PHYSICAL LAYER SECRECY PERFORMANCE ANALYSIS OF TAS/ MRC SYSTEM OVER RAYLEIGH/ NAKAGAMI FADING CHANNELS

Nguyen Van Tho[1], Van Phu Tuan[1], Vo Tan Loc[2], Ha Dac Binh[1]

[1]Duy Tan University; nguyenvantho@duytan.edu.vn
[2]Pham Van Dong University

Abstract - The broadcast nature of radio propagation makes wireless communication extremely vulnerable to eavesdropping attack. In this paper, we investigate the physical layer secrecy performance of multiple-input multiple-output (MIMO) system with transmission antenna selection (TAS) and receiver maximal-ratio combining (MRC) in the presence of a single antenna passive eavesdropper over dissimilar fading channels. We consider two scenarios: 1) The legal / illegal channels are subject to Rayleigh /Nakagami fading, respectively; 2) The legal /illegal channels undergo Nakagami /Rayleigh fading, respectively. Especially, the exact close-form expressions for the probability of non-zero secrecy capacity and the secrecy outage probability using statistical characteristics of the signal-to-noise ratio (SNR) of these scenarios is derived. These expressions allow us to assess the security capability of the considered system. The numerical result discussion provides practical design of the effect of various system parameters, such as average SNRs, Nakagami fading model, and number of transmission antennas on the secrecy performance of the considered system.

Key words - physical layer secrecy; secrecy capacity; TAS/RMC system; Rayleight fading; Nakanami fading.

1. Introduction

The increase in exchange information demand becomes a motivation for development of wireless communication. Because wireless communication is a flexible data communication, it leads the explosive growth in recent decades. However, the broadcast nature of wireless medium makes the security risk always be challenges. In recent years, physical layer (PHY) security has become an attractive topic due to its low complexity, latency and ability to combine with other mechanisms in order to improve a capability of overall ensuring security. Shannon [1], Wyner [2], and Leung-Yan-Cheong [3] were pioneers in the research on physical layer secure communication. There are many extensive works aimed at im- proving the secrecy performances of wireless communications by exploiting the multiple antennas. Some of them are [4]–[10] that present a quasi-static Rayleigh fading wiretap channel multiple antenna devices. In [4], the authors have investigated the PHY secrecy performance of a communication scheme consisting of a multiple antenna transmitter using TAS and a single antenna receiver in the presense of a multiple antenna eavesdropper. Their results show that high levels of security can be achieved when the number of antennas at transmitter increases, even when eavesdropper has multiple antennas. The authors in [5] analyze the impact of antenna correlation on secrecy performance of MIMO wiretap channels where transmitter employs transmission antenna selection while receiver and eavesdropper perform MRC with arbitrary correlation. Nan Yang et al. [6] analyzed secrecy performance of MIMO wiretap channel in Nakagami-m fading environments with non-identical fading parameters for the main channel and the eavesdroppers channel. The authors in [7] proposed an opportunistic scheduling with TAS to enhance physical layer security. At the transmitter, a single antenna is selected to maximize the instantaneous SNR of the main channel, while at the receiver and the eavesdropper, MRC or selection combining (SC) is applied. They can also conclude that the secrecy outage probability is almost independent of the number of antennas and eavesdroppers in high SNR region. The physical layer security performance of MRC systems under two-waves with diffuse power fading channels is analyzed in [8]. Two practical scenarios are taken into account, depending on whether or not the channel state information (CSI) of the eavesdropper is known at the transmitter. For the first scenario where eavesdropper's CSI is not known, the expressions for the exact and asymptotic average secrecy capacity are derived. For the second scenario where eavesdropper's CSI is known, the authors derive the expressions for the exact and asymptotic secrecy outage probability. Based on these, we show that the secrecy diversity order is solely dependent on the number of receive antennas at the legitimate receiver and independent of the number of antennas at the eavesdropper. The PHY secrecy performance of multiple-input single-output (MISO) Ultra-Wideband (UWB) system with TAS is evaluated in [9] and the time-reversal technique is used to improve the secrecy capacity in MIMO UWB system [10].

From above studies and to the best of our knowledge, most of previous works on PHY security consider the similarity between legal channel and illegal channel. However, due to the mobility of mobile devices, the difference in fading characteristics between two channels must be examined, practically. In this paper, we investigate the physical layer secrecy performance analysis of MIMO system using TAS/MRC in the presence of a single antenna passive eavesdropper over dissimilar Rayleigh/ Nakagami fading channels. The main contribution of this paper resides in the derivation of the exact closed-form expressions of the probability of non-zero secrecy capacity and the secrecy outage probability overmixed Rayleigh/ Nakagami fading channels.In addition, we also show the results of simulation and analysis to clarify the secrecy performance of this considered system.

The rest of this paper is organized as follows. Section II presents the system and channel model. Physical layer secrecy performance of the considered system is analyzed in Section III. In Section IV, we show the numerical results. We conclude our work in Section V.

2. System and channel model

We consider the system illustrated in Figure 1. Alice and Bob are two legitimate users equipped with N_a and N_b antennas respectively while Eve is a single antenna passive eavesdropper which tries to extract information sent from Alice without active attack. Let H denote the N_b×N_a channel matrix between Alice and Bob. Its entries are the fading coefficients h_{ij}; $1 \le i \le N_b$, $1 \le j \le N_a$. An N_b×1 vector h, which is a column of H, is used to denote the channel between the single selected transmission antenna and Nb reception antennas. The single selected transmission antenna NK; $1 \le K \le N_a$ which maximizes the total received signal power, is determined by

$$K = \underset{1 \le j \le N_a}{argmax}\left\{C_j = \sum_{i=1}^{N_b}\left|h_j^i\right|^2\right\} \tag{1}$$

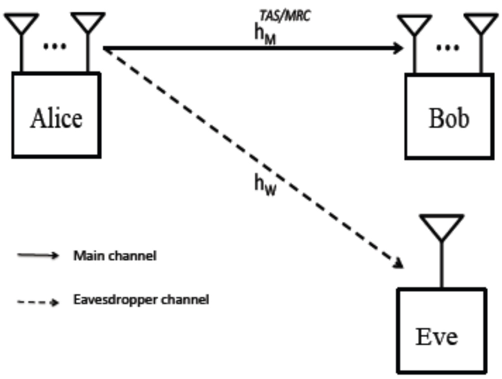

***Figure 1.** System model*

We consider two scenarios: The legal/ illegal channels respectively, are subject to 1) Rayleigh/ Nakagami fading; 2) Nakagami/Rayleigh fading.

A. The legal/ illegal channels are subject to Rayleigh/ Nakagami fading

The legal channel is assumed to undergo Rayleigh fading, while the eavesdropper experiences Nakagami fading. Alice sends the signal x(t) on the jth antenna, the received signal at Bob y(t) = [y1, y2,…, yN_b]^T has the following form

$$y(t) = h_{M,j}x(t) + n_M \tag{2}$$

where $h_{M,j} = [h_{M,ij}, h_{M,2j},…, h_{M,Nbj}]^T$ is the jth column of H, $n_M = [n_{M,1}, n_{M,2},…, n_{M,Nb}]^T$ is the zero-mean additive white Gaussian noise (AWGN) vector at Bob with power NM, and superscript (.)T denotes the transposition operator.

The instantaneous SNR and the average SNR at ith antenna at Bob are $\gamma_{M,ij} = \frac{P\,|\,h_{M,ij}\,|^2}{N_M}$ and $\bar{\gamma}_{M,ij} = \frac{PE[|\,h_{M,ij}\,|^2]}{N_M}$ respectively. P is the average transmission signal power at Alice. Assuming that $\bar{\gamma}_{M,ij}$ of each link from Alice to Bob has the same value $\bar{\gamma}_M$. The probability density function (PDF) of $\gamma_{M,ij}$ is

$$f_{\gamma_{M,j}^i}\left(\gamma_{M,j}^i\right) = \frac{1}{\bar{\gamma}_M}e^{-\frac{\gamma_{M,j}^i}{\bar{\gamma}_M}} \tag{3}$$

The received signals at Bob are combined by using MRC. Let $\gamma_{M,ij} = \gamma_M \sum_{i=1}^{N_b}|\,h_{M,ij}\,|^2$ be the instantaneous SNR at Bob when using MRC. The PDF of M; j has the following form

$$f_{\gamma_{M,j}}\left(\gamma_{M,j}\right) = \frac{\gamma_{M,j}^{N_b-1}}{\Gamma(N_b)\bar{\gamma}_M^{N_b}}e^{-\frac{\gamma_{M,j}}{\bar{\gamma}_M}} \tag{4}$$

Where Γ denotes the Gamma function.

The transmiter chooses the best antenna which achieves the highest SNR by using (1). The instantaneous SNR of TAS/MRC system is $\gamma_M = \max\limits_{1 \le j \le N_a}[\gamma_{M,j}]$. The PDF of M has the following form

$$f_{\gamma_M}\left(\gamma_M\right) = \frac{N_a\gamma_M^{N_b-1}}{\Gamma(N_b)\bar{\gamma}_M^{N_b}}e^{-\frac{\gamma_M}{\bar{\gamma}_M}}\sum_{i=0}^{N_a-1}\binom{N_a-1}{i}(-1)^i e^{-\frac{i\gamma_M}{\bar{\gamma}_M}} \times\left(\sum_{k=0}^{N_b-1}\frac{1}{k!}\left(\frac{\gamma_M}{\bar{\gamma}_M}\right)^k\right)^i \tag{5}$$

Eve is capable of eavesdropping the signal sent by Alice. The received signal z(t) at Eve is as follows

$$z(t) = h_W x(t) + n_W \tag{6}$$

where h_W is the Nakagami fading coefficient between the selected transmission antenna at Alice and the reception antenna at Eve, n_W is zero-mean AWGN with power N_W.

The instantaneous SNR at Eve is $\gamma_W = \frac{P\,|\,h_W\,|^2}{N_W}$, while the average SNR is $\bar{\gamma}_W = \frac{PE[|\,h_W\,|^2]}{N_W}$. The PDF of γ_W is

$$f_{\gamma_W}\left(\gamma_W\right) = \frac{m^m}{\bar{\gamma}_W^m\Gamma(m)}\gamma_W^{m-1}e^{-\frac{m\gamma_W}{\bar{\gamma}_W}} \tag{7}$$

B. The legal/ illegal channels are subject to Nakagami/ Rayleigh fading

The legal channel is assumed to undergo Nakagami fading, while the illegal channel is assumed to undergo Rayleigh fading. Similarly, the PDF of $\gamma_{M,ij}$ is as follows

$$f_{\gamma_{M,j}^i}\left(\gamma_{M,j}^i\right) = \frac{m^m}{\Gamma(m)\bar{\gamma}_M^m}\left(\gamma_{M,j}^i\right)^{m-1}e^{-\frac{m\gamma_{M,j}^i}{\bar{\gamma}_M}} \tag{8}$$

The PDF of $\gamma_{M,ij}$has the following form

$$f_{\gamma_{M,j}}\left(\gamma_{M,j}\right) = \frac{m^{mN_b}\gamma_{M,j}^{mN_b-1}}{\Gamma(mN_b)\bar{\gamma}_M^{mN_b}}e^{-\frac{m\gamma_M}{\bar{\gamma}_M}} \tag{9}$$

The PDF of γ_M is given by

$$f_{\gamma_M}\left(\gamma_M\right) = \frac{N_a m^{mN_b}\gamma_M^{mN_b-1}}{\Gamma(mN_b)\bar{\gamma}_M^{mN_b}}e^{-\frac{m\gamma_M}{\bar{\gamma}_M}}\sum_{i=0}^{N_a-1}(-1)^i\binom{N_a-1}{i} \times e^{-\frac{im\gamma_M}{\bar{\gamma}_M}}\left(\sum_{k=0}^{mN_b-1}\frac{1}{k!}\left(\frac{m\gamma_M}{\bar{\gamma}_M}\right)^k\right)^i \tag{10}$$

The PDF of γ_W is as follows

$$f_{\gamma_W}\left(\gamma_W\right) = \frac{1}{\bar{\gamma}_W}e^{-\frac{\gamma_W}{\bar{\gamma}_W}} \tag{11}$$

3. Secrecy capacity analysis

A. Preliminaries

Channel capacity of link between two legitimate users is

$$C_M = \log_2(1+\gamma_M) \tag{12}$$

Channel capacity of link to illegitimate user is

$$C_W = \log_2(1+\gamma_W). \tag{13}$$

The instantaneous secrecy capacity is given by

$$C_S = [C_M - C_W]^+ = \begin{cases} \log_2(\frac{1+\gamma_M}{1+\gamma_W}), \gamma_M > \gamma_W \\ 0, \gamma_M \le \gamma_W \end{cases} \tag{14}$$

B. Probability of Non-zero Secrecy Capacity

1) The legal/ illegal channels are subject to Rayleigh/ Nakagami fading: Assuming that the main channel and the eavesdropper channel are independent of each other, we can derive the probability of a non-zero secrecy capacity as follows

$$\begin{aligned} P(C_S) &= P(\gamma_M > \gamma_W) \\ &= 1-\int_0^\infty\int_{\gamma_M}^\infty f_{\gamma_M}(\gamma_M) f_{\gamma_W}(\gamma_W) d\gamma_W d\gamma_M \\ &= 1-\int_0^\infty\int_{\gamma_M}^\infty f_{\gamma_M}(\gamma_M)\frac{m^m}{\bar\gamma_W^m\Gamma(m)}\gamma_W^{m-1}e^{-\frac{m\gamma_W}{\bar\gamma_W}} d\gamma_W d\gamma_M \\ &= 1-\sum_{i=0}^{N_a-1}\sum_{l=0}^{m-1}\int_0^\infty \frac{(-1)^i N_a m^l \gamma_M^{N_b+l-1}}{\Gamma(N_b) l! \bar\gamma_M^{N_b}\bar\gamma_W^l}\binom{N_a-1}{i}\left(\sum_{k=0}^{N_b-1}\frac{1}{k!}\left(\frac{\gamma_M}{\bar\gamma_M}\right)^k\right)^i e^{-\gamma_M\beta_1} d\gamma_M \\ &= 1-\sum_{i=0}^{N_a-1}\sum_{l=0}^{m-1}\sum_{\substack{\sum p_k = i \\ 0<k<N_b-1}}\frac{(-1)^i N_a m^l}{\Gamma(N_b) l! \bar\gamma_M^{u_1}\bar\gamma_W^l} \\ &\times\binom{N_a-1}{i}\binom{i}{p_0,\ldots,p_{N_b-1}}\left[\prod_{0<k<N_b-1}\left(\frac{1}{k!}\right)^{p_k}\right]\int_0^\infty \gamma_M^{u_1+l-1}e^{-\gamma_M\beta_1}d\gamma_M \\ &= 1-\sum_{i=0}^{N_a-1}\sum_{l=0}^{m-1}\sum_{\substack{\sum p_k = i \\ 0<k<N_b-1}}\frac{(-1)^i N_a m^l (u_1+l-1)!}{\Gamma(N_b) l! \bar\gamma_M^{u_1}\bar\gamma_W^l\beta_1^{u_1+l}} \\ &\times\binom{N_a-1}{i}\binom{i}{p_0,\ldots,p_{N_b-1}}\left[\prod_{0<k<N_b-1}\left(\frac{1}{k!}\right)^{p_k}\right] \end{aligned} \tag{15}$$

where $u_1 = N_b + \sum_{0<k<N_b-1} kp_k$, $\beta_1 = \frac{(i+1)}{\bar\gamma_M}+\frac{m}{\bar\gamma_W}$,

and $\binom{i}{p_0,\ldots,p_{N_b-1}} = \frac{i!}{p_0!p_2!\ldots p_{N_b-1}!}$.

2) The legal/ illegal channels are subject to Nakagami/ Rayleigh fading: This process is similar to the previous one, we derive the probability of a non-zero secrecy capacity as

$$\begin{aligned} P^{'}(C_S>0) &= P^{'}(\gamma_M > \gamma_W) \\ &= \int_0^\infty\int_0^{\gamma_M} f_{\gamma_M\gamma_W}(\gamma_M,\gamma_W)d\gamma_W d\gamma_M \\ &= 1-\sum_{i=0}^{N_a-1}\sum_{\substack{\sum p_k=i \\ 0<k<N_b-1}}\frac{(-1)^i N_a m^{u_2}(u_2-1)!}{\Gamma(\mathrm{m} N_b)\bar\gamma_M^{u_2}\beta_3^{u_2}} \\ &\times\binom{N_a-1}{i}\binom{i}{p_0,\ldots,p_{N_b-1}}\left[\prod_{0<k<mN_b-1}\left(\frac{1}{k!}\right)^{p_k}\right] \end{aligned} \tag{16}$$

where $u_2 = mN_b + \sum_{0<k<mN_b-1} kp_k$, and $\beta_3 = \frac{(i+1)m}{\bar\gamma_M}+\frac{m}{\bar\gamma_W}$.

C. Secrecy Outage Probability.

The secrecy outage probability can be defined as the probability that the achievable secrecy rate is less than a predetermined secrecy rate of transmission RS (RS > 0). The secrecy outage event occurs when transmission rate is below RS. In other words, at this time we cannot ensure the secure transmission.

The legal/ illegal channels are subject to Rayleigh/ Nakagami fading: The secrecy outage probability of Rayleigh/ Nakagami fading channels can be calculated as follows.

$$\begin{aligned} \mathcal{O}(R_S) &= P(C_S<R_S) = 1-\int_0^\infty\int_y^\infty f_{\gamma_M}(\gamma_M) f_{\gamma_W}(\gamma_W) d\gamma_M d\gamma_W \\ &= 1-\int_0^\infty\sum_{i=0}^{N_a-1}\sum_{\substack{\sum p_k = i \\ 0<k<N_b-1}}\frac{(-1)^i N_a}{\Gamma(N_b)}\binom{N_a-1}{i}\binom{i}{p_0,\ldots,p_{N_b-1}}\left[\prod_{0<k<N_b-1}\left(\frac{1}{k!}\right)^{p_k}\right] \\ &\times\int_y^\infty \frac{\gamma_M^{u_1-1}}{\bar\gamma_M^{N_b}}e^{-\frac{(i+1)\gamma_M}{\bar\gamma_M}}d\gamma_M f_{\gamma_W}(\gamma_W)d\gamma_W \\ &= 1-\sum_{i=0}^{N_a-1}\sum_{\substack{\sum p_k = i \\ 0<k<N_b-1}}\sum_{j=0}^{u_1-1}\frac{(-1)^i N_a (u_1-1)! m^m 2^{jR_S}}{\Gamma(N_b)(i+1)^{u_1-j} j!\Gamma(m)\bar\gamma_M^j\bar\gamma_W^m} \\ &\times\binom{N_a-1}{i}\binom{i}{p_0,\ldots,p_{N_b-1}}\left[\prod_{0<k<N_b-1}\left(\frac{1}{k!}\right)^{p_k}\right] \\ &\times e^{\frac{(i+1)(1-2^{R_S})}{\bar\gamma_M}}\int_0^\infty(\gamma_W+b)^j\gamma_W^{m-1}e^{-\gamma_W\beta_2}d\gamma_W \\ &= 1-\sum_{i=0}^{N_a-1}\sum_{\substack{\sum p_k = i \\ 0<k<N_b-1}}\sum_{j=0}^{u_1-1}\sum_{l=0}^{j}\frac{(-1)^i N_a (u_1-1)! m^m 2^{jR_S} b^{j-l}(l+m-1)!}{\Gamma(N_b)(i+1)^{u_1-j} j!\Gamma(m)\bar\gamma_M^j\bar\gamma_W^m\beta_2^{l+m}} \\ &\times\binom{N_a-1}{i}\binom{j}{l}\binom{i}{p_0,\ldots,p_{N_b-1}}\times\left[\prod_{0<k<N_b-1}\left(\frac{1}{k!}\right)^{p_k}\right]e^{\frac{(i+1)(1-2^{R_S})}{\bar\gamma_M}} \end{aligned} \tag{17}$$

Where $b = 1-\frac{1}{2^R s}$ and $\beta_2 = \frac{(i+1)2^{R_S}}{\bar\gamma_M}+\frac{m}{\bar\gamma_W}$..

The legal/ illegal channels are subject to Nakagami/ Rayleigh fading: Similarly, the secrecy outage probability of Nakagami/ Rayleigh fading channels is given by

$$\begin{aligned} \mathcal{O}^{'}(R_S) &= P^{'}(C_S<R_S) = \int_0^\infty\int_0^y f_{\gamma_M\gamma_W}(\gamma_M,\gamma_W)d\gamma_M d\gamma_W \\ &= 1-\sum_{i=0}^{N_a-1}\sum_{\substack{\sum p_k=i \\ 0<k<mN_b-1}}\sum_{j=0}^{u_2-1}\sum_{l=0}^{j}\frac{(-1)^i N_a(u_2-1)!}{\Gamma(\mathrm{m} N_b)(i+1)^{u_2-j}} \\ &\times\frac{(b\beta_4)^l}{\bar\gamma_W l!\beta_4^{j+1}}\left(\frac{m2^{R_s}}{\bar\gamma_M}\right)\binom{N_a-1}{i}\binom{j}{l}\binom{i}{p_0,\ldots,p_{m-1}} \\ &\times\left[\prod_{0<k<mN_b-1}\left(\frac{1}{k!}\right)^{p_k}\right]e^{\frac{m(i+1)(1-2^{R_S})}{\bar\gamma_M}} \end{aligned} \tag{18}$$

where $\beta_4 = \frac{m(i+1)2^{R_S}}{\bar\gamma_M}+\frac{1}{\bar\gamma_W}$.

4. Numerical Results

In this section, we discuss some results based on the theoretical analysis and Monte-Carlo simulations of the probability of existence of non-zero secrecy capacity and the secrecy outage probability of considered system in the effect of various system parameters, such as average SNRs, Nakagami fading model, and number of transmission antennas.

A. Effect of average SNR

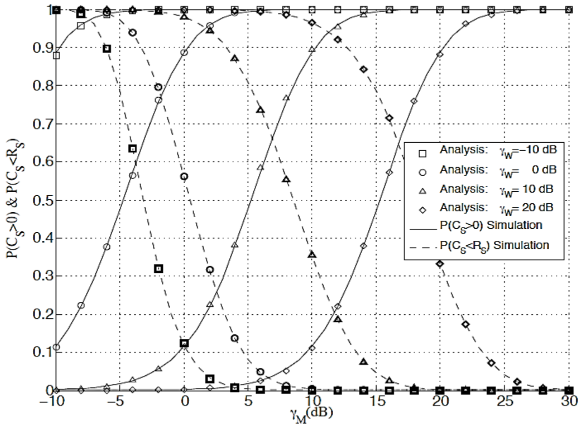

Figure 2. *The probability of non-zero secrecy capaciy and the secrecy outage probability (Rayleigh/ Nakagami, m=2, Na=Nb=2, RS=1 bit/s/Hz)*

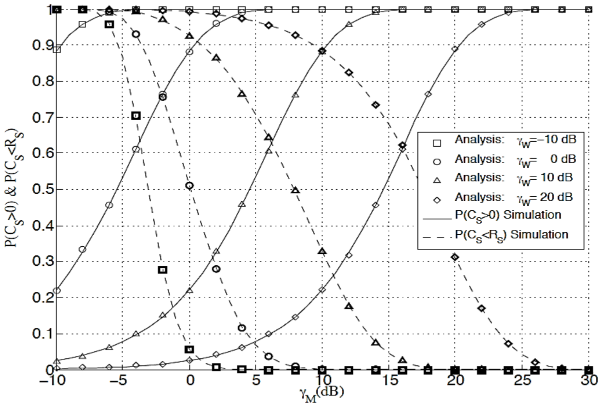

Figure 3. *The probability of non-zero secrecy capaciy and the secrecy outage probability (Nakagami/ Rayleigh, m = 2, N$_a$=N$_b$=2, R$_S$=1 bit/s/Hz)*

Figure 2 and Figure 3 show the probability of non-zero secrecy capacity and the secrecy outage probability in two scenarios: Rayleigh/ Nakagami fading $\left(P\left(C_S\right), \mathcal{O}\left(R_S\right)\right)$ and Nakagami/ Rayleigh fading $\left(P^{'}\left(C_S\right), \mathcal{O}^{'}\left(R_S\right)\right)$, respectively, versus γ_M for different γ_W with the shape parameter m=2, the number of transmission antennas N$_a$ = 2 and the number of reception antennas N$_b$ = 2. In these figures, P (C$_S$) and P$^{'}$(C$_S$) increase, while O(R$_S$) and O$^{'}$(R$_S$) decrease when Bob's SNR $\bar{\gamma}_M$ increases, on the contrary, P(C$_S$) and P$^{'}$(C$_S$) decrease, while O(R$_S$) and O$^{'}$(R$_S$) increase with increasing $\bar{\gamma}_W$. These assessments are resonable because when $\bar{\gamma}_M$ increases, the received signal at Bob is better than that at Eve so that the capacity of legitimate users will be larger than the capacity of illegitimate users. From these two figures, we can see that the secrecy performance over Rayleigh/ Nakagami fading channels is worse than Nakagami/ Rayleigh fading channels. In other words, the secrecy performance is better when the Nakagami fading is on the main link due to the Line of Sight (LOS) component.

B. Effect of Nakagami fading model

Figure 4 and Figure 5 depict the probability of non-zero secrecy capacity and the secrecy outage probability for Rayleigh/ Nakagami and Nakagami/ Rayleigh fading, respectively with different shape parameter m for $\bar{\gamma}_W = 10dB$, N$_a$= N$_b$ =2. We can see that the secrecy performance is better with increasing m when $\bar{\gamma}_M > \bar{\gamma}_W$.

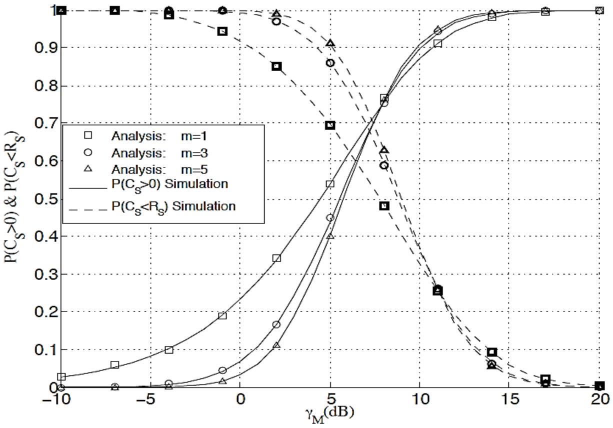

Figure 4. *The probability of non-zero secrecy capaciy and the secrecy outage probability (Rayleigh/ Nakagami, $\bar{\gamma}_W = 10dB$, N$_a$=N$_b$=2, R$_S$=1 bit/s/Hz)*

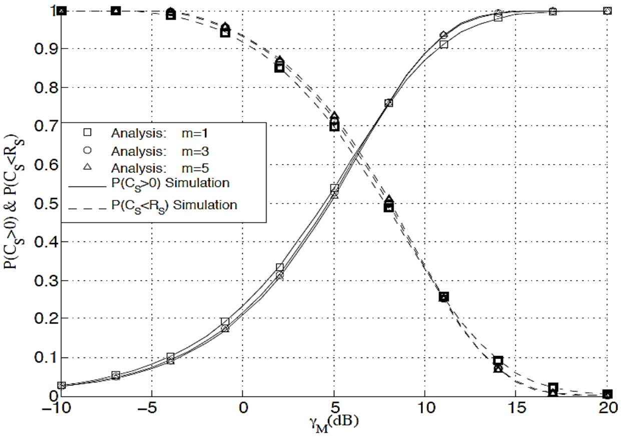

Figure 5. *The probability of non-zero secrecy capaciy and the secrecy outage probability (Nakagami/ Rayleigh, $\bar{\gamma}_W = 10dB$, N$_a$=N$_b$=2, R$_S$=1 bit/s/Hz)*

C. Effect of the number of antennas

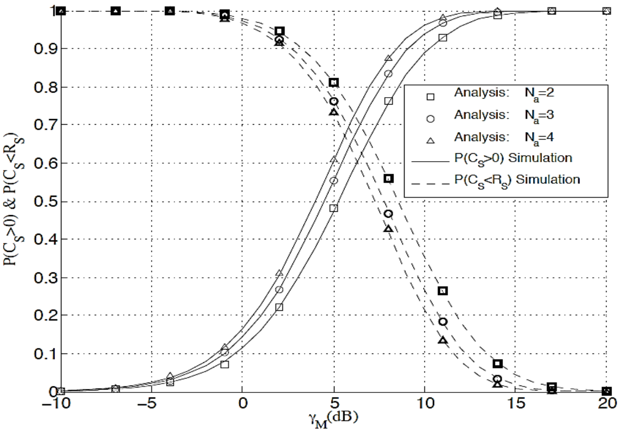

Figure 6. *The probability of non-zero secrecy capaciy and the secrecy outage probability (Rayleigh/ Nakagami, m = 2, $\bar{\gamma}_W$ =10dB, N$_b$=2, R$_S$=1 bit/s/Hz)*

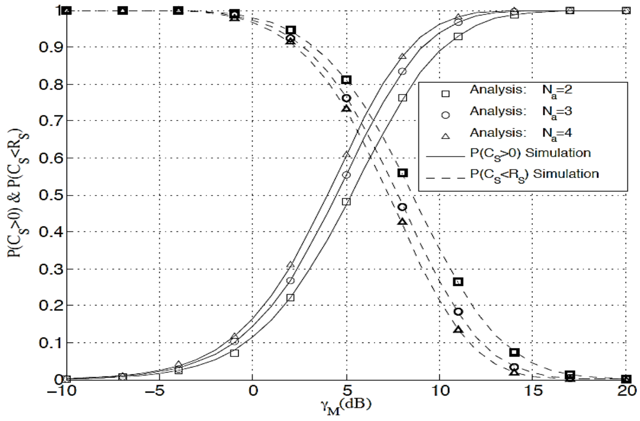

Figure 7. *The probability of non-zero secrecy capaciy and the secrecy outage probability (Nakagami/ Rayleigh, m = 2, N_b=2, $\bar{\gamma}_W$ =10dB, R_S=1 bit/s/Hz)*

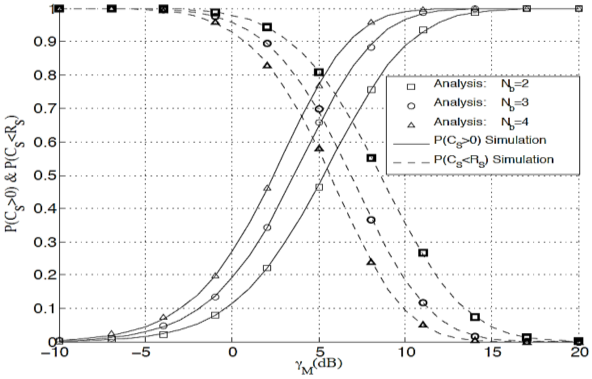

Figure 8. *The probability of non-zero secrecy capaciy and the secrecy outage probability (Rayleigh/Nakagami, m = 2, N_a=2, $\bar{\gamma}_W$ =10dB, R_S=1 bit/s/Hz)*

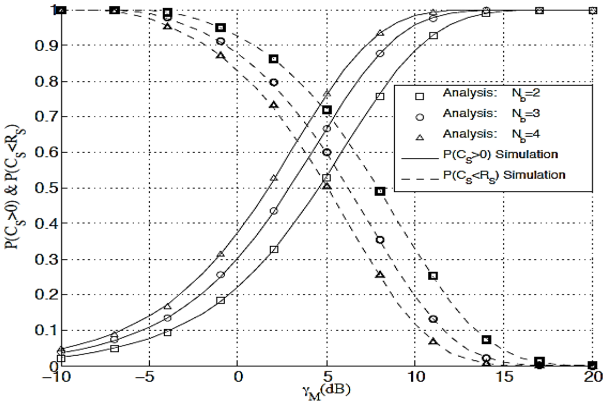

Figure 9. *The probability of non-zero secrecy capaciy and the secrecy outage probability (Nakagami/Rayleigh, m = 2, N_a=2, $\bar{\gamma}_W$ =10dB, R_S=1 bit/s/Hz)*

Figure 6, Figure 7, Figure 8 and Figure 9 illustrate the variation of the probability of non-zero secrecy capacity and the secrecy outage probability with respect to the number of transmission antennas N_a and the number of reception antennas N_b in two approaches: Rayleigh/ Nakagami and Nakagami/ Rayleigh respectively. When N_a or N_b increases, the secrecy performance becomes better. Obviously, in order to enhance the secrecy performance of this considered system we can increase the number of transmission antennas or the number of reception antennas of legal devices.

As it can be observed clearly from above figures, the secrecy performance is improved with: the increase in SNR at Bob receiver or the decrease in SNR at Eve or the increase of the number of antennas at Alice and Bob. The good agreement between analytical and simulation results verifies the correctness of our analysis.

5. Conclusion

In this paper, we focus on PHY secrecy performance analysis of MIMO system using TAS/MRC in the presence of a single antenna passive eavesdropper in two scenarios: the main channel undergoes Rayleigh fading, while the eavesdropper's channel is subject to Nakagami fading and vice versa. The exact closed form expressions of probability of non-zero secrecy capacity and the secrecy outage probability have been derived and validated by Monte-Carlo simulations. In addition, our results show that the secrecy performance of the Nakagami/ Rayleigh fading channels outperforms that of the Rayleigh/ Nakagami fading channels due to the LOS component. Our results also show that increasing the number of transmission antennas or the number of reception antennas can improve the secrecy performance of the considered system.

REFERENCES

[1] C. E. Shannon, "Communication theory of secrecy systems", *Bell Syst. Technol. J.*, vol. 28, pp. 656–715, Oct. 1949.

[2] A. D. Wyner, "The wire-tap channel", *Bell Syst. Technol. J.*, vol. 54,no. 8, pp. 1355–1387, Oct. 1975.

[3] S. Leung-Yan-Cheong and M. Hellman, "The gaussian wire-tap channel", *IEEE Trans. Inf. Theory*, vol. 24, no. 4, pp. 451–456, July 1978.

[4] H. Alves, R. D. Souza, M. Debbah, and M. Bennis, "Performance of transmit antenna selection physical layer security schemes", *in IEEE Signal Process. Lett.*, vol. 19(6), 2012, pp. 372–375.

[5] N. Yang, H. A. Suraweera, I. B. Collings, and C. Yuen, "Physical layer security of TAS/MRC with antenna correlation*", IEEE Transactions on Information Forensics and Security*, vol. 8(1), pp. 254–259, 2013.

[6] N. Yang, P. L. Yeoh, M. Elkashlan, R. Schober, and I. B. Collings, "Transmit antenna selection for security enhancement in MIMO wiretap channels", *IEEE Transactions on Communications*, vol. 61(1), pp. 144 – 154, 2013.

[7] A. P. Shrestha and K. S. Kwak, "Performance of opportunistic scheduling for physical layer security with transmission antenna selection", *EURASIP Journal on Wireless Communications and Networking*, vol. 2014:33, pp. 1–9, 2014.

[8] L. Wang, N. Yang, M. Elkashlan, P. L. Yeoh, and J. Yuan, "Physical layer security of maximal ratio combining in two-wave with diffuse power fading channels", *IEEE Transactions on Information Forensics and Security*, vol. 9(2), pp. 247–258, 2014.

[9] D.-B. Ha, N. G. Nguyen, D.-D. Tran, and T.-H. Nguyen, "Physical layer security in UWB communication systems with Transmit Antenna Selection", *in The 2th IEEE International Conference on Computing, Managements and Telecommunications 2014 (ComManTel 2014)*, DaNang, Vietnam, April 27-29, 2014, pp. 280–285.

[10] V. T. Tan, D.-B. Ha, and D.-D. Tran, "Evaluation of physical layer security in MIMO ultra-wideband system using time-reversal technique", *in The 2th IEEE International Conference on Computing, Managements and Telecommunications 2014 (ComManTel 2014),* Da Nang, Vietnam, April 27-29, 2014, pp. 70–74.

(The Board of Editors received the paper on 07/09/2015, its review was completed on 10/23/2015)