On the Secrecy Capacity of Fading Wireless Channel with Multiple Eavesdroppers

Peiya Wang, Guanding Yu, and Zhaoyang Zhang
Department of Information Science and Electronic Engineering
Zhejiang University, Hangzhou 310027, China
Email: yuguanding@zju.edu.cn

***Abstract*—This paper studies the secrecy capacity of fading wireless channel in presence of multiple eavesdroppers. The eavesdroppers are mutually independent and the information is secure if it cannot be eavesdropped by any eavesdropper. We first generalize the work in [4] into multiple-eavesdropper case and investigate the secrecy capacity in terms of outage probability and outage capacity. We show that the results presented in [4] serves as some special cases of our works. We also characterize the ergodic secrecy capacity of fading wireless channel with multiple eavesdroppers. Our work gives the analytical results of secrecy capacity with different number of eavesdroppers.**

I. Introduction

The investigation of privacy and security in wireless communication networks has played an extremely important part with the development of wireless networks. The conventional computational security model, which assumes limited capability of calculation at the eavesdropper, will be obsolete with the rapid development of computing technologies and devices. This motivates the research of information-theoretic security model, which puts no computational restrictions on the eavesdropper. The conception of the information-theoretic security was first introduced by Shannon [1], who proved that perfect information-theoretic security demands that the eavesdropper shouldn't attain any information about the transmitted message from the signal received. Later, Wyner [2] introduced the wiretap channel and assumed that the signal received by the eavesdropper is a degraded version of the signal received by the legitimate receiver. Accounting for the compromise between the transmission error rate and the security of the transmitted message, Wyner showed that it is possible to implement secure communication. Csiszár and Körner [3] extended the research to non-degraded channels and proved that a non-zero secrecy capacity is achievable as long as the main channel is better than the wiretap channel. More recently, the impact of channel fading on the secrecy capacity was studied in [4]. The author pointed out that the secure communication is feasible over quasi-static fading channel with one eavesdropper, even if the main channel is worse than the wiretap channel on the average. And in [5], the authors studied how to maximize the secrecy capacity and derived the optimal power allocation policies under different assumptions at the transmitter. The secrecy capacity has also been extended into multiple access channel [6] and broadcasting channel [7].

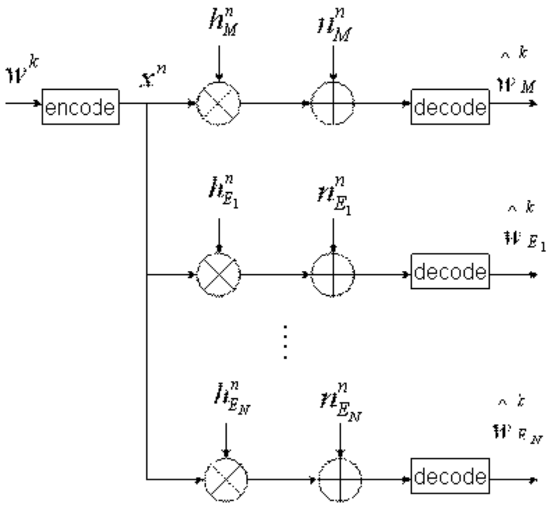

Fig. 1. System Model

In this paper, we concentrate on secrecy capacity over ergodic fading channels with multiple eavesdroppers. We assume that all eavesdroppers are mutually independent and the information is secure if it cannot be eavesdropped by any eavesdropper. The transmitter doesn't know any channel side information and sends message with constant power level. We first extend the work in [4] into multiple eavesdroppers case, i.e., the existence of a non-zero secrecy capacity is analyzed and the secrecy capacity in terms of the outage probability is characterized. We show that the results obtained in [4] correspond to some special cases of our works. Then, we investigate the ergodic secrecy capacity, in presence of multiple eavesdroppers. The main contribution of this paper is the analytical results of secrecy capacities (in terms of both outage capacity and ergodic capacity) of fading wireless channel with different number of eavesdroppers.

The rest of the paper is organized as follows. Section II characterizes the system model of the problem. Section III analyzes the secrecy capacity of wireless channels with multiple eavesdroppers, in terms of both outage capacity and ergodic capacity. Section IV provides some numerical results and conclusions are given in Section V.

II. System Model

The system model is illustrated in Fig. 1. A legitimate user communicates with its corresponding receiver in the presence of several eavesdroppers E_1, E_2, $\ldots$, E_N. At the transmitter,

1-4244-1429-6/07/$25.00 ©2007 IEEE

the message block w^k is encoded into the codeword $x^n = [x(1), x(2), \ldots, x(i), \ldots, x(n)]$, which is suitable to be transmitted on the quasi-static fading channel (the main channel). And the receiver can obtain information about transmitted message by decoding the signal received. Assuming that all the channels experience flat fading and remain constant during each symbol interval, the output at the legitimate receiver is

$$y_M(i) = g_M(i)x(i) + n_M(i),$$

where $g_M(i)$ is the main (legitimate) channel gain and $n_M(i)$ is the Additive White Gaussian Noise (AWGN) of main channel. The capacity of the main channel is $C_M = \log(1 + |g_M|^2 P/N_M)$, where P is the transmit power and N_M is the noise power of the main channel. We can denote the effective channel gain as $h_M(i) = g_M(i)^2/N_M$, which is exponentially distributed in the Rayleigh fading channel, i.e.,

$$f(h_M) = \frac{1}{\bar{\gamma}_M} \exp\left(-\frac{h_M}{\bar{\gamma}_M}\right), h_M > 0. \tag{1}$$

Here, $\bar{\gamma}_M$ is the average power gain of the main channel. Therefore, the capacity of the main channel can be written as a function of effective channel gain h_M as follows, $C_M = \log(1 + h_M P)$.

We assume that the number of the wiretap channels is N and the tab of the eavesdropper is k. Likewise, the kth eavesdropper is able to acquire information about the transmitted message more or less by observing the channel output

$$y_{E_k}(i) = g_{E_k}(i)x(i) + n_{E_k}(i), k = 1, 2, \ldots, N.$$

The wiretap channel is a fading channel with the fading gain $g_{E_k}(i)$ and AWGN $n_{E_k}(i)$. In order to simplify the analysis, we assume that the wiretap channels are mutually independent and their channel gains satisfy the same distribution. Similarly, we can define effective channel gain of wiretap channel as $h_{E_k} = g^2_{E_k}/N_E$, where N_E is the noise power of the wiretap channel. Hence, the capacity of the kth wiretap channel is $\log(1 + h_{E_k} P)$. If $N = 1$, we know that the information can be transmitted confidentially over the fading channel when the instantaneous power gain of the main channel is larger than that of the wiretap channel. Likewise, we can transmit message safely only when the effective channel gain of main channel is larger than the effective channel gain of any eavesdropper. So we define h_E as the maximum channel gain among all eavesdroppers, whose distribution function is

$$F(h_E) = \left(1 - \exp\left(-\frac{h_E}{\bar{\gamma}_E}\right)\right)^N. \tag{2}$$

Accordingly, we can get its probability density function (pdf)

$$f(h_E) = N\left(1 - \exp\left(-\frac{h_E}{\bar{\gamma}_E}\right)\right)^{N-1} \frac{1}{\bar{\gamma}_E} \exp\left(-\frac{h_E}{\bar{\gamma}_E}\right). \tag{3}$$

An important equation which will be used in the following section is presented as follows,

$$\int_0^\infty \exp(-ax)[1 - \exp(-bx)]^N dx = \frac{N!}{a} \prod_{i=1}^{N} \frac{b}{a + bi}. \tag{4}$$

The proof can be found in the Appendix.

III. Secrecy Capacity with Multiple Eavesdroppers

If the transmitter doesn't know any state information about the channels, one advisable strategy is sending message with constant power level. Therefore, the main channel's capacity is,

$$C_M = \log(1 + h_M P),$$

and the capacity of the wiretap channels is,

$$C_E = \log(1 + h_E P).$$

According to Wyner's model, the secrecy capacity can be denoted by

$$C_S = C_M - C_E.$$

Thus when $h_E \geq h_M$, one would not send message unless he doesn't want to keep the information out of being eavesdropped. So we may write the secrecy capacity as

$$C_s = \begin{cases} \log(1 + h_M P) - \log(1 + h_E P), & \text{if } h_M > h_E \\ 0, & \text{if } h_M \leq h_E \end{cases} \tag{5}$$

A. Existence of Non-zero Secrecy Capacity

In [4], the authors have shown that there exists a non-zero secrecy capacity in fading channel even when the wiretap channel is statistically better than the main channel. In the follows, we will generalize the existence of a non-zero secrecy capacity into multiple eavesdroppers case. We have

$$\begin{aligned} \Pr(C_s > 0) &= \Pr(h_M > h_E) \\ &= \int_0^\infty \int_0^{h_M} f(h_M) f(h_E) dh_E dh_M \\ &= \int_0^\infty \frac{1}{\bar{\gamma}_M} \exp\left(-\frac{\gamma_M}{\bar{\gamma}_M}\right)\left[1 - \exp\left(-\frac{\gamma_M}{\bar{\gamma}_E}\right)\right]^N d\gamma_M. \end{aligned}$$

By simply replacing $a = \frac{1}{\bar{\gamma}_M}$ and $b = \frac{1}{\bar{\gamma}_E}$ in Eq. (4), we can obtain the result as follows

$$\Pr(C_s > 0) = \prod_{i=1}^{N} \frac{1}{\bar{\gamma}_E} \frac{i}{\frac{i}{\bar{\gamma}_E} + \frac{1}{\bar{\gamma}_M}} = \prod_{i=1}^{N} \frac{i}{\theta + i}. \tag{6}$$

Here, $\theta = \bar{\gamma}_E / \bar{\gamma}_M$.

From the above, a non-zero secrecy capacity exists even when $\bar{\gamma}_M \leq \bar{\gamma}_E$. We can also get a special result by taking $N = 1$:

$$\Pr(C_s > 0) = \frac{1}{\theta + 1} = \frac{\bar{\gamma}_M}{\bar{\gamma}_E + \bar{\gamma}_M},$$

which corresponds to the Eq. (5) in [4].

B. Outage Probability and Outage Capacity

Now we will characterize the outage probability

$$P_{out}(R_s) = \Pr(C_s < R_s).$$

The significance of the definition is that when the secrecy rate is set to R_s, the confidential communication will be ensured only if $C_s > R_s$, otherwise the secure transmission will not be guaranteed.

From the total probability theorem, we can get the outage probability.

$$\begin{aligned}
&\Pr(C_s < R_s) = \Pr(C_s < R_s | h_M > h_E)\Pr(h_M > h_E)\\
&+ \Pr(C_s < R_s | h_M \le h_E)\Pr(h_M \le h_E)\\
&= \Pr(h_M < [2^{R_s}(1 + h_E P) - 1]/P | h_M > h_E)\Pr(h_M > h_E)\\
&+ \Pr(C_s < R_s | h_M \le h_E)\Pr(h_M \le h_E).
\end{aligned}$$

We can see that $C_s = 0$ when $h_M \le h_E$, i.e., $\Pr(C_s < R_s | h_M \le h_E) = 1$. Then, the above formula can be written as

$$\begin{aligned}
&\Pr(C_s < R_s) = \Pr(h_M \le h_E)\\
&+ \Pr(h_M < [2^{R_s}(1 + h_E P) - 1]/P | h_M > h_E)\Pr(h_M > h_E)\\
&= \int_0^\infty \int_{h_E}^x f(h_M) f(h_E) dh_M dh_E + Pr(h_M \le h_E)\\
&= \int_0^\infty \int_{h_E}^\infty f(h_M) f(h_E) dh_M dh_E\\
&- \int_0^\infty \int_x^\infty f(h_M) f(h_E) dh_M dh_E + \Pr(h_M \le h_E)\\
&= \Pr(h_M > h_E) + \Pr(h_M \le h_E)\\
&- \int_0^\infty \int_x^\infty f(h_M) f(h_E) dh_M dh_E\\
&= 1 - \int_0^\infty \int_x^\infty f(h_M) f(h_E) dh_M dh_E.\\
&= 1 - \int_0^\infty \exp\,(-\frac{2^{R_s} - 1}{\bar{\gamma}_M P} - \frac{2^{R_s} h_E}{\bar{\gamma}_M}) f(h_E) dh_E\\
&= 1 - \frac{N}{\bar{\gamma}_E} \exp\,(-\frac{2^{R_s} - 1}{\bar{\gamma}_M P})\\
&\int_0^\infty \exp\,[-(\frac{2^{R_s}}{\bar{\gamma}_M} + \frac{1}{\bar{\gamma}_E}) h_E][1 - \exp\,(-\frac{h_E}{\bar{\gamma}_E})]^{N-1} dh_E.
\end{aligned}$$

Here, $x = [2^{R_s}(1 + h_E P) - 1]/P$.

By replacing $a = \frac{2^{R_s}}{\bar{\gamma}_M} + \frac{1}{\bar{\gamma}_E}$ and $b = \frac{1}{\bar{\gamma}_E}$ in Eq. (4), we can obtain

$$\begin{aligned}
&\frac{N}{\bar{\gamma}_E} \int_0^\infty \exp\,[-(\frac{2^{R_s}}{\bar{\gamma}_M} + \frac{1}{\bar{\gamma}_E}) h_E][1 - \exp\,(-\frac{h_E}{\bar{\gamma}_E})]^{N-1} dh_E.\\
&= \frac{N}{\bar{\gamma}_E} \frac{(N-1)!}{a} \prod_{i=1}^{N-1} \frac{b}{a + bi}\\
&= \frac{N}{\bar{\gamma}_E} \frac{(N-1)!}{a} \prod_{i=1}^{N-1} \frac{\frac{1}{\bar{\gamma}_E}}{\frac{2^{R_s}}{\bar{\gamma}_M} + \frac{1}{\bar{\gamma}_E}(i+1)}\\
&= N! \prod_{i=1}^{N} \frac{\frac{1}{\bar{\gamma}_E}}{\frac{2^{R_s}}{\bar{\gamma}_M} + \frac{i}{\bar{\gamma}_E}}\\
&= \prod_{i=1}^{N} \frac{i}{2^{R_s}\theta + i}.
\end{aligned}$$

Therefore, the outage probability is given by

$$P_{out}(R_s) = 1 - \exp\,(-\frac{2^{R_s} - 1}{\bar{\gamma}_M P}) \prod_{i=1}^{N} \frac{i}{2^{R_s}\theta + i}. \qquad (7)$$

The ϵ-outage secrecy capacity, defined as the largest secrecy rate such that the outage probability is less than ϵ, can be found by:

$$P_{out}(C_{out}(\epsilon)) = \epsilon.$$

We can also give a special result corresponding to the case of one eavesdropper,

$$P_{out}(R_s) = 1 - \exp\,(-\frac{2^{R_s} - 1}{\bar{\gamma}_M P}) \frac{1}{2^{R_s}\theta + 1}.$$

This equation is exactly the Eq. (7) in [4].

C. Ergodic Secrecy Capacity

We turn to calculate the ergodic secrecy capacity of wireless channel with multiple eavesdroppers, which serves as another important metric of wireless fading channel. The ergodic capacity is calculated as the average of instantaneous capacity over h_M and h_E. First, for a given h_M, the average secrecy capacity over h_E can be written as,

$$\begin{aligned}
&\bar{C}_s(h_M) = \int_0^{h_M} [\log(1 + h_M P) - \log(1 + h_E P)]\, f(h_E) dh_E\\
&= \log(1 + h_M P)\left[1 - \exp(-\frac{h_M}{\bar{\gamma}_E})\right]^N - \int_0^{h_M} \log(1 + h_E P) dF(h_E)\\
&= \log(1 + h_M P)\left[1 - \exp(-\frac{h_M}{\bar{\gamma}_E})\right]^N - \log(1 + h_E P) F(h_E)|_0^{h_M}\\
&+ \int_0^{h_M} \left[1 - \exp(-\frac{h_E}{\bar{\gamma}_E})\right]^N d\log(1 + h_E P)\\
&= \int_0^{h_M} \frac{P}{1 + h_E P} \left[1 - \exp(-\frac{h_E}{\bar{\gamma}_E})\right]^N dh_E\\
&= \int_0^{h_M} \frac{P}{1 + h_E P} dh_E + \sum_{i=1}^{N} \binom{N}{i} (-1)^i \int_0^{h_M} \frac{P}{1 + h_E P} \exp(-\frac{i h_E}{\bar{\gamma}_E}) dh_E\\
&= \log(1 + h_M P)\\
&+ \sum_{i=1}^{N} \binom{N}{i} (-1)^i \exp(\frac{i}{\bar{\gamma}_E P}) \left[Ei(\frac{i}{\bar{\gamma}_E P}) - Ei(\frac{i}{\bar{\gamma}_E P} + \frac{i h_M}{\bar{\gamma}_E})\right].
\end{aligned} \qquad (8)$$

Here,

$$Ei(x) = \int_x^\infty \frac{\exp(-t)}{t} dt.$$

Therefore, the ergodic secrecy capacity is

$$\begin{aligned}
&\bar{C}_s = \int_0^\infty \bar{C}_s(h_M) f(h_M) dh_M\\
&= \int_0^\infty f(h_M)\{\log(1 + h_M P)\\
&+ \sum_{i=1}^{N} \binom{N}{i} (-1)^i \exp\,(\frac{i}{\bar{\gamma}_E P})[Ei(\frac{i}{\bar{\gamma}_E P}) - Ei(\frac{i}{\bar{\gamma}_E P} + \frac{i h_M}{\bar{\gamma}_E})]\} dh_M.
\end{aligned} \qquad (9)$$

It is hard to obtain the ergodic secrecy capacity. We will give some numerical results in the following section.

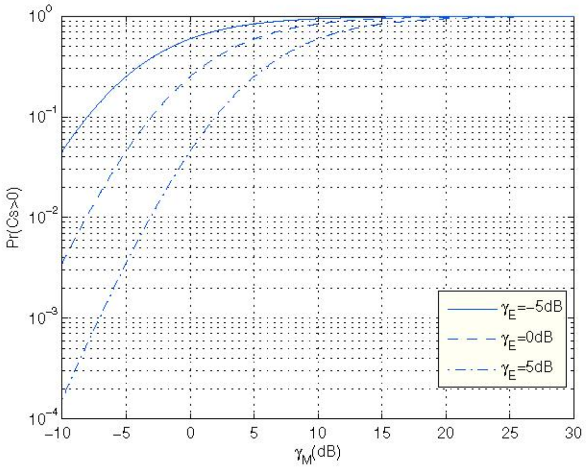

Fig. 2. The probability of the non-zero secrecy capacity versus $\bar{\gamma}_M$, $N = 3$, the probability increases with $\bar{\gamma}_M$

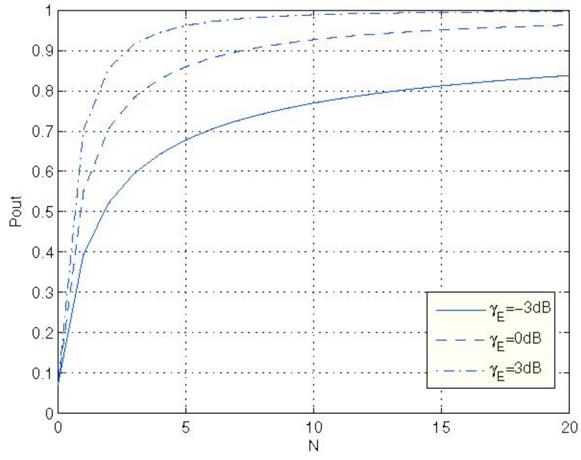

Fig. 4. The outage probability versus N, $R_s = 0.1, \bar{\gamma}_M = 0dB$, the outage probability increase with N.

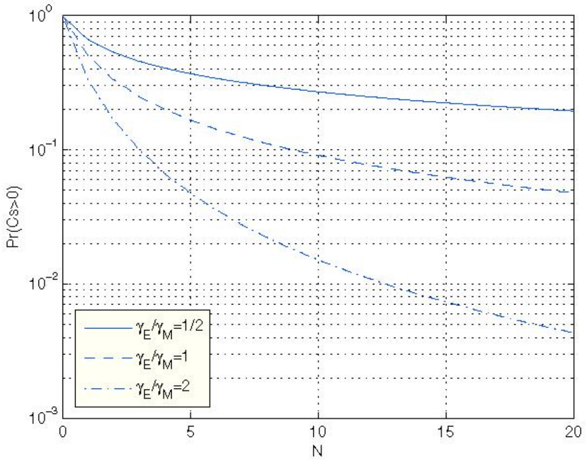

Fig. 3. The probability of the non-zero secrecy capacity versus N, $\bar{\gamma}_M = 0dB$, the probability decreases with N.

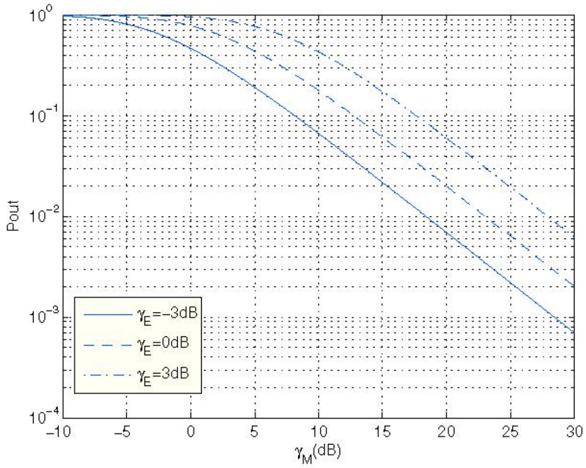

Fig. 5. The outage probability versus $\bar{\gamma}_M$, $R_s = 0.1, N = 3$, the outage probability decrease with $\bar{\gamma}_M$.

IV. Numerical Results

Fig.2 and Fig.3 depict the probability of non-zero secrecy capacity. The results are obtained from Eq. (6). Fig.2 shows the probability versus $\bar{\gamma}_M$. We see that for a fixed N, the better the main channel, the larger the value of the probability. On the contrary, the probability decreases as $\bar{\gamma}_E$ increases. Fig.3 gives the probability as N increases. For given transmit power, $\bar{\gamma}_E$ and $\bar{\gamma}_M$, we can find that probability of non-zero secrecy capacity decreases as the number of eavesdroppers increases. If $N \to \infty$, $\Pr(C_s > 0) \to 0$. In other words, the transmitter can hardly send any message safely over the main channel as the number of eavesdroppers goes to infinite. From the curve, we find that the non-zero secrecy capacity still exists even when $\bar{\gamma}_M/\bar{\gamma}_E = 0.5$. This result proves the idea that a non-zero secrecy capacity is achievable in the fading channel even when the wiretap channels are better than the main channel (on the average).

The outage probability is depicted in Fig.4 (versus N), Fig.5 (versus $\bar{\gamma}_M$) and Fig.6 (versus R_s), by using Eq. (7). From the curve, it is clear that the outage probability is changing with the number of the eavesdroppers if other parameters, like $\bar{\gamma}_M$, $\bar{\gamma}_E$, R_s are given. If $N \to \infty$, $P_{out}(R_s) \to 1$. This means outage will definitely occur when the number of eavesdroppers goes to infinite. If there is no eavesdropper (N=0), the secure communication will not be broke off, which corresponds to the outage probability of conventional fading channel. We see from Fig. 5 that the outage probability decreases as the main channel becomes better but increases with the average gain of wiretap channel. Also, from Fig. 6, it is easy to find that the larger the secrecy rate, the higher the outage probability. From Eq. (7), it follows that when $R_s \to 0$, $P_{out} \to 1 - \prod_{i=1}^{N} \frac{i}{\theta+i}$, and when $R_s \to \infty$, $P_{out} \to 1$.

The ergodic secrecy capacity is given in Fig. 7 (versus P) and Fig. 8 (versus N) by calculating Eq. (9). We see that the ergodic secrecy capacity increases with P but decreases with N. And, for a given $\bar{\gamma}_M$, ergodic secrecy capacity decreases as $\bar{\gamma}_E$ increases. When $\bar{\gamma}_M/\bar{\gamma}_E = 0.5$, the ergodic secrecy is still greater than zero.

V. Conclusion

In this paper, we have presented the analytical results of secrecy capacity of fading wireless channel with multiple eavesdroppers. We first characterized the existence of the confidential communication over the quasi-static fading channel and then calculated the secrecy capacities in terms of outage capacity and ergodic capacity as well. We have shown that the results in [4] correspond to some special cases of our work.

Appendix
The Proof of Equation (4)

$$\begin{aligned}
&\int_0^\infty \exp(-ax)[1-\exp(-bx)]^N dx \\
&= -\frac{1}{a}\int_0^\infty [1-\exp(-bx)]^N d\exp(-ax) \\
&= -\frac{1}{a}\{\exp(-ax)[1-\exp(-bx)]^N|_0^\infty \\
&- \int_0^\infty \exp(-ax)d[1-\exp(-bx)]^N\} \\
&= \frac{Nb}{a}\int_0^\infty \exp[-(a+b)x][1-\exp(-bx)]^{N-1}dx \\
&= \frac{Nb}{a}\frac{1}{a+b}\int_0^\infty [1-\exp(-bx)]^{N-1}d\exp[-(a+b)x] \\
&= \frac{Nb}{a}\frac{1}{a+b}\int_0^\infty \exp[-(a+b)x]d[1-\exp(-bx)]^{N-1} \\
&= \frac{N(N-1)b^2}{a(a+b)}\int_0^\infty \exp[-(a+2b)x][1-\exp(-bx)]^{N-2}dx.
\end{aligned}$$

Through N steps of similar formulation, we can finally get

$$\int_0^\infty \exp(-ax)[1-\exp(-bx)]^N dx = \frac{1}{a}\prod_{i=1}^{N}\frac{bi}{a+bi}.$$

Acknowledgment

This work is supported by the National Natural Science Foundation of China (No. 60472079 and No. 60572115).

References

[1] C. E. Shannon, "Communication theory of secrecy systems," *Bell System Technical Journal*, vol. 28, pp. 656–715, 1949.

[2] A. D. Wyner, "The wiretap channel," *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975.

[3] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Transactions on Information Theory*, vol. 24, pp. 339–348, 1978.

[4] J. Barros and M. R. D. Rodrigues, "Secrecy capacity of wireless channels," in *proc. IEEE ISIT 2006*, pp. 356–360, July 2006.

[5] P. K. Gopala, L. Lai and H. El Gamal, "On the secrecy capacity of the fading channels," *IEEE Transactions on Information Theory*, submitted.

[6] E. Tekin and A. Yener, "The gaussian multiple access wire-tap channel with collective secrecy constraints," in *proc. IEEE ISIT 2006*, pp.1164–1168, July 2006.

[7] Y. Liang, H. V. Poor and S. Shamai, "Secure communication over fading channels," *IEEE Transactions on Information Theory*, submitted.

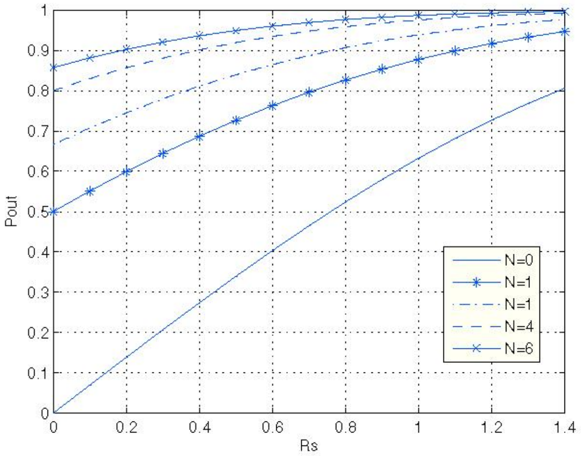

Fig. 6. The outage probability versus R_s, $\bar{\gamma}_M = 0dB, \bar{\gamma}_E = 0dB$, the outage probability increase with R_s.

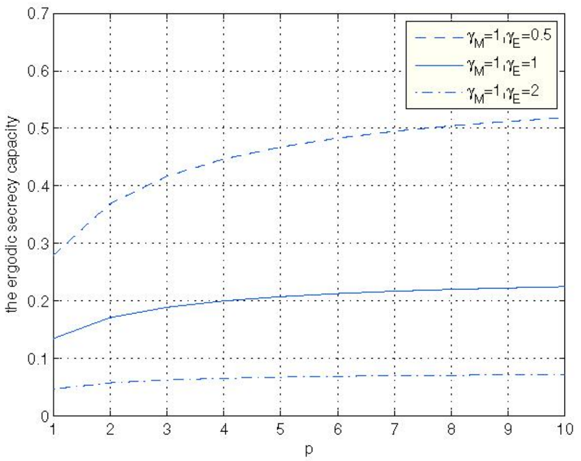

Fig. 7. The ergodic secrecy capacity for different P. N=3. The ergodic secrecy capacity increases with P.

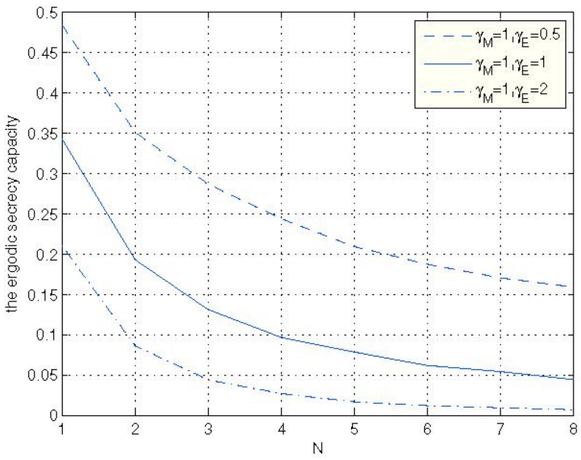

Fig. 8. The ergodic secrecy capacity versus N. P = 0dB. The ergodic secrecy capacity decreases as N increases.