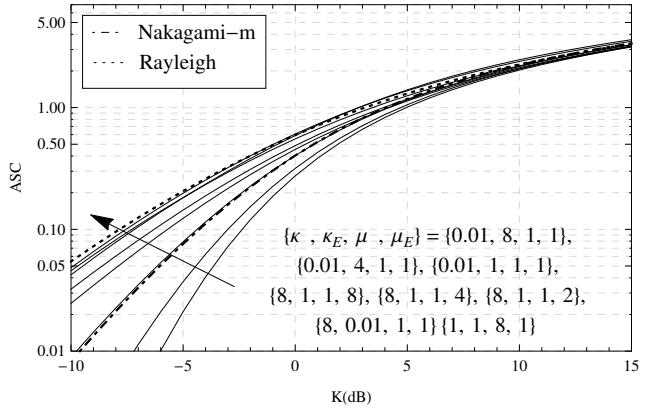

Fig. 1. ASC under κ-μ shadowed fading channel by K, varying κ_R,κ_E,μ_R and μ_E.

The κ-μ shadowed curve was more adequate and better fitted to specific cases, determined by the κ, μ and m parameters. Compared to the other curves, the Rayleigh and the Nakagami-m, also shown in Fig. 1, κ-μ shadowed was able to better specify the environment, the other curves are more optimistic, not really conveying the interested environment.

The increase of μ in the main channel improves the ASC observed, in the case of SOP, there is a decrease of the

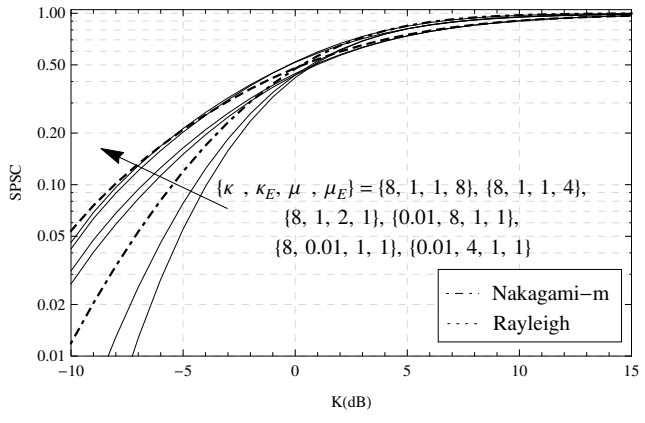

Fig. 2. SPSC under κ-μ shadowed fading channel by K, varying κ_R,κ_E,μ_R and μ_E.

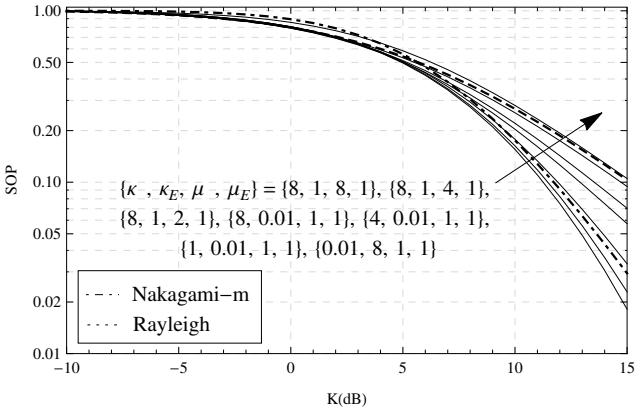

Fig. 3. SOP under κ-μ shadowed fading channel by K, varying κ_R,κ_E,μ_R and μ_E.

observed values and in the SPSC, an increase of the Strictly Positive Secrecy Capacity probability. When the κ of the main channel increases in relation to the intruder channel there is also a better observed ASC, a lower SOP, and an increase of SPSC. With an increase between the relation of the dominant components total power and the scattered waves total power there is a higher SNR in the main channel, thus improving the ASC and SPSC obtained and consequently, reducing the SOP. A greater number of multipath clusters also allows a better reconstruction of the signal, thus increasing the ASC and SPSC obtained, and decreasing SOP.

Figs. 4, 5 and 6 present the ASC, the SOP and the SPSC curves, respectively, for the κ-μ shadowed fading channel with different techniques of diversity, being them the MIMO with the N_R equals to 2 and 4, and the N_S equals to 2 and 4. The MRC with L equal to 2. The SC with L equals to 2 and 4 and the κ-μ shadowed fading channel with no diversity technique. The parameters chosen was $\kappa_R = 0.01$, $\kappa_E = 8$, $\mu_R = 1$ and $\mu_E = 1$.

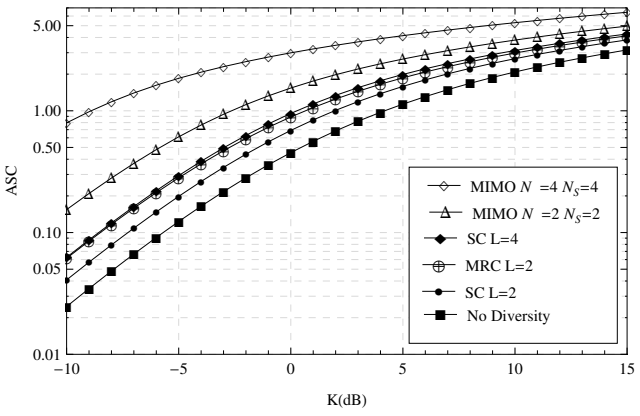

Fig. 4. ASC under κ-μ shadowed fading channel by K with different techniques of diversity.

With the scenario described above, it is possible to verify that when diversity techniques are used, a better ASC and SPSC is obtained, and consequently a lower SOP. The best case is with the use of the MIMO with 16 links ($N_R = 4$ and

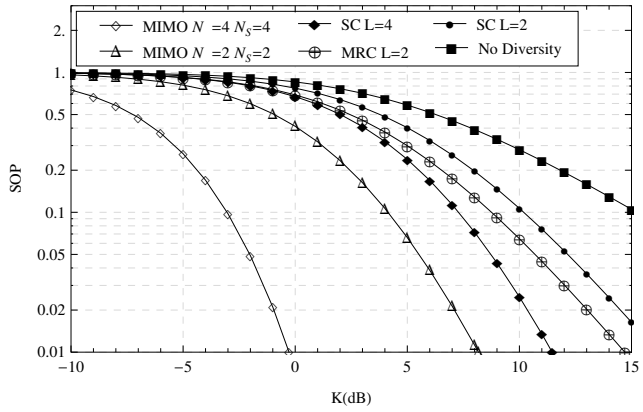

Fig. 5. SOP under κ-μ shadowed fading channel by K with different techniques of diversity.

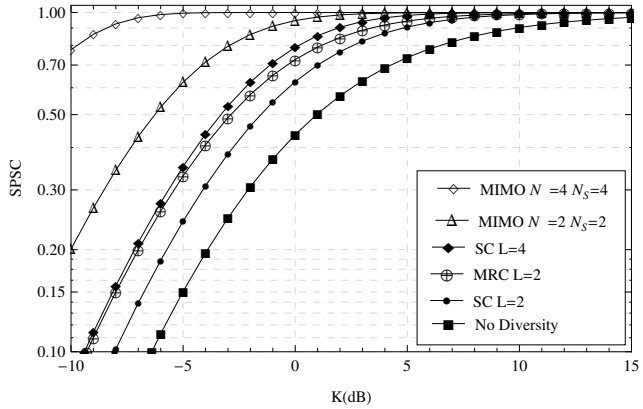

Fig. 6. SPSC under κ-μ shadowed fading channel by K with different techniques of diversity.

$N_S = 4$) and the worst case is without the use of any technique of diversity. The diversity techniques can provide focused transmit selectivity of both information and noise toward desired and undesired receivers. Consequently, MIMO signal processing techniques must be carefully designed in order to ensure both the reliability of the desired communication links and the degradation of those for the intruders.

VII. Conclusion

In this paper a physical layer security analysis was presented for Wyner's classic wiretap model under independents κ-μ shadowed channels, and some diversity techniques were analysed too. The Secrecy Outage Probability, the Probability of Strictly Positive Secrecy Capacity and the Average Secrecy Capacity was calculated for various channel parameters considering the improvement or degradation in the main channel SNR and in the intruder channel SNR. We observed a better fit of the κ-μ shadowed fading channel curves in relation to other fading models. The same analysis was performed for the use of different diversity techniques, such as selecting combining, maximun ratio combining and MIMO. In which a safer environment was observed with the use of MIMO in comparison with the others ones.

References

[1] X. Liu, "Strictly Positive Secrecy Capacity of Log-Normal Fading Channel with Multiple Eavesdroppers," in *Communications (ICC), 2014 IEEE International Conference on*. IEEE, 2014, pp. 775–779.

[2] X. Liu., "Secrecy Capacity of Wireless Links Subject to Log-Normal Fading," in *7th International Conference on Communications and Networking in China*. IEEE, 2012, pp. 167–172.

[3] X. Liu, "Probability of Strictly Positive Secrecy Capacity of The Rician-Rician Fading Channel," *Wireless Communications Letters, IEEE*, vol. 2, no. 1, pp. 50–53, 2013.

[4] X. Liu,, "Probability of Strictly Positive Secrecy Capacity of The Weibull Fading Channel," in *2013 IEEE Global Communications Conference (GLOBECOM)*, 2013.

[5] X. Liu., "Outage Probability of Secrecy Capacity Over Correlated Log-Normal Fading Channels," *IEEE communications letters*, vol. 17, no. 2, pp. 289–292, 2013.

[6] X. Sun, J. Wang, W. Xu, and C. Zhao, "Performance of Secure Communications Over Correlated Fading Channels," *Signal Processing Letters, IEEE*, vol. 19, no. 8, pp. 479–482, 2012.

[7] Y. Zou, J. Zhu, X. Wang, and V. Leung, "Improving Physical-Layer Security in Wireless Communications Using Diversity Techniques," *Network, IEEE*, vol. 29, no. 1, pp. 42–48, 2015.

[8] Y. Zou, X. Wang, and W. Shen, "Optimal Relay Selection For Physical-Layer Security in Cooperative Wireless Networks," *Selected Areas in Communications, IEEE Journal on*, vol. 31, no. 10, pp. 2099–2111, 2013.

[9] Y. Zou, B. Champagne, W.-P. Zhu, and L. Hanzo, "Relay-Selection Improves the Security-Reliability Trade-Off in Cognitive Radio Systems," *Communications, IEEE Transactions on*, vol. 63, no. 1, pp. 215–228, 2015.

[10] L. Kong, H. Tran, and G. Kaddoum, "Performance Analysis of Physical Layer Security Over α–μ Fading Channel," *Electronics Letters*, vol. 52, no. 1, pp. 45–47, 2015.

[11] X. Liu, "Strictly Positive Secrecy Capacity of Log-Normal Fading Channel with Multiple Eavesdroppers," in *Communications (ICC), 2014 IEEE International Conference on*. IEEE, 2014, pp. 775–779.

[12] X. Liu., "Secrecy Capacity of Wireless Links Subject to Log-Normal Fading," in *7th International Conference on Communications and Networking in China*. IEEE, 2012, pp. 167–172.

[13] X. Liu, "Probability of Strictly Positive Secrecy Capacity of The Rician-Rician Fading Channel," *Wireless Communications Letters, IEEE*, vol. 2, no. 1, pp. 50–53, 2013.

[14] X. Liu, "Probability of Strictly Positive Secrecy Capacity of the Weibull Fading Channel," in *2013 IEEE Global Communications Conference (GLOBECOM)*, 2013.

[15] X. Liu., "Outage Probability of Secrecy Capacity Over Correlated Log-Normal Fading Channels," *IEEE communications letters*, vol. 17, no. 2, pp. 289–292, 2013.

[16] X. Sun, J. Wang, W. Xu, and C. Zhao, "Performance of Secure Communications Over Correlated Fading Channels," *Signal Processing Letters, IEEE*, vol. 19, no. 8, pp. 479–482, 2012.

[17] Pan, G., Tang, C., Zhang, X., Li, T., Weng, Y., and Chen, Y. "Physical-Layer Security Over Non-Small-Scale Fading Channels." *IEEE Transactions on Vehicular Technology*, 65(3), 1326-1339, 2016.

[18] J. F. Paris, "Statistical Characterization of κ–μ Shadowed Fading," *Vehicular Technology, IEEE Transactions on*, vol. 63, no. 2, pp. 518–526, 2014.

[19] Wyner, Aaron D. The WireTap Channel," *Bell Labs Technical Journal*, v. 54, n. 8, p. 1355-1387, 1975.

[20] Sun, X., Wang, J., Xu, W., and Zhao, C. "Performance of Secure Communications Over Correlated Fading Channels," *IEEE Signal Processing Letters*, v. 19, n. 8, p. 479-482, 2012.

[21] Bloch, M., Barros, J., Rodrigues, M. R., and McLaughlin, S. W. "Wireless Information-Theoretic Security," *IEEE Transactions on Information Theory*, 54(6), 2515-2534, 2008.

[22] Salahat, E., and Hakam, A. "Maximal Ratio Combining Diversity Analysis of Underwater Acoustic Communications Subject to κ-μ Shadowed Fading Channels," *Annual Conference of the IEEE Industrial Electronics Society*,2016