On Secure Beamforming for Wiretap Channels with Partial Channel State Information at the Transmitter

Pin-Hsun Lin*, Shih-Chun Lin†, Szu-Hsiang Lai* and Hsuan-Jung Su*
* Department of Electrical Engineering and Graduate Institute of Communication Engineering
National Taiwan University, Taipei, Taiwan 10617
† Department of Electrical Engineering, National Taiwan University of Science and Technology, Taipei, Taiwan 10607
*pinhsunlin@gmail.com, †sclin2@ntu.edu.tw, *r98942061@ntu.edu.tw, *hjsu@cc.ee.ntu.edu.tw

***Abstract*— In this paper, we consider the secure transmission in ergodic fast fading multiple-input single-output single-antenna-eavesdropper (MISOSE) wiretap channels with only the statistics of eavesdropper's channel state information at the transmitter (CSIT). Two kinds of the legitimate CSIT are assumed, that is, full and statistical legitimate CSIT. With full legitimate CSIT, we generalize and optimize the previously proposed artificial noise (AN) aided secure beamforming to improve its secrecy rate performance. The AN covariance matrix in our scheme is more flexible than previous scheme and the region of non-zero secrecy rate is enlarged significantly according to our simulations. For the case with statistical legitimate CSIT, we further prove that the secure beamforming is secrecy capacity achieving for the Rayleigh faded channels. In this case, the AN is not necessary. Extensions to cases where legitimate receiver and eavesdropper have multiple antennas will also be discussed.**

I. Introduction

In a wiretap channel, a source node wishes to transmit confidential messages securely to a legitimate receiver and to keep the eavesdropper as ignorant of the message as possible. As a special case of the broadcast channels with confidential messages [1], Wyner [2] characterized the secrecy capacity of the discrete memoryless wiretap channel. The secrecy capacity is the largest rate communicated between the source and destination nodes with the eavesdropper knowing no information of the messages. Motivated by the demand of high data rate transmission and improving the connectivity of the network [3], the multiple antenna systems with security concern are considered by several authors. Shafiee and Ulukus [4] first proved the secrecy capacity of a Gaussian channel with two-input, two-output, single-antenna-eavesdropper. The authors of [5]–[7] proved the secrecy capacity of a Gaussian multiple-input multiple-output (MIMO), multiple-antenna-eavesdropper channel using different techniques. Moreover, due to the characteristics of wireless channels, the impacts of fading channels on the secrecy transmission were considered in [5], [8] with full channel state information at the transmitter (CSIT). Considering practical issues, the perfect CSIT may not be available. Several papers discussed the partial CSIT issue [5], [9]–[13]. However, the secrecy capacities for channels with partial CSIT are known only for the limited case [11] where the transmitter has single antenna with block fading.

In this paper, we consider an important type of wiretap channels with partial CSIT, namely, the multiple-input multiple-output single-antenna-eavesdropper (MISOSE) fast faded wiretap channel with only the channel statistics information of the eavesdropper known at the transmitter. The transmitter is assumed to have the statistics or the full knowledge of the legitimate receiver's channel. In both cases, the secure beamformings are adopted as transmission schemes. However, in the full legitimate CSIT case, we adopt the celebrated artificial noise (AN) assisted secure beamforming [10] [5]. This signaling can also be treated as one kind of linear prefixing where the channel input is the message-bearing signal plus the AN, and the AN is aimed to disrupt the eavesdropper's reception. However, we remove the restriction in [10] [5] where the AN must be allocated in the null space of the main channel. Thus our scheme is a generalized scheme of that in [10] [5].

The main contributions of this paper are twofold. For the statistical legitimate CSIT case, we show that the secure beamforming is secrecy capacity achieving. To prove that, we propose a new secrecy capacity upper bound. Then we analytically solve the optimal channel input covariance matrix to fully characterize the secrecy capacity, while such an optimization problem is solved numerically in [13] without guaranteeing the optimality. For the full legitimate CSIT case, we show that the complicated covariance matrix optimization problem for the message bearing signal and the AN can be simplified as a power allocation problem. Based on our results, we show that the AN selected in [10] is suboptimal. The simplification is based on the following two facts. First, the eigenvectors of the optimal covariance matrices of both message-bearing signal and generalized AN are the same, which equals to the right singular vectors of the main channel *. Second, the power of AN should be allocated uniformly over these eigenvectors. Contrary to [10], we provide rigorous proofs for these facts. Simulation results verifies the above claim, especially the non-zero rate region is enlarged. Note that the secure connectivity in a network is assured by the

This work was supported by the National Science Council, Taiwan, R.O.C., under grant NSC 101-2221-E-027-085-MY3, 100-2628-E-007-025-MY3, and 100-2221-E-002-133

*_main_ channel is also called _legitimate_ channel in this paper

non-zero secrecy rate of the transmitter-receiver pairs [3]. Thus our scheme is very useful for the large scale wireless network application, which is an important application of the MISOSE wiretap channel [3]. Finally, we will also discuss the extensions of our MISOSE results to the cases where the legitimate receiver and/or eavesdropper has multiple antennas.

The rest of the paper is organized as follows. In Section II we introduce the considered system model. In Section III we prove the capacity of the fast fading MISOSE wiretap channel when the transmitter only knows the statistics of both channels. In Section IV, we provide an achievable secrecy rate of the fast fading MISOSE wiretap channel when there is full CSIT of the main channel but the transmitter only knows the statistics of the eavesdropper's channel. The extensions to multiple received antennas in given in Section V. In Section VI we demonstrate the simulation results. Finally, Section VII concludes this paper.

II. System Model

We consider the following MISOSE system model where the transmitter has n_t[†] antennas, while the legitimate receiver and eavesdropper each has singe antenna as

$$y = \mathbf{h}^H \mathbf{x} + n_1, \tag{1}$$

$$z = \mathbf{g}^H \mathbf{x} + n_2, \tag{2}$$

where n_1 and n_2 are circularly symmetric complex additive white Gaussian noises with unit variance, respectively. We also assume the power constraint such that

$$\mathrm{tr}(E[\mathbf{x}\mathbf{x}^H]) \leq P_T. \tag{3}$$

In this MISOSE system model, we assume that only the channel statistics of the eavesdropper is known at transmitter. The legitimate receiver knows the realizations of $\mathbf{h}$ while the eavesdropper knows both the realizations of $\mathbf{h}$ and $\mathbf{g}$. The MISOSE secrecy capacity is defined as

Definition 1 (Secrecy Capacity [2] [14] [11]): Perfect secrecy is achievable with rate R if, for any $\varepsilon' > 0$, there exists a sequence of $(2^{NR}, N)$-codes and an integer N_0 such that for any $N > N_0$

$$I(w; z^N, \mathbf{h}^N, \mathbf{g}^N)/N < \varepsilon', \tag{4}$$

$$\text{and} \quad \Pr(\hat{w} \neq w) \leq \varepsilon',$$

where w is the secret message.

The **secrecy capacity** *C_s is the supremum of all achievable secrecy rates.*

[†]In this paper, lower and upper case bold alphabets denote vectors and matrices, respectively. The superscript $(.)^H$ denotes the transpose complex conjugate. $|\mathbf{A}|$ and $|a|$ represent the determinant of the square matrix $\mathbf{A}$ and the absolute value of the scalar variable a, respectively. A diagonal matrix whose diagonal entries are $a_1 \ldots a_k$ is denoted by $diag(a_1 \ldots a_k)$. The trace of $\mathbf{A}$ is denoted by $\mathrm{tr}(\mathbf{A})$. We define $C(x) \triangleq \log(1+x)$ and $(x)^+ \triangleq \max\{0, x\}$. The mutual information between two random variables is denoted by $I(;)$. $\mathbf{I}_n$ denotes the n by n identity matrix. $A \succ 0$ and $A \succeq 0$ denote the set of positive definite and positive semi-definite matrices, respectively. $\otimes$ denotes the Kronerker product.

From Csiszár and Körner's seminal work [1], we know that the discrete memoryless channel secrecy capacity is

$$C_s = \max_{U \to \mathbf{x} \to (y,\mathbf{h}),(z,\mathbf{h},\mathbf{g})} I(U; y, \mathbf{h}) - I(U; z, \mathbf{h}, \mathbf{g}), \tag{5}$$

where U is a auxiliary random variable. However, the optimal choice of U of considered fast fading MISOSE channels are *unknown*.

III. Fast fading MISOSE channels with statistical CSIT of the main channel

With only statistical CSIT of the legitimate channel $\mathbf{h}$, (5) becomes

$$C_s = \max_{U \to \mathbf{x} \to (y,\mathbf{h}),(z,\mathbf{h},\mathbf{g})} I(U; y|\mathbf{h}) - I(U; z|\mathbf{g}). \tag{6}$$

It results from the fact that the transmitter does not have the knowledge of $\mathbf{h}$ and $\mathbf{g}$. In this section, we consider the Rayleigh fading channels, where $\mathbf{h} \sim CN(0, \sigma_{\mathbf{h}}^2 \mathbf{I}_{n_t})$ and $\mathbf{g} \sim CN(0, \sigma_{\mathbf{g}}^2 \mathbf{I}_{n_t})$. We will first show that the optimal auxiliary random variable is $U \equiv \mathbf{x}$ (no prefixing) as the following Theorem.

Theorem 1: For the MISOSE fast Rayleigh fading wiretap channel (1)(2) with the statistical CSIT of $\mathbf{h}$ and $\mathbf{g}$, using Gaussian $\mathbf{x}$ without prefixing $U \equiv \mathbf{x}$ is the optimal transmission strategy

We provide the sketch of proof here. From [13], we know that using Gaussian $\mathbf{x}$ without prefixing can serves as a secrecy capacity lower-bound. Now we focus on the secrecy capacity upper bound. The key for establishing such an upper bound is introducing an same marginal legitimate channel $p(y', \mathbf{h}'|\mathbf{x})$ for (1), which is formed by replacing $\mathbf{h}$ in y with $\mathbf{h}' = (\sigma_{\mathbf{h}}/\sigma_{\mathbf{g}})\mathbf{g}$ as

$$\begin{aligned} y' &= (\mathbf{h}')^H \mathbf{x} + n_y \\ &= (\sigma_{\mathbf{h}}/\sigma_{\mathbf{g}}) \mathbf{g}^H \mathbf{x} + n_y. \end{aligned} \tag{7}$$

Then the secrecy capacity upper bound of [1] can be applied. This upper bound will match the lower bound in [13], and validate our claim in Theorem 1.

From above, we know that secure beamforming (no prefixing) is optimal. Now we find the capacity achieving channel input covariance matrix for the secure beamforming.

Theorem 2: For the MISOSE secrecy capacity optimization problem

$$\max_{\Sigma_{\mathbf{x}}} \left(\mathbb{E}_{\mathbf{h}} \left[\log \left(1 + \mathbf{h}^H \Sigma_{\mathbf{x}} \mathbf{h} \right) \right] - \mathbb{E}_{\mathbf{g}} \left[\log \left(1 + \mathbf{g}^H \Sigma_{\mathbf{x}} \mathbf{g} \right) \right] \right), \tag{8}$$

the optimal $\Sigma_{\mathbf{x}} = \mathbf{U}\mathbf{D}\mathbf{U}^H$ happens when $\mathbf{D}$ is a scaled identity matrix.

We also provide sketch of proof here. Since all entries of both $\mathbf{h}$ and $\mathbf{g}$ are i.i.d., we can express $\mathbf{h} = a\mathbf{g}$, where $a = \sigma_{\mathbf{h}}/\sigma_{\mathbf{g}}$. Then (8) becomes

$$\max_{\Sigma_{\mathbf{x}}} \left(\mathbb{E}_{\mathbf{g}} \left[\log \left(1 + a^2 \mathbf{g}^H \mathbf{D} \mathbf{g} \right) \right] - \mathbb{E}_{\mathbf{g}} \left[\log \left(1 + \mathbf{g}^H \mathbf{D} \mathbf{g} \right) \right] \right), \tag{9}$$

Recall that composition with affine function preserves convexity [15], i.e., if f is convex, then $f(Ax+b)$ is convex. Thus if

$$f \triangleq \log\det\left(\mathbf{I} + a^2 \mathbf{D}\right) - \log\det(\mathbf{I} + \mathbf{D}),$$

is concave in $\mathbf{D}$, we know that C_s is also concave of $\mathbf{D}$. The fact that f is concave can be proved via methods in [15, p.74]. Therefore C_s is concave of $\mathbf{D}$. Moreover, we can show that C_s is Schur concave in $\mathbf{D}$. Then we know that the optimal $\mathbf{D}$ is a scaled identity matrix, that is, the uniform power allocation over transmit antenna is optimal.

IV. Fast fading MISOSE channels with full CSIT of the main channel

When there is full CSIT of the main channel but only the statistical CSIT of the eavesdropper's channel, (5) becomes

$$C_s = \max_{U\rightarrow\mathbf{x}\rightarrow y,(z,\mathbf{h},\mathbf{g})} I(U;y) - I(U;Z|\mathbf{h},\mathbf{g}). \tag{10}$$

For simplicity, in the following we assume $\sigma_{\mathbf{g}}^2 = 1$ and $\mathbf{g} \sim CN(\mathbf{0},\mathbf{I}_{n_t})$ Although suboptimal, we adopt the AN-assisted secure beamforming (linear channel prefixing $p(\mathbf{x}|\mathbf{u})$) as following

$$\mathbf{x} = \mathbf{u} + \mathbf{v} \tag{11}$$

where $\mathbf{u} \sim CN(\mathbf{0},\mathbf{S_u})$ and $\mathbf{v} \sim CN(\mathbf{0},\mathbf{S_v})$ are independent vectors to convey the message and artificial noise, respectively. Substituting (1), (2), and (11) into the right-hand-size (RHS) of (10), we then have the achievable secrecy rate as

$$\max_{\mathbf{S_u},\mathbf{S_v}} \left(\log\left(\frac{1+\mathbf{h}\left(\mathbf{S_u}+\mathbf{S_v}\right)\mathbf{h}^H}{1+\mathbf{h}\mathbf{S_v}\mathbf{h}^H}\right) - \mathbb{E}\left[\log\left(\frac{1+\mathbf{g}^H\left(\mathbf{S_u}+\mathbf{S_v}\right)\mathbf{g}}{1+\mathbf{g}^H\mathbf{S_v}\mathbf{g}}\right)\right]\right)^+, \tag{12}$$

such that $\mathrm{tr}\left(\mathbf{S_u}+\mathbf{S_v}\right) \le P_T$.

Note that in (12), we generalize the AN proposed in [10], which is limited to be in the null space of the main channel, to be transmitted in all possible directions without limitations. By exploring the KKT conditions of (12), we have the following two Theorems.

Theorem 3: For the MISOSE fast faded wiretap channel with the perfect information of the legitimate channel $\mathbf{h}$, and only the mean and covariance matrix of the eavesdropper channel $\mathbf{g} \sim CN(0,\mathbf{I})$ known at the transmitter, the optimal signaling is beamforming in the direction of the legitimate channel. That is, $\mathbf{S_u} = P_U \frac{\mathbf{h}\mathbf{h}^H}{||\mathbf{h}||^2}$, where P_U is the power allocated to messages.

Theorem 4: For the MISOSE fast faded wiretap channel with the perfect information of the legitimate channel $\mathbf{h}$, and only the mean and covariance matrix of the eavesdropper channel $\mathbf{g} \sim CN(0,\mathbf{I})$ known at the transmitter, the optimal power of AN in the null space of the legitimate channel is uniformly allocated. That is, $P_{V_2} = \cdots = P_{V_{n_T}}$.

Due to limited space, we do not prove the above two theorems here. Based on Theorem 3 and 4, we can simplify the optimization problem in (12) as

$$\max_{P_U,P_{V_1},P_{V_2}} \log\left(1+\frac{P_U||\mathbf{h}||^2}{1+P_{V_1}||\mathbf{h}||^2}\right) - E\left[\log\left(1+\frac{P_U\tilde{G}_1}{1+P_{V_1}\tilde{G}_1+P_{V_2}\sum_{i=2}^{n_T}\tilde{G}_i}\right)\right]. \tag{13}$$

An iterative algorithm can be developed to solve the above optimization problem.

V. Extension to Multiple-Input Multiple-Output Multi-Antenna Eavesdropper Channels

In this section, we briefly discuss how to extend the results of previous section to the cases where the legitimate receiver and/or the eavesdropper has multiple antennas. The channel model becomes

$$\mathbf{y} = \mathbf{H}^H\mathbf{x} + \mathbf{n}_1, \tag{14}$$

$$\mathbf{z} = \mathbf{G}^H\mathbf{x} + \mathbf{n}_2,, \tag{15}$$

where $\mathbf{H}$ and $\mathbf{G}$ are the random channel matrices. Again, only the statistics of $\mathbf{G}$ is known at the transmitter. We first consider the case when there is perfect CSIT of the main channel. We can still use the KKT conditions to find the necessary condition of the optimal input covariance matrix of the optimization problem corresponding to (12). The optimal covariance matrix of the message-bearing signal can be shown to have rank smaller or equal to that of the legitimate channel. Similarly, we can found the power allocations of the AN as in Theorem (4). The uniform power allocation in the null space of the legitimate channel is still optimal. Based on these results, the complicated secrecy rate optimization problem can be simiplifed a lot.

For the case when there is only statistical CSIT of the main channel. Our results in Section III can be generalized to the case where the legitimate receiver and eavesdropper have the same number of antenna, and both the two channels undergo the i.i.d. Rayleigh fading. In this case, the same marginal channel as (7) can also be formed, and by extending the derivations in Section III we can also find the secrecy capacity. However, if the two channels are not i.i.d. Rayleigh faded, we cannot replace $\mathbf{H}$ by a scaled version of $\mathbf{G}$ to form the same marginal channel. This case is more involved and is our future work.

VI. Simulation

In this section, with full legitimate CSIT, we first illustrate the performance gain of the proposed transmission scheme over Goel and Negi's scheme [10] in Fig. 1. We use a 2 by 1 by 1 channel as an example. Assume the noise variances are normalized to 1. The channel states we use in the simulation is $||\mathbf{h}||^2 = 0.05$. From Fig. 1, we can easily see that the proposed scheme indeed provides apparent rate gains over Goel and Negi's scheme in moderate SNR regions. Note that the region where the secrecy rate is non-zero is significantly

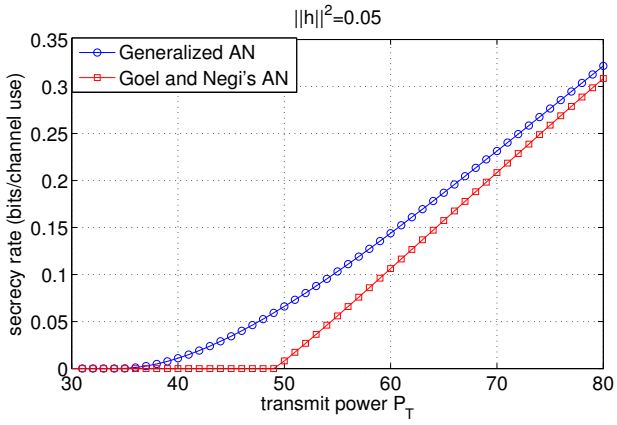

Fig. 1. The secrecy rate versus transmit power with full legitimate CSIT $\mathbf{h}$ and $||\mathbf{h}||^2 = 0.05$.

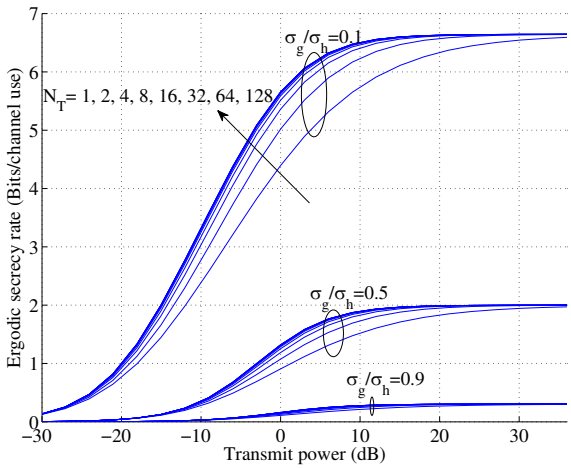

Fig. 2. With only statistical legitimate CSIT, comparison of the secrecy capacities.

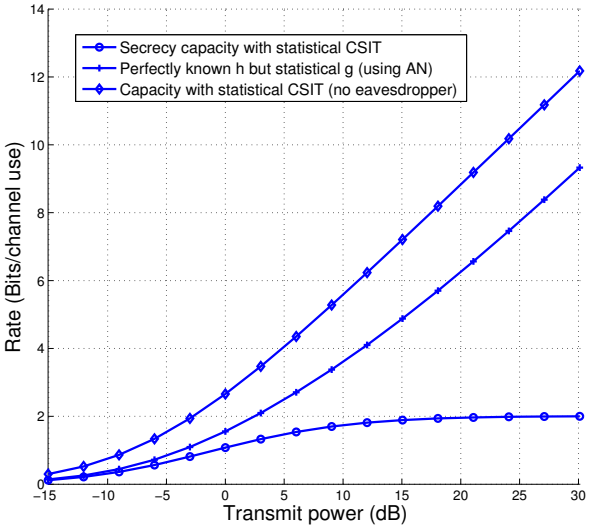

Fig. 3. Comparison of rates in different fast fading channel settings: wiretap channel with statistical CSIT, wiretap channel with perfect CSIT of legitimate channel, and channel with statistical CSIT but without eavesdropper.

enlarged, which is benefit to enhance the connectivity of a secure network [3]. We can find that the rate gains decrease with increasing $||\mathbf{h}||^2$, which is consistent with the results in [9]. We also find that the range of P_T which provides the largest rate gain also decreases with increasing $||\mathbf{h}||^2$. This is because the gain provided by the AN in the signal direction is more evident when the legitimate receiver's received SNR is relatively small compared to that of the eavesdropper.

With only statistical legitimate CSIT, we compare the secrecy capacities in Fig. 2. The secrecy capacities with different N_T's under different $\sigma_{\mathbf{g}}/\sigma_{\mathbf{h}}$ are shown. We can find that the capacities increase with decreasing $\sigma_{\mathbf{g}}/\sigma_{\mathbf{h}}$. Also the secrecy capacity converges to $2\log(\sigma_{\mathbf{h}}/\sigma_{\mathbf{g}})$ when the SNR is high. We can also find that the secrecy capacity converges when N_T is large enough. Finally, we compare secrecy capacities/achievable rates of different channel settings in Fig. 3, where $N_T = 2$ and $\sigma_{\mathbf{g}}/\sigma_{\mathbf{h}} = 0.5$. As expected, the capacity of channel with statistical CSIT but without eavesdropper in [16] is much larger than the MISOSE secrecy capacity with only statistical CSIT. Moreover, unlike our secrecy capacity results, such capacities scale with the SNR. We also plot the achievable secrecy rate of AN-assisted secure beamforming when the transmitter has perfect CSIT of the legitimate channel $\mathbf{h}$ but only statistical CSIT of $\mathbf{g}$. Unlike the secrecy capacity with statistical CSIT of $\mathbf{h}$ and $\mathbf{g}$, the achievable secrecy rates based on perfect CSIT of $\mathbf{h}$ scale with P. It reveals that even only the feedback of the channel state (realization) of the legitimate channel $\mathbf{h}$ is very beneficial to increase the secrecy rate.

VII. Conclusion

In this paper, we studied the performance of secure beamforming in the fast fading MISOSE channels with partial CSIT. We showed that secure beamforming is capacity achieving for the fast fading MISOSE wiretap channels with statistical CSIT of both legitimate and eavesdropper's channels. When the full legitimate CSIT is known, we also generalized Goel and Negi's AN-assisted secure beamforming. Instead of transmitting AN in the null space of the legitimate channel, we considered injecting AN in all directions, including the direction for conveying the dedicated messages. Through simulations, we verified that the proposed scheme outperforms Goel and Negi's AN scheme under certain channel conditions, especially when the legitimate channel is poor.

References

[1] I. Csiszár and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Inform. Theory*, vol. 24, no. 3, pp. 339–348, 1978.
[2] A. D. Wyner, "The wire-tap channel," *Bell. Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Jan. 1975.
[3] X. Zhou, R. K. Ganti, and J. G. Andews, "Secure wireless network connectivity with multi-antenna transmission," vol. 10, no. 2, pp. 425–430, Feb. 2011.
[4] S. Shafiee and S. Ulukus, "Towards the secrecy capacity of the Gaussian MIMO wire-tap channel: the 2-2-1 channel," *IEEE Trans. Inform. Theory*, vol. 55, no. 9, pp. 4033–4039, Sept. 2009.

[5] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas-I: The MISOME wiretap channe," *IEEE Trans. Inform. Theory*, vol. 56, no. 7, pp. 3088–3104, July 2010.
[6] F. Oggier and B. Hassibi, "The secrecy capacity of the mimo wiretap channel," submitted to *IEEE Trans. Inf. Theory*, July 2008. Also available at [arXiv:0710.1920].
[7] T. Liu and S. S. (Shitz), "A note on the secrecy capacity of the multiple-antenna wiretap channel," vol. 55, no. 6, pp. 2547–2553, JUNE 2009.
[8] Y. Liang, V. Poor, and S. S. (Shitz), "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 communication with a fading eavesdropper channel," in *Information Theory, 2007. ISIT 2007. IEEE International Symposium on*, Jun. 2007, pp. 1296–1300.
[10] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, Jun. 2008.
[11] P. Gopala, L. Lai, and H. El Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inform. Theory*, vol. 54, no. 10, pp. 4687–4698, 2008.
[12] S. Gerbracht, A. Wolf, and E. Jorswieck, "Beamforming for Fading Wiretap Channels with Partial Channel Information," in *Proc. of International ITG Workshop on Smart Antennas (WSA)*, Bremen, Germany, Feb. 2010.
[13] J. Li and A. Petropulu, "On ergodic secrecy rate for gaussian miso wiretap channels," *IEEE Trans. Wireless Commun.*, vol. 10, no. 4, pp. 1176 –1187, April 2011.
[14] Y. Liang and H. V. Poor, "Multiple access channels with confidential messages," *IEEE Trans. Inform. Theory*, vol. 54, pp. 976–1002, Mar. 2008.
[15] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge University Press, 2004.
[16] D. Tse and P. Viswanath, *Fundamentals of Wireless Communication*. Cambridge University Press, 2005.