Maximal Ratio Diversity Combining Enhanced Security

Fangming He, *Member, IEEE,* Hong Man, *Senior Member, IEEE,* and Wei Wang, *Member, IEEE*

***Abstract*—In this paper, we present a method of utilizing channel diversity to increase secrecy capacity in wireless communication. With the presence of channel diversity, an intended receiver can achieve a relatively high secrecy capacity even at low SNRs. We present a theoretical analysis on the outage probability at a normalized target secrecy capacity in Rayleigh fading environment. Our numerical results strongly support our conclusion that maximal ratio combining of channel diversity can enhance the security of the wireless communication system in normal operating scenarios.**

***Index Terms*—Physical security, secrecy capacity, diversity.**

I. Introduction

DUE to the broadcast nature of wireless links, it is difficult to prevent an eavesdropper from intercepting wireless communications. The study on physical layer secure communication was pioneered by Shannon [1], Wyner [2], and Leung-Yan-Cheong [3]. Recently, Bloch *et al*. [4] investigated the average secure communication rates and outage probability in a quasi-static Rayleigh fading channel with an eavesdropper observing the transmission through a second independent quasi-statistic fading channel. Liang *et al*. [5] discussed the ergodic secrecy capacity region for fading broadcast channel with confidential messages. Gopala *et al*. [6] studied the secrecy capacity of a block-ergodic fading channel. Oggier and Hassibi [7] derived the perfect secrecy capacity of the MIMO wire-tap channel. Khisti *et al.* [8] and Liu *et al.* [9] characterized the secrecy capacity of the MIMOME channel, in which the sender, receiver and eavesdropper all have multiple antennas. Dong [10], Oohama [11], Yuksel and Erkip [12], Lai and El Gamal [13] discussed various strategies for a relay node to enhance the secrecy of a wire-tap channel.

An observation from these studies is that the secrecy capacity decreases dramatically as the SNR of the legitimate user decreases. In this work, we propose a solution which can take the advantage of possible channel diversity to improve the secrecy capacity, even under very low SNRs. This work extends the system model and outage probability formulation in [4] with maximum ratio diversity combining. It is also related to the MIMO channel models in [5]–[9]. However we focus more on the diversity combining effects instead of power allocation schemes, and we are interested in studying the outage probability at a normalized target secrecy capacity instead of the secrecy capacity itself. The outage probability at a target secrecy capacity in Rayleigh fading environment is analyzed under the assumption of an ideal forwarding strategy.

II. System Model

We consider a wireless network composed of distributed legitimate users as well as eavesdroppers. An eavesdropper (Eve) is able to overhear the information exchange between two legitimate users (Alice and Bob). According to [4], which follows the previous results of [3], the secrecy capacity C_s in this scenario can be expressed as

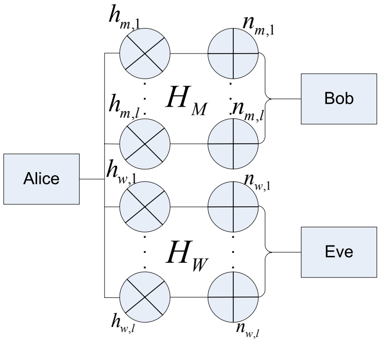

Fig. 1. Diagram of the system model.

$$C_s = C_M - C_W, \tag{1}$$

where C_M is the capacity of the main channel, and C_W is the capacity of the eavesdropper's channel. This expression is also consistent with the conclusions of [2], [4], [6], [7].

If Bob can identify or establish multiple independent channels with Alice, as shown in Fig.1, the main channel capacity C_M can be improved by employing diversity combining techniques. From equation (1), we can see that such increase in C_M can lead to an increase in the overall secrecy capacity C_s. Furthermore, as a security strategy, one can slightly decrease the transmitting power of Alice so to reduce C_W, and still maintain an acceptable level of C_M by exploiting diversity combining.

A possible mechanism to obtain multiple channels between Alice and Bob is through MIMO or virtual MIMO. In virtual MIMO, several relay nodes will receive messages from Alice and forward them to Bob or Eve. Such relay nodes can be prefigured or negotiated on-the-fly, and they do not have to access the message content. A proper access control protocol can be employed to minimize the chance for Eve to obtain such cooperative relays. In normal operating scenarios, we assume that the legitimate users have better chance to acquire channel diversity through cooperative relays than the eavesdroppers.

III. Maximal Ratio Combining Enhanced Security

In our study, all channels are subjected to Rayleigh fading. According to [14], the PDF of the SNR under Maximal Ratio Combining (MRC) for Rayleigh Channels is expressed as

$$\begin{aligned} p(\gamma_M) &= \frac{\gamma_M^{L_M-1} e^{-\gamma_M/\bar{\gamma}_M}}{\bar{\gamma}_M^{L_M}(L_M-1)!}, \qquad &(\gamma_M > 0) \\ p(\gamma_W) &= \frac{\gamma_W^{L_W-1} e^{-\gamma_W/\bar{\gamma}_W}}{\bar{\gamma}_W^{L_W}(L_W-1)!}, \qquad &(\gamma_W > 0). \end{aligned} \tag{2}$$

Manuscript received November 29, 2010. The associate editor coordinating the review of this letter and approving it for publication was I. Maric.

The authors are with the Department of Electrical and Computer Engineering, Stevens Institute of Technology, Hoboken, NJ, 07030 USA (e-mail: fhe, hman, wwang3@stevens.edu).

Digital Object Identifier 10.1109/LCOMM.2011.030911.102343

1089-7798/11$25.00 © 2011 IEEE

γ_M, γ_W, $\bar{\gamma}_M$ and $\bar{\gamma}_W$ are the SNR and the average SNR of the main channel and eavesdropper channel respectively; L_M and L_W are their diversity orders.

Based on the definition of strictly positive secrecy capacity in [1], the probability of achieving it under the MRC technique is

$$\begin{aligned}
P(C_s > 0) &= P(\gamma_M > \gamma_W) \\
&= \int_0^{\infty}\int_0^{\gamma_M} \frac{\gamma_M^{L_M-1}e^{-\frac{\gamma_M}{\bar{\gamma}_M}}}{(L_M-1)!\bar{\gamma}_M^{L_M}} \frac{\gamma_W^{L_W-1}e^{-\frac{\gamma_W}{\bar{\gamma}_W}}}{(L_W-1)!\bar{\gamma}_W^{L_W}} d\gamma_W d\gamma_M \\
&= \int_0^{\infty} \frac{\gamma_M^{L_M-1}e^{-\frac{\gamma_M}{\bar{\gamma}_M}}}{(L_M-1)!\bar{\gamma}_M^{L_M}} [1 - e^{\frac{\gamma_M}{\bar{\gamma}_W}} \sum_{k=0}^{L_W-1} \frac{(\frac{\gamma_M}{\bar{\gamma}_W})^k}{k!}] d\gamma_M \\
&= 1 - \sum_{k=0}^{L_W} \frac{(L_M+k-1)!(\frac{1}{\bar{\gamma}_W})^k(\frac{1}{\bar{\gamma}_M})^{L_M}}{(L_M-1)!k!(\frac{1}{\bar{\gamma}_M}+\frac{1}{\bar{\gamma}_W})^{L_M+k}} \qquad (3) \\
&\quad \int_0^{\infty} \frac{(\frac{1}{\bar{\gamma}_M}+\frac{1}{\bar{\gamma}_W})^{L_M+k}}{(L_M+k-1)!} \gamma_M^{L_M+k-1} e^{-\gamma_M(\frac{1}{\bar{\gamma}_M}+\frac{1}{\bar{\gamma}_W})} d\gamma_M \\
&= 1 - \sum_{k=0}^{L_W-1} \binom{L_M+k-1}{k} \frac{(\bar{\gamma}_M)^k \bar{\gamma}_W^{L_M}}{(\bar{\gamma}_M+\bar{\gamma}_W)^{L_M+k}}.
\end{aligned}$$

The last step in equation (3) is derived from Γ distribution.

For the expected normalized secrecy capacity R_s, the outage probability [4] is defined as

$$\begin{aligned}
P_{out}(R_s) &= P_{out}(C_s < R_s) \\
&= P(C_s < R_s|\gamma_M > \gamma_W)P(\gamma_M > \gamma_W) + P(\gamma_M < \gamma_W).
\end{aligned} \qquad (4)$$

From Appendix A, we get

$$\begin{aligned}
P(C_s < R_S|\gamma_M > \gamma_W) = A \sum_{k=0}^{L_M-1} \binom{L_W+k-1}{k} \frac{\bar{\gamma}_W^k \bar{\gamma}_M^{L_W}}{(\bar{\gamma}_W+\bar{\gamma}_M)^{L_W+k}} \\
- \frac{Ae^{-\frac{2^{R_s}-1}{\bar{\gamma}_M}}}{(L_W-1)!} \sum_{k=0}^{L_M-1}\sum_{n=0}^{k} \frac{\binom{k}{n}2^{nR_s}(2^{R_s}-1)^{k-n}(L_W+n-1)!\bar{\gamma}_W^n}{k!\bar{\gamma}_M^{k-L_w-n}(\bar{\gamma}_M+2^{R_s}\bar{\gamma}_W)^{L_W+n}},
\end{aligned} \qquad (5)$$

where $A = 1/P(\gamma_M > \gamma_W)$.

To substitute (3) and (5) into (4), we formulate the outage probability of the secrecy capacity as

$$\begin{aligned}
P_{out}(R_s) = &\sum_{k=0}^{L_W-1} \binom{L_M+k-1}{k} \frac{\bar{\gamma}_M^k \bar{\gamma}_W^{L_M}}{(\bar{\gamma}_M+\bar{\gamma}_W)^{L_M+k}} \\
&+ \sum_{k=0}^{L_M-1} \binom{L_W+k-1}{k} \frac{\bar{\gamma}_W^k \bar{\gamma}_M^{L_W}}{(\bar{\gamma}_W+\bar{\gamma}_M)^{L_W+k}} \\
- \frac{e^{-\frac{2^{R_s}-1}{\bar{\gamma}_M}}}{(L_W-1)!} &\sum_{k=0}^{L_M-1}\sum_{n=0}^{k} \frac{\binom{k}{n}2^{nR_s}(2^{R_s}-1)^{k-n}(L_W+n-1)!\bar{\gamma}_W^n}{k!\bar{\gamma}_M^{k-L_W-n}(\bar{\gamma}_M+2^{R_s}\bar{\gamma}_W)^{L_W+n}}.
\end{aligned} \qquad (6)$$

The first term in (6) is the probability of $P(\gamma_M < \gamma_W)$ and the following two terms are boundaries of $P(C_s < R_s)$ under $\gamma_M > \gamma_W$.

It is important to examine the asymptotic behavior of the outage probability for the target secrecy rate R_s. When $L_W = 1$ and $L_M \gg L_W$, equation (6) becomes

$$\begin{aligned}
&P_{out}(R_s) = \\
&1 - e^{-\frac{2^{R_s}-1}{\bar{\gamma}_M}} \sum_{k=0}^{L_M-1}\sum_{n=0}^{k} \frac{(k-n)!2^{nR_s}(2^{R_s}-1)^{k-n}\bar{\gamma}_W^n}{\bar{\gamma}_M^{k-n-1}(\bar{\gamma}_M+2^{R_s}\bar{\gamma}_W)^{n+1}}.
\end{aligned} \qquad (7)$$

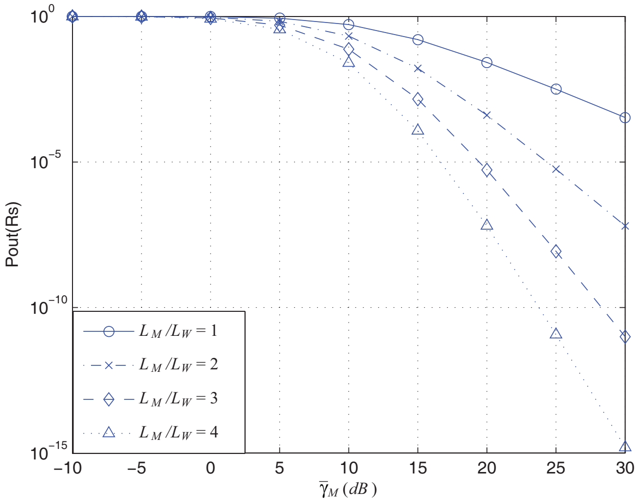

Fig. 2. $P_{out}(R_s = 0.1)$ V.S. $\bar{\gamma}_M$ various L_M/L_W.

It indicates the outage probability of the secrecy capacity when the acquired diversity in the intended receiver is much higher than that of eavesdroppers.

In the case of $\bar{\gamma}_M \gg \bar{\gamma}_W$, the outage probability can be expressed as

$$\begin{aligned}
P_{out}(R_s) = &\sum_{k=0}^{L_M-1} \binom{L_W+k-1}{k} (\frac{\bar{\gamma}_W}{\bar{\gamma}_M})^k \\
&+ \sum_{k=0}^{L_W-1} \binom{L_M+k-1}{k} (\frac{\bar{\gamma}_W}{\bar{\gamma}_M})^{L_M} - \frac{e^{-\frac{2^{R_s}-1}{\bar{\gamma}_M}}}{(L_W-1)!} \qquad (8) \\
&\sum_{k=0}^{L_M-1}\sum_{n=0}^{k} \frac{\binom{k}{n}(2^{R_s}\bar{\gamma}_W)^n(2^{R_s}-1)^{k-n}(L_W+n-1)!}{\bar{\gamma}_M^{k-1}k!}.
\end{aligned}$$

IV. Numerical Results and Discussions

Figure 2 shows the outage probability $P_{out}(R_s)$ of the expected secrecy capacity $R_s = 0.1$ for $L_W = 2$ and $\bar{\gamma}_W = 10dB$ under different $\bar{\gamma}_M$ and ratios of L_M/L_W. It illustrates that $P_{out}(R_s)$ decreases with the increase of the diversity order. In the extreme case that the available diversity for intended receiver is much larger than that of eavesdropper (i.e. $L_M/L_W \to \infty$), $P_{out}(R_s) \to 0$.

Figure 3 shows the outage probability with two different R_s ($R_s = 0.1$ and $R_s = 1$) as functions of $\bar{\gamma}_M$ under different $\bar{\gamma}_M$. Here, L_M and L_W are fixed to be 4 and 2 respectively. It could be observed that the outage probability under $R_s = 0.1$ is always lower than that under $R_s = 1$. It also depicts that the higher $\bar{\gamma}_M$, the lower outage probability; and the higher $\bar{\gamma}_W$, the higher the probability of an outage. With respect to the asymptotic behavior of the outage secrecy capacity, it may be observed that when $\bar{\gamma}_M \gg \bar{\gamma}_W$ and $\bar{\gamma}_M \to \infty$, $P_{out}(R_s) \to 0$. Therefore, for the wireless channel with a low SNR, we can utilize the diversity to increase $\bar{\gamma}_M$ and improve the secrecy capacity.

V. Conclusion

Based on our formulation and numerical results, we conclude that legitimate users can take advantage of possible cooperative diversities to increase the secrecy capacity. In order

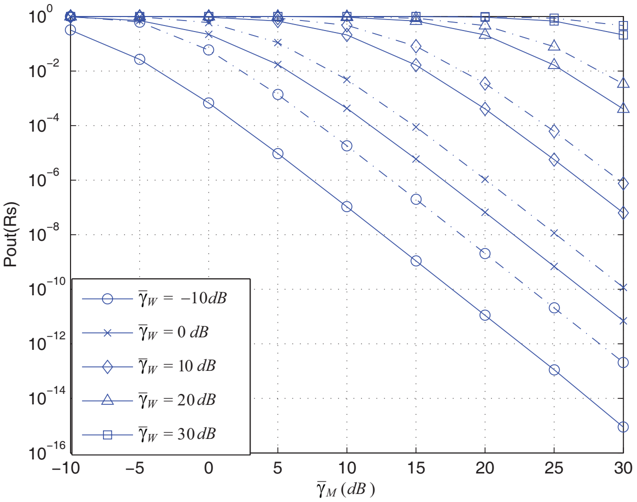

Fig. 3. $P_{out}(R_s = 0.1)$ (solid line) and $P_{out}(R_s = 1)$ (dash line) V.S. $\bar{\gamma}_M$ with various $\bar{\gamma}_W$.

to obtain the target secrecy capacity with a reasonably low outage probability, we can adjust the transmission power and diversity order. Increasing the diversity order can effectively reduce the outage probability of a normalized target secrecy capacity.

Appendix A

From [4], we can get

$$\begin{aligned}
&P(C_s < R_s|\gamma_M > \gamma_W)\\
&= \int_0^{\infty}\int_{\gamma_W}^{2^{R_s}(1+\gamma_W)-1} p(\gamma_M, \gamma_W|\gamma_M > \gamma_W)d\gamma_W d\gamma_M\\
&= A\int_0^{\infty}\int_{\gamma_W}^{2^{R_s}(1+\gamma_W)-1} \frac{\gamma_W^{L_W-1}e^{-\frac{\gamma_W}{\bar{\gamma}_W}}}{(L_W-1)!\bar{\gamma}_W^{L_W}}\frac{\gamma_M^{L_M-1}e^{-\frac{\gamma_M}{\bar{\gamma}_M}}}{(L_M-1)!\bar{\gamma}_M^{L_M}}d\gamma_M d\gamma_W,
\end{aligned} \tag{9}$$

where $A = 1/[1 - \sum_{k=0}^{L_W-1}\frac{(L_M+k-1)!}{(L_M-1)!k!}\frac{(\bar{\gamma}_M)^k\bar{\gamma}_W^{L_M}}{(\bar{\gamma}_M+\bar{\gamma}_W)^{L_M+k}}]$. To simplify the calculation, we may calculate the lower bound $(\gamma_M = \gamma_W)$ and the upper bound $(\gamma_M = 2^{R_s}(1+\gamma_W)-1)$ respectively. For the lower bound, it is

$$\begin{aligned}
F_1 =& - A\sum_{k=0}^{L_M-1}\int_0^{\infty}\frac{\gamma_W^{L_W+k-1}e^{-\gamma_W(\frac{1}{\bar{\gamma}_W}+\frac{1}{\bar{\gamma}_M})}}{(L_W-1)!k!\bar{\gamma}_W^{L_W}\bar{\gamma}_M^k}d\gamma_W\\
=& - A\sum_{k=0}^{L_M-1}\frac{(L_W+k-1)!\frac{1}{(\frac{1}{\bar{\gamma}_W}+\frac{1}{\bar{\gamma}_M})^{L_W+k}}}{(L_W-1)!k!\bar{\gamma}_W^{L_W}\bar{\gamma}_M^k}\\
&\int_0^{\infty}\frac{(\frac{1}{\bar{\gamma}_W}+\frac{1}{\bar{\gamma}_M})^{L_W+k}\gamma_W^{L_W+k-1}e^{-\gamma_W(\frac{1}{\bar{\gamma}_W}+\frac{1}{\bar{\gamma}_M})}}{(L_W+k-1)!}d\gamma_W\\
=& - A\sum_{k=0}^{L_M-1}\frac{(L_W+k-1)!}{(L_W-1)!k!}\frac{\bar{\gamma}_W^k\bar{\gamma}_M^{L_W}}{(\bar{\gamma}_W+\bar{\gamma}_M)^{L_W+k}}.
\end{aligned} \tag{10}$$

Similarly, the upper bound can be formulated as

$$\begin{aligned}
F_2 =& - A\int_0^{\infty}\frac{\gamma_W^{L_W-1}e^{-\frac{\gamma_W}{\bar{\gamma}_W}}e^{-\frac{a(1+\gamma_W)-1}{\bar{\gamma}_M}}}{(L_W-1)!\bar{\gamma}_W^{L_W}}\\
&\sum_{k=0}^{L_M-1}\frac{[a(1+\gamma_W)-1]^k}{k!\bar{\gamma}_M^k}d\gamma_W.
\end{aligned} \tag{11}$$

where $a = 2^{R_s}$. Based on Binomial Distribution, we can get

$$\begin{aligned}
F_2 =& - \frac{Ae^{-\frac{a-1}{\bar{\gamma}_M}}}{(L_W-1)!\bar{\gamma}_W^{L_W}}\sum_{k=0}^{L_M-1}\\
&\int_0^{\infty}e^{-\gamma_W(\frac{1}{\bar{\gamma}_W}+\frac{a}{\bar{\gamma}_M})}\gamma_W^{L_w-1}\frac{\sum_{n=0}^{k}\binom{k}{n}a^n\gamma_W^n(a-1)^{k-n}}{k!\bar{\gamma}_M^{k-1}}d\gamma_W\\
=& - \frac{Ae^{-\frac{a-1}{\bar{\gamma}_M}}}{(L_W-1)!\bar{\gamma}_W^{L_W}}\sum_{k=0}^{L_M-1}\sum_{n=0}^{k}\frac{\binom{k}{n}a^n(a-1)^{k-n}(L_W+n-1)!}{k!\bar{\gamma}_M^k(\frac{1}{\bar{\gamma}_W}+\frac{a}{\bar{\gamma}_M})^{L_W+n}}\\
&\int_0^{\infty}\frac{e^{-\gamma_W(\frac{1}{\bar{\gamma}_W}+\frac{a}{\bar{\gamma}_M})}\gamma_W^{L_W+n-1}(\frac{1}{\bar{\gamma}_W}+\frac{a}{\bar{\gamma}_M})^{L_W+n}}{(L_W+n-1)!}d\gamma_W.
\end{aligned} \tag{12}$$

According to the Γ distribution, F_2 can be written as

$$\begin{aligned}
&F_2 =\\
&-\frac{Ae^{-\frac{a-1}{\bar{\gamma}_M}}}{(L_W-1)!}\sum_{k=0}^{L_M-1}\sum_{n=0}^{k}\frac{\binom{k}{n}a^n(a-1)^{k-n}(L_W+n-1)!\bar{\gamma}_W^n}{k!\bar{\gamma}_M^{k-L_W-n}(\bar{\gamma}_M+a\bar{\gamma}_W)^{L_W+n}}.
\end{aligned} \tag{13}$$

Then, we can get

$$\begin{aligned}
&P(C_s < R_S|\gamma_M > \gamma_W)\\
=&A\sum_{k=0}^{L_M-1}\binom{L_W+k-1}{k}\frac{\bar{\gamma}_W^k\bar{\gamma}_M^{L_W}}{(\bar{\gamma}_W+\bar{\gamma}_M)^{L_W+k}}\\
&-\frac{Ae^{-\frac{a-1}{\bar{\gamma}_M}}}{(L_W-1)!}\sum_{k=0}^{L_M-1}\sum_{n=0}^{k}\frac{\binom{k}{n}a^n(a-1)^{k-n}(L_W+n-1)!\bar{\gamma}_W^n}{k!\bar{\gamma}_M^{k-L_w-n}(\bar{\gamma}_M+a\bar{\gamma}_W)^{L_W+n}}.
\end{aligned} \tag{14}$$

References

[1] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Techn. J.*, vol. 28, pp. 656–715, Oct. 1949.

[2] A. D. Wyner, "The wire-tap channel," *Bell Syst. Techn. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[3] S. Leung-Yan-Cheong and M. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 24, no. 4, pp. 451–456, July 1978.

[4] M. Bloch, J. Barros, M. Rodrigues, and S. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, 2008.

[5] Y. Liang, H. Poor, and S. Shamai, "Secure communication over fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2470–2492, 2008.

[6] P. Gopala, L. Lai, and H. El Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4687–4698, 2008.

[7] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," in *Proc. IEEE International Symposium on Information Theory*, 2008, pp. 524–528.

[8] A. Khisti and G. Wornell, "The MIMOME channel," in *Proc. 45th Allerton Conference on Communication, Control and Computing*, Sep. 2007, pp. 625–632.

[9] T. Liu and S. Shamai, "A note on the secrecy capacity of the multiple-antenna wiretap channel," *IEEE Trans. Inf. Theory*, vol. 55, no. 6, pp. 2547–2553, 2009.

[10] L. Dong, Z. Han, A. Petropulu, and H. Poor, "Secure wireless communications via cooperation," in *Proc. 46th Annual Allerton Conference on Communication, Control, and Computing*, Sep. 2008, pp. 1132–1138.

[11] Y. Oohama, "Coding for relay channels with confidential messages," in *Proc. IEEE Information Theory Workshop*, 2001, pp. 87–89.

[12] M. Yuksel and E. Erkip, "Secure communication with a relay helping the wire-tapper," in *Proc. IEEE Information Theory Workshop*, 2007, pp. 595–600.

[13] L. Lai and H. El Gamal, "Cooperative secrecy: the relay-eavesdropper channel," in *Proc. IEEE International Symposium on Information Theory*, 2007, pp. 931–935.

[14] A. Goldsmith, *Wireless Communication*. Cambridge University Press, pp. 199–200, Aug. 2005.