Journal of Information Processing Vol.21 No.4 640–649 (Oct. 2013)

[DOI: 10.2197/ipsjjip.21.640]

Regular Paper

Effects of Channel Correlation on Outage Secrecy Capacity

Jinxiao Zhu[1,a)] Xiaohong Jiang[1,b)] Osamu Takahashi[1] Norio Shiratori[2]

Received: November 27, 2012, Accepted: June 14, 2013

Abstract: We consider the transmission of confidential data over a wireless quasi-static fading wiretap channel when the main and eavesdropper channels are correlated there. Under the assumption that before transmission the transmitter only knows the channel state information (CSI) of the main channel but has no idea about the CSI of the eavesdropper channel, we derive the asymptotic outage probability and also asymptotic outage secrecy capacity as the transmission power goes to infinity, which cover the corresponding results when the main and eavesdropper channels are independent as special cases. Based on the theoretical results, the effects of channel correlation on the asymptotic outage probability and asymptotic outage secrecy capacity are explored. Remarkably, our results reveal that the correlation between the main and eavesdropper channels has a significant impact on both the asymptotic outage probability and asymptotic outage secrecy capacity and that such an impact can be helpful or harmful depending on the relative channel condition between the main and eavesdropper channels.

Keywords: physical layer security, outage secrecy capacity, Rayleigh fading channel, channel state information, channel correlation

1. Introduction

As is well known, the broadcast nature of wireless medium makes information security one of the most important and difficult problems in wireless networks. Traditionally, information security is ensured by applying cryptographic methods (e.g., RSA and AES), which are implemented above the physical layer with the assumption that an error-free physical link has already been established. Recently, there has been a considerable attention on the fundamental ability of the physical layer to provide wireless communication security. This emerging paradigm is called physical layer security, which relies on channel coding techniques that exploit the inherent randomness of propagation channels to ensure the transmitted messages cannot be decoded by malicious eavesdroppers. Within this new security method, secrecy capacity is used to measure the maximum information transmission rate that can be achieved without information leakage.

The secrecy capacity of wireless networks has been studied under various channel models. Based on Shannon's notion of perfect secrecy [1], Wyner first proposed a wiretap channel, where the source node transmits a message to the destination node through a discrete memoryless channel and another malicious node called wire-tapper eavesdrops this message through another degraded version of the discrete memoryless channel, then studied the tradeoff between the information transmission rate and the achievable secrecy level of such channel model [2]. A natural extension of Wyner's problem to a Gaussian channel was provided by Cheong and Hellman, where the secrecy capacity is shown to be the difference between the capacities of the main and eavesdropper channels [3]. Csiszar and Korner then generalized Wyner's result to a broadcast channel, where the source node also has a common message for both receivers in addition to a confidential message for only one of them, and moreover, the eavesdropper channel is not a degraded version of the main channel there [4]. It is noticed that the results in the above early works showed that a positive secrecy capacity can be achieved if the intended receiver has a better channel than the eavesdropper. Recently, the secrecy capacity has also been studied under other channel models, such as fading channel, multiple access channel, multi-antenna channel, relay channel and cognitive interference channel [5], [6], [7], [8], [9], [10], [11], [12], [13], [14], [15], [16], [17], [18], [19].

It is notable that the fading channel model is able to capture the basic time-varying property of wireless channels, and hence understanding such a channel model is critical for solving security issues in wireless applications [20]. There are many intervals when the main channel's instantaneous channel gain is worse than the eavesdropper channel's because of the fading phenomenon. Thus, an interesting question is what is the performance of secure communication under the fading wiretap channel. The secrecy capacity of fading channels was recently explored [5], [6], [7], [8], [9], [10]. Specifically, Refs. [5] and [6] focused on the fading broadcast channels with only two receivers and multiple receivers, respectively. In Ref. [7], the authors extended Wyner's work to the case of the single-input multiple-outputs (SIMO) fading channel and showed that the use of multiple receive antennas provides an advantage with respect to a single-antenna one. Bloch et al. [9] studied the average secrecy capacity under the fading wiretap channel when the transmitter

[1] The School of Systems Information Science, Future University Hakodate, Hakodate, Hokkaido 041–8655, Japan

[2] GITS, Waseda University, Tokyo and RIEC, Tohoku University, Sendai, Japan

[a)] JinxiaoZhu.FUN@gmail.com

[b)] jiang@fun.ac.jp

knows the channel state information (CSI) of both the main and eavesdropper channels[*1], while [10] explored the ergodic secrecy capacity of a slow fading wiretap channel based on an optimal power allocation strategy, which is optimized based on the available amount of CSI. Remarkably, they showed that fading alone guarantees that information-theoretic security is achievable, even when the main channel has a worse average channel gain than the eavesdropper channel. However, all the above results were derived under the assumption of independent channels, thus the possible correlations among channels were neglected there.

In real radio communication scenarios, correlations between channels from a transmitter to different receivers have been frequently observed [21], [22], [23]. Such correlation levels depend on many factors in communication environments, such as the presence or absence of scatters around the transmitter and receivers, the clearance of the signal path, and the physical deployment of receiver antennas, etc. Moreover, it is possible that eavesdroppers intentionally induce the correlation, e.g., by approaching legitimate receivers. It is also known that channel correlations degrade the performance of multi antenna systems [24]. Although channel correlation is a very important factor determining the similarity of fading behaviors of different channels, there are only a few works that consider the effect of channel correlation on secrecy capacity.

Some works have been done on the secrecy capacity of correlated fading channels [11], [12]. The paper [11] explored the asymptotic ergodic secrecy capacity of correlated fading channels when the signal-to-noise ratio (SNR) is infinite, while the paper [12] studied the secrecy capacity over a correlated Rayleigh fading channel with limited SNR, under the assumption that the transmitter knows the full CSI (channel gains of both main and eavesdropper channels) before transmission. Notice that wireless channels are always fluctuating and it is very difficult (if not impossible) to acquire the real time CSI of channels. Thus the full CSI assumption is not really realistic with current technologies. For the more realistic scenarios where the transmitter only knows the CSI of the main channel, a better performance measure is the outage secrecy capacity, which is defined as the maximum information rate that can be maintained such that the maximum secrecy outage probability is no more than the specified value. 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 greater interest [7], [8], [9], [25]. 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 the above observations, this paper explores the outage secrecy capacity over the correlated fading wiretap channel without knowing the real time CSI of the eavesdropper channel. Our main contributions are summarized as follows: (a) We consider the general problem of confidential transmission under the scenario that the transmitter does not know the real time CSI of the eavesdropper channel and characterize the asymptotic outage probability and asymptotic outage secrecy capacity for the correlated fading wiretap channel as the transmission power goes to infinite, which cover the corresponding results under the independent channel scenario [8] as special cases and (b) We analyse the impact of the correlation on the asymptotic outage probability and asymptotic outage secrecy capacity, and reveal that channel correlation can be helpful in certain conditions, which is a very inspiring result and has never been exposed, as far as we know. We also investigate the tradeoff between the outage probability and outage secrecy capacity of the correlated fading channels.

The remainder of this paper is organized as follows. In Section 2, we formally describe the system model including the basic secure communication channel model and the correlated channel model. Then Section 3 analyzes the secrecy capacity of the correlated Rayleigh fading wiretap channel and derives the theoretic results of the asymptotic outage probability and asymptotic outage secrecy capacity. In Section 4, the implications of the above results are discussed, such as the impact of channel correlations on outage secrecy capacity. Finally, concluding remarks are given in Section 5.

2. System Model

We consider the wireless system setup illustrated in **Fig. 1**, where the legitimate user (Alice) sends confidential messages to another user (Bob) over a wireless fading channel, while an eavesdropper (Eve) eavesdrops the messages through another wireless fading channel. Alice encodes a message block, represented by random variable (RV) $W \in \mathcal{W}$, into a codeword, represented by RV $X^n \in \mathcal{X}^n$. The codeword X^n is then transmitted over the wireless channel. The signal received at Bob is denoted by RV $Y^n \in \mathcal{Y}^n$, while the signal received at Eve is denoted by RV $Z^n \in \mathcal{Z}^n$. The message estimated by Bob is denoted by $\hat{W} = \phi(Y^n)$. Here, $\mathcal{W}$, $\mathcal{X}$, $\mathcal{Y}$ and $\mathcal{Z}$ are the finite sets of source, the channel input alphabet, the channel output alphabet of main channel and the channel output alphabet of the eavesdropper channel, respectively. Moreover, the members of X^n will be written as $X^n = (X(1), X(2), \dots, X(n))$, and a similar convention applies to other vectors, like Y^n, Z^n, G^n_m, G^n_e, H^n_m, H^n_e, N^n_m, N^n_e.

The signal $Y(i)$ received by Bob and the signal $Z(i)$ received by Eve can be determined as

$$Y(i) = G_m(i)X(i) + N_m(i)$$
$$Z(i) = G_e(i)X(i) + N_e(i), i = 1, 2, ..., n$$

where n is the length of the transmitted signal, $G_m(i)$ and $G_e(i)$ denote the circularly symmetric complex Gaussian RVs with zero-mean representing 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

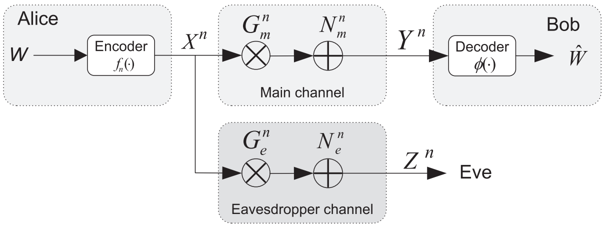


Fig. 1 System model.

[*1] For more details about CSI, please refer to Section 2.1.

zero mean and unit variance at the legitimate receiver and eavesdropper, respectively. The fading channel power gains of the main and eavesdropper channels are denoted by $H_m(i) = |G_m(i)|^2$ and $H_e(i) = |G_e(i)|^2$, respectively.

It is assumed that both the main channel (the channel from Alice to Bob) and the eavesdropper channel (the channel from Alice to Eve) are quasi-static fading channels. In other words, the fading coefficients, albeit random, are constant during the transmission of an entire codeword and independent from codeword to codeword. Moreover, the fading coefficients of the main and eavesdropper channels in any coherence interval are assumed to have correlation between them.

In this paper, a $(2^{nR_s}, n)$ code is adopted. A $(2^{nR_s}, n)$ code consists of the following elements: 1) a message set $\mathcal{W}$ whose cardinality is $|\mathcal{W}| = 2^{nR_s}$; 2) a stochastic encoder $f_n(\cdot)$ at Alice that maps message $W \in \mathcal{W}$ to codeword $X^n \in \mathcal{X}^n$; 3) a decoder $\phi(\cdot)$ at Bob that maps the received sequence $Y^n \in \mathcal{Y}^n$ to the message $\hat{W} \in \mathcal{W}$. The performance of the coding scheme will be quantified by the following measures. The average error probability is defined as

$$P_e = \Pr(\hat{W} \neq W). \tag{1}$$

This probability is used to measure the level of reliable communication between Alice and Bob. The measure for eavesdropper's uncertainty about w, which is called the equivocation rate, is defined as

$$R_{eq} = \frac{1}{n} H(W|Z^n), \tag{2}$$

where $H(W|Z^n)$ is the remaining entropy of W given that the value of Z^n is known. It indicates the secrecy level of confidential messages against the eavesdropper.

In this paper we consider only perfect secrecy which requires the equivocation rate R_{eq} to be as large as the secured information rate $R_s = H(W)/n$. The perfect secrecy rate R_s is said to be achievable if there exists a $(2^{nR_s}, n)$ code such that $R_{eq} \geq R_s - \epsilon$ and $P_e \leq \epsilon$ for any given $\epsilon > 0$. The secrecy capacity C_s is defined as the maximum achievable perfect secrecy rate [9], i.e.,

$$C_s \triangleq \sup_{P_e \leq \epsilon} R_s. \tag{3}$$

Notice that the condition for perfect secrecy used here (and also in Refs. [2], [9], [11]) is weaker than the one proposed by Maurer and Wolf in Ref. [26], where the information leaked to the eavesdropper is negligibly small not just in terms of rate but in absolute terms. Maurer and Wolf showed that the notions could be used interchangeably for discrete memoryless channels, but this result was then extended to the Gaussian case in Ref. [27].

2.1 Channel State Information

In wireless communication, channel state information (CSI) refers to channel properties of a communication link, including channel gain, fading distribution, noise strength, and spatial correlation, which can be used to describe how a signal propagates from the transmitter to the receiver. There are basically two levels of CSI, namely instantaneous CSI and statistical CSI. The instantaneous CSI means the current channel conditions are known, while the statistical CSI refers to a statistical characterization of the channel is known, which can be in turn determined if the instantaneous CSI is known. The instantaneous CSI makes it possible to adapt transmissions to the current channel conditions, which is crucial for reliable communication, while the statistical CSI has no such advantage. In this work, we focus on the CSI assumption that the instantaneous CSI (i.e., the real time channel gains in particular) of the eavesdropper channel cannot be achieved but the CSI of the main channel and the statistical CSI of eavesdropper channel are known. These assumptions are realistic for the quasi-static fading wireless environment under consideration: both receivers can always obtain close to perfect channel estimates, and Bob feeds back the channel estimates to Alice while Eve is a purely passive and malicious node who does not feed back any information to Alice [9]. In this work, the full CSI assumption means the CSIs of both the main and eavesdropper channels are known.

2.2 Correlated Channel Model

In this subsection, we emphasize how to calculate the correlation coefficient between the channels, for which the similar correlated channel model as in Ref. [11] is adopted. Since[*2] G_m and G_e are circularly symmetric complex Gaussian RVs, the joint distribution of their envelops becomes the bivariate Rayleigh distribution [28]. Such assumption is indeed suitable to the channel model of a narrow-band system under a rich scattering environment which produces multiple propagation waves, where the in-phase and quadrature components of G_m and G_e can be considered as Gaussian processes by the central limit theorem.

We denote the random variables G_m and G_e as $G_m = G_{mc} + jG_{ms}$ and $G_e = G_{ec} + jG_{es}$, respectively. For the spatial fading correlation between the main and eavesdropper channels, we consider the following situations:

- The in-phase component of G_m is spatially correlated with the in-phase component of G_e, while it is independent of quadrature components of G_m and G_e. In the same manner, the quadrature components of G_m and G_e are spatially correlated to each other.
- The level of spatial fading correlation between the in-phase components is identical to that between the quadrature components.

In this setting, we denote the correlation coefficient between G_m and G_e as $\rho_{G_mG_e}$, and we have

$$\rho_{G_mG_e} = \frac{\mathrm{cov}(G_{mc}, G_{ec})}{\sqrt{\mathrm{var}(G_{mc})\mathrm{var}(G_{ec})}} = \frac{\mathrm{cov}(G_{ms}, G_{es})}{\sqrt{\mathrm{var}(G_{ms})\mathrm{var}(G_{es})}}.$$

Denoting the correlation coefficient between the power gains H_m and H_e as ρ, we have

$$\rho = \frac{\mathrm{cov}(H_m, H_e)}{\sqrt{\mathrm{var}(H_m)\mathrm{var}(H_e)}},$$

and $0 \leq \rho < 1$ here [11]. ρ is also related to the channel correlation coefficient by $\rho = |\rho_{G_mG_e}|^2$. Moreover, simple and intuitive

[*2] For simplicity, we omit here the component identification in $G_m(i)$ and $G_e(i)$ and simply use G_m and G_e to denote the channel gains for the main and eavesdropper channels. A similar convention applies to the power gains $H_m(i)$ and $H_e(i)$.

geometrical interpretations of the fading statistics are suggested in Ref. [29] where the spatial fading correlation is effectively described by several spatial parameters: the angular spread, the angular constriction, and the azimuthal direction of maximum fading.

3. Outage Secrecy Capacity of Correlated Fading Channels

This section characterizes the asymptotic outage probability and corresponding asymptotic 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 asymptotic secrecy capacity as the transmission power goes to infinity. Finally, we characterize the asymptotic outage probability and asymptotic outage secrecy capacity based on the above results.

3.1 Preliminaries

We begin with the secrecy capacity for one realization of the fading channels at a coherence interval during which the channel gains are assumed to be constant. It is assumed that the transmission power is P. As stated in Ref. [9], it is reasonable to view the main channel in this scenario as a complex additive white gaussian noise (AWGN) channel with its SNR PH_m and capacity

$$C_m = \log(1 + PH_m). \tag{4}$$

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

$$C_e = \log(1 + PH_e). \tag{5}$$

It is known that the secrecy capacity of a complex AWGN wiretap channel is just the difference between the main and eavesdropper channels there [9]. Thus, the secrecy capacity for one realization of the fading coefficients is derived as

$$C_s = \begin{cases} \log(1 + PH_m) - \log(1 + PH_e), & \text{if } H_m > H_e; \\ 0, & \text{if } H_m \leq H_e. \end{cases} \tag{6}$$

3.2 High SNR Regime

It is easy to deduce from Eq. (4) 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 Eq. (6), when the main channel gain is better than the eavesdropper channel gain (e.g., $H_m > H_e$), the asymptotic secrecy capacity for one pair of channel gains is given by

$$\begin{aligned} C_s &= \log(1 + PH_m) - \log(1 + PH_e) \\ &= \log\left(\frac{\frac{1}{P} + H_m}{\frac{1}{P} + H_e}\right) \\ &\overset{(a)}{\leq} \log\left(\frac{H_m}{H_e}\right) \triangleq C_s^{lim}, \end{aligned} \tag{7}$$

where the equality in (a) holds as 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 power gain ratio.

3.3 Outage Probability and Outage Secrecy Capacity

We say outage happens when the instantaneous secrecy capacity[*3] is less than a target secrecy rate $R_{st} > 0$. Thus, the outage probability is defined as

$$\mathcal{P}_{out}(R_{st}) = \mathcal{P}(C_s < R_{st}). \tag{8}$$

The operational significance of this definition of outage probability is threefold. First, it provides the fraction of fading realizations for which a secrecy rate of R_{st} cannot be supported. Second, it provides a security metric for the situation where Alice is not sure about the real time CSI of eavesdropper channel, which is more realistic compared with the full CSI assumption. In this case, Alice has no choice but to set the secret transmission rate to a constant R_{st} based on the channel statistical properties. By doing so, Alice is assuming that the capacity of the eavesdropper channel is given by $C_e^{'} = C_m - R_{st}$. As long as $R_{st} < C_s$, the eavesdropper channel is worse than Alice's estimate, i.e., $C_e < C_e^{'}$, and the wiretap codes used by Alice can ensure perfect secrecy. Otherwise, if $R_{st} > C_s$, then $C_e > C_e^{'}$ and the physical layer security is compromised. Third, for a delay-sensitive application, we can achieve much higher communication rates by allowing some outage probability. If no outage is allowed, we can hardly transmit any information in poor channel conditions.

Adopting the same notations as that in Ref. [11], we 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 ρ. Under the Rayleigh fading assumption, the probability density function (PDF) of the channel power gain ratio U is derived as Ref. [11]

$$f_U(u) = \kappa \frac{(1-\rho)(u+\kappa)}{[(u+\kappa)^2 - 4\rho\kappa u]^{3/2}}, u \geq 0. \tag{9}$$

Thus, we have the following lemma.

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

$$\mathcal{P}\left(C_s^{lim} > \tau\right) = \frac{1}{2} - \frac{2^\tau - \kappa}{2\sqrt{(2^\tau + \kappa)^2 - 4\rho\kappa 2^\tau}}. \tag{10}$$

Proof.

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

□

[*3] The instantaneous secrecy capacity is used to denote the secrecy capacity determined by the instantaneous channel gains of both main and eavesdropper channels. This notation is also used in Ref. [9].

Remarks: When the main and eavesdropper channels 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

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

which is just the upper bound of the similar probability in Ref. [9] when the main channel SNR goes to infinity.

Notice that the outage secrecy capacity is the maximum secrecy rate that can be maintained under any fading condition during nonoutage such that the allowed average transmission outage probability is satisfied. In other words, if the target transmission rate is R_{st}, and the secrecy outage probability corresponding to R_{st} is ϵ, then R_{st} is called the ϵ-outage secrecy capacity, [8], [30], i.e.,

$$C_{out}(\epsilon) \triangleq \max_{\mathcal{P}_{out}(R_{st}) \leq \epsilon} (R_{st}). \tag{11}$$

Since the upper bound of the probability that the instantaneous secrecy capacity is larger than a specified value is derived in Lemma 1, we can obtain the lower bound of the outage probability for a target secrecy rate R_{st} and also the corresponding upper bound of the outage secrecy capacity in a closed-form, as summarized in Theorem 1. Notice that the bounds of the outage probability and outage secrecy capacity are denoted as $\mathcal{P}_{out}^{lim}(R_{st})$ and $C_{out}^{lim}(\epsilon)$, since they are derived based on the asymptotic secrecy capacity as the transmitting power P goes to infinity (i.e., high SNR).

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 transmission power P increases, the outage probability for a target secrecy rate R_{st} is lower bounded by

$$\begin{aligned}\mathcal{P}_{out}^{lim}(R_{st}) &= \mathcal{P}\left(C_s^{lim} \leqslant R_{st}\right)\\ &= \frac{1}{2} + \frac{2^{R_{st}} - \kappa}{2\sqrt{(2^{R_{st}} + \kappa)^2 - 4\rho\kappa 2^{R_{st}}}};\end{aligned} \tag{12}$$

and the outage secrecy capacity is upper bounded by

$$C_{out}^{lim}(\epsilon) = \begin{cases}\left[\log\left(-\kappa(\sqrt{\varphi^2 - 1} + \varphi)\right)\right]^+, & \text{if } 0 < \epsilon \leq \frac{1}{2};\\ \left[\log\left(\kappa(\sqrt{\varphi^2 - 1} - \varphi)\right)\right]^+, & \text{if } \frac{1}{2} < \epsilon < 1.\end{cases} \tag{13}$$

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

Proof.

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

By substituting Eq. (10) into the above equation, the result Eq. (12) then follows. Based on Eqs. (11) and (12), Eq. (13) can be proved by simple mathematical inversion operations, which is presented in Appendix A.1. □

Remarks:

1) From Eq. (12), when $R_{st} \to 0$ and $\rho \to 0$, it follows that,

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

which corresponds to the independent channel case in Ref. [8].

2) When the main and eavesdropper channels are completely correlated, i.e., $\rho \to 1$, the outage probability for a target secrecy rate R_{st} becomes

$$\lim_{\rho \to 1} \mathcal{P}_{out}^{lim}(R_{st}) = \begin{cases} 0, & \text{if } R_{st} < \log\kappa;\\ 1, & \text{if } R_{st} \geq \log\kappa.\end{cases} \tag{14}$$

On one hand, Eq. (14) shows that outage must happen when the target secrecy rate R_{st} is greater than the asymptotic secrecy capacity at the average channel power gain ratio (i.e., $R_{st} \geq \log\kappa$). On the other hand, if the main and eavesdropper channels are completely correlated, the information outage can be avoided by choosing a target secrecy rate R_{st} less than the asymptotic secrecy capacity at the average channel power gain ratio (i.e., $R_{st} < \log\kappa$).

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

About the impact of correlation on the asymptotic outage secrecy capacity, we have the following lemma.

Lemma 2: When $0 < \epsilon \leq \frac{1}{2}$, $C_{out}^{lim}(\epsilon)$ increases as the correlation coefficient ρ grows; when $\frac{1}{2} < \epsilon < 1$, it decreases as ρ grows.

Proof. First, since $\epsilon \in (0, 1)$ and $\rho \in [0, 1)$, it is easy to derive that $\varphi = \frac{(2\epsilon-1)^2(1-2\rho)+1}{(2\epsilon-1)^2-1}$ is monotonically increasing with respect to ρ and $\varphi < 0$. Second, let $f_1(\varphi) = -\kappa(\sqrt{\varphi^2 - 1} + \varphi)$ and $f_2(\varphi) = \kappa(\sqrt{\varphi^2 - 1} - \varphi)$. Then, the derivatives of them are given by

$$f_1^{'}(\varphi) = -\kappa\left(1 + \frac{\varphi}{\sqrt{\varphi^2 - 1}}\right) \tag{15}$$

and

$$f_2^{'}(\varphi) = \kappa\left(-1 + \frac{\varphi}{\sqrt{\varphi^2 - 1}}\right), \tag{16}$$

respectively. Since $\kappa > 0$ and $\varphi < 0$, we can find that $f_1^{'}(\varphi) > 0$, which indicates that $f_1(\varphi)$ monotonically increases with $\varphi < 0$, and $f_2^{'}(\varphi) < 0$, which indicates that $f_2(\varphi)$ monotonically decreases with $\varphi < 0$. Finally, combined with the fact that the logarithm does not change the monotonicity, the above lemma can be proved. □

4. Numerical Results and Discussion

Based on the theoretical models derived in this paper, this section provides some numerical values to explore the potential impact of channel correlation on the outage performances and also some inherent performance tradeoffs.

4.1 Impact of Correlation on Outage Probability

From Eq. (12), it is easy to find that when the target secrecy rate R_{st} is less than the asymptotic secrecy capacity at CGR κ

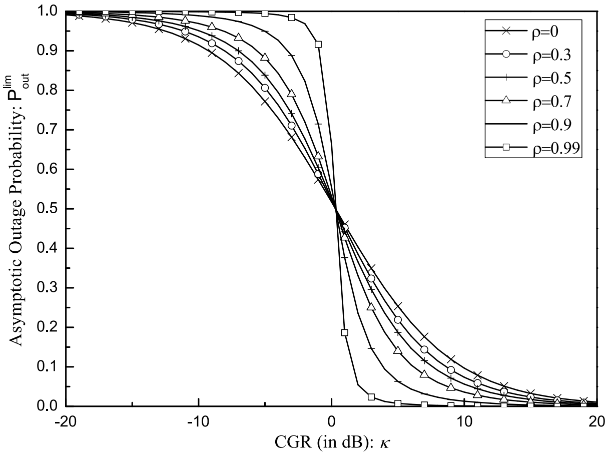


Fig. 2 Outage probability versus channel power gain ratio (CGR), for some selected values of channel power correlation coefficient (PCC) and for the target secrecy rate R_{st} equal to 0.1 bits.

(i.e., $R_{st} < \log\kappa$), the outage probability that can be achieved is less than 1/2. When the target secrecy rate R_{st} is greater than the asymptotic secrecy capacity at CGR κ (i.e., $R_{st} > \log\kappa$), we can still transmit a secret message but with outage probability greater than 1/2.

To examine the impact of CGR and PCC on the outage probability, **Fig. 2** depicts the asymptotic outage probability versus CGR, for some selected values of PCC and for the target secrecy rate R_{st} equal to 0.1 bits. It is noticed that the asymptotic outage probability decreases as the CGR grows, which is reasonable since the outage probability decreases as the main channel gets better. Moreover, if the asymptotic secrecy capacity at CGR $\log\kappa$ is larger than the target secrecy rate $R_{st} = 0.1$ bits (i.e., $\kappa > 0.3$ dB), then the asymptotic outage probability is less than 1/2; otherwise the outage probability becomes greater than 1/2. It is also important to observe that the impact of correlation on the asymptotic outage probability has different behaviors in the low and high CGR regimes. In the low CGR regime, the outage probability increases as the correlation grows. However, in the high CGR regime, the outage probability decreases as the correlation grows. Thus, the possible correlation should be considered to determine the target secrecy rate or the outage probability in real applications. Notice that channel correlation becomes helpful only when $\kappa > 0$ dB and $R_{st} < \log\kappa$ (i.e., $P_{out} < 1/2$). If the main channel's average gain is worse than the eavesdropper's (i.e., $\kappa < 0$ dB), a positive secrecy rate can still be achieved, though the corresponding outage probability will be over 1/2. The above phenomenon is reasonable since if $\kappa > 0$ dB, then the larger the correlation level, the higher the probability of having $H_m > H_e$.

4.2 Impact of Correlation on Outage Secrecy Capacity

Now, we investigate the impact of correlation on the outage secrecy capacity at the low and high outage probabilities, respectively[*4].

Figures 3 and **4** depict the asymptotic outage secrecy capacity versus CGR, for some selected values of PCC and for the case that the asymptotic outage probability is less than 1/2 (0.1 here) and the case that the asymptotic outage probability is larger than 1/2 (0.75 here), respectively. We can see that the asymptotic outage secrecy capacity grows as the CGR increases for both 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 increases as the PCC grows when the outage probability is less than 1/2, while it degrades as the PCC grows when the outage probability is greater than 1/2, which indicates that the correlation is helpful when $\epsilon < 1/2$ but becomes harmful when $\epsilon > 1/2$. Notice that the numerical results agree with the theoretical analysis in Lemma 2 well. The physical reason of such phenomenon is given as follows. Let U_{st} denote the target channel power gain ratio (i.e., $U_{st} = 2^{R_{st}}$). From Eq. (12), it is obvious that $U_{st} < \kappa$ when $\epsilon < 1/2$ and $U_{st} > \kappa$ when $\epsilon > 1/2$. As the PCC ρ grows, the power gain of the main channel H_m and that of the eavesdropper channel H_e vary much more similarly for any coherence interval, which indicates that the probability of having the real time channel power gain ratio $U = H_m/H_e$ close to the average one

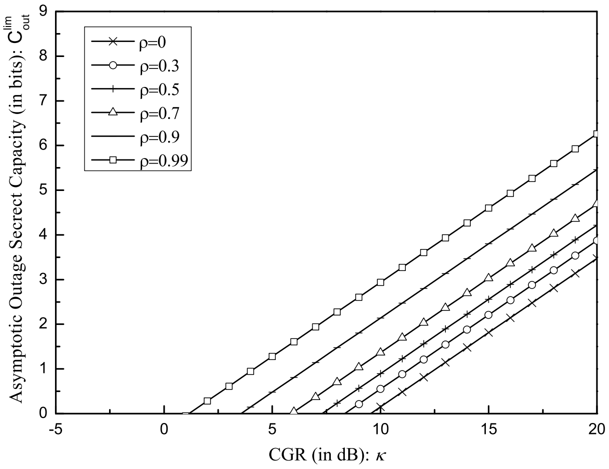


Fig. 3 The asymptotic outage secrecy capacity versus channel power gain ratio (CGR), for some selected values of channel power correlation coefficients (PCC) and for the outage probability equal to 0.1.

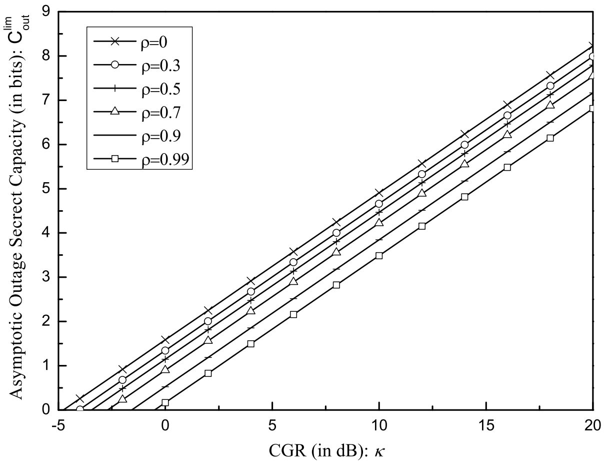


Fig. 4 The asymptotic outage secrecy capacity versus channel power gain ratio (CGR), for some selected values of channel power correlation coefficients (PCC) and for the outage probability equal to 0.75.

[*4] Although the high outage probability is not pursued in real applications, it is desirable for us to understand the impact of correlation under this scenario.

$\kappa = \mathbb{E}[H_m]/\mathbb{E}[H_e]$ increases (i.e., the variance of U decreases in statistics). Thus, the value of the target channel power gain ratio U_{st} for a specified ϵ increases as ρ grows when $U_{st} < \kappa$, and decreases as ρ grows when $U_{st} > \kappa$. Therefore, the target secrecy rate R_{st} and thus the asymptotic outage secrecy capacity increases as the PCC grows when $\epsilon < 1/2$, but decreases when $\epsilon > 1/2$.

4.3 Outage Probability vs. Outage Secrecy Capacity

In this subsection, we examine the relation between the asymptotic outage probability and asymptotic 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.

Figures 5, **6** and **7** show the asymptotic outage secrecy capacity versus outage probability for some selected values of PCC and for the three scenarios that the main channel's condition is better than the eavesdropper's ($\kappa = 10$ dB), the main channel's condition is the same as the eavesdropper's ($\kappa = 0$ dB) and the main channel's condition is worse than the eavesdropper's ($\kappa = -10$ dB). 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 positive outage secrecy capacity can be achieved even when the main channel's condition is much worse than the eavesdropper's, even though the outage probability is greater than 0.9. This is due to the reason that, although $\mathbb{E}[H_m] < \mathbb{E}[H_e]$ (i.e., $\kappa < 0$ dB), it is possible to have coherence intervals during which H_m is larger than H_e since both the main and eavesdropper channels are fading and not perfectly correlated there. From the three figures, we can find that for a given outage probability the asymptotic outage secrecy capacity at $\kappa = 10$ dB is the largest in comparison with the other two cases, which indicates that the main channel's condition should be maintained as good as possible. Moreover, one can observe from Fig. 5 that the correlation between the main and eavesdropper channels 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 the outage secrecy capacity can be enlarged by allowing a larger outage probability.

4.4 PCC vs. CGR

It is noticed from the above discussions that channel correlation becomes helpful when the target transmission rate is less than the asymptotic secrecy capacity at the CGR. So, it is desirable to make the PCC as high as possible while keeping the CGR high in a practical design of wireless communication. However, in real wireless networks, an active eavesdropper can not only increase the PCC but also decrease the CGR by approaching the legitimate receiver on purpose. Two natural questions are: What is the tradeoff between the CGR and PCC? Is it necessary to keep a guard zone, defined as the region around the receiver in which the eavesdroppers are not allowed?

Figures 8 and **9** show examples of the tradeoff between CGR and PCC for some selected target secrecy rates and for the cases that outage probability is less than 1/2 (0.1 here) and larger than 1/2 (0.75 here), respectively. It is observed that the CGR decreases as the PCC grows for the case when the outage probability is less than 1/2, while the CGR increases as the PCC grows for the case when the outage probability is greater than 1/2, which confirms our previous result that channel correlation becomes helpful if the target transmission rate is less than the asymptotic

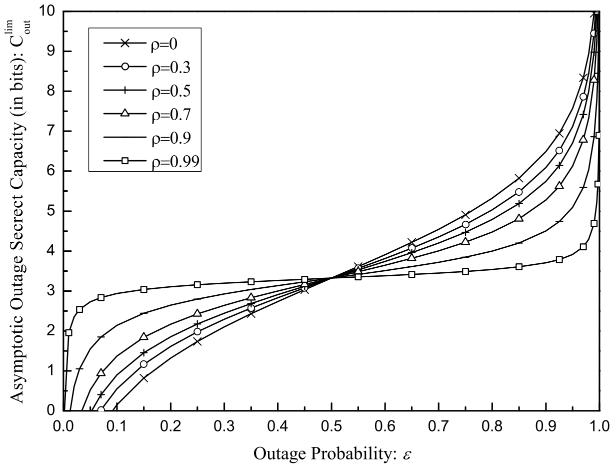


Fig. 5 The asymptotic outage secrecy capacity versus outage probability, for some selected values of channel power correlation coefficients (PCC) and for the channel scenario of $\kappa = 10$ dB.

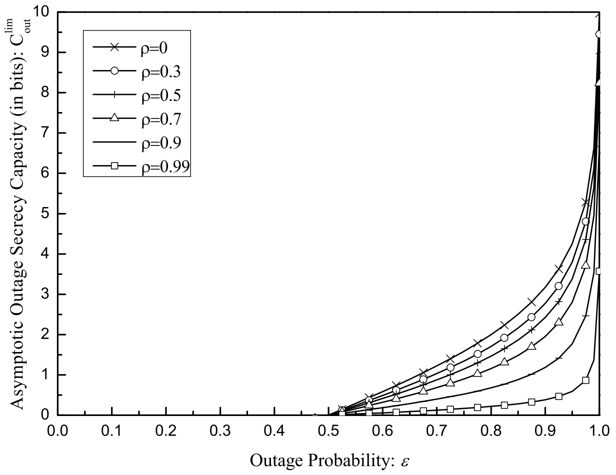


Fig. 6 The asymptotic outage secrecy capacity versus outage probability, for some selected values of channel power correlation coefficients (PCC) and for the channel scenario of $\kappa = 0$ dB.

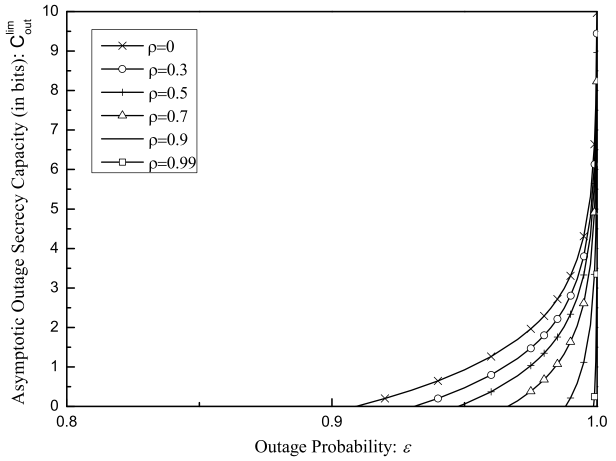


Fig. 7 The asymptotic outage secrecy capacity versus outage probability, for some selected values of channel power correlation coefficients (PCC) and for the channel scenario of $\kappa = -10$ dB.

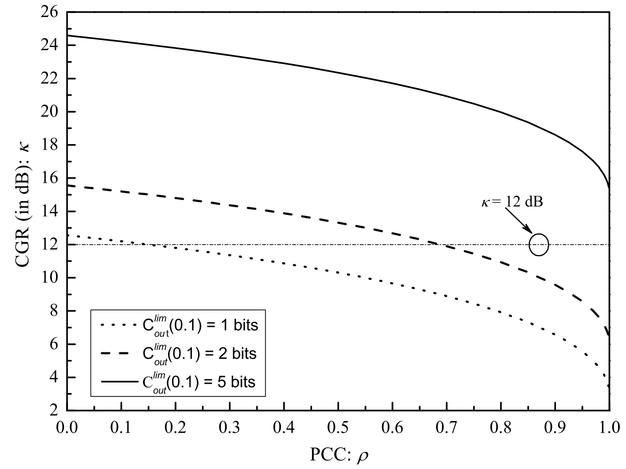


Fig. 8 Channel power gain ratio (CGR) versus channel power correlation coefficient (PCC), for some selected values of target secrecy rates with the outage probability $\epsilon = 0.1$.

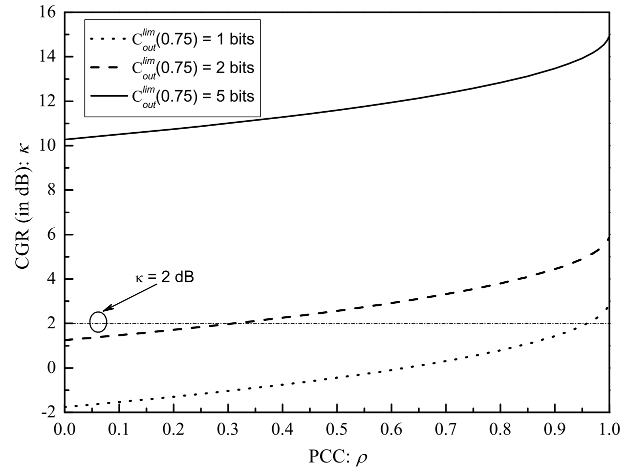


Fig. 9 Channel power gain ratio (CGR) versus channel power correlation coefficient (PCC), for some selected values of target secrecy rates with the outage probability $\epsilon = 0.75$.

secrecy capacity at the CGR. Moreover, a more exact tradeoff between CGR and PCC is needed so that it can provide a baseline to determine if an eavesdropper's approaching is harmful or not. We draw lines $\kappa = 12$ dB and $\kappa = 2$ dB in Figs. 8 and 9, respectively, and find that to increase one bit in the target transmission rate, a more than fifty percent improvement of correlation level is needed for a fixed CGR, or about 3 dB improvement of CGR is needed for a specified PCC. Thus, in practical network design, if an eavesdropper is approaching the main receiver to eavesdrop messages, the situation for the eavesdropper does not become better if the PCC is increased more than fifty percent when the CGR is decreased less than about a 3 dB, which is a very impressive result for current studies which always assume the eavesdropper's approach is destructive.

4.5 Ergodic Secrecy Capacity vs. Outage Secrecy Capacity

In this subsection, we show the differences between the results in this paper and the previous results in Ref. [11] which consider the asymptotic ergodic secrecy capacity of the correlated Rayleigh fading wiretap channel.

Figures 10 and **11** compare the asymptotic ergodic secrecy capacity (i.e., Eq. (5) in Ref. [11]) with the asymptotic outage secrecy capacity (i.e., Eq. (13) in this paper) under the assumption that the channels are independent and correlated, respectively. It is noticed that the asymptotic outage secrecy capacity is no larger than the asymptotic ergodic secrecy capacity when the allowed outage probability is small (0.1 here). However, if the allowed outage probability can be larger (0.75 here), the corresponding asymptotic outage secrecy capacity is much larger than the asymptotic ergodic secrecy capacity. Moreover, it is also observed that the difference between the asymptotic ergodic secrecy capacity and asymptotic outage secrecy capacity becomes less as the correlation level grows irrespective of outage probability. It is important to notice that the above ergodic secrecy capacity is achieved under the assumption that the CSIs of both the main and eavesdropper channels are available. For situations when full CSI cannot be achieved before transmission or when the delay-limited transmission is required, the transmitter has to transmit the information with some probability of outage and the outage secrecy capacity becomes the main performance measure to refer to.

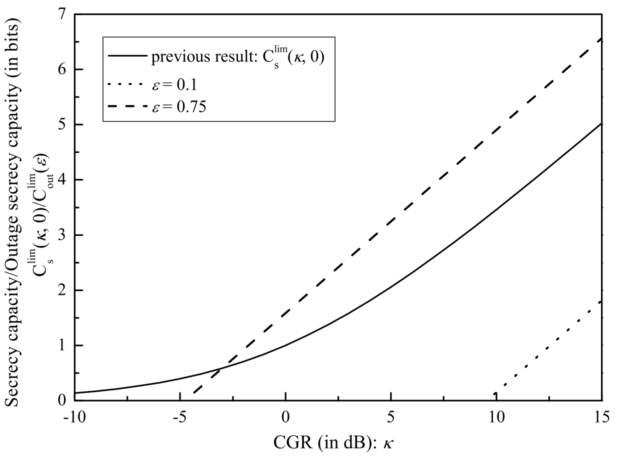


Fig. 10 Asymptotic ergodic secrecy capacity and asymptotic outage secrecy capacity versus channel power gain ratio (CGR) when the channels are independent.

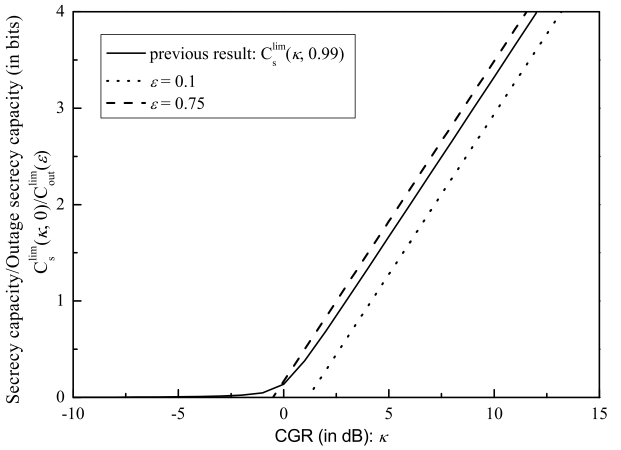


Fig. 11 Asymptotic ergodic secrecy capacity and asymptotic outage secrecy capacity versus channel power gain ratio (CGR) when the channels are highly correlated.

5. Conclusion

In this paper, we derived the closed-form expression of the asymptotic outage probability and asymptotic outage secrecy capacity under the correlated Rayleigh fading wiretap channel, which cover the special cases when the main and eavesdropper channels are independent. We then analyzed the impact of correlation on the asymptotic outage probability and asymptotic outage secrecy capacity, and observed that the asymptotic outage probability decreases as the channel correlation grows in the high CGR regime, and the asymptotic outage secrecy capacity increases as the channel correlation grows when the outage probability is less than 1/2. Then, we analyzed the tradeoff between the asymptotic outage secrecy capacity and outage probability which showed that the asymptotic outage secrecy capacity can be increased by sacrificing the outage probability. Furthermore, the tradeoff between the PCC and CGR is discussed, from which we find that the situation for the eavesdropper does not become better if the PCC is increased more than fifty percent while the CGR is decreased less than about 3 dB. This represents the scenario that the eavesdropper is approaching the main receiver on purpose. Remarkably, our results reveal that the correlation between the main and eavesdropper channels becomes helpful when the main channel's average channel gain is better than the eavesdropper channel's and the outage probability is less than 1/2, and becomes harmful otherwise.

References

[1] Shannon, C.E.: Communication theory of secrecy systems, *Bell System Technical Journal*, Vol.28, No.4, pp.656–715 (1949).

[2] Wyner, A.D.: The wire-tap channel, *Bell System Technical Journal*, Vol.54, No.8, pp.1355–1387 (1975).

[3] Leung-Yan-Cheong, S.K. and Hellman, M.E.: The Gaussian wire-tap channel, *IEEE Trans. Inf. Theory*, Vol.24, No.4, pp.451–456 (1978).

[4] Csiszar, I. and Korner, J.: Broadcast channels with confidential messages, *IEEE Trans. Inf. Theory*, Vol.24, No.3, pp.339–348 (1978).

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

[6] Khisti, A., Tchamkerten, A. and Wornell, G.: Secure broadcasting over fading channels, *IEEE Trans. Inf. Theory*, Vol.54, No.6, pp.2453–2469 (2008).

[7] Parada, P. and Blahut, R.: Secrecy capacity of SIMO and slow fading channels, *IEEE Int. Symp. Information Theory* (*ISIT*), pp.2152–2155, IEEE (2005).

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

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

[10] Gopala, P.K., Lai, L. and Gamal, H.E.: On the Secrecy Capacity of Fading Channels, *IEEE Trans. Inf. Theory*, Vol.54, No.10, pp.4687–4698 (2008).

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

[12] Sun, X., Zhao, C. and Jiang, M.: Closed-Form Expressions for Secrecy Capacity over Correlated Rayleigh Fading Channels (2010), available from ⟨http://arxiv.org/ftp/arxiv/papers/0712/0712.3896.pdf⟩.

[13] Debbah, M., El-Gamal, H., Poor, H. and Shamai, S.: Wireless physical layer security, *EURASIP Journal on Wireless Communications and Networking*, Vol.2009, p.150 (2009).

[14] Liang, Y. and Poor, H.V.: Multiple-access channels with confidential messages, *IEEE Trans. Inf. Theory*, Vol.54, No.3, pp.976–1002 (2008).

[15] Liu, R. and Poor, H.: Multi-antenna Gaussian broadcast channels with confidential messages, *IEEE Int. Symp. Information Theory* (*ISIT*), Toronto, ON, Canada, IEEE, pp.2202–2206 (2008).

[16] Ekrem, E. and Ulukus, S.: Secrecy in cooperative relay broadcast channels, *IEEE Trans. Inf. Theory*, Vol.57, No.1, pp.137–155 (2011).

[17] Lai, L. and El Gamal, H.: The relay–eavesdropper channel: Cooperation for secrecy, *IEEE Trans. Inf. Theory*, Vol.54, No.9, pp.4005–4019 (2008).

[18] Liang, Y., Somekh-Baruch, A., Poor, H., Shamai, S. and Verdu, S.: Capacity of cognitive interference channels with and without secrecy, *IEEE Trans. Inf. Theory*, Vol.55, No.2, pp.604–619 (2009).

[19] Liu, R., Liang, Y. and Poor, H.: Fading cognitive multiple-access channels with confidential messages, *IEEE Trans. Inf. Theory*, Vol.57, No.8, pp.4992–5005 (2011).

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

[21] Lee, W.C.-Y.: Effects on correlation between two mobile radio base-station antennas, *IEEE Trans. Commun.*, Vol.21, No.11, pp.1214–1224 (1973).

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

[23] Shiu, D., Foschini, G., Gans, M. and Kahn, J.: Fading correlation and its effect on the capacity of multielement antenna systems, *IEEE Trans. Commun.*, Vol.48, No.3, pp.502–513 (2000).

[24] Tulino, A.M., Lozano, A. and Verdu, S.: Impact of antenna correlation on the capacity of multiantenna channels, *IEEE Trans. Inf. Theory*, Vol.51, No.7, pp.2491–2509 (2005).

[25] Zhou, X., McKay, M., Maham, B. and Hjorungnes, A.: Rethinking the secrecy outage formulation: A secure transmission design perspective, *IEEE Commun. Lett.*, Vol.15, No.3, pp.302–304 (2011).

[26] Maurer, U. and Wolf, S.: Information-theoretic key agreement: From weak to strong secrecy for free, *Advances in Cryptology-Eurocrypt 2000* (*Lecture Notes in Computer Science*), Vol.1807, Berlin, Germany, Springer, pp.351–368 (2000).

[27] Nitinawarat, S.: Secret key generation for correlated Gaussian sources, *IEEE Int. Symp. Information Theory* (*ISIT*), pp.702–706 (2008).

[28] Davenport, W. and Root, W.: *An introduction to the theory of random signals and noise*, Vol.11, No.6, McGraw-Hill, New York (1958).

[29] Durgin, G. and Rappaport, T.: Theory of multipath shape factors for small-scale fading wireless channels, *IEEE Trans. Antennas and Propag.*, Vol.48, No.5, pp.682–693 (2000).

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

Appendix

A.1 Proof of Eq. (13)

In this proof, we will first show that $C_{out}^{lim}(\epsilon)$ equals the target secrecy rate R_{st} under the condition that $\mathcal{P}_{out}^{lim}(R_{st}) = \epsilon$, and then determine the actual value of $C_{out}^{lim}(\epsilon)$ based on the monotonicity of $\mathcal{P}_{out}^{lim}(R_{st})$ with respect to R_{st}.

Based on Eq. (12), the derivative of $\mathcal{P}_{out}^{lim}(R_{st})$ is given by

$$\left(\mathcal{P}_{out}^{lim}(R_{st})\right)' = \frac{2^{R_{st}}\kappa(1-\rho)(2^{R_{st}}+\kappa)\ln 2}{\left[(2^{R_{st}}+\kappa)^2 - 4\kappa\rho 2^{R_{st}}\right]^{3/2}}. \tag{A.1}$$

Since $R_{st} > 0$, $\kappa > 0$ and $0 \leq \rho < 1$, it is easy to see that $2^{R_{st}}\kappa(1-\rho)(2^{R_{st}}+\kappa)\ln 2 > 0$. Moreover, we have $(2^{R_{st}}+\kappa)^2 - 4\kappa\rho 2^{R_{st}} > 0$ due to that $2^{2R_{st}} + \kappa^2 \geq 2\kappa 2^{R_{st}} > 2\kappa\rho 2^{R_{st}}$. Therefore, we have $\left(\mathcal{P}_{out}^{lim}(R_{st})\right)' > 0$, which indicates $\mathcal{P}_{out}^{lim}(R_{st})$ monotonically increases with R_{st}. In other words, R_{st} monotonically increases with the outage probability. Thus, according to the definition of ϵ-outage secrecy capacity in Eq. (11), we find that $C_{out}^{lim}(\epsilon) = R_{st}$ with condition that $\mathcal{P}_{out}^{lim}(R_{st}) = \epsilon$.

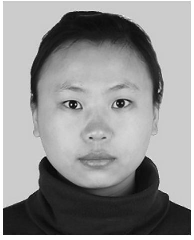
By letting $\mathcal{P}_{out}^{lim}(R_{st}) = \epsilon$, we get

$$(2^{R_{st}} + \kappa\varphi)^2 = \kappa^2(\varphi^2 - 1), \tag{A.2}$$

where $\varphi = \frac{(2\epsilon-1)^2(1-2\rho)+1}{(2\epsilon-1)^2-1}$. The derivative of φ with respect to ϵ can be derived by

$$\varphi' = -\frac{8(2\epsilon-1)(1-\rho)}{\left[(2\epsilon-1)^2-1\right]^2}. \tag{A.3}$$

From Eq. (A.3), we find the fact that φ monotonically increases with ϵ in the region $\epsilon \in (0, 1/2]$ and strictly decreases with ϵ in the region $\epsilon \in (1/2, 1)$, and the maximum value is achieved as $\varphi = -1$ at the point $\epsilon = 1/2$. We then let $f_1(\varphi) = -\kappa(\sqrt{\varphi^2 - 1} + \varphi)$ and $f_2(\varphi) = \kappa(\sqrt{\varphi^2 - 1} - \varphi)$. We find the fact that $f_1(\varphi)$ monotonically increases with φ and $f_2(\varphi)$ monotonically decreases with φ in the region $\varphi \in (-\infty, -1)$. Combining the above two facts and also the fact that $C_{out}^{lim}(\epsilon)$ monotonically increases with ϵ, the result Eq. (13) then follows. □



Jinxiao Zhu received her B.S. and M.S. degrees both in Software Engineering from Xidian University in 2008 and 2011, respectively. She is currently working towards a Ph.D. degree at the School of Systems Information Science at Future University Hakodate. Her research interests are in physical layer security for wireless communications, including point-to-point network, ad-hoc networks, and mobile networks.

Xiaohong Jiang received his B.S., M.S. and Ph.D. degrees all from Xidian University, China. He is currently a full professor of Future University Hakodate, Japan. Dr. Jiang was an associate professor of Tohoku University, Japan, from February 2005 to March 2010, an assistant professor in Japan Advanced Institute of Science and Technology (JAIST), from October 2001 to January 2005. Dr. Jiang was a JSPS research fellow at JAIST from October 1999–October 2001. He was a research associate at the University of Edinburgh from March 1999–October 1999. Dr. Jiang's research interests include computer communications networks, mainly wireless networks, optical networks, etc. He has published over 200 technical papers at premium international journals and conferences, which include over 20 papers published in IEEE journals like IEEE/ACM Transactions on Networking, IEEE Journal of Selected Areas on Communications, etc. Dr. Jiang was the winner of the Best Paper Award and Outstanding Paper Award of IEEE WCNC 2012, IEEE WCNC 2008, IEEE ICC 2005's Optical Networking Symposium, and IEEE/IEICE HPSR 2002. He is a Senior Member of IEEE and a member of IEICE.

Osamu Takahashi received his degree from Hokkaido University in 1975. He worked for NTT research laboratory and NTTDoCoMo research laboratory. He is currently a professor at the Department of System Information Science at Future University Hakodate. His research interest includes ad-hoc networks, network security, and mobile computing. He is a fellow of IPSJ and a member of IEEE and IEICE.

Norio Shiratori is currently an Emeritus and Research Professor at the RIEC (Research Institute of Electrical Communication), Tohoku University, Japan. He is also a board member of Future University of Hakodate and a visiting professor of Chuo University, Japan. He is a fellow of IEEE, IPSJ and IEICE. He was the president of the IPSJ from 2009 to 2011. He has published more than 15 books and over 400 refereed papers in computer science and related fields. He was the recipient of the IPSJ Memorial Prize Winning Paper Award in 1985, the Telecommunication Advancement Foundation Incorporation Award in 1991, the Best Paper Award of ICOIN-9 in 1994, the IPSJ Best Paper Award in 1997, and many others including the most recent Outstanding Paper Award of UIC-07 in 2007.