Outage Secrecy Capacity Over Correlated Fading Channels at High SNR

Jinxiao Zhu, Osamu Takahashi, Xiaohong Jiang, Yoshitaka Nakamura and Yoh Shiraishi

School of Systems Information Science, Future University Hakodate
116-2, Kameda Nakano-Cho, Hakodate, Hokkaido, 041-8655, Japan
JinxiaoZhu.FUN@gmail.com
{Osamu, jiang, y-nakamr, siraisi}@fun.ac.jp

ABSTRACT

We investigate the outage probability and outage secrecy capacity of ergodic fading wiretap channel when the main and eavesdropper channels are correlated there. Under the assumption that before transmitting the transmitter knows the statistical properties of main and eavesdropper channels but it has no idea about the actual channel side information (CSI) of both channels, we derive the lower-bound of outage probability and also the upper-bound of outage secrecy capacity in the high signal-to-noise ratio (SNR) regime, which cover the corresponding results when the main channel and eavesdropper channel are independent as special cases. Remarkably, our results reveal that the correlation between main and eavesdropper channels has a significant impact on both outage probability and outage secrecy capacity and such impact can be helpful or harmful depending on the relative channel condition between the main and eavesdropper channels.

Keywords: Outage secrecy capacity, outage probability, fading wiretap channel, information-theoretic security, channel side information.

1 INTRODUCTION

The broadcast nature of wireless transmission makes the information security an increasingly important issue in wireless networks. Secrecy capacity of wireless channels, defined as the maximum information rate of the main channel (i.e., the transmitter-to-legitimate receiver channel) with the total ignorance at the eavesdropper [1], has been a central concept in information theoretic security used to understand the communication capacity of secrecy-constrained wireless networks.

The secrecy capacity of wireless channels has been studied under various channel models. For discrete and memoryless wiretap channel, the tradeoff between the main channel information rate and the ignorance about this information at the eavesdropper was explored in [2]. For Gaussian wiretap channel, it was showed in [1] that the secrecy capacity there is actually determined as the difference between the capacities of the main and eavesdropper channels. For broadcast wiretap channel, it was proved that the secrecy capacity can be always positive when the main channel is less noisy [3]. For multiple access wiretap channel, the inner and outer bounds on the capacity-equivocation region were derived in [4].

It is widely accepted that the fading channel model is of great importance in the study of wireless channel because of the natural fading phenomena in real wireless communication environment [5]. The secrecy capacity of fading wiretap channel was recently explored in [6], [7], [8], [9]. For delay-tolerant applications, the secrecy capacity was derived in [6], [7]. For delay sensitive applications, the secrecy capacity was characterized in [8], [9]. In particular, [6] characterized the ergodic secrecy capacity of fading channels and identified the optimal power allocation and transmission strategy in which messages are transmitted opportunistically when the main channel has a better instantaneous channel gain than that of the eavesdropper channel. For fading broadcast channel, the secrecy capacity has been further investigated in [7].

It is notable that above results on secrecy capacity of fading channels were developed under the assumption that the main channel and eavesdropper channel are independent, so the possible correlation among these channels was neglected in these work. In real wireless communication scenarios, however, correlations between channels are frequently observed in radio transmission environment [10], [11]. Recently, the upper bound of secrecy capacity was investigated over the correlated fading wiretap channel under the assumption that the transmitter knows the full channel side information (CSI) of both the main and eavesdropper channels [12]. Notice that wireless channels are always fluctuating and it is very difficult (if not impossible) to acquire the real time CSI of channels, the full CSI assumption is not really realistic with the current technologies. For the more realistic scenarios that the transmitter has no CSI of both the main and eavesdropper channels, a better performance measure is the outage secrecy capacity, which is defined as the maximum instantaneous mutual information rate that can be maintained such that a specified outage probability is satisfied. Also, for delay sensitive applications, where we need to ensure a high data rate by allowing a certain probability of outage, the outage secrecy capacity is of more interest [8], [9]. To the best of our knowledge, however, no work is available on the outage secrecy capacity study under the more realistic correlated fading wiretap channel.

Motivated by above observation, this paper explores the outage secrecy capacity over the correlated ergodic fading wiretap channel with no CSI at the transmitter. Our main contributions are summarized as follows: (a) an information-theoretic formulation of the secure communication problem over wireless fading channels at one realization of coherence interval in the high SNR regime; (b) a characterization of the outage probability and outage secrecy capacity for the corre-

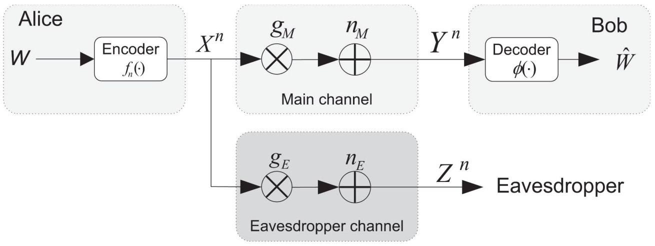

Figure 1: System model

lated wiretap channel, which cover the independent channel scenario [8] as a special case; (c) an analysis about the impact of the correlation on the outage probability and outage secrecy capacity, and an analysis about the relation between the outage probability and outage secrecy capacity.

The remainder of this paper is organized as follows. In Section 2, the system model is formally stated. Then section 3 analyzes the outage probability and outage secrecy capacity over correlated ergoidc fading channels. In Section 4, the implications of the above results are discussed. Finally, we conclude the paper in Section 5.

2 SYSTEM MODEL

Consider the system model illustrated in Fig. 1. A legitimate user, named Alice, wants to send messages to another user, named Bob, while the eavesdropper attempts to eavesdrop the messages. Both the main channel, the channel from Alice to Bob, and the eavesdropper channel, the channel from Alice to eavesdropper, are assumed to experience ergodic block fading, where the channel gains remain constants during each coherence interval and change independently from one coherence interval to the next. The fading process is assumed to be ergodic with a bounded continuous distribution. Moreover, the fading coefficients of the main channel and the eavesdropper channel in any coherence interval are assumed to have correlation between them.

The received signals at the Bob and eavesdropper, respectively, are given by

$$y(i) = g_M(i)x(i) + n_M(i)$$
$$z(i) = g_E(i)x(i) + n_E(i), i = 1, 2, ..., n$$

where n is the length of the transmitted signal, $g_M(i)$ and $g_E(i)$ denote the channel gains of the main and eavesdropper channels respectively, and $n_M(i)$ and $n_E(i)$ represent the independent and identically distributed (i.i.d.) Gaussian noise with zero mean and unit variance at the legitimate receiver and eavesdropper respectively. The fading channel power gains of the main and the eavesdropper channels are denoted by $h_M(i) = |g_M(i)|^2$ and $h_E(i) = |g_E(i)|^2$, which are constants during one coherence interval (e.g. $h_M(i) = h_M$ and $h_E(i) = h_E$).

Based on the random coding argument introduced in [12], we assume that Alice encodes a message block, represented by random variable (RV) $W \in \mathcal{W} = \{1, \dots, M\}$, into a codeword, represented by RV $x^n = \{x(1), x(2), \dots, x(n)\} \in \mathcal{X}^n$, by using a stochastic encoder $f_n(\cdot) : \mathcal{W} \to \mathcal{X}^n$. The entropy $H(W)$ is the amount of information of this transmitted message W. Bob then decodes the received signals $y^n = \{y(1), y(2), \dots, y(n)\} \in \mathcal{Y}^n$ by using a decoder $\phi(\cdot) : \mathcal{Y}^n \to \mathcal{W}$. The message estimated by Bob is denoted by $\hat{w} = \phi(y^n)$.

In this setup, the transmission rate from Alice to Bob is given by $R = H(W)/n$ and the average error probability is defined as

$$P_e^n = \frac{1}{M} \sum_{w \in \mathcal{W}} Pr(\hat{w} \neq w | w\ is\ sent),$$

where w is an instance of the random variable W.

The measure for eavesdropper's uncertainty about w, which is called the equivocation rate, is defined as

$$R_e = \frac{1}{n} H(W|Z^n),$$

where $H(W|Z^n)$ is the remaining entropy of W given that the value of Z^n is known.

We say that the rate R_s is achievable with weak secrecy if there exists a $(2^{nR_s}, n)$ code for a sufficient large n such that $R_e \geq R_s - \epsilon$ and $P_e^n \leq \epsilon$ for any given $\epsilon > 0$ [13]. The secrecy capacity is then the supremum of achievable transmission rates with weak secrecy, i.e.,

$$C_s \triangleq \sup\{R_s : R_s \text{ is achievable with weak secrecy}\}.$$

Throughout this paper, we assume that before transmitting the transmitter has no idea about the CSI of the main channel and eavesdropper channel. However, the statistic properties of both the main and eavesdropper channels are assumed to be available to the transmitter.

3 OUTAGE SECRECY CAPACITY OVER CORRELATED FADING CHANNELS

This section characterizes the outage probability and outage secrecy capacity when the main channel is correlated with the eavesdropper channel. We first establish the secrecy capacity in a single realization of the fading coefficients, and then derive the secrecy capacity in the high SNR regime. Finally, we characterize the outage probability and outage secrecy capacity based on the above results.

3.1 Preliminaries

We begin with the secrecy capacity for one realization of a pair of ergodic fading channels at a coherence interval. Assume that the transmitting power is restricted to P. As stated in [14], it is reasonable to view the main channel in this scenario as a complex additive white gaussian noise (AWGN) channel with SNR Ph_M and capacity

$$C_M = \log(1 + Ph_M). \tag{1}$$

Similarly, the eavesdropper channel is a complex AWGN channel with SNR Ph_E and capacity

$$C_E = \log(1 + Ph_E). \tag{2}$$

It is known that the secrecy capacity is just the difference between the main channel and eavesdropper channel when both the main and eavesdropper channels are complex AWGN channels [14]. Thus, we can derive the secrecy capacity for one realization of the fading scenario as

$$C_s = \begin{cases} \log(1+Ph_M) - \log(1+Ph_E), & \text{if } h_M > h_E; \\ 0, & \text{if } h_M \leq h_E. \end{cases} \tag{3}$$

3.2 High SNR Regime

It is easy to deduce from (1) that the channel capacity without secrecy constraint grows nearly logarithmically with the SNR. However, the secrecy capacity shows a different behavior as the SNR increases.

From (3), when the main channel gain is better than the eavesdropper channel gain (e.g. $h_M > h_E$), the secrecy capacity of a complex AWGN channel is given by

$$\begin{aligned} C_s &= \log(1+Ph_M) - \log(1+Ph_E) \\ &= \log(\frac{\frac{1}{P}+h_M}{\frac{1}{P}+h_E}) \\ &\overset{(a)}{\leq} \log(\frac{h_M}{h_E}) \triangleq C_s^{lim}, \end{aligned} \tag{4}$$

where the equality in (a) holds if P goes to infinity (i.e., high SNR), and the asymptotic secrecy capacity is denoted as C_s^{lim}. Thus, the asymptotic secrecy capacity is controlled by the channel gain ratio.

3.3 Outage Probability and Outage Secrecy Capacity

Since the transmitter has no idea about the CSI of both the main channel and eavesdropper channel, it is a good choice for the transmitter to set up a constant information transmission rate based on the statistical properties of the channels. We say outage happens when the instantaneous secrecy capacity is less than a target secrecy rate $R_s > 0$. Thus, the outage probability is defined as

$$\mathcal{P}_{out}(R_s) = \mathcal{P}(C_s < R_s). \tag{5}$$

The operational significance of this definition of outage probability can be found in [14].

Adopting the same notations as that in [12], we use H_M and H_E to denote the random variables of the fading power gains for the main and eavesdropper channel and let $U = H_M/H_E$. The average Channel power Gain Ratio (CGR) is denoted as $\kappa = \mathbb{E}[H_M]/\mathbb{E}[H_E]$, and the channel Power Correlation Coefficient (PCC) between H_M and H_E is denoted by ρ. Under the Rayleigh fading assumption, the probability density function (pdf) of the correlated channel power gain ratio U is derived as [12]

$$f_U(u) = \kappa \frac{(1-\rho)(u+\kappa)}{[(u+\kappa)^2 - 4\rho\kappa u]^{3/2}}, u \geq 0. \tag{6}$$

Lemma 1: If the main channel is correlated with the eavesdropper channel, and the joint pdf of them follows the bivariate Rayleigh distribution, as the SNR increases, the probability that the instantaneous secrecy capacity is larger than τ ($\tau \geq 0$) is upper bounded by

$$\mathcal{P}(C_s^{lim} > \tau) = \frac{1}{2} - \frac{2^\tau - \kappa}{2\sqrt{(2^\tau+\kappa)^2 - 4\rho\kappa 2^\tau}}. \tag{7}$$

Proof:

$$\begin{aligned} \mathcal{P}(C_s^{lim} > \tau) &= \mathcal{P}(\log(\frac{h_M}{h_E}) > \tau) = \mathcal{P}(\log u > \tau) \\ &= \int_{2^\tau}^{\infty} f_U(u) du \\ &= \left[\frac{u-\kappa}{2\sqrt{(u+\kappa)^2 - 4\rho\kappa u}}\right]_{2^\tau}^{\infty} \\ &= \frac{1}{2} - \frac{2^\tau - \kappa}{2\sqrt{(2^\tau+\kappa)^2 - 4\rho\kappa 2^\tau}} \end{aligned}$$

□

Remarks: When the main channel and eavesdropper channel are not correlated, that is $\rho = 0$, the probability that the instantaneous secrecy capacity is larger than τ ($\tau \geq 0$) is upper bounded by

$$\mathcal{P}(C_s^{lim} > \tau) = \frac{\kappa}{2^\tau + \kappa},$$

which is corresponding to the upper bound of the similar probability in [14] when the main channel SNR goes to infinity.

Notice that outage secrecy capacity is the maximum secrecy rate that can be maintained under any fading condition such that the outage probability is less than a predefined value ϵ [8], [15], i.e.,

$$C_{out}(\epsilon) \triangleq \max_{\mathcal{P}_{out}(R_s) \leq \epsilon} (R_s). \tag{8}$$

In other words, if the target transmission rate is R_s, and the maximum secrecy outage probability corresponding to R_s is ϵ, then R_s is called the ϵ-outage secrecy capacity.

Since the upper bound of the probability that the instantaneous secrecy capacity is larger than a predefined value is derived in Lemma 1, we can obtain a lower bound of the outage probability $\mathcal{P}_{out}$ for a target secrecy rate R_s and thus corresponding upper bound of the outage secrecy capacity in a closed-form, as summarized in Theorem 1.

Theorem 1: If the main channel is correlated with the eavesdropper channel and the joint pdf of them follows the bivariate Rayleigh distribution, as the SNR increases, the outage probability for a target secrecy rate R_s is lower bounded by

$$\begin{aligned} \mathcal{P}_{out}(R_s) &= \mathcal{P}(C_s^{lim} \leqslant R_s) \\ &= \frac{1}{2} + \frac{2^{R_s} - \kappa}{2\sqrt{(2^{R_s}+\kappa)^2 - 4\rho\kappa 2^{R_s}}}; \end{aligned} \tag{9}$$

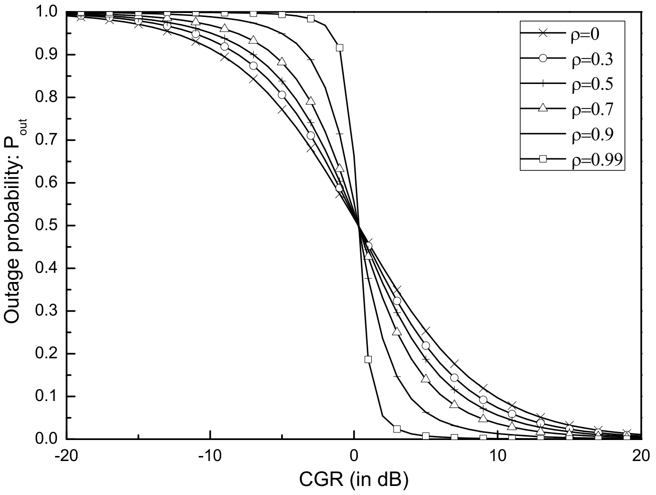

Figure 2: Outage probability versus CGR, for selected values of PCC and for a target secrecy rate equals to 0.1 bits.

and the outage secrecy capacity is upper bounded by

$$C_{out}(\epsilon) = \begin{cases} \left[\log\left(-\kappa\left(\sqrt{\varphi^2-1}+\varphi\right)\right)\right]^+, & \text{if } 0 < \epsilon \leq \frac{1}{2}; \\ \left[\log\left(\kappa\left(\sqrt{\varphi^2-1}-\varphi\right)\right)\right]^+, & \text{if } \frac{1}{2} < \epsilon < 1. \end{cases} \tag{10}$$

where $\varphi = \frac{(2\epsilon-1)^2(1-2\rho)+1}{(2\epsilon-1)^2-1}$, $[x]^+ = max\{0, x\}$ and ϵ is a specified outage probability.

Proof:

$$\begin{aligned} \mathcal{P}_{out}(R_s) &= \mathcal{P}(C_s^{lim} \leqslant R_s) \\ &= 1 - \mathcal{P}(C_s^{lim} > R_s). \end{aligned}$$

Thus, the equation (9) can be proved. Then, from (8) and (9), the equation (10) can be proved by simple mathematical inversion operations. □

Remarks:

1) From (9), when $R_s \to 0$ and $\rho \to 0$, it follows that ,

$$\mathcal{P}_{out} \to \frac{1}{1+\kappa},$$

which corresponds to the uncorrelated channel case in [8].

2) When the main channel and eavesdropper channel are completely correlated, i.e., $\rho \to 1$, the outage probability for a target secrecy rate R_s becomes

$$\lim_{\rho\to 1} \mathcal{P}_{out}(R_s) = \begin{cases} 0, & \text{if } R_s < \log\kappa; \\ 1, & \text{if } R_s \geq \log\kappa. \end{cases} \tag{11}$$

On one hand, (11) shows that outage must happen when the target secrecy rate R_s is greater than the secrecy capacity at the average channel power gain ratio. On the other hand, if the main channel and eavesdropper channel are totally correlated, the information outage can be avoided by choosing a target secrecy rate R_s less than the secrecy capacity at the average channel power gain ratio.

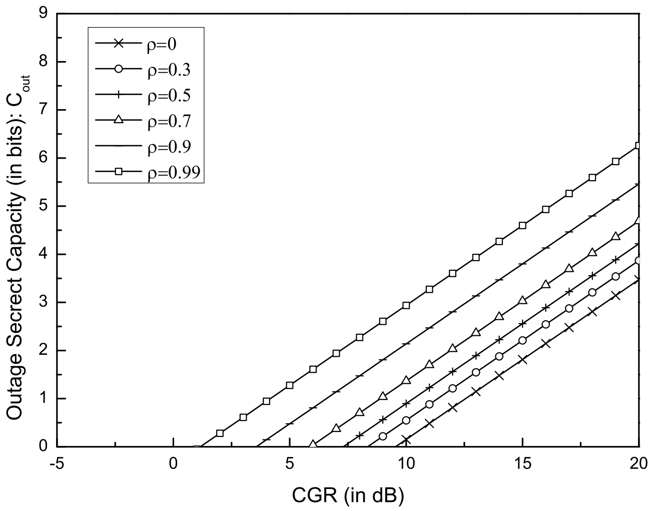

Figure 3: The asymptotic outage secrecy capacity versus CGR, for selected values of PCC and for an outage probability of 0.1.

3) Regardless of the correlation coefficient, the outage probability goes to 0 if the target secrecy rate is far below the secrecy capacity at the average channel power gain ratio (e.g., $R_s \ll \log\kappa$), and goes to 1 if the target secrecy rate is far above the secrecy capacity at the average channel power gain ratio (e.g., $R_s \gg \log\kappa$).

4 NUMERICAL RESULTS AND DISCUSSION

4.1 Impact of Correlation on Outage Probability

From Theorem 1, it follows that when the target secrecy rate R_s is less than the asymptotic secrecy capacity at CGR κ (e.g., $R_s < \log\kappa$), the outage probability is less than $1/2$. When the target secrecy rate R_s is greater than the asymptotic secrecy capacity at CGR κ (e.g., $R_s > \log\kappa$), we can still transmit secret message albeit with outage probability greater than $1/2$. It means that when the main channel is better than the eavesdropper channel (that is $\kappa > 1$), we can achieve a positive outage secrecy capacity with outage probability less than $1/2$.

To examine the impact of CGR and PCC on the outage probability, Fig. 2 depicts the outage probability versus CGR, for selected values of PCC and for a target secrecy rate equals to 0.1 bits. Observe that the higher CGR, the lower the outage probability. Moreover, if the asymptotic secrecy capacity at CGR is greater than 0.1 bits, then the outage probability is less than $1/2$. It is also important to observe that the impact of correlation on outage probability has different behaviors in the low and high CGR regimes. In the low CGR regime, the correlation significantly increases the outage probability. However, in the high CGR regime, the outage probability is decreased as the correlation increases, which implies that the correlation becomes helpful when the main channel is better

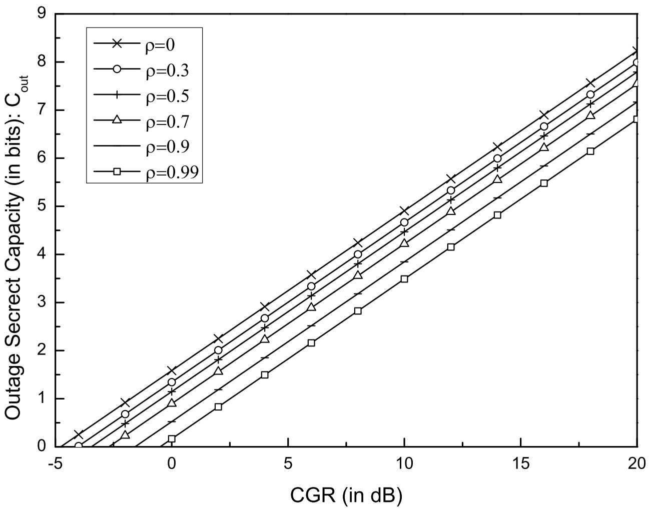

Figure 4: The asymptotic outage secrecy capacity versus C-GR, for selected values of PCC and for an outage probability of 0.75.

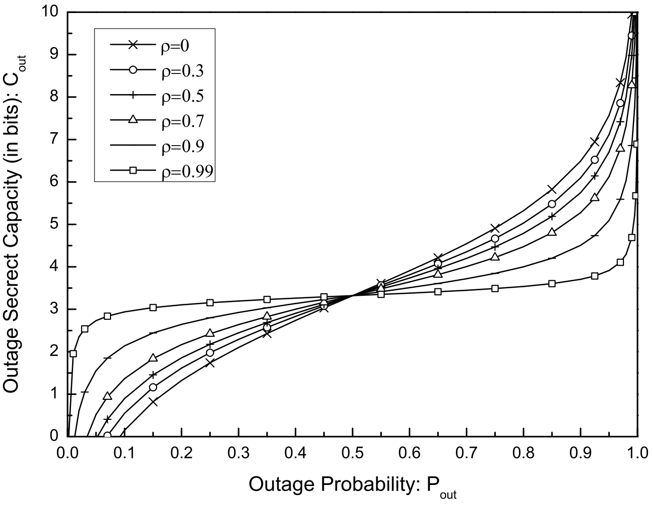

Figure 5: The asymptotic outage secrecy capacity versus outage probability, for selected values of PCC and for the scenario when the main channel's condition is better than the eavesdropper's ($\kappa = 10dB$).

than the eavesdropper channel. In the real situation, when the transmission rate is less than the secrecy capacity at CGR (or in the high CGR), we should improve the correlation between the main channel and eavesdropper channel as much as possible in order to reduce the outage probability.

4.2 Impact of Correlation on Outage Secrecy Capacity

Next, we investigate the impact of the correlation on the outage secrecy capacity at the low and the high outage probabilities respectively. Fig. 3 and Fig. 4 depict the asymptotic outage secrecy capacity versus CGR, for selected values of PCC and for the case that outage probability is less than $1/2$ (0.1 here) and also for the case that outage probability is larger than than $1/2$ (0.75 here), respectively. We can see that the asymptotic outage secrecy capacity grows as the CGR increases for different outage probability requirements there. For the same CGR and the same PCC, it is also noticed that the asymptotic outage secrecy capacity grows as the outage probability increases. Furthermore, the asymptotic outage secrecy capacity grows as the PCC increases when the outage probability is less than $1/2$, while it degrades as the PCC increases when the outage probability is greater than $1/2$, which indicates that the correlation becomes helpful when the main channel is better than the eavesdropper channel and harmful when the main channel is worse than the eavesdropper chan-

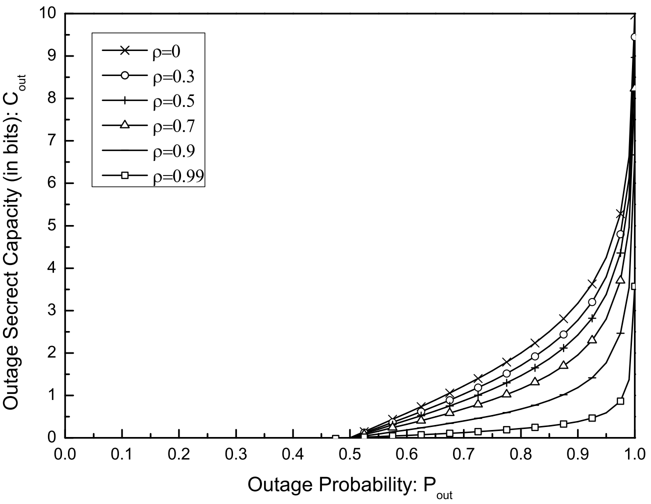

Figure 6: The asymptotic outage secrecy capacity versus outage probability, for selected values of PCC and for the scenario when the main channel's condition is the same as eavesdropper's ($\kappa = 0dB$).

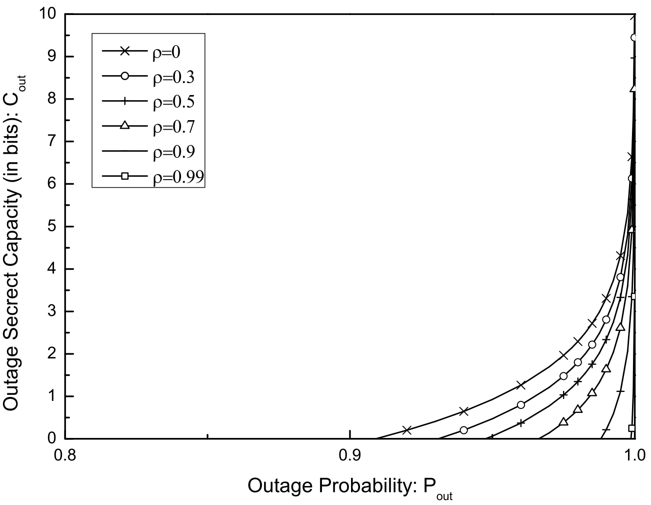

Figure 7: The asymptotic outage secrecy capacity versus outage probability, for selected values of PCC and for the scenario when the main channel's condition is worse than the eavesdropper's ($\kappa = -10dB$).

nel.

4.3 Outage Probability vs. Outage Secrecy Capacity

In this subsection, we examine the relation between the outage probability and outage secrecy capacity under the following three cases: 1) the main channel's condition is better than the eavesdropper's; 2) the main channel's condition is the same as the eavesdropper's; 3) the main channel's condition is worse than the eavesdropper's.

Figs. 5, 6 and 7 show the asymptotic outage secrecy capacity versus outage probability for selected values of PCC and for three scenarios that the main channel's condition is better than the eavesdropper's ($\kappa = 10dB$), the main channel's condition is the same as the eavesdropper's ($\kappa = 0dB$) and the main channel's condition is worse than the eavesdropper's ($\kappa = -10dB$). In Fig. 6, it is noticed that the outage secrecy capacity is 0 when the outage probability is less than 0.5. In Fig. 7, it is also noticed that the outage secrecy capacity is 0 when the outage probability is less than 0.9. The results in Figs. 5, 6 and 7 show that for a given outage probability the outage secrecy capacity at $\kappa = 10dB$ is the largest in comparison with the other two cases, which implicates that the main channel's condition should be maintained as good as possible to ensure a high outage secrecy capacity. Moreover, if the main channel is no better than the eavesdropper channel, we are still able to achieve a positive outage secrecy capacity albeit with outage probability greater than $1/2$. For the same channel conditions, we also find that the correlation between the main and eavesdropper channel is constructive when the outage probability is less than $1/2$, and becomes destructive when the outage probability is greater than $1/2$. It is also observed that we can enlarge the outage secrecy capacity by allowing a large outage probability.

5 CONCLUSION

In this paper, we derived the closed-form upper bound of outage secrecy capacity and also the lower bound of outage probability under correlated fading wiretap channel, which cover the corresponding results when the main channel and eavesdropper channel are independent as special cases. We then analyzed the impact of correlation on the outage probability and outage secrecy capacity, and observed that the outage probability decreases as the channel correlation increases in the high CGR regime, and the outage secrecy capacity grows as the the channel correlation increases when the outage probability is less than $1/2$. We also analyzed the tradeoff between the outage probability and outage secrecy capacity. Remarkably, our results reveal that the correlation between the main and eavesdropper channels is helpful when the main channel is better than the eavesdropper channel, and becomes harmful when the main channel is worse than the eavesdropper channel.

In this work, we have assumed that the transmitter has no CSI of both the main channel and the eavesdropper channel. But in some modern communication schemes, the estimated CSI of the main channel is available at the transmitter. So we plan to analyze this case as a future work.

REFERENCES

[1] S. Leung-Yan-Cheong, and M. E. Hellman, The Gaussian Wire-tap Channel, IEEE Trans. Inf. Theory, Vol. 24, No. 4, pp. 451–456 (1978).

[2] A. D. Wyner, The Wire-tap Channel, Bell Sys. Tech. J., Vol. 54, No. 8, pp. 1355–1367 (1975).

[3] I. Csiszar, and J. Korner, Broadcast Channels with Confidential Messages, IEEE Trans. Inf. Theory, Vol. 24, No. 3, pp. 339–348 (1978).

[4] Y. Liang, and H. V. Poor, and S. Shamai, Multiple-access Channels with Confidential Messages, IEEE Trans. Inf. Theory, Vol. 54, No. 3, pp. 976–1002 (2008).

[5] B. Sklar, Rayleigh fading channels in mobile digital communication systems. I. Characterization, IEEE Communications Magazine, Vol. 35, No. 7, pp. 90–100 (1997).

[6] 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. 4687–4698 (2008).

[7] Y. Liang, H. V. Poor, and S. Shamai, Secure communication over fading channels, IEEE Trans. Inf. Theory, Vol. 54, No. 6, pp. 2470–2492 (2008).

[8] J. Barros, and M. R. D. Rodrigues, Secrecy Capacity of Wireless Channels, in IEEE Int. Symp. Information Theory, Seattle, WA, pp. 356–360 (2006).

[9] P. Parada, and R. Blahut, Secrecy Capacity of SIMO and Slow Fading Channels, in IEEE Int. Symp. Information Theory, Adelaide, SA, pp. 2152–2155 (2005).

[10] W. C.-Y. Lee, Effects on Correlation between Two Mobile Radio Base-station Antennas, IEEE Trans. Commun., Vol. 21, No. 11, pp. 1214–1224 (1973).

[11] S. B. Rhee, and G. I. Zysman, Results of Suburban Base Station Spatial Diversity Measurements in the UHF Band, IEEE Trans. Commun., Vol. 22, No. 10, pp. 1630–1636 (1974).

[12] H. Jeon, N. Kim, J. Choi, H. Lee, and J. Ha, Bounds on Secrecy Capacity Over Correlated Ergodic Fading Channels at High SNR, IEEE Trans. Inf. Theory, Vol. 57, No. 4, pp. 1975–1983 (2011).

[13] U. Maurer, and s. Wolf, Information-theoretic key agreement: From weak to strong secrecy for free, in Proc. EUROCRYPT 2000, Lecture Notes in Comput. Sci., Vol. 1807, pp. 351–368 (2000).

[14] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, Wireless Information-Theoretic Security, IEEE Trans. Inf. Theory, Vol. 54, No. 6, pp. 2515–2534 (2008).

[15] L. Li, N. Jindal and A. Goldsmith, Outage Capacities and Optimal Power Allocation for Fading Multiple-Access Channels, IEEE Trans. Inf. Theory, Vol. 51, No. 4, pp. 1326–1347 (2005).