Physical Layer Secrecy Performance over Rayleigh/Rician Fading Channels

Dac-Binh Ha, Trung Q. Duong, Duc-Dung Tran, Hans-Jürgen Zepernick, Truong Tien Vu

International Conference on Advanced Technologies for Communications

2014 Hanoi, Vietnam

Physical Layer Secrecy Performance over Rayleigh/Rician Fading Channels

Dac-Binh Ha[†], Trung Q. Duong[††], Duc-Dung Tran[†], Hans-Jürgen Zepernick[†††], and Truong Tien Vu[†]
[†]Duy Tan University, Vietnam (hadacbinh@duytan.edu.vn, dung.td.1227@gmail.com, truongtienvu@dtu.edu.vn)
[††]Queen's University Belfast, United Kingdom (trung.q.duong@qub.ac.uk)
[†††]Blekinge Institute of Technology, Karlskrona, Sweden (hans-jurgen.zepernick@bth.se)

***Abstract*—In this paper, we investigate the physical layer secrecy performance of a single-input single-output system that consists of single antenna devices and operates in the presence of a single antenna passive eavesdropper over dissimilar fading channels. In particular, we consider two scenarios in terms of dissimilar fading channel arrangements: 1) The legal/illegal channels are subject to Rayleigh/Rician fading, respectively; 2) The legal/illegal channels are subject to Rician/Rayleigh fading, respectively. Specifically, analytical expressions for the probability of the existence of a non-zero secrecy capacity and the secrecy outage probability are derived by using statistical characteristics of the signal-to-noise ratio. Numerical results are provided for selected scenarios to illustrate applications of the developed analytical expressions.**

I. INTRODUCTION

Information security has become an increasingly important issue in communications, especially in government, military, finance and banking services. Data encryption and decryption, e.g. the public-key system developed by Rivest, Shamir, and Adleman (RSA) and the data encryption standard (DES), have been employed to ensure information security at the application layer. These approaches are based on assumptions such as having an error-free physical layer link between transmitter and receiver, while eavesdroppers have restricted computational power and lack efficient algorithms. However, the tremendous advances in computational power and processor structures of state-of-the-art hardware platforms have weakened the latter assumption as they can hold sophisticated and increasingly efficient algorithms. In addition, in wireless communication systems, the distributed nature of the transmission channel over radio spectrum makes it easier for third parties to attack or eavesdropping the communication. This applies in particular to distributed networks such as wireless sensor networks and ad hoc wireless networks. The current solutions adapted in wireless communications for protecting the legitimate users from illegal activities of third parties, i.e. applying complex data encryption and decryption techniques at the application layer, are not efficient any more, especially in fast fading radio environments. More importantly, within large-scale networks such encryption protection is infeasible.

To solve this problem, researchers have recently focused on information security issues at the physical layer (PHY) following mainly key-based secrecy [1]–[4] and keyless security [5]–[7] approaches. The first approach is to find a security key based on the characteristics of the transmission environment. For example, different users typically receive a different noisy version of the transmitted signal. This characteristic allows to abstract the security key which is then 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 eavesdropping devices. This is done by mapping each message to many codewords according to an appropriate probability distribution. As a result, maximum ambiguity is obtained at the eavesdropping devices which facilitates the communication to be safe without using a security key.

The methods of evaluating whether a system is capable of ensuring security at the PHY have also received increasing attention by many 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], the security problem of two legitimate partners communicating over the same independent fading channel as the eavesdropper channels has been studied. In particular, an information-theoretic problem formulation is used to defined the so-called secrecy capacity in terms of outage probability. Accordingly, the work reveals the maximum transmission rate at which it would not be possible for an eavesdropper to decode any information. In [9], the PHY secrecy of a communication scheme is investigated that consists of a multiple antenna transmitter along with transmit antenna selection and a single antenna receiver. It is assumed that this system is subject to a multiple antenna eavesdropper. Furthermore, the work presented in [10], is focused on analyzing the impact of antenna correlation on secrecy performance of multiple-input multiple-output wiretap channels. It is assumed that transmit antenna selection is employed at the transmitter of the legitimate user while both receiver and eavesdropper device use maximal-ratio combining and experience arbitrary correlation.

Until now, most of the previous works on PHY secrecy in the context of wireless communications have assumed that the legal channels are basically the same or rather similar to the illegal channels. However, this assumption does not hold in many practical scenarios because the mobility of mobile devices results in two channels typically having different fading characteristics. One of the few studies that consider dissimilar channels is the work of Li et al. [11] which examined the achievable secrecy rate for the case that the legal and illegal

channels, respectively, undergo additive white Gaussian noise (AWGN) and Rayleigh fading in the presence of AWGN.

To the best of our knowledge, there has been no previous work that mentioned assessing the secrecy capacity of systems comprising of single antenna devices, for dissimilar legal/illegal channels subject to Rayleigh/Rician fading or vice versa. In this paper, we therefore derive analytical expressions for the probability of existence of non-zero secrecy capacity as well as the secrecy outage probability for these combinations of dissimilar channels. These analytical expressions allow us to assess the security capability of the considered single-input single-output (SISO) systems.

The rest of this paper is organized as follows. Section II presents the system and channel model. The secrecy capacity of the considered SISO system is analyzed in Section III. In Section IV, we provide numerical results for same selected example scenarios. We conclude our work in Section V.

II. SYSTEM AND CHANNEL MODEL

In the sequel, we consider the SISO system model shown in Fig. 1. Alice and Bob represent the two legitimate users of the SISO system. Alice wants to communicate with Bob, while Eve is a purely passive eavesdropper which attempts to extract information from Alice. Apparently, the three entities in the system, Alice, Bob and Eve are single antenna devices. In this paper, we consider two scenarios: The legal/illegal channels, respectively, are subject to 1) Rayleigh/Rician fading, 2) Rician/Rayleigh fading.

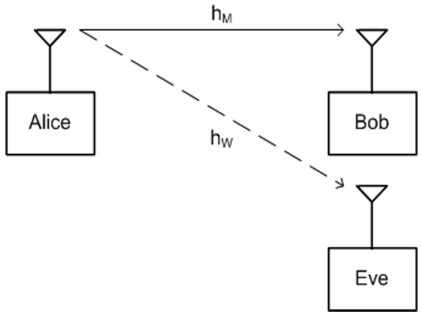

Figure 1. Model of the considered SISO system with legal (main) and illegal (eavesdropping) channel.

A. The legal/illegal channels undergo Rayleigh/Rician fading

The legal channel is assumed to undergo Rayleigh fading, while the eavesdropper experiences Rician fading. Alice sends the signal $x(t)$ to Bob who receives the signal

$$y(t) = h_M x(t) + n_M, \tag{1}$$

where h_M is the Rayleigh fading coefficient associated with the channel between Alice and Bob. Furthermore, n_M denotes complex Gaussian noise with zero mean and variance N_M. The instantaneous SNR and average SNR at Bob are $\gamma_M = P_M|h_M|^2/N_M$ and $\bar{\gamma}_M = P_M E\left[|h_M|^2\right]/N_M$, respectively, where P_M is the average receive power at Bob. The probability density function (PDF) of γ_M on the Rayleigh fading channel is [9]:

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

Eve eavesdrops the signal of Alice and receives the signal

$$z(t) = h_W x(t) + n_W, \tag{3}$$

where h_W is the Rician fading coefficient of the channel between Alice and Eve while n_W denotes complex Gaussian noise with zero mean and variance N_W.

The instantaneous SNR and average SNR at Eve are $\gamma_W = P_W|h_W|^2/N_W$ and $\bar{\gamma}_W = P_W E\left[|h_W|^2\right]/N_W$, respectively, where P_W is the average receive power at Eve. The PDF of γ_W on the Rician channel is given as [12]

$$f_{\gamma_W}(\gamma_W) = \frac{(K+1)e^{-K}}{\bar{\gamma}_W} e^{-\frac{(K+1)\gamma_W}{\bar{\gamma}_W}} I_0\left(2\sqrt{\frac{K(K+1)\gamma_W}{\bar{\gamma}_W}}\right), \tag{4}$$

where K is referred to as Rician K-factor which is defined as the ratio of the powers of the line-of-sight (LOS) components to the powers of the scattered components. Here, $I_0(.)$ is the zero-th order modified Bessel function of the first kind. Furthermore, we can rewrite (4) as follows

$$f_{\gamma_W}(\gamma_W) = a e^{-b\gamma_W} I_0\left(2\sqrt{bK\gamma_W}\right), \tag{5}$$

where $a = (K+1)e^{-K}/\bar{\gamma}_W$ and $b = (K+1)/\bar{\gamma}_W$.

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

The legal channel is assumed to undergo Rician fading, while the eavesdropper experiences Rayleigh fading. Similarly, we have the PDF of γ_M as

$$f_{\gamma_M}(\gamma_M) = p e^{-q\gamma_M} I_0\left(2\sqrt{qK\gamma_M}\right), \tag{6}$$

where $p = (K+1)e^{-K}/\bar{\gamma}_M$ and $q = (K+1)/\bar{\gamma}_M$. On the other hand, the PDF of γ_W is given as

$$f_{\gamma_W}(\gamma_W) = \frac{1}{\bar{\gamma}_W} e^{-\frac{\gamma_W}{\bar{\gamma}_W}}. \tag{7}$$

III. SECRECY CAPACITY ANALYSIS

Let us first recall the varies capacities that are involved in the secrecy capacity analysis. The channel capacity of the SISO main channel and the SISO eavesdropping channel, respectively, are defined as

$$C_M = \log_2\left[1+\gamma_M\right], \tag{8}$$

$$C_W = \log_2\left[1+\gamma_W\right]. \tag{9}$$

Then, the instantaneous secrecy capacity is given by [8]

$$C_S = \{[C_M - C_W]^+ = \begin{cases} \log_2\left[1+\gamma_M\right] - \log_2\left[1+\gamma_W\right], & \gamma_M > \gamma_W \\ 0, & \gamma_M \leq \gamma_W \end{cases} \tag{10}$$

A. The legal/illegal channels undergo Rayleigh/Rician fading

1) Existence of Secrecy Capacity: Let us assume that the main and eavesdropper channel are mutually independent. In this case, the probability of the existence of a non-zero secrecy capacity can be derived as (see also (20) in the Appendix for a more detailed derivation):

$$\begin{aligned} P(C_S>0) &= P(\gamma_M>\gamma_W) \\ &= \int_0^{\infty}\int_0^{\gamma_M} f_{\gamma_M\gamma_W}(\gamma_M,\gamma_W)d\gamma_M d\gamma_W \\ &= \int_0^{\infty}\int_0^{\gamma_M} f_{\gamma_M}(\gamma_M)f_{\gamma_W}(\gamma_W)d\gamma_M d\gamma_W \\ &= \frac{a}{b}\sum_{l=0}^{\infty}\frac{K^l}{l!}\left[1-\sum_{m=0}^{l}\frac{b^m\bar{\gamma}_M^m}{(b\bar{\gamma}_M+1)^{m+1}}\right]. \quad (11) \end{aligned}$$

Note that we have used the following infinite-series representation of $I_0(x)$ [12]:

$$I_0(x)=\sum_{l=0}^{\infty}\frac{x^{2l}}{2^{2l}(l!)^2}. \quad (12)$$

2) Secrecy Outage Probability: The secrecy outage probability can be defined as [8]

$$\begin{aligned} \mathcal{O}(R_S) &= P(C_S<R_S) \\ &= P(C_S<R_S|\gamma_M>\gamma_W)P(\gamma_M>\gamma_W) \\ &+ P(C_S<R_S|\gamma_M\le\gamma_W)P(\gamma_M\le\gamma_W) \\ &= \Phi_1+\Phi_2, \quad (13) \end{aligned}$$

where $R_S>0$ is the secrecy rate and Φ_1, Φ_2 have been determined as follows, respectively, (similar to [8], [9])

$$\begin{aligned} \Phi_1 &= \int_0^{\infty}\int_{\gamma_W}^{y} f_{\gamma_M}(\gamma_M)f_{\gamma_W}(\gamma_W)d\gamma_M d\gamma_W \\ \Phi_2 &= P(\gamma_M\le\gamma_W)=1-P(\gamma_M>\gamma_W) \\ &= 1-\frac{a}{b}\sum_{l=0}^{\infty}\frac{K^l}{l!}\left[1-\sum_{m=0}^{l}\frac{b^m\bar{\gamma}_M^m}{(b\bar{\gamma}_M+1)^{m+1}}\right]. \quad (14) \end{aligned}$$

By using [13, eqs. 6.451, 8.350, and 8.352], we calculate Φ_1 as (22) (see Appendix). Substituting (14) and (22) into (13), we obtain the secrecy outage probability $\mathcal{O}(R_S)$ as follows:

$$\begin{aligned} \mathcal{O}(R_S) &= 1-\frac{a}{b}\sum_{l=0}^{\infty}\frac{K^l}{l!}\left[1-\sum_{m=0}^{l}\frac{b^m\bar{\gamma}_M^m}{(b\bar{\gamma}_M+1)^{m+1}}\right] \\ &+ a\sum_{l=0}^{\infty}\frac{(bK)^l\bar{\gamma}_M^{l+1}}{l!(b\bar{\gamma}_M+1)^{l+1}} \\ &- a\sum_{l=0}^{\infty}\frac{(bK)^l\bar{\gamma}_M^{l+1}e^{-\frac{2^{R_S}-1}{\bar{\gamma}_M}}}{l!(b\bar{\gamma}_M+2^{R_S})^{l+1}}. \quad (15) \end{aligned}$$

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

1) Existence of Secrecy Capacity: Similar to the above derivation, we assume that the main and eavesdropper channels are mutually independent. Accordingly, it is straightforward to derive the probability of the existence of a non-zero secrecy capacity as (see also (22) in the Appendix for details)

$$\begin{aligned} P'(C_S>0) &= P(\gamma_M>\gamma_W) \\ &= \int_0^{\infty}\int_0^{\gamma_M} f_{\gamma_M}(\gamma_M)f_{\gamma_W}(\gamma_W)d\gamma_M d\gamma_W \\ &= p\sum_{l=0}^{\infty}\frac{(qK)^l}{l!}\left[\frac{1}{q^{l+1}}-\left(\frac{\bar{\gamma}_W}{q\bar{\gamma}_W+1}\right)^{l+1}\right] \quad (16) \end{aligned}$$

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

$$\begin{aligned} \mathcal{O}'(R_S) &= P(C_S<R_S) \\ &= \Phi_1'+\Phi_2', \quad (17) \end{aligned}$$

where $R_S>0$ is the secrecy rate and Φ_1', Φ_2' have been, respectively, determined as follows (similar to [8], [9]):

$$\begin{aligned} \Phi_1' &= \int_0^{\infty}\int_{\gamma_W}^{y} f_{\gamma_M}(\gamma_M)f_{\gamma_W}(\gamma_W)d\gamma_M d\gamma_W \\ \Phi_2' &= P(\gamma_M\le\gamma_W)=1-P(\gamma_M>\gamma_W) \\ &= 1-p\sum_{l=0}^{\infty}\frac{(qK)^l}{l!}\left[\frac{1}{q^{l+1}}-\left(\frac{\bar{\gamma}_W}{q\bar{\gamma}_W+1}\right)^{l+1}\right]. \quad (18) \end{aligned}$$

By using [13, eqs. 6.451, 8.350, and 8.352], we calculate Φ_1' as (23) (see Appendix). Substituting (18) and (23) into (17), we obtain the secrecy outage probability $\mathcal{O}'(R_S)$ as follows:

$$\begin{aligned} \mathcal{O}'(R_S) &= 1-p\sum_{l=0}^{\infty}\frac{(qK)^l}{l!}\left[\frac{1}{q^{l+1}}-\left(\frac{\bar{\gamma}_W}{q\bar{\gamma}_W+1}\right)^{l+1}\right] \\ &+ p\sum_{l=0}^{\infty}\sum_{n=0}^{l}\frac{K^l q^{n-1}\bar{\gamma}_W^n}{l!(1+q\bar{\gamma}_W)^{n+1}} \\ &- \frac{pe^{\frac{2^{R_S}-1}{2^{R_S}\bar{\gamma}_W}}}{2^{R_S}\bar{\gamma}_W}\sum_{l=0}^{\infty}\sum_{m=0}^{l}\frac{K^l q^{m-1}}{m!l!} \\ &\times \left(\frac{2^{R_S}\bar{\gamma}_W}{1+2^{R_S}q\bar{\gamma}_W}\right)^{m+1}\Gamma(m+1,r). \quad (19) \end{aligned}$$

IV. NUMERICAL RESULTS

Monte Carlo simulations and analysis are used to demonstrate the performance of physical layer secrecy of our considered system. The number of trials for each simulation result is 10^6 and we use the first 20 terms of the infinite series ($l=20$) for our analysis (refer to [12]). We provide numerical results for the probability that secrecy capacity exists and the secrecy outage probability of two cases: Rayleigh/Rician fading and Rician/Rayleigh fading.

A. Probability of existence of secrecy capacity

Figures 2 and 3 show the probabilities that secrecy capacity exists for Rayleigh/Rician fading and Rician/Rayleigh fading, respectively, with the ratio of the powers of the LOS component to the scattered components $K=6$. In these figures, we can see with Eve's fixed SNR γ_W, when Bob's SNR γ_M increases then the existence probabilities of secrecy capacity $P(C_S>0)$ and $P'(C_S>0)$ quickly increase. With γ_M

fixed, when γ_W increases then $P(C_S > 0)$ and $P'(C_S > 0)$ decrease. From (10), these assessments are reasonable because when γ_M increases, the received signal at Bob is better than the received signal at Eve. In other words, when γ_M increases, capacity of the legal channel is larger than the capacity of the illegal channel.

B. Secrecy outage probability

Similarly, Figs. 4 and 5 show the secrecy outage probabilities for Rayleigh/Rician fading and Rician/Rayleigh fading, respectively. In these figures, we can see with Eve's fixed SNR γ_W, when Bob's SNR γ_M increases then the secrecy outage probabilities $\mathcal{O}(R_S)$ and $\mathcal{O}'(R_S)$ quickly decrease. With γ_M fixed, when γ_W increases then $\mathcal{O}(R_S)$ and $\mathcal{O}'(R_S)$ increase. From (13), these assessments are reasonable because when γ_M increases, the received signal at Bob is better than the received signal at Eve. In other words, when γ_M increases, capacity of the legal channel is larger than the capacity of the illegal channel.

Comparing these four figures (Figs. 2, 3, 4, 5), we can see that the secrecy performance over Rayleigh/Rician fading channels is worse than Rician/Rayleigh fading channels. In other words, the secrecy performance is better when the Rician fading is on the main link due to the LOS component.

To confirm the correctness of our analysis, we also do simulation and analytical calculation for Rayleigh/Rayleigh fading channels ($K = 0$). Since MATHEMATICA cannot run with our calculated expressions when $K = 0$ because of indeterminate expression 0^0, we select $K = 0.001$ instead of $K = 0$. As we can see from Fig. 6 and Fig. 7, the simulation and analytical results are also matching very well.

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.

V. CONCLUSION

In this paper, we have derived expressions for the probability that secrecy capacity exists and the secrecy outage probability in the presence of dissimilar fading channels. The obtained four expressions are in the form of infinite-series representations. Specifically, we have evaluated the secrecy capacity performance of the considered SISO systems in two scenarios: the main channel undergoes Rayleigh fading, while the eavesdropper's channel is subject to Rician fading and vice versa. The numerical results have been accompanied by simulations to verify the analysis for the considered example scenarios.

APPENDIX

Here we calculate $P(C_S > 0)$, $P'(C_S > 0)$, Φ_1 and Φ_1' as (20), (22), (22) and (23), respectively. Note that $y = 2^{R_S}(1+\gamma_W)-1$, $\Gamma(.)$ is the gamma function, $\gamma(\,,\,)$ is the lower incomplete gamma function, $\Gamma(\,,\,)$ is the upper incomplete gamma function and

$$r = \left(\frac{1}{2^{R_S}\bar{\gamma}_W} + q\right)(2^{R_S} - 1).$$

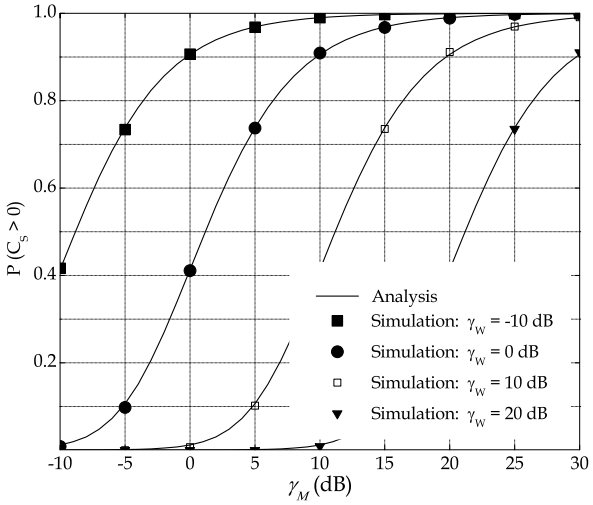

Figure 2. The probability of the existence of a non-zero secrecy capacity (Rayleigh/Rician fading, $K = 6$).

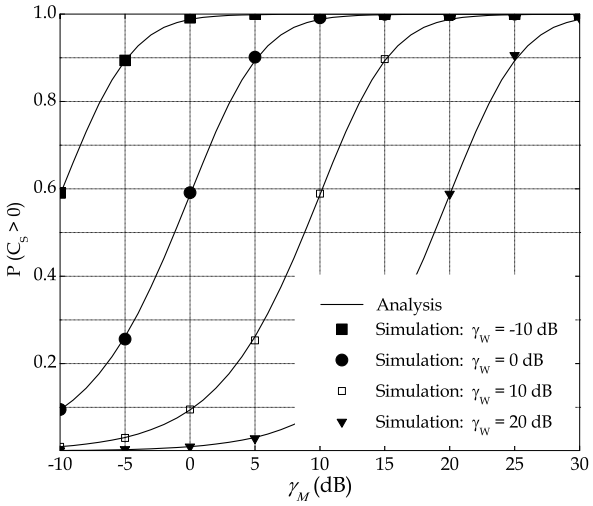

Figure 3. The probability of the existence of a non-zero secrecy capacity (Rician/Rayleigh fading, $K = 6$).

ACKNOWLEDGEMENT

This research is funded by the Vietnam National Foundation for Science and Technology Development (NAFOSTED) under grant number 102.04-2013.13.

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*

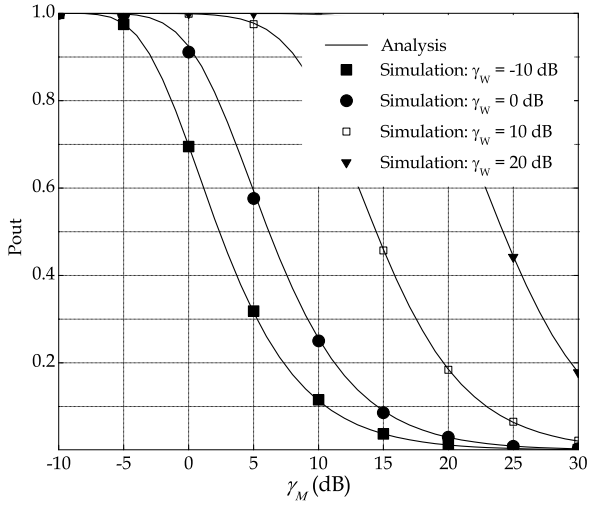

Figure 4. Secrecy outage probability (Rayleigh/Rician fading, $K = 6$).

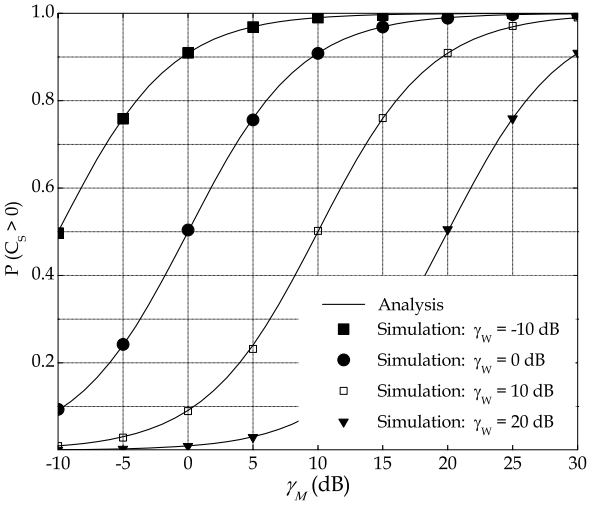

Figure 6. The probability of the existence of a non-zero secrecy capacity (Rayleigh/Rayleigh fading, $K = 0.001$).

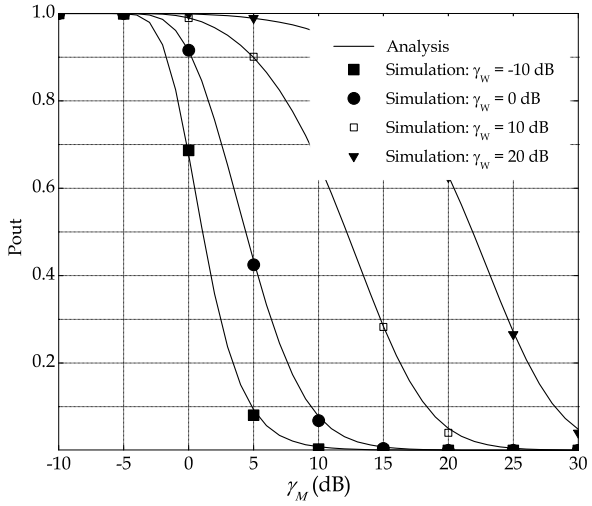

Figure 5. The secrecy outage probability (Rician/Rayleigh fading, $K = 6$).

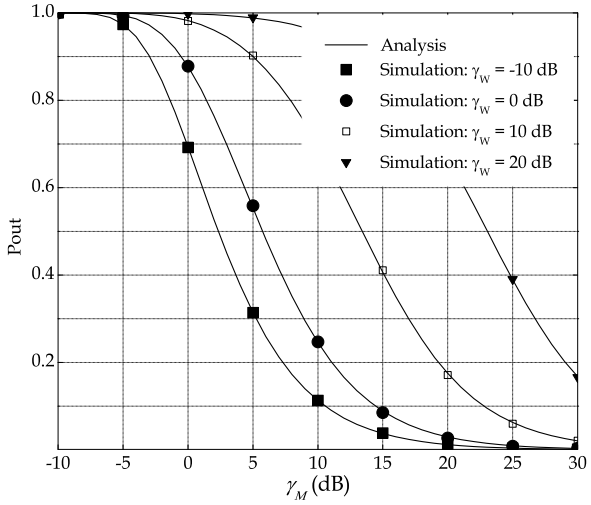

Figure 7. Secrecy outage probability (Rayleigh/Rayleigh fading, $K = 0.001$).

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] 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.

[12] H. A. Suraweera, G. K. Karagiannidis, and P. J. Smith, "Performance analysis of the dual-hop asymmetric fading channel," *IEEE Trans. on Wireless Communi.*, vol. 8, no. 6, pp. 2783–2788, 2009.

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

$$
\begin{aligned}
P(C_S>0) &= \int_0^{\infty}\int_0^{\gamma_M}\frac{1}{\bar{\gamma}_M}e^{-\frac{\gamma_M}{\bar{\gamma}_M}}ae^{-b\gamma_W}I_0\left(2\sqrt{bK\gamma_W}\right)d\gamma_M d\gamma_W \\
&= \frac{a}{\bar{\gamma}_M}\int_0^{\infty}e^{-\frac{\gamma_M}{\bar{\gamma}_M}}\int_0^{\gamma_M}e^{-b\gamma_W}\sum_{l=0}^{\infty}\frac{1}{2^{2l}(l!)^2}\left(2\sqrt{bK\gamma_W}\right)^{2l}d\gamma_W d\gamma_M \\
&= \frac{a}{\bar{\gamma}_M}\sum_{l=0}^{\infty}\frac{(bK)^l}{(l!)^2}\int_0^{\infty}e^{-\frac{\gamma_M}{\bar{\gamma}_M}}\int_0^{\gamma_M}\gamma_W^l e^{-b\gamma_W}d\gamma_W d\gamma_M \\
&= \frac{a}{b\bar{\gamma}_M}\sum_{l=0}^{\infty}\frac{K^l}{(l!)^2}\int_0^{\infty}e^{-\frac{\gamma_M}{\bar{\gamma}_M}}\gamma\left(l+1,b\gamma_M\right)d\gamma_M \\
&= \frac{a}{b\bar{\gamma}_M}\sum_{l=0}^{\infty}\frac{K^l}{l!}\int_0^{\infty}e^{-\frac{\gamma_M}{\bar{\gamma}_M}}\left(1-e^{-b\gamma_M}\sum_{m=0}^{l}\frac{(b\gamma_M)^m}{m!}\right)d\gamma_M \\
&= \frac{a}{b}\sum_{l=0}^{\infty}\frac{K^l}{l!}\left[1-\sum_{m=0}^{l}\frac{b^m\bar{\gamma}_M^m}{\left(b\bar{\gamma}_M+1\right)^{m+1}}\right] \qquad (20)
\end{aligned}
$$

$$
\begin{aligned}
\Phi_1 &= \int_0^{\infty}\int_{\gamma_W}^{y}\frac{1}{\bar{\gamma}_M}e^{-\frac{\gamma_M}{\bar{\gamma}_M}}ae^{-b\gamma_W}I_0\left(2\sqrt{bK\gamma_W}\right)d\gamma_M d\gamma_W \\
&= a\int_0^{\infty}\left(e^{-\frac{\gamma_W}{\bar{\gamma}_M}}-e^{-\frac{y}{\bar{\gamma}_M}}\right)e^{-b\gamma_W}\sum_{l=0}^{\infty}\frac{1}{2^{2l}(l!)^2}\left(2\sqrt{bK\gamma_W}\right)^{2l}d\gamma_W \\
&= a\sum_{l=0}^{\infty}\frac{(bK)^l}{(l!)^2}\left[\int_0^{\infty}\gamma_W^l e^{-\left(\frac{1}{\bar{\gamma}_M}+b\right)\gamma_W}d\gamma_W-\int_0^{\infty}\gamma_W^l e^{-\left(\frac{y}{\bar{\gamma}_M}+b\right)}d\gamma_W\right] \\
&= a\sum_{l=0}^{\infty}\frac{(bK)^l}{(l!)^2}\left[\frac{\bar{\gamma}_M^{l+1}l!}{(b\bar{\gamma}_M+1)^{l+1}}-\frac{\bar{\gamma}_M^{l+1}l!}{(b\bar{\gamma}_M+2^{R_S})^{l+1}}e^{-\frac{2^{R_S}-1}{\bar{\gamma}_M}}\right] \\
&= a\sum_{l=0}^{\infty}\frac{(bK)^l\bar{\gamma}_M^{l+1}}{l!}\left[\frac{1}{(b\bar{\gamma}_M+1)^{l+1}}-\frac{e^{-\frac{2^{R_S}-1}{\bar{\gamma}_M}}}{(b\bar{\gamma}_M+2^{R_S})^{l+1}}\right] \qquad (21)
\end{aligned}
$$

$$
\begin{aligned}
P'(C_S>0) &= \int_0^{\infty}\int_0^{\gamma_M}pe^{-q\gamma_M}I_0\left(2\sqrt{qK\gamma_M}\right)\frac{1}{\bar{\gamma}_W}e^{-\frac{\gamma_W}{\bar{\gamma}_W}}d\gamma_M d\gamma_W \\
&= p\sum_{l=0}^{\infty}\frac{(4qK)^l}{2^{2l}(l!)^2}\int_0^{\infty}\gamma_M^l e^{-q\gamma_M}\left[1-e^{-\frac{\gamma_M}{\bar{\gamma}_W}}\right]d\gamma_M \\
&= p\sum_{l=0}^{\infty}\frac{(qK)^l}{(l!)^2}\left[\frac{1}{q^{l+1}}-\left(\frac{\bar{\gamma}_W}{q\bar{\gamma}_W+1}\right)^{l+1}\right]\Gamma(l+1) \\
&= p\sum_{l=0}^{\infty}\frac{(qK)^l}{l!}\left[\frac{1}{q^{l+1}}-\left(\frac{\bar{\gamma}_W}{q\bar{\gamma}_W+1}\right)^{l+1}\right] \qquad (22)
\end{aligned}
$$

$$
\begin{aligned}
\Phi_1' &= \int_0^{\infty}\int_{\gamma_W}^{y}pe^{-q\gamma_M}I_0\left(2\sqrt{qK\gamma_M}\right)\frac{1}{\bar{\gamma}_W}e^{-\frac{\gamma_W}{\bar{\gamma}_W}}d\gamma_M d\gamma_W \\
&= \frac{p}{\bar{\gamma}_W}\sum_{l=0}^{\infty}\frac{(4qK)^l}{2^{2l}(l!)^2}\int_0^{\infty}e^{-\frac{\gamma_W}{\bar{\gamma}_W}}\int_{\gamma_W}^{y}\gamma_M^l e^{-q\gamma_M}d\gamma_M d\gamma_W \\
&= \frac{p}{q\bar{\gamma}_W}\sum_{l=0}^{\infty}\frac{K^l}{(l!)^2}\int_0^{\infty}e^{-\frac{\gamma_W}{\bar{\gamma}_W}}\left[\gamma\left(l+1,qy\right)-\gamma\left(l+1,q\gamma_W\right)\right]d\gamma_W \\
&= \frac{p}{q\bar{\gamma}_W}\sum_{l=0}^{\infty}\frac{K^l}{l!}\left[\sum_{n=0}^{l}\frac{q^n}{n!}\int_0^{\infty}\gamma_W^n e^{-\left(\frac{1}{\bar{\gamma}_W}+q\right)\gamma_W}d\gamma_W-\sum_{m=0}^{l}\frac{q^m}{m!}\int_0^{\infty}y^m e^{-\left(\frac{\gamma_W}{\bar{\gamma}_W}+qy\right)}d\gamma_W\right] \\
&= p\sum_{l=0}^{\infty}\sum_{n=0}^{l}\frac{K^l q^{n-1}\bar{\gamma}_W^n}{l!(1+q\bar{\gamma}_W)^{n+1}}-\frac{pe^{\frac{2^{R_S}-1}{2^{R_S}\bar{\gamma}_W}}}{2^{R_S}\bar{\gamma}_W}\sum_{l=0}^{\infty}\sum_{m=0}^{l}\frac{K^l q^{m-1}}{m!l!}\left(\frac{2^{R_S}\bar{\gamma}_W}{1+2^{R_S}q\bar{\gamma}_W}\right)^{m+1}\Gamma\left(m+1,r\right) \qquad (23)
\end{aligned}
$$
