SECRECY CAPACITY OVER CORRELATED ERGODIC FADING CHANNEL

Hyoungsuk Jeon, Namshik Kim, Minki Kim, Hyuckjae Lee, and Jeongseok Ha

School of Engineering, Information and Communications University, Daejeon, Korea
e-mail: {hschun, nskim, mankigud, hjlee, jsha}@icu.ac.kr.

ABSTRACT

We investigate the secrecy capacity of an ergodic fading wiretap channel in which the main channel is correlated with the eavesdropper channel. In this study, the full Channel State Information (CSI) is assumed, and thus the transmitter knows the channel gains of the legitimate receiver and the eavesdropper. By analyzing the resulting secrecy capacity we quantify the loss of the secrecy capacity due to the correlation. In addition, we study the asymptotic behavior of the secrecy capacity as Signal-to-Noise Ratio (SNR) tends to infinity. The capacity of an ordinary fading channel logarithmically increases with SNR. On the contrary, the secrecy capacity converges to a limit which can be an upper bound on the secrecy capacity over the fading wiretap channel. We find a closed form of the upper bound for the correlated Rayleigh wiretap channel which also includes the independent case as a special one. Our work shows that the upper bound is determined by only two channel parameters; the correlation coefficient and the ratio of the main to the eavesdropper channel gains that will be called the average Channel Gain Ratio (CGR). The analysis of the upper bound tells how the two channel parameters affect the secrecy capacity and leads to the conclusion that the excessively large signal power does not provide any advantage in the secrecy capacity and the loss due to the correlation is especially serious in low CGR regime.

INTRODUCTION

The notion of information-theoretic secrecy [1] was first introduced by Shannon where he showed that the transmitter and the legitimate receiver need to share a random key of length k to secure k bit information from the eavesdropper. That is, the transmitted message W is independent of the eavesdropper's observation Z ; $I(W;Z)=0$ which is called *perfect secrecy*. Although the perfect secrecy provides unconditional secrecy, such a system called a *one-time pad* requires a new random key for each new message. Thus, it may not be considered as a feasible solution in some practical situations.

In the meantime, Wyner also considered the information-theoretic secrecy on a channel model called *wiretap channel* [2] where a legitimate receiver communicates over a main channel, and observations at a wiretapper are degraded from the ones at the legitimate receiver. He showed that the information rate to the legitimate receiver and the ignorance at the wiretapper can be traded off when the wiretapper has a degraded channel. In his work, the maximum information rate of the main channel with the total ignorance at the wiretapper is defined as *secrecy capacity*, and he proved the existence of channel codes achieving the secrecy capacity. Hence the perfect secrecy is now achievable without sharing random keys. After his work, there have been numerous related works [3], [4], [5] for variations of the wiretap channel.

Particularly, in the wireless environment, it is proved that the inherent randomness of wireless channels gives an opportunity to achieve a positive secrecy capacity even if the eavesdropper channel is better in the average sense. On slow fading channels, the secrecy capacity is investigated in terms of outage probability [6], [7]. Further studies on the secrecy capacity of wireless channels have been done in many difference aspects; the ergodic secrecy capacity of fading in [8], [9], [10], secure broadcasting in [11], multiple antenna system [12], [13], [14] and etc.

In this paper, we investigate the secrecy capacity of an ergodic fading wiretap channel in which the main channel is correlated with the eavesdropper channel. The ergodic fading wiretap channel was already studied in [10] where messages are transmitted opportunistically when the main channel has a better instantaneous channel gain than that of the eavesdropper channel. Although the main channel is noisier, due to the opportunistic transmission, a positive secrecy capacity is still achievable. However, if the two channels are correlated, such an opportunistic scheme loses the chance to transmit and thus leads to a loss of the secrecy capacity. In real radio environments, correlation between two channels is frequently observed [15], [16]. The level of the correlation highly depends on antenna deployments, proximity of the legitimate receiver and eavesdropper, and scatterers around them [15], [16], [17], [18]. For example, antenna deployments at high altitude in rural or suburban area generate dominant line-of-sight paths, which results in high correlation between the two receivers. Moreover, it is also possible that the eavesdropper actively makes the correlation, e.g., by approaching the legitimate receiver. Although the

978-1-4244-2677-5/08/$25.00 ©2008 IEEE

correlation is a crucial channel parameter affecting the secrecy capacity, to the best of our knowledge, no previous study has been done on this topic.

Motivated by the practical scenario, we first derive the secrecy capacity for the correlated wiretap channel and analyze the impact of the correlation on the secrecy capacity, which quantitatively shows how much of the secrecy capacity will be lost due to the correlation. However, we are more interested in the analytic study on the secrecy capacity with different values of channel parameters. To do so, we investigate the asymptotic behaviors of the secrecy capacity as Signal-to-Noise Ratio (SNR) tends to infinity. The capacity of an ordinary fading channel logarithmically increases with SNR [18]. On the contrary, the secrecy capacity converges to a limit which can be an upper bound on the secrecy capacity over the fading wiretap channel. We find a closed form of the upper bound for the correlated Rayleigh wiretap channel which also includes the independent case [10] as a special one. Our work shows that the upper bound is determined by only two channel parameters; the correlation coefficient and the ratio of the main to the eavesdropper channel gains. The analysis of the upper bound tells how the two channel parameters affect the secrecy capacity and leads to the conclusion that the excessively large signal power does not provide any advantage in the secrecy capacity. In addition, we will show that the loss due to the correlation is especially detrimental where the channel gain ratio is small. We believe our work makes the results in [10] more comprehensive and also provides a way to evaluate the required SNR margin due to the active eavesdropper who intentionally makes the correlation. Although we focus on the secrecy capacity of the correlated ergodic fading wiretap channel, the analysis can be easily applicable to other scenarios such as the outage probability analysis on the slow fading channel [6], [7].

The remainder of this paper is organized as follows. In Section II, we describe the system model considered in our work. The secrecy capacity for the correlated ergodic fading channel is presented in Section III. The upper bound of the formulated secrecy capacity is also derived in a closed-form expression in Section III. In Section IV we present the numerical results and discuss the relation between the correlation and the loss of the secrecy capacity. Finally, we summarize our results in Section V.

SYSTEM MODEL

Let us consider a fading wiretap channel model depicted in Figure 1. A transmitter constructs an (M,n) code and wishes to send the message to a destination with an arbitrarily low probability of error, while securing against eavesdropping of an unintended user.

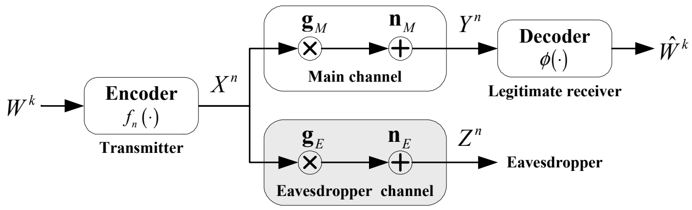

Figure 1. System model

Specifically, the transmitter maps confidential messages $W \in \mathcal{W} = \{1,\ldots,M\}$ to a codeword $x^n \in \mathcal{X}^n$ by using a stochastic encoder $f_n(\cdot):\mathcal{W} \to \mathcal{X}^n$. Then, the received signals of the legitimate receiver and the eavesdropper at the i-th coherent time are given as follows:

$$y(i) = g_M(i)x(i) + n_M(i)$$
$$z(i) = g_E(i)x(i) + n_E(i),$$

where $n_M(i)$ and $n_E(i)$ are the independent and identically distributed (i.i.d.) Gaussian noise with zero mean and unit variance, and $g_M(i)$ and $g_E(i)$ denote the channel gains of the main and eavesdropper channels respectively. We assume that the main channel is correlated with the eavesdropper channel, and the both are ergodic block fading channels. The legitimate receiver then decodes received signals $y^n \in \mathcal{Y}^n$ using a function $\phi(\cdot):\mathcal{Y}^n \to \mathcal{W}$. Let $\hat{w} = \phi(y^n)$ be the estimated messages at the legitimate receiver, then the average error probability of an (M,n) code is defined as

$$P_e^n = \frac{1}{M}\sum_{w\in\mathcal{W}} \Pr\left(\hat{w} \neq w \mid w \text{ is sent}\right).$$

Let us denote the channel power gains of the main and eavesdropper channels as $h_M(i) = |g_M(i)|^2$ and $h_E(i) = |g_E(i)|^2$ respectively and assume the full channel state information (CSI) at the transmitter. Then the equivocation rate which measures the secrecy level of confidential messages against the eavesdropper is defined as

$$R_e \triangleq \frac{1}{n} H\left(W \mid Z^n, h_M^n, h_E^n\right),$$

where h_M^n and h_E^n are the vectors of the channel power gains for the main and the eavesdropper channels respectively. Adopting the definition from [10], we say that the rate R_s is achievable with perfect secrecy if, for any given $\epsilon > 0$, there exists a $(2^{nR_s}, n)$ code of sufficient large n such that

$$\begin{aligned} P_e^n &\le \epsilon \\ R_e &\ge R_s - \epsilon \end{aligned}$$

The secrecy capacity is then the supremum of achievable secret rates

$$C_s \triangleq \sup_{P_e^n \le \epsilon} \{R_s : R_s \text{ is achievable}\}$$

SECRECY CAPACITY OVER CORRELATED CHANNELS

We begin with introducing the secrecy capacity when the main channel is correlated with the eavesdropper channel. Let $f_{H_M,H_E}(h_M, h_E)$ be the joint pdf of H_M and H_E. Assuming that the perfect CSIs of both channels are available at the transmitter, we modified the theorem in [10] as follows.

Theorem 1 (Gopala'08): When the main channel is correlated with the eavesdropper channel, the secrecy capacity is given by

$$\begin{aligned} C_s = \max_{P(h_M,h_E)} \int_0^\infty \int_{h_E}^\infty & \frac{\log\left(1+h_M P\left(h_M,h_E\right)\right)}{\log\left(1+h_E P\left(h_M,h_E\right)\right)} \\ & \times f_{H_M,H_E}\left(h_M,h_E\right) dh_M dh_E \qquad (1) \end{aligned}$$

$$\text{such that } \mathbb{E}\left\{P\left(h_M,h_E\right)\right\} \le \overline{P}$$

Proof: We modify the proof in [10] to include correlation. A detailed proof is given in [19] □

A. UPPER BOUND ON THE SECRECY CAPACITY

It is well known that the capacity of the wireless channel without secrecy constraints highly depends on the received power. If other resources such as the bandwidth and channel gains are fixed, the capacity logarithmically increases with the SNR. In other words, the capacity has been on the increase with the SNR, even though the effect of the SNR on the capacity gets smaller due to the concavity of a logarithm function. However, for the wiretap channel the secrecy capacity converges to a certain value. This behavior is in a striking contrast with the ordinary capacity case because increasing the power in this domain does not affect the secrecy capacity at all. Natural questions are then what is the limiting value to which the secrecy capacity converges eventually as the SNR increases and how this limit depends on other resources and/or parameters in the wiretap channel.

Let us rewrite the secrecy capacity of correlated channels from (1) as

$$C_s = \max_{P(h_M,h_E)} \mathbb{E}_{h_M > h_E} \left[\frac{\log\left(1+h_M P\left(h_M,h_E\right)\right)}{\log\left(1+h_E P\left(h_M,h_E\right)\right)} \right] \qquad (2)$$

At high SNR regime, using $\log(1+x) \approx \log(x)$ for large x, we get the secrecy capacity as follows:

$$C_s \approx \mathbb{E}_{h_M > h_E}\left[\log\left(h_M / h_E\right)\right] \qquad (3)$$

As shown in (3), unlike the traditional wireless communication scenario, the power allocation strategy is completely ineffective. This results in the convergence of secrecy capacity. Under the Rayleigh fading assumption, we now derive limiting value (upper bound) of the secrecy capacity for the wiretap channel in a closed form. To this end, let $U = H_M / H_E$. We will prove the following lemma that the pdf of U is determined by the average channel power gain ratio, $\kappa = \mathbb{E}[H_M] / \mathbb{E}[H_E]$, and the power correlation coefficient, ρ between H_M and H_E. Then the upper bound of the secrecy capacity, i.e., $C_s^{\lim}(\kappa, \rho)$, in (3) can be expressed in terms of a single random variable U:

$$C_s^{\lim}(\kappa, \rho) = \int_1^\infty \log u \, f_U(u)\, du \qquad (4)$$

To solve (4), we first introduce the following lemma.

Lemma 1: Let H_M and H_E be the correlated exponential distributions. Then $U = H_M / H_E$ has the pdf given as

$$f_U(u) = \kappa \frac{(1-\rho)(u+\kappa)}{\left[(u+\kappa)^2 - 4\rho\kappa u\right]^{3/2}} \qquad (5)$$

Proof: Suppose $H_E = h_E$ is given, then $U = H_M / h_E$ is a function of a single random variable H_M. Therefore the conditional pdf of U is $f_U(u \mid h_E) = h_E f_{H_M}(u h_E \mid h_E)$ for $h_E \ge 0$. Then the pdf of U is expressed in terms of the conditional pdf as

$$\begin{aligned} f_U(u) &= \int f_U(u \mid h_E') f_{H_E}(h_E') dh_E' \\ &= \int h_E' f_{H_M}(u h_E' \mid h_E') f_{H_E}(h_E') dh_E' \qquad (6) \\ &= \int h_E' f_{H_M H_E}(u h_E', h_E') dh_E' \end{aligned}$$

Let $\overline{\gamma}_M = \mathbb{E}[H_M]$ and $\overline{\gamma}_E = \mathbb{E}[H_E]$. By applying the joint pdf of H_M and H_E in [Appendix, 19] to (6), we have

$$f_U(u)=\int_0^\infty \frac{h'_E}{\bar{\gamma}_M\bar{\gamma}_E(1-\rho)}\exp\left[-\frac{h'_E}{1-\rho}\left(\frac{u}{\bar{\gamma}_M}+\frac{1}{\bar{\gamma}_E}\right)\right]$$
$$\times I_0\left(\frac{2h'_E}{1-\rho}\sqrt{\frac{\rho u}{\bar{\gamma}_M\bar{\gamma}_E}}\right)dh'_E$$
$$\overset{(a)}{=}\frac{\dfrac{1}{\bar{\gamma}_M\bar{\gamma}_E(1-\rho)^2}\left(\dfrac{u}{\bar{\gamma}_M}+\dfrac{1}{\bar{\gamma}_E}\right)}{\left[\left(\dfrac{1}{1-\rho}\left(\dfrac{u}{\bar{\gamma}_M}+\dfrac{1}{\bar{\gamma}_E}\right)\right)^2-\left(\dfrac{2}{1-\rho}\sqrt{\dfrac{\rho u}{\bar{\gamma}_M\bar{\gamma}_E}}\right)^2\right]^{3/2}}$$
$$=\frac{\bar{\gamma}_M}{\bar{\gamma}_E}(1-\rho)\left(u+\frac{\bar{\gamma}_M}{\bar{\gamma}_E}\right)\left[\left(u+\frac{\bar{\gamma}_M}{\bar{\gamma}_E}\right)^2-4\rho\frac{\bar{\gamma}_M}{\bar{\gamma}_E}u\right]^{-3/2}$$

where $I_0(x)\triangleq(1/2\pi)\int_0^{2\pi}e^{x\cos\theta}d\theta$ is the zero order modified Bessel function of the first kind and (a) follows from the table of integrals in [20],

$$\int_0^\infty x\exp(-\alpha x)I_0(\beta x)\,dx=\alpha\left(\alpha^2+\beta^2\right)^{-3/2}$$

for $\mathrm{Re}\{\alpha\}>|\mathrm{Re}\{\beta\}|$. Introducing a new variable $\kappa=\bar{\gamma}_M/\bar{\gamma}_E$, we obtain the pdf of U . □

In the following, we call ρ and κ as the power correlation coefficient (PCC) and the average channel gain ratio (CGR) respectively. Applying *Lemma 1* to (4) we obtain the following theorem.

Theorem 2: If the main channel is correlated with the eavesdropper channel, and the joint pdf of them is bivariate Rayleigh distribution, the secrecy capacity converges into the following limiting value as the SNR increases

$$C_s^{\lim}(\kappa,\rho)=\log(1+\kappa)+\log\left(\frac{1}{2}+\sqrt{\frac{1}{4}-\frac{\rho\kappa}{(1+\kappa)^2}}\right) \quad (7)$$

Proof: It is possible to express the upper bound of the secrecy capacity $C_s^{\lim}(\kappa,\rho)$ in (4) as

$$C_s^{\lim}(\kappa,\rho)=\left[\log uF_U(u)\right]_1^\infty-\int_1^\infty\frac{1}{u}F_U(u)\,du\,, \quad (8)$$

with the integration by parts rule where $F_U(u)$ is the indefinite integral of $f_U(u)$. From *Lemma 1*, $F_U(u)$ is given by

$$F_U(u)\ =\int f_U(u)\,du=\frac{u-\kappa}{2\sqrt{(u+\kappa)^2-4\rho\kappa u}} \quad (9)$$

Hence, we can obtain the indefinite integral of the second term on the right side of (8) as follows:

$$\int\frac{1}{u}F_U(u)\,du=\frac{1}{2}\log\left(-\frac{4(1-\rho)\Phi(u)}{\kappa u}\right) \quad (10)$$

where $\Phi(u)=(u+\kappa)^2+(u+\kappa)\sqrt{(u+\kappa)^2-4\rho\kappa u}-2\rho\kappa u$. By substituting (9) and (10) into (8), finally, we have the secrecy capacity limit as follows (A detailed proof is given in [19]):

$$C_s^{\lim}(\kappa,\rho)=\log(1+\kappa)+\log\left(\frac{1}{2}+\sqrt{\frac{1}{4}-\frac{\rho\kappa}{(1+\kappa)^2}}\right) \quad (11)$$

□

B. ASYMPTOTIC PROPERTIES OF THE SECRECY CAPACITY

To investigate the relative loss with respect to the independent case where the secrecy capacity limit is maximized, we find upper and lower bounds of the secrecy capacity limit $C_s^{\lim}(\kappa,\rho)$ in terms of $C_s^{\lim}(\kappa,0)$ and ρ . Such bounds are summarized in *Corollary 1*.

Corollary 1: For given κ and ρ , $C_s^{\lim}(\kappa,\rho)$ is bounded by

$$(1-\rho)C_s^{\lim}(\kappa,0)\le C_s^{\lim}(\kappa,\rho)\le C_s^{\lim}(\kappa,0)$$

Proof: The proof is equivalent to showing that

$$1-\rho\le C_s^{\lim}(\kappa,\rho)/C_s^{\lim}(\kappa,0)\le 1 \quad (12)$$

It is easily verified that $C_s^{\lim}(\kappa,\rho)/C_s^{\lim}(\kappa,0)$ monotonically increases with the CGR ($\kappa\ge 0$). Thus we can obtain the lower and upper bounds by letting $\kappa\to 0$ and $\kappa\to\infty$ respectively. First, we can see that $C_s^{\lim}(\kappa,\rho)$ in (7) tends to $\log(1+\kappa)=C_s^{\lim}(\kappa,0)$ as κ increases, which gives us the upper bound. By applying the L'Hôpital's rule to $\lim_{\kappa\to 0}C_s^{\lim}(\kappa,\rho)/C_s^{\lim}(\kappa,0)$, we have the lower bound as

$$\lim_{\kappa\to 0}\frac{\log(1+\kappa)+\log\left(\dfrac{1}{2}+\sqrt{\dfrac{1}{4}-\dfrac{\rho\kappa}{(1+\kappa)^2}}\right)}{\log(1+\kappa)}=1-\rho$$

which finishes this proof. □

In the next section, we will see how the two channel parameters κ and ρ affect the secrecy capacity in a quantitative manner.

NUMERICAL RESULTS

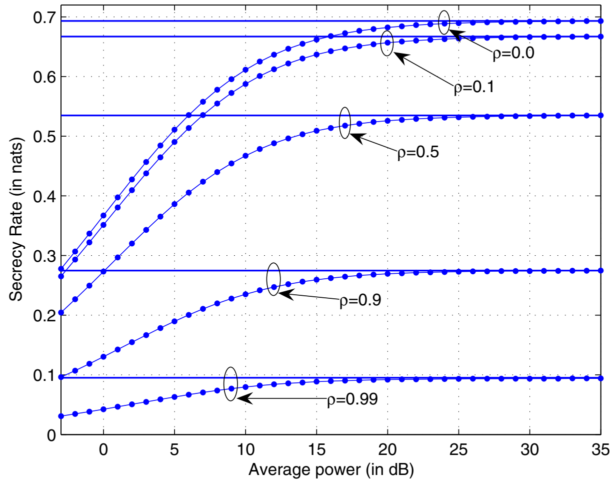

Figure 2. Symmetric scenario (CGR=1.0); The solid lines indicate the upper bounds on secrecy capacity in (7), and the lines with filled circles represent the numerical evaluations of the secrecy capacity in (1).

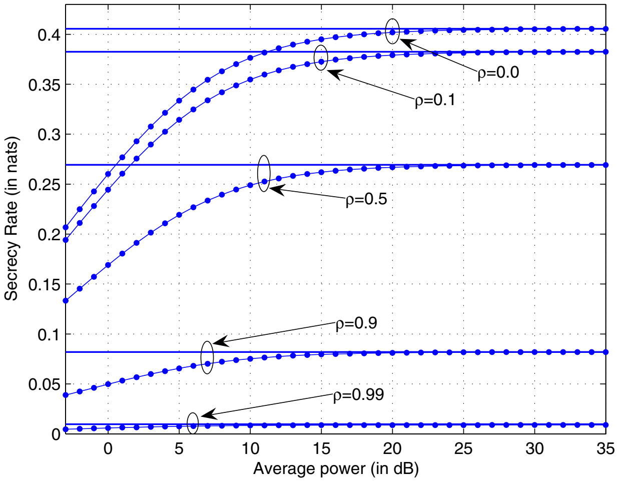

Figure 3. Asymmetric scenario (CGR=0.5); The solid lines indicate the upper bounds on secrecy capacity in (7), and the lines with filled circles represent the numerical evaluations of the secrecy capacity in (1).

We first plot the secrecy capacity, i.e., (1), for the Rayleigh fading channel as a function of average power in Figure 2 and Figure 3. For the correlated scenario, the bivariate Rayleigh distribution [21] is employed as the joint pdf of the main and the eavesdropper channels.

To compare with results from [10], symmetric (CGR=1.0) and asymmetric (CGR=0.5) cases are depicted. In both cases, we observe that the correlation between the main and the eavesdropper channels reduces the secrecy capacity. To confirm our work, we also evaluate the limits of the secrecy capacity in (7) and compare them with the secrecy capacity curves. The comparisons show that the secrecy capacity curves with the different PCC values converge into the limit of the secrecy capacity $C_s^{\lim}(\kappa,\rho)$. As aforementioned, such convergence implies that the signal power becomes more inefficient as it grows, and eventually the secrecy capacity is independent of the signal power.

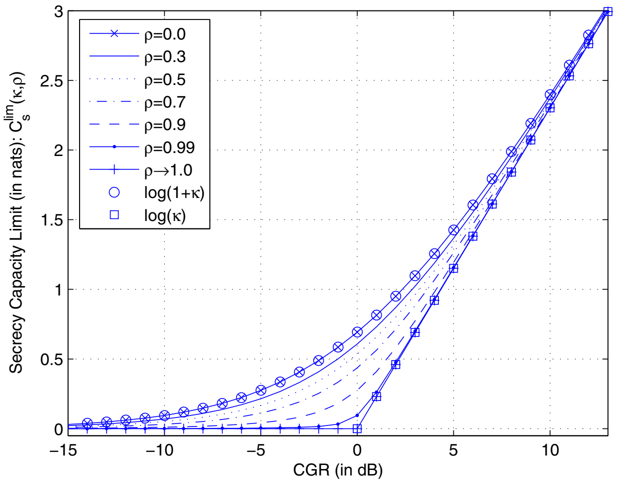

Figure 4. Secrecy capacity limit versus CGR

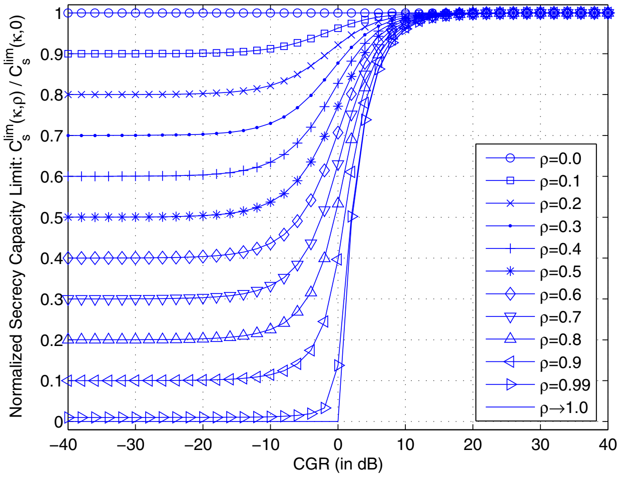

Figure 5. Normalized secrecy capacity limit versus CGR

Figure 4 and Figure 5 show the impact of the CGR and the PCC on the limiting value of the secrecy capacity. In Fig. 4, the limit of the secrecy capacity $C_s^{\lim}(\kappa,\rho)$ in (7) is evaluated at a few PCC values where $C_s^{\lim}(\kappa,\rho)$ has different behaviors in low and high CGR regimes. In low CGR regime, the correlation significantly degrades the limit of the secrecy capacity. Since the loss due to the correlation is especially serious in low CGR regime an active eavesdropper efficiently decreases the secrecy capacity by approaching the legitimate receiver, which thus results in not only high PCC but also low CGR. Equivalently, if the transmitter does not know or underestimate the correlation, the overestimated secrecy capacity results in information leak to the eavesdropper. Thus, the transmission rate must be determined in a conservative way to consider the possible correction.

On the contrary, the impact of the correlation becomes negligible as CGR increases, and all curves for the correlated fading scenario eventually approach the secrecy capacity limit of i.i.d. fading scenario. Thus, the correlation is not an efficient way to break the security in high CGR regime. In Figure. 4, it is also noticed that even if the channel are completely correlated, we have a positive secrecy capacity when CGR is larger than one (0 dB).

The quantity of the loss can immediately be seen in Figure 5, which shows the normalized secrecy capacity limit as a function of the CGR. The normalization is with respect to (12). It clearly demonstrates that the secrecy capacity limit has the bound of $(1-\rho)C_s^{\lim}(\kappa,0)\le C_s^{\lim}(\kappa,\rho)\le C_s^{\lim}(\kappa,0)$

CONCLUSIONS

We investigate the secrecy capacity of an ergodic fading wiretap channel in which the main channel is correlated with the eavesdropper channel. In this study, the full Channel State Information (CSI) is assumed, and thus the transmitter knows the channel gains of the legitimate receiver and the eavesdropper. To see the detrimental effect of the correlation, we find the joint probability density function of the correlated Rayleigh fading wiretap channel with which we evaluate the secrecy capacity. In the evaluation, it is noticed that the secrecy capacity converges into a limit with the growing signal-to-noise ratio as opposed to ever increasing capacity of conventional communication channels. Since it is also interesting to see the roles of the channel parameters in the secrecy capacity, we try to find the limit of the secrecy capacity in a closed form and extensively study the behaviors of the limit in various situations.

Our study tells that the limit of the secrecy capacity determined by the two channel parameters; average channel gain ratio (CGR) and power correlation coefficient (PCC). The study also shows that the correlation is especially detrimental when CGR is small. Thus, by approaching a legitimate receiver an active eavesdropper can efficiently incapacitate the wiretap channel codes even if the transmitter can afford high transmit signal power since such close proximity leads to low CGR and high PCC

On the other hand, the correlation does not affect the secrecy capacity when CGR is high. Thus, although we do not propose a specific way here, our study indicates that the most efficient way to defeat the active eavesdropper is to improve CGR, which will be pursued in our future research.

The analysis on the limit of the secrecy capacity is confirmed by evaluating the secrecy capacity in a numerical way and comparing them with the analytic results. Although the correlation is one of important parameters, to our best knowledge, the effects of the correlation on wiretap channel codes have not been investigated. We believe that our work paves the way for a new study on the correlation wiretap channel.

ACKNOWLEDGMENT

This work was supported by 2nd Phase of Brain Korea 21 project sponsored by Ministry of Education, Science and Technology, Korea

REFERENCES

[1] C. E. Shannon, “Communication theory of secrecy systems,” *Bell Syst. Tech. J.*, vol. 28, no. 4, pp. 656 – 715, Oct. 1949.

[2] A. D. Wyner, “The Wire-tap channel,” *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[3] I. Csiszár and J. Körner, “Broadcast channels with confidential messages,” *IEEE Trans. Inform. Theory*, vol. IT-24, no. 3, pp. 339 – 348, May 1978.

[4] S. K. Leung-Yan-Cheong and M. E. Hellman, “The Gaussian wire-tap channel,” *IEEE Trans. Inform. Theory*, vol. IT-24, no. 4, pp. 451 – 456, Jul. 1978.

[5] L. H. Ozarow and A. D. Wyner, “Wire-tap channel II,” *Bell Syst. Tech. J.*, vol. 63, no. 10, pp. 2135 – 2157, Dec. 1984.

[6] J. Barros and M. R. D. Rodrigues, “Secrecy capacity of wireless channels,” in *Proc. Int. Symp. Information Theory*, Seattle, U.S.A, Jul. 2006, pp. 356 – 360.

[7] M. Bloch, J. Barros, M. R. D. Rodrigues, and S.W. McLaughlin, “Wireless information-theoretic security,” *IEEE Trans. Inform. Theory*, vol. 54, no. 6, pp. 2515 – 2534, Jun. 2008.

[8] Y. Liang, H. V. Poor, and S. Shamai, “Secure communication over fading channels,” *IEEE Trans. Inform. Theory*, vol. 54, no. 6, pp. 2470 – 2492, Jun. 2008.

[9] Z. Li, R. Yates, and W. Trappe, “Secret capacity of independent parallel channels,” in *Proc. Annu. Allerton Conf.*, Monticello, IL, U.S.A, Sep. 2006. 16

[10] P. K. Gopala, L. Lai, and H. E. Gamal, “On the secrecy capacity of fading channels,” *IEEE Trans.*

Inform. Theory, vol. 54, no. 10, pp. 4687 – 4698, Oct. 2008.

[11] A. Khisti, G. Wornell, and A. Tchamkerten, "Secure broadcasting with multiuser diversity," in *Proc. Annu. Allerton Conf.*, Monticello, IL, U.S.A, Sep.

[12] I. A. O. Hero, "Secure space-time communication," *IEEE Trans. Inform. Theory*, vol. 49, no. 12, pp. 3235 – 3249, Dec. 2003.

[13] S. Shafiee, N. Liu, and S. Ulukus, "Towards the secrecy capacity of the Gaussian MIMO wire-tap channel: The 2-2-1 channel," *IEEE Trans. Inform. Theory*, submitted 2007. [Online] Available to: http://arxiv.org/PS_cache/arxiv/pdf/0709/0709.3541v1.pdf

[14] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *IEEE Trans. Inform. Theory*, submitted 2007. [Online]. Available to: http://aps.arxiv.org/PS_cache/arxiv/pdf/0710/0710.1920v1.pdf

[15] W. C.-Y. Lee, "Effects on correlation between two mobile radio base-station antennas," *IEEE Trans. Commun.*, vol. COM- 21, no. 11, pp. 1214 – 1224, Nov. 1973.

[16] S. B. Rhee and G. I. Zysman, "Results of suburban base-station spatial diversity measurements on the UHF bands," *IEEE Trans. Commun.*, vol. COM-22, no. 10, pp. 1630 – 1634, Oct. 1974.

[17] D.-S. Shiu, G. J. Foschini, M. J. Gans, and J. M. Kahn, "Fading correlation and its effect on the capacity of multielement antenna systems," *IEEE Trans. Commun.*, vol. 48, no. 3, pp. 502 – 513, Mar. 2000.

[18] D. Tse and P. Viswanath, *Fundamentals of Wireless Communication*. Cambridge: Cambridge University Press, 2005.

[19] H. Jeon, N. Kim, M. Kim, H. Lee, and J. Ha, "Secrecy capacity over correlated ergodic fading channel," *IEEE Trans. Inform. Theory*, submitted, 2008. [Online]. Available to: http://arxiv.org/PS_cache/arxiv/pdf/0809/0809.5212v1.pdf

[20] I. S. Gradshteyn, I. M. Ryzhik, A. Jeffrey, and D. Zwillinger, *Table of Integrals, Series, and Products*. Academic Press, 2000.

[21] M. K. Simon and M.-S. Alouini, *Digital Communication over Fading Channels*, 2nd ed. Wiley-IEEE Press, 2004.