Physical Layer Secrecy Performance Analysis over Rayleigh/Nakagami Fading Channels

Dac-Binh Ha, Phu-Tuan Van, and Truong Tien Vu

[1] ***Abstract*—The broadcast nature of wireless communications makes it vulnerable to attack or eavesdropping. Therefore, information security is an important issue in wireless communications, especially in distributed networks such as wireless sensor networks and ad hoc wireless networks. In this paper, we present the physical layer secrecy performance analysis of single-input single-output (SISO) systems consisting of single antenna devices, in the presence of a single antenna passive eavesdropper over dissimilar Rayleigh/Nakagami fading channels. Especially, we derive exact close-form expressions for the probability that secrecy capacity exists and the secrecy outage probability using statistical characteristics of the signal-to-noise ratio. These expressions allow us to assess the security capability of the considered single-input single- output systems. The analytical result are verified by Monte-Carlo simulation.**

***Index Terms*—Physical layer secrecy, Rayleigh fading, Nakagami fading, secrecy capacity**

I. INTRODUCTION

Today, wireless networks become the most popular way to communicate. The broadcast nature of wireless communication make them particularly vulnerable to eavesdrop. Therefore, information security is an important issue in wireless communication, especially in government, military, finance and banking services. To ensure information security, many data encryption and decryption algorithms have been applied at application layer based on several assumptions. For instance, it is assumed that the link between the transmitter and receiver (physical layer) is error-free, while eavesdroppers have restricted computational power and lack efficient algorithms. However, the latter assumption is being weakened with the development of efficient algorithms as well as the increase in computational power of modern computers, e.g. quantum computers. To solve this problem, many researchers have recently focused on information security issues at the physical layer (PHY) which obtain secrecy by exploiting the PHY properties such as thermal noise, interference and the time-varying nature of fading channels.

Most of researchers have recently focused on information security issues at the PHY in two main approaches: key-based secrecy [1]–[4] and keyless security [5]–[7]. The first approach is to find a security key based on the characteristics of the transmission environment. For example, different users will have a different noisy version of the transmitted signal, which allows to abstract the security key and this key is used to ensure the security between legitimate users. The second approach focuses on building a random encryption mechanism, which aims to hide the flow of information in the community in order to weaken interference eavesdropping devices by mapping each message to many codewords according to an appropriate probability distribution. In this way, maximum ambiguity is caused at eavesdropping devices, which indicates that the communication can be safe without using the security key.

The methods of evaluating whether the system is capable of ensuring security at the PHY are also attracting more researchers in this field [8]–[10]. In these works, PHY secrecy for a quasi-static Rayleigh fading wiretap channel with single antenna and multiple antenna devices has been investigated. In [8], based on an information-theoretic problem formulation in which two legitimate partners communicate over the same independent fading channel with an eavesdropper channel, the authors have defined the secrecy capacity in terms of outage probability and provided a complete characterization of the maximum transmission rate at which the eavesdropper is unable to decode any information. In [9], the authors have investigated the PHY secrecy of a communication scheme consisting of a multiple antenna transmitter using transmit antenna selection and a single antenna receiver, in the presence of a multiple antenna eavesdropper. The authors of [10] have analyzed the impact of antenna correlation on secrecy performance of multiple-input multiple-output wiretap channels where the transmitter employs transmit antenna selection while the receiver and eavesdropper perform maximal-ratio combining with arbitrary correlation. The PHY secrecy performance of multiple-input single-output Ultra-Wideband (UWB) system is evaluated in [11] and the time-reversal technique is used to improve the secrecy capacity in MIMO UWB system [12].

Until now, most of previous works on PHY secrecy have assumed that the legal channels are similar to the illegal channels. However, in many practical scenarios, this assumption does not hold since the two channels have different fading characteristics due to the mobility of mobile devices. Li et al. [13] examined an achievable secrecy rate for an additive white Gaussian noise (AWGN) communication channel, while the eavesdropper's channel is Rayleigh fading with AWGN. To the best of our knowledge, there has been no previous work that mentioned evaluating the secrecy capacity of the

[1]Dac-Binh Ha is with Institute of Research and Development, Duy Tan University, Da Nang, Vietnam (email: hadacbinh@duytan.edu.vn).
Phu-Tuan Van is with Department of Electronics and Telecommunications, Duy Tan University, Da Nang, Vietnam (email: phutuan87@gmail.com).
Truong Tien Vu is with Department of Information Technology, Duy Tan University, Da Nang, Vietnam (email: truongtienvu@dtu.edu.vn).

ISBN: 978-988-19253-7-4
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

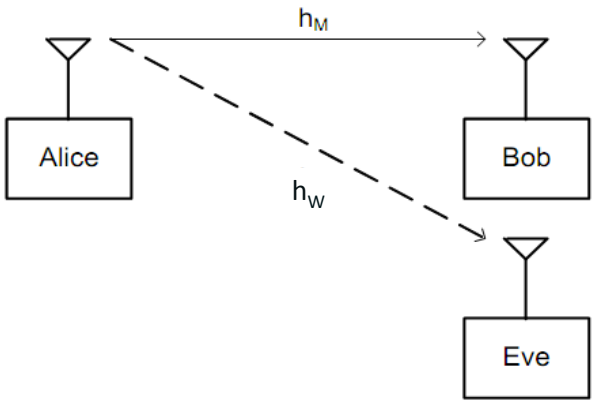

Figure 1. SISO system

systems consisting of a couple of single antenna devices, in the presence of a single antenna passive eavesdropper over dissimilar Rayleigh/Nakagami fading channels. In this paper, we derive the exact closed-form expressions of probability of existence of secrecy capacity and the secrecy outage probability base on the statistical characteristics of the signal-to-noise ratio (SNR). By using these expressions, we can assess the security capability of SISO systems over Rayleigh/Nakagami fading channels.

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

II. SYSTEM AND CHANNEL MODEL

We consider the system as illustrated in Fig. 1. Alice and Bob are two legitimate users of the SISO system. Alice wants to send messages to Bob, while Eve is a passive eavesdropper which tries to extract information from Alice without actively attacking. Alice, Bob and Eve are single antenna devices. 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 undergo Rayleigh/Nakagami fading

The legal channel is assumed to undergo Rayleigh fading, while the eavesdropper experiences Nakagami fading. Alice sends the signal $x(t)$ to Bob. The received signal $y(t)$ at Bob has the following form:

$$y\left(t\right)=h_{M}x\left(t\right)+n_{M}, \tag{1}$$

where h_M is the Rayleigh fading coefficient between the transmit antenna at Alice and the receive antenna at Bob, n_M is zero-mean complex Gaussian random variable with power N_M.

The instantaneous SNR at Bob is $\gamma_M=\frac{P_M|h_M|^2}{N_M}$, while the average SNR is $\bar{\gamma}_M=\frac{P_M E\left[|h_M|^2\right]}{N_M}$, where P_M is the average received power at Bob. The probability density function (PDF) of γ_M is [9]:

$$f_{\gamma_M}\left(\gamma_M\right)=\frac{1}{\bar{\gamma}_M}e^{-\frac{\gamma_M}{\bar{\gamma}_M}}. \tag{2}$$

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

$$z\left(t\right)=h_{W}x\left(t\right)+n_{W}, \tag{3}$$

where h_W is the Nakagami fading coefficient between the transmit antenna at Alice and the receive antenna at Eve, n_W is zero-mean complex Gaussian random variable with power N_W.

The instantaneous SNR at Eve is $\gamma_W=\frac{P_W|h_W|^2}{N_W}$, while the average SNR is $\bar{\gamma}_W=\frac{P_W E\left[|h_W|^2\right]}{N_W}$, where P_W is the average received power at Eve. The PDF of γ_W is [9]:

$$f_{\gamma_W}\left(\gamma_W\right)=\frac{m^m}{\bar{\gamma}_W^m\Gamma\left(m\right)}\gamma_W^{m-1}e^{-\frac{m\gamma_W}{\bar{\gamma}_W}}, \tag{4}$$

where $\Gamma(\,)$ denotes the Gamma function.

B. The legal/illegal channels undergo Nakagami/Rayleigh fading

The legal channel is assumed to undergo Nakagami fading and the illegal channel is assumed to undergo Rayleigh fading. Similarly, the PDF of γ_M is as follows:

$$f_{\gamma_M}\left(\gamma_M\right)=\frac{m^m}{\bar{\gamma}_M^m\Gamma\left(m\right)}\gamma_M^{m-1}e^{-\frac{m\gamma_M}{\bar{\gamma}_M}}. \tag{5}$$

The PDF of γ_W is as follows:

$$f_{\gamma_W}\left(\gamma_W\right)=\frac{1}{\bar{\gamma}_W}e^{-\frac{\gamma_W}{\bar{\gamma}_W}}. \tag{6}$$

III. SECRECY CAPACITY ANALYSIS

A. Preliminaries

Channel capacity of link between two legitimate users is:

$$C_M=\log_2\left(1+\gamma_M\right). \tag{7}$$

Channel capacity of link to illegitimate user is:

$$C_W=\log_2\left(1+\gamma_W\right). \tag{8}$$

The instantaneous secrecy capacity is given by [8]:

$$\begin{aligned} C_S &= \left[C_M-C_W\right]^+ \\ &= \begin{cases} \log_2\left(\frac{1+\gamma_M}{1+\gamma_W}\right) & ,\gamma_M>\gamma_W \\ 0 & ,\gamma_M\leq\gamma_W \end{cases} \end{aligned} \tag{9}$$

ISBN: 978-988-19253-7-4
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

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

1) Existence of Secrecy Capacity: Assume that the main channel and the eavesdropper channel are independent with each other, we can derive the probability of the existence of a non-zero secrecy capacity as follows

$$\begin{aligned} P\left(C_S>0\right) &= P\left(\gamma_M>\gamma_W\right) \\ &= \int_0^{\infty}\int_0^{\gamma_M} f_{\gamma_M\gamma_W}\left(\gamma_M,\gamma_W\right)d\gamma_W d\gamma_M \\ &= \int_0^{\infty}\int_0^{\gamma_M} f_{\gamma_M}\left(\gamma_M\right)f_{\gamma_W}\left(\gamma_W\right)d\gamma_W d\gamma_M \\ &= 1-\sum_{i=0}^{m-1}\frac{\bar{\gamma}_W\left(\bar{\gamma}_M m\right)^i}{\left(m\bar{\gamma}_M+\bar{\gamma}_W\right)^{i+1}}. \end{aligned} \quad (10)$$

For further calculation details see in Appendix.

2) Secrecy Outage Probability: The secrecy outage probability can be defined as

$$\begin{aligned} P\left(C_S<R_S\right) &= \int_0^{\infty}\int_0^{y} f_{\gamma_M\gamma_W}\left(\gamma_M,\gamma_W\right)d\gamma_M d\gamma_W \\ &= 1-\left(\frac{m\bar{\gamma}_M}{m\bar{\gamma}_M+\bar{\gamma}_W 2^{R_S}}\right)^m e^{\frac{1-2^{R_S}}{\bar{\gamma}_M}}, \end{aligned} \quad (11)$$

where $R_S>0$ is the secrecy rate and $y=2^{R_S}\left(1+\gamma_W\right)-1$. For further calculation details see in Appendix.

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

1) Existence of Secrecy Capacity: This process is similarly to previous one, we derive the probability of the existence of a non-zero secrecy capacity as

$$\begin{aligned} P'\left(C_S>0\right) &= P\left(\gamma_M>\gamma_W\right) \\ &= \int_0^{\infty}\int_0^{\gamma_M} f_{\gamma_M\gamma_W}\left(\gamma_M,\gamma_W\right)d\gamma_W d\gamma_M \\ &= 1-\left(\frac{m\bar{\gamma}_W}{m\bar{\gamma}_W+\bar{\gamma}_M}\right)^m. \end{aligned} \quad (12)$$

For further calculation details see in Appendix.

2) Secrecy Outage Probability: The secrecy outage probability can be defined as

$$\begin{aligned} P'\left(C_S<R_S\right) &= \int_0^{\infty}\int_0^{y} f_{\gamma_M\gamma_W}\left(\gamma_M,\gamma_W\right)d\gamma_M d\gamma_W \\ &= 1-\frac{e^{\frac{-mb2^{R_S}}{\bar{\gamma}_M}}}{\bar{\gamma}_W}\sum_{i=0}^{m-1}\frac{\left(\frac{m2^{R_S}}{\bar{\gamma}_M}\right)^i}{k^{i+1}}\sum_{s=0}^{i}\frac{(kb)^s}{s!}, \end{aligned} \quad (13)$$

where $k=\frac{\bar{\gamma}_M+m2^{R_S}\bar{\gamma}_W}{\bar{\gamma}_M\bar{\gamma}_W}$ and $b=1-\frac{1}{2^{R_S}}$. For further calculation details see in Appendix.

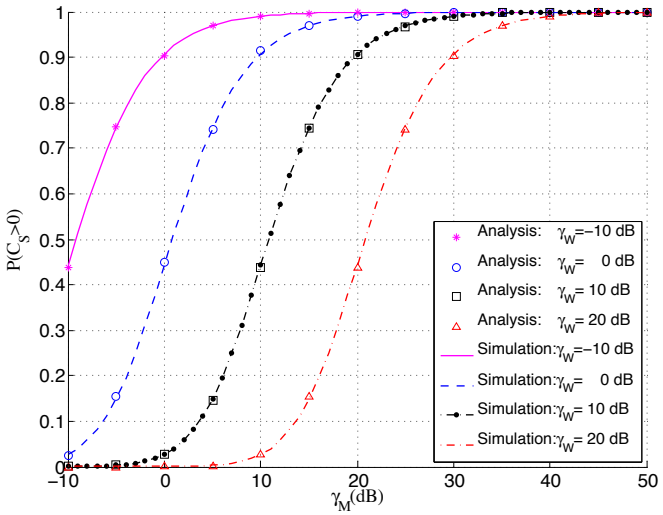

Figure 2. The probability of the existence of a non-zero secrecy capacity (Rayleigh/Nakagami, m = 2).

IV. NUMERICAL RESULTS

In this section, we discusses some results based on the theoretical analysis and Monte-Carlo simulations of the probability of existence of secrecy capacity and the secrecy outage probability in two cases: Rayleigh/Nakagami fading and Nakagami/Rayleigh fading.

A. Probability of existence of secrecy capacity

Figure 2 and 3 show the probability of the existence of secrecy capacity in two scenarios: Rayleigh/Nakagami and Nakagami/Rayleigh fading respectively, with the shape parameter $m=2$. In these figures, the existing secrecy capacity probabilities $P\left(C_S>0\right)$ and $P'\left(C_S>0\right)$ increase rapidly when we fix Eve's SNR γ_W and increase Bob's SNR γ_M. On the other hand, with fixed γ_M, $P\left(C_S>0\right)$ and $P'\left(C_S>0\right)$ decrease when γ_W increases. From (9), these assessments are reasonable because when γ_M increases, the received signal at Bob is better than Eve so that the capacity of legitimate user is lager than the capacity of illegitimate user.

B. Secrecy outage probability

Similarly, figure 4 and 5 show the secrecy outage probabilities for Rayleigh/Nakagami and Nakagami/Rayleigh fading, respectively. With fixed γ_W, the secrecy outage probabilities $P\left(C_S<R_S\right)$ and $P'\left(C_S<R_S\right)$ decrease rapidly when γ_M increases. On the other hand, with fixed γ_M, $P\left(C_S<R_S\right)$ and $P'\left(C_S<R_S\right)$ increase when γ_W increases. From (11), These assessments are reasonable because when γ_M increases, the received signal at Bob is better than Eve so that the capacity of legitimate user is lager than the capacity of illegitimate user.

Compare between four figures (Fig. 2, 3, 4 and 5), we can see that $m=2$ the secrecy performance over Rayleigh/Nakagami fading channels is worse than Nakagami/Rayleigh fading channels. In other words, the values

ISBN: 978-988-19253-7-4
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

$$
\begin{aligned}
P\left(C_S>0\right) &= \int_0^{\infty}\int_0^{\gamma_M} f_{\gamma_M\gamma_W}\left(\gamma_M,\gamma_W\right)d\gamma_W d\gamma_M \\
&= \int_0^{\infty}\int_0^{\gamma_M} f_{\gamma_M}\left(\gamma_M\right) f_{\gamma_W}\left(\gamma_W\right)d\gamma_W d\gamma_M \\
&= \int_0^{\infty}\int_0^{\gamma_M} \frac{1}{\bar{\gamma}_M}e^{-\frac{\gamma_M}{\bar{\gamma}_M}}\frac{m^m}{\bar{\gamma}_W^m\Gamma\left(m\right)}\gamma_W^{m-1}e^{-\frac{m\gamma_W}{\bar{\gamma}_W}}d\gamma_W d\gamma_M \\
&= \int_0^{\infty}\frac{1}{\bar{\gamma}_M}e^{-\frac{\gamma_M}{\bar{\gamma}_M}}\left(1-e^{-\frac{m\gamma_M}{\bar{\gamma}_W}}\sum_{i=0}^{m-1}\frac{\left(\frac{m\gamma_M}{\bar{\gamma}_W}\right)^i}{i!}\right)d\gamma_M \\
&= 1-\sum_{i-0}^{m-1}\frac{1}{\bar{\gamma}_M i!}\int_0^{\infty}\left(\frac{m\gamma_M}{\bar{\gamma}_W}\right)^i e^{-\gamma_M\left(\frac{1}{\bar{\gamma}_M}+\frac{m}{\bar{\gamma}_W}\right)}d\gamma_M \\
&= 1-\sum_{i=0}^{m-1}\frac{\bar{\gamma}_W\left(\bar{\gamma}_M m\right)^i}{\left(m\bar{\gamma}_M+\bar{\gamma}_W\right)^{i+1}}.
\end{aligned}
\tag{14}
$$

$$
\begin{aligned}
P\left(C_S<R_S\right) &= \int_0^{\infty}\int_0^{y} f_{\gamma_M\gamma_W}\left(\gamma_M,\gamma_W\right)d\gamma_M d\gamma_W \\
&= \int_0^{\infty}\int_0^{y} f_{\gamma_M}\left(\gamma_M\right) f_{\gamma_W}\left(\gamma_W\right)d\gamma_M d\gamma_W \\
&= \int_0^{\infty}\int_0^{y} \frac{1}{\bar{\gamma}_M}e^{-\frac{\gamma_M}{\bar{\gamma}_M}}\frac{m^m}{\bar{\gamma}_W^m\Gamma\left(m\right)}\gamma_W^{m-1}e^{-\frac{m\gamma_W}{\bar{\gamma}_W}}d\gamma_M d\gamma_W \\
&= \int_0^{\infty}\frac{m^m}{\bar{\gamma}_W^m\Gamma\left(m\right)}\gamma_W^{m-1}e^{-\frac{m\gamma_W}{\bar{\gamma}_W}}\left(1-e^{-\frac{2^{R_S}}{\bar{\gamma}_M}\left(\gamma_W+1-\frac{1}{2^{R_S}}\right)}\right)d\gamma_W \\
&= 1-\frac{m^m}{\bar{\gamma}_W^m\Gamma\left(m\right)}e^{\frac{1-2^{R_S}}{\bar{\gamma}_M}}\int_0^{\infty}\gamma_W^{m-1}e^{-\gamma_W\left(\frac{m}{\bar{\gamma}_W}+\frac{2^{R_S}}{\bar{\gamma}_M}\right)}d\gamma_W \\
&= 1-\left(\frac{m\bar{\gamma}_M}{m\bar{\gamma}_M+\bar{\gamma}_W 2^{R_S}}\right)^m e^{\frac{1-2^{R_S}}{\bar{\gamma}_M}}.
\end{aligned}
\tag{15}
$$

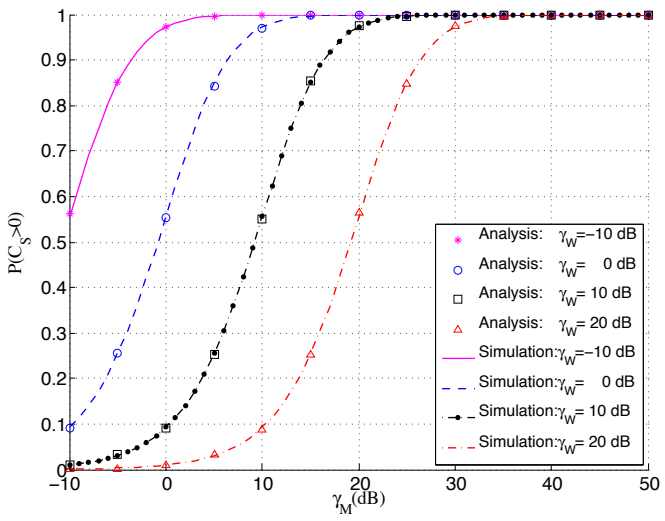

Figure 3. The probability of the existence of a non-zero secrecy capacity (Nakagami/Rayleigh, m = 2).

of m greater than one correspond to fading less severe than Rayleigh fading.

To confirm the right of our analysis, we also consider Rayleigh/Rayleigh fading case (Nakagami with $m = 1$). The matching of both existing secrecy capacity probabilities and the secrecy outage probabilities in two scenarios show that our analysis is correct.

As can clearly be observed from all figures, the probability that secrecy capacity exists decreases and secrecy outage performance increases with the increase of SNRs at Bob receiver. The good agreement between analytical and simulation results verifies the correctness of our analysis.

V. CONCLUSION

In this paper, we have focused on analysis of PHY secrecy of system consisting two legitimate single antenna devices and one single antenna passive eavesdropper. The exact closed form expressions of probability of existence of secrecy capacity and the secrecy outage probability have been derived. Based on these expressions, we have evaluated the secrecy capacity performance of the considered SISO systems in two

ISBN: 978-988-19253-7-4
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

$$
\begin{aligned}
P'\left(C_S>0\right) &= \int_0^{\infty}\int_0^{\gamma_M} f_{\gamma_M}\left(\gamma_M\right) f_{\gamma_W}\left(\gamma_W\right) d\gamma_W d\gamma_M \\
&= \int_0^{\infty}\int_0^{\gamma_M} \frac{1}{\bar{\gamma}_W} e^{-\frac{\gamma_W}{\bar{\gamma}_W}} \frac{m^m}{\bar{\gamma}_M^m \Gamma\left(m\right)} \gamma_M^{m-1} e^{-\frac{m\gamma_M}{\bar{\gamma}_M}} d\gamma_W d\gamma_M \\
&= \int_0^{\infty} \frac{m^m}{\bar{\gamma}_M^m \Gamma\left(m\right)} \gamma_M^{m-1} e^{-\frac{m\gamma_M}{\bar{\gamma}_M}} \left(1-e^{-\frac{\gamma_M}{\bar{\gamma}_W}}\right) d\gamma_M \\
&= 1-\left(\frac{m\bar{\gamma}_W}{m\bar{\gamma}_W+\bar{\gamma}_M}\right)^m . \qquad (16)
\end{aligned}
$$

$$
\begin{aligned}
P\left(C_S<R_S\right) &= \int_0^{\infty}\int_0^{y} f_{\gamma_M}\left(\gamma_M\right) f_{\gamma_W}\left(\gamma_W\right) d\gamma_M d\gamma_W \\
&= \int_0^{\infty}\int_0^{y} \frac{1}{\bar{\gamma}_W} e^{-\frac{\gamma_W}{\bar{\gamma}_W}} \frac{m^m}{\bar{\gamma}_M^m \Gamma\left(m\right)} \gamma_M^{m-1} e^{-\frac{m\gamma_M}{\bar{\gamma}_M}} d\gamma_M d\gamma_M \\
&= \int_0^{\infty} \frac{1}{\bar{\gamma}_W} e^{-\frac{\gamma_W}{\bar{\gamma}_W}} \left(1-e^{-\frac{m2^{R_S}\left(\gamma_W-b\right)}{\bar{\gamma}_M}} \sum_{i=0}^{m-1} \frac{\left(\frac{m2^{R_S}\left(\gamma_W-b\right)}{\bar{\gamma}_M}\right)^i}{i!}\right) d\gamma_W \\
&= 1-\frac{e^{\frac{-mb2^{R_S}}{\bar{\gamma}_M}}}{\bar{\gamma}_W} \sum_{i=0}^{m-1} \left(\frac{m2^{R_S}}{\bar{\gamma}_M}\right)^i \int_0^{\infty} \frac{\left(\gamma_W+b\right)^i}{i!} e^{-k\gamma_W} d\gamma_W \\
&= 1-\frac{e^{\frac{-mb2^{R_S}}{\bar{\gamma}_M}}}{\bar{\gamma}_W} \sum_{i=0}^{m-1} \left(\frac{m2^{R_S}}{\bar{\gamma}_M}\right)^i \frac{1}{k^{i+1}} \sum_{s=0}^{i} \frac{(kb)^s}{s!} . \qquad (17)
\end{aligned}
$$

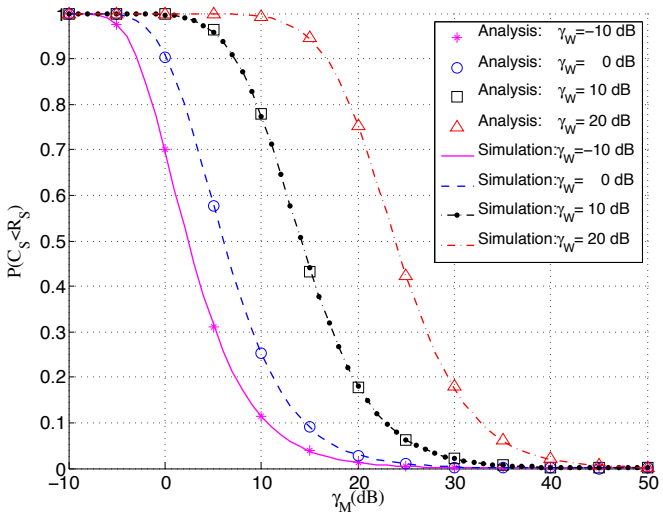

Figure 4. The secrecy outage probability (Rayleigh/Nakagami, m = 2, R_S = 1 bits/s/Hz).

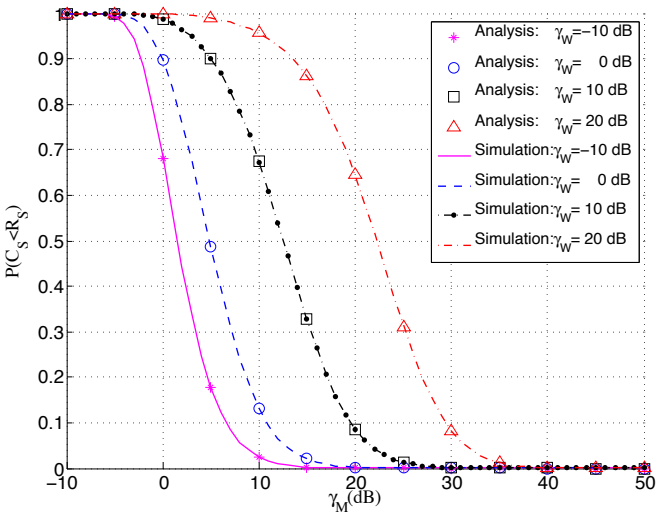

Figure 5. The secrecy outage probability (Nakagami/Rayleigh, m = 2, R_S = 1 bits/s/Hz).

scenarios: the main channel undergoes Rayleigh fading, while the eavesdropper's channel is subject to Nakagami fading and vice versa. The correctness of our analysis has been demonstrated by the analytical and simulation results.

APPENDIX

Here, by using [14, eqs. 6.451, 8.350, and 8.352], we calculate $P\left(C_S>0\right)$, $P'\left(C_S>0\right)$, $P\left(C_S<R_S\right)$ and $P'\left(C_S<R_S\right)$ as (14), (15), (16) and (17), respectively.

ISBN: 978-988-19253-7-4
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

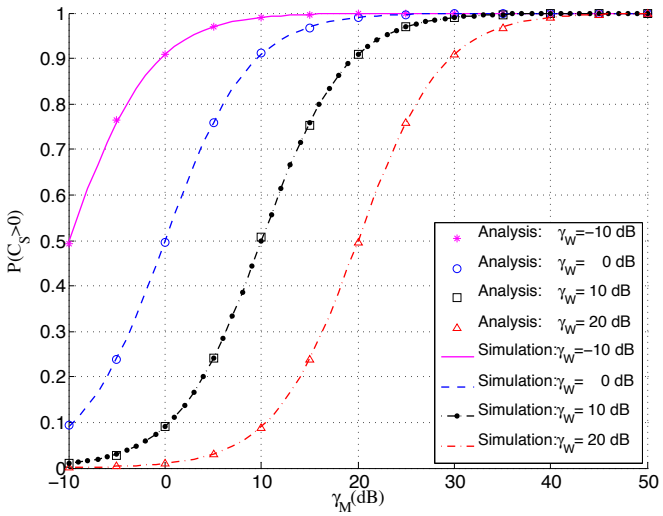

Figure 6. The probability of the existence of a non-zero secrecy capacity (Rayleigh/Rayleigh, m = 1).

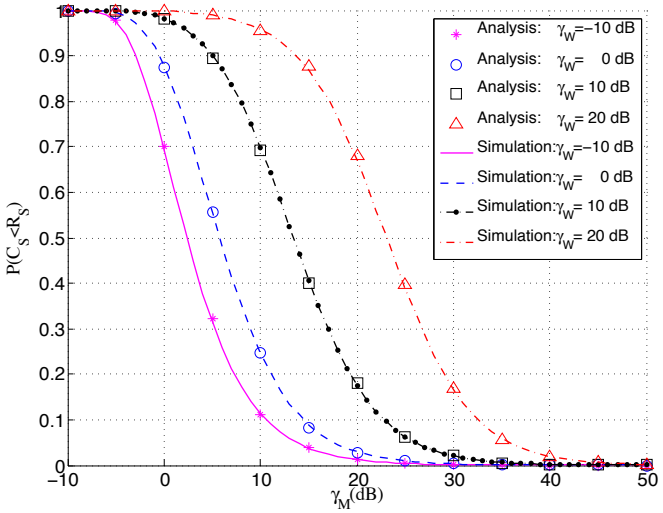

Figure 7. The secrecy outage probability (Rayleigh/Rayleigh, m = 1, $R_S = 1$ bits/s/Hz).

REFERENCES

[1] U. Maurer, "Secret key agreement by public discussion form common information," *IEEE Trans. Info. Theory*, vol. 39, no. 3, pp. 733–742, 1993.

[2] T. Aono, K. Higuchi, T. Ohira, B. Komiyama, and H. Sasaoka, "Wireless secret key generation exploiting reactance-domain scalar response of multipath fading channels," *IEEE Trans. Antennas and Propagation*, vol. 53, no. 11, pp. 3776–3784, 2005.

[3] B. Azimi-Sadjadi, A. Kiayias, A. Mercado, and B. Yener, "Robust key generation from signal envelopes in wireless networks," in *Proc. 14th ACM Conf. Computer and Comm. Security (CCS)*, Alexandria, USA, Oct. 29 - Nov. 2, 2007, pp. 401–410.

[4] C. Ye, S. Mathur, A. Reznik, Y. Shah, W. Trappe, and N. Mandayam, "Information-theoretically secret key generation for fading wireless channels," *IEEE Trans. Info. Forensics Security*, vol. 5, no. 2, pp. 240–254.

[5] A. Wyner, "The wire-tap channel," *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975.

[6] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Info. Theory*, vol. 24, no. 3, pp. 339–348, 1978.

[7] P. K. Gopala, L. Lai, and H. E. Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4687–5403, 2008.

[8] J. Barros and M. Rodrigues, "Secrecy capacity of wireless channels," in *Proc. IEEE Int. Symp. Information Theory (ISIT)*, Seattle, USA, July 2006, pp. 356–360.

[9] H. Alves, R. D. Souza, M. Debbah, and M. Bennis, "Performance of transmit antenna selection physical layer security schemes," *IEEE Signal Process. Lett.*, vol. 19, no. 6, pp. 372–375, 2012.

[10] 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, no. 1, pp. 254 – 259, 2013.

[11] 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)*, Da Nang, Vietnam, April 27-29, 2014, pp. 280–285.

[12] 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.

[13] Z. Li, R. Yates, and W. Trappe, "Secure communication with a fading eavesdropper channel," in *Proc. IEEE Int. Symp. Information Theory (ISIT)*, Nice, France, June 24-26, 2007, pp. 1296–1300.

[14] I. Gradshteyn and I. Ryzhik, *Table of Integrals, Series, and Products*, D. Zwillinger, Ed. Elsevier Academic Press, 2007.

ISBN: 978-988-19253-7-4
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)