Optimal Power Allocation for Joint Beamforming and Artificial Noise Design in Secure Wireless Communications

Haohao Qin, Xiang Chen, Yin Sun, Ming Zhao, Jing Wang

State Key Laboratory on Microwave and Digital Communications
Tsinghua National Laboratory for Information Science and Technology
Department of Electronic Engineering, Tsinghua University, Beijing 100084, P. R. China
email: {haohaoqin07, chenxiang98, sunyin02, zhaoming29}@gmail.com

***Abstract*— This paper studies the secure communication between a multiple-antenna transmitter (Alice) and a single-antenna destination (Bob) in the presence of more than one eavesdroppers (Eves). The optimal beamforming weights and the covariance matrix of artificial noise (AN) are obtained by minimizing the total transmission power of Alice, subject to a target secrecy rate constraint for Bob. We propose a two-level optimization method, where the inner-level optimization is solved by an interesting semidefinite relaxation method of W. C. Liao et al., and the outer-level optimization is solved by the golden section method. Our algorithm converges quite fast. Some properties of the optimal solution are also provided to illustrate the features of this problem.**

***Index Terms*— Artificial noise, beamforming, physical layer security, power allocation.**

I. Introduction

Since everybody within the communication range can receive wireless signals freely, privacy and security are serious issues in next generation wireless networks. Traditionally, security is provided by upper-layer data encryption techniques, and is viewed as an independent topic discussed beyond the scope of the physical layer. However, the eavesdropper can extract the key as long as it gets enough message [1], and issues such as key distribution and management are vulnerable in wireless communications. Recently, physical layer security has received considerable attentions as an alternative or a complement to cryptographic encryption.

Physical layer security was firstly studied from an information-theoretic perspective in [2], where Wyner considered a wire-tap channel. The secrecy capacity is defined as the maximum achievable rate from the transmitter to the legitimate receiver while keeping the eavesdropper completely ignorant of the transmitted massage. Later, Wyner's result was extended to Gaussian channel in [3], recently to parallel channels in [4] and fading channels in [5].

This work is supported by Tsinghua-Qualcomm Joint Research Program, National S&T Major Project (2008ZX03O03-004), National Basic Research Program of China (2007CB310608), Chinas 863 Project (2009AA011501), National Natural Science Foundation of China (60832008) and PCSIRT.

In the scenarios of single-input-single-output (SISO) communications, if the channel between transmitter and legitimate receiver is worse than that between transmitter and eavesdropper, the secrecy rate is zero. Fortunately, this can be overcome by taking advantage of multiple antenna beamforming techniques. Secrecy capacity in multi-antenna wiretap channels was addressed in [6]-[9]. In addition to these researches on security from an information theoretic aspect, lots of work has been done from a signal processing aspect to design and optimize secure transmission schemes (see [11]-[17]). By adding an artificial noise (AN) in the transmitted signal, the interference level at the eavesdroppers (Eves) can be raised [15]. Then, [16] extended this scheme by jointly optimizing the beamforming vector and the AN covariance matrix to achieve diverse signal to interference plus noise ratio (SINR) constraints for the legitimate receiver (Bob) and Eves.

In this paper, we focus on the optimal power allocation for joint beamforming and AN design in secure wireless communications, where the transmitter (Alice) is equipped with multiple antennas while the destination (Bob) and multiple eavesdroppers (Eves) are equipped with single antenna, respectively. Here, the channel state information (CSI) of Bob and all Eves is assumed to be perfectly known to Alice [16]. However, our optimization problem is different from that in [16]. We derive the optimal power allocation by minimizing the total transmitted power subject to a target secrecy rate constraint. We adopt golden section method [19] which has very fast convergence rate. In addition, several structural properties of the optimal solution are given.

The remainder of this paper is organized as follows. Section II provides the system model and problem formulation. Problem solution and its properties are presented in Section III. Simulation results and conclusions are given in Section IV and V, respectively.

978-1-61284-955-3/11/$26.00 ©2011 IEEE

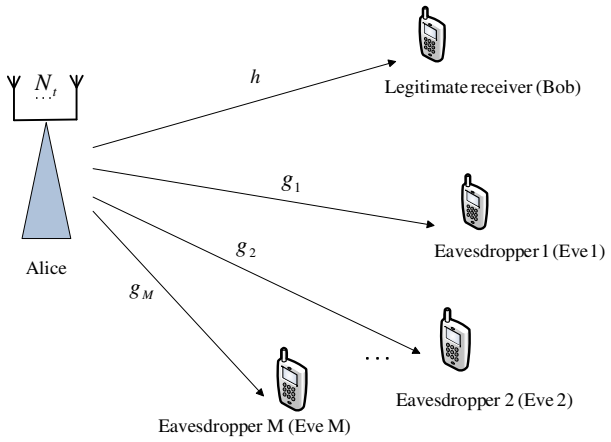

Fig. 1. Illustration of system model.

II. System Model and Problem Formulation

A. System Model

We consider a wireless communication channel with a transmitter (Alice), a legitimate receiver (Bob) and M eavesdroppers (Eves), where Alice is equipped with N_t antennas, while Bob and Eves are equipped with single antenna (see Fig. 1). Bob and Eves' CSIs are perfectly known to Alice.

Let $x(t) \in \mathbb{C}^{N_t}$ denotes the signal vector transmitted form Alice, and let $h \in \mathbb{C}^{N_t}$ and $g_m \in \mathbb{C}^{N_t}$ denote the channel vectors form Alice to Bob and the mth Eve, respectively. Additive noise at Bob and mth Eve, denoted by $n(t)$ and $v_m(t)$, are assumed to be independent and identically distributed (i.i.d.) zero-mean, complex Gaussian random variables with variances equal to σ_b^2 and $\sigma_{e,m}^2$, respectively. The received signals at Bob and Eves can be expressed as:

$$y_b(t) = h^H x(t) + n(t), \tag{1}$$

$$y_{e,m}(t) = g_m^H x(t) + v_m(t), m = 1, \cdots, M, \tag{2}$$

where the symbols $(\cdot)^H$ represent matrix Hermitian.

We use transmission scheme proposed in [16], which guarantees secrecy by utilizing AN and is proved to be more power efficient than the scheme without AN [16]. The transmitted signal $x(t)$ is

$$x(t) = ws(t) + z(t). \tag{3}$$

Here, $s(t) \in \mathbb{C}$ is the data stream intended for Bob only, and we assume $s(t) \sim \mathcal{CN}(0, 1)$ without loss of generality, where $\mathbb{C}$ represents the set of complex number and $\mathcal{CN}(a, b)$ denotes a circularly symmetric complex Gaussian random variable with mean of a and variance of b; $w \in \mathbb{C}^{N_t}$ is the beamforming vector corresponding to $s(t)$; $z(t) \in \mathbb{C}^{N_t}$ is the AN generated by Alice to interfere Eves, and $z(t) \sim \mathcal{CN}(0, \Sigma)$, $\Sigma \succeq 0$. We can rewrite (1) (2) as

$$y_b(t) = h^H ws(t) + h^H z(t) + n(t), \tag{4}$$

$$y_{e,m}(t) = g_m^H ws(t) + g_m^H z(t) + v_m(t), m = 1, \cdots, M. \tag{5}$$

The SINRs at Bob and Eves can be deduced as

$$\text{SINR}_b = \frac{w^H R_h w}{\text{Tr}(R_h \Sigma) + \sigma_b^2}, \tag{6}$$

$$\text{SINR}_{e,m} = \frac{w^H R_{g,m} w}{\text{Tr}(R_{g,m} \Sigma) + \sigma_{e,m}^2}, \tag{7}$$

respectively [16], where $R_h = hh^H$, $R_{g,m} = g_m g_m^H$ and $\text{Tr}(\cdot)$ denotes the trace of a matrix.

B. Problem Formulation

For the case of multiple receivers and multiple eavesdroppers, an achievable secrecy rate is given by [10]

$$R_s = \max_{P_{U,X}(u,x)} \min_{j,k} [I(U; Y_j) - I(U; Z_k)], \tag{8}$$

where Y_j and Z_k denote the received messages of the jth receiver and kth eavesdropper, respectively, and $I(X, Y)$ denotes the mutual information between X and Y. The maximum is taken over all distributions $P_{U,X}(u, x)$ that satisfy the Markov chain relationship: $U \to X \to (Y_j, Z_k)$ for $j = 1, \cdots, J$ and $k = 1, \cdots, K$. And (8) can be interpreted as the worst-case result, i.e. the eavesdropper with the best channel and the receiver with the worst channel dominate the secrecy rate.

Assuming U is a complex Gaussian random variable and $X = U$, according to (8), the achievable secrecy rate of our problem with M eavesdroppers is given by

$$R_s = \min_{m \in \{1, \cdots, M\}} \log_2\left(1 + \frac{w^H R_h w}{\text{Tr}(R_h \Sigma) + \sigma_b^2}\right) - \log_2\left(1 + \frac{w^H R_{g,m} w}{\text{Tr}(R_{g,m} \Sigma) + \sigma_{e,m}^2}\right). \tag{9}$$

The average transmitted power is given by

$$\mathbb{E}\{\|x(t)\|^2\} = \|w\|^2 + \text{Tr}(\Sigma), \tag{10}$$

where $\|\cdot\|$ represents the Euclidean norm of a vector.

Following the power minimization criterion, the design formulation with the secrecy rate constraint for beamforming and AN scheme is given,

$$\begin{aligned} \min_{w, \Sigma} \quad & \|w\|^2 + \text{Tr}(\Sigma) \\ \text{s.t.} \quad & R_s \geqslant \gamma, \\ & w \in \mathbb{C}^{N_t}, \\ & \Sigma \succeq 0, \end{aligned} \tag{11}$$

where R_s is defined in (9).

The aim of Alice is to optimize power allocation for joint beamforming and AN design, i.e. w and Σ, subject to a target secrecy rate γ. This problem is solved in section III using a two-level optimization method. An algorithm with a fast convergence rate for the optimal solution is proposed. Some properties of the optimal solution are also provided in the same section. This problem differs from that in [16] because of their different constraints.

III. Problem Solution and Its Properties

A. Problem Solution

As the first constraint in problem (11) involves the subtraction of two logarithms, the problem is non-convex. We remove one of two logarithms to the other side of the inequality. Then the first constraint can be rewritten as

$$\frac{2^{-\gamma}w^H R_h w}{\mathrm{Tr}(R_h\Sigma)+\sigma_b^2}+2^{-\gamma}-1\geq \max_{m\in\{1,\cdots,M\}}\frac{w^H R_{g,m} w}{\mathrm{Tr}(R_{g,m}\Sigma)+\sigma_{e,m}^2}. \quad (12)$$

We introduce an assistant variable t to simplify (12) and let $W = ww^H$. By this, the problem (11) is reformulated,

$$\begin{aligned}\min_{W,\Sigma,t}\quad & \mathrm{Tr}(W)+\mathrm{Tr}(\Sigma)\\ \text{s.t.}\quad & \tfrac{2^{-\gamma}\mathrm{Tr}(R_h W)}{\mathrm{Tr}(R_h\Sigma)+\sigma_b^2}+2^{-\gamma}-1\geq t,\\ & \tfrac{\mathrm{Tr}(R_{g,m}W)}{\mathrm{Tr}(R_{g,m}\Sigma)+\sigma_{e,m}^2}\leq t, m=1,\cdots,M,\\ & W\succeq 0,\ \mathrm{rank}(W)=1,\\ & \Sigma\succeq 0.\end{aligned} \quad (13)$$

Problem (13) is still a non-convex. For this, we utilize a two-level optimization structure. We first fix t and solve the *inner-level* problem to get $P^*(t)$,

$$\begin{aligned}P^*(t)=\min_{w,\Sigma}\quad & \mathrm{Tr}(W)+\mathrm{Tr}(\Sigma)\\ \text{s.t.}\quad & \tfrac{2^{-\gamma}\mathrm{Tr}(R_h W)}{\mathrm{Tr}(R_h\Sigma)+\sigma_b^2}+2^{-\gamma}-1\geq t,\\ & \tfrac{\mathrm{Tr}(R_{g,m}W)}{\mathrm{Tr}(R_{g,m}\Sigma)+\sigma_{e,m}^2}\leq t, m=1,\cdots,M,\\ & W\succeq 0,\ \mathrm{rank}(W)=1,\\ & \Sigma\succeq 0,\end{aligned} \quad (14)$$

in which t is a constant, and then solve the *outer-level* problem

$$\begin{aligned}\min_{t}\quad & P^*(t)\\ \text{s.t.}\quad & t\geq 0.\end{aligned} \quad (15)$$

The problem (14) was first addressed in an interesting paper [16], where the authors employed a semi-definite relaxation (SDR) method to transform (14) to a convex optimization problem. Then, one can use standard convex programming tools, such as SeDuMi [18] and CVX, to solve it.

The optimal value of the inner-level problem (14), i.e. $P^*(t)$, is shown in Fig. 2. One can simply observe that the function $P^*(t)$ is strictly decreasing for $t \leq t^*$ and strictly increasing for $t \geq t^*$, where $t^* > 0$ is the optimal solution to the outer-level problem (15). Such a property is called *unimodal* in numerical analysis textbooks, e.g. [19].

There is an efficient method for unimodal minimization problem, called *golden section search* method [19]. In each the golden section search step, the size of search interval is reduced by $\tau = \frac{\sqrt{5}-1}{2} \approx 0.618$ times, with the cost of computing only one new function evaluation [19]. The details of the two-level optimization algorithm are provided in Tab. I. The first several iterations of the algorithm are shown in Fig. 2. The computation is terminated once the size of search interval becomes smaller than a specified tolerance, which is denoted by *tol*.

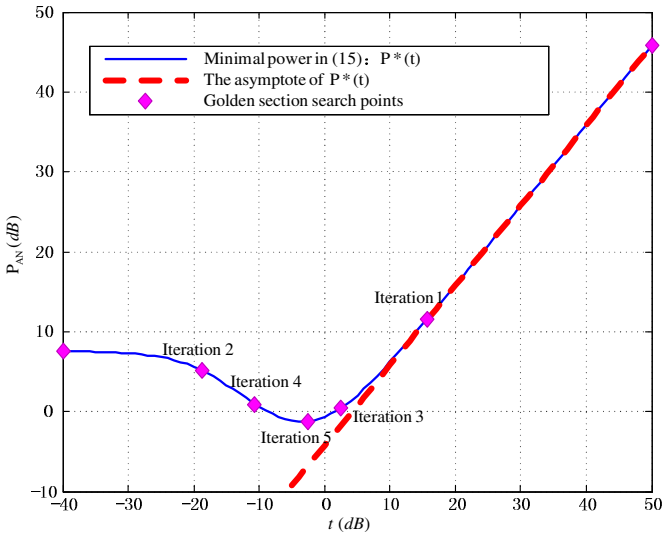

Fig. 2. The power consumption of the problem (14), i.e. $P^*(t)$, with $N_t = 4$, $M = 3$, $1/\sigma_b^2 = 10$ dB, $1/\sigma_v^2 = 10$ dB.

TABLE I
Algorithm for Optimal Solution of Problem (11)

Algorithm 1

$\tau = \frac{\sqrt{5}-1}{2}$
$t_1 = a + (1-\tau)(b-a)$
$t_2 = a + \tau(b-a)$
Compute $P^*(t_1)$ and $P^*(t_2)$ with SeDuMi
while $((b-a) < tol)$ **repeat**
  if $(P^*(t_1) > P^*(t_2))$ **do**
    $a = t_1$
    $t_1 = t_2$
    $P^*(t_1) = P^*(t_2)$
    $t_2 = a + \tau(b-a)$
    Compute $P^*(t_2)$ with SeDuMi
  else
    $b = t_2$
    $t_2 = t_1$
    $P^*(t_2) = P^*(t_1)$
    $t_1 = a + (1-\tau)(b-a)$
    Compute $P^*(t_1)$ with SeDuMi
  end
end

As we just explained, the convergence rate of the golden section method is given by

$$\frac{|e_{k+1}|}{|e_k|} = \tau = \frac{\sqrt{5}-1}{2} \approx 0.618, \quad (16)$$

where e_k is the error at the kth iteration. Therefore, the golden section method has *linear* convergence rate [19]. In our simulations, the outer-level iterations converge in only 10-20 times.

One can easily deduce that $P^*(0) = P_0 < \infty$. According to Feature 2 in Sec. III-B, we can always find a t_0 satisfying $P^*(t_0) \geq P_0$. Then, $[a, b] = [0, t_0]$ can be set as the initial search interval of Algorithm 1 in Tab. I. The value of t_0 can be searched by: $t_0 = kt_0$ if $P^*(t_0) \leq P_0$, where $k > 1$.

B. Features of optimal solution

In order to have a better understanding of the optimal beamforming and AN design, we provide some properties of the optimal solution now.

Feature 1: Let $(w^*,\ \Sigma^*)$ be the optimal solution of problem (11). Suppose the CSI of Bob is perfectly known to Alice and denote $W^* = w^* w^{*H}$. Then $(W^*,\ \Sigma^*)$ satisfy

$$\frac{2^{-\gamma}\mathrm{Tr}(R_h W^*)}{\mathrm{Tr}(R_h\Sigma^*)+\sigma_b^2} + 2^{-\gamma} - 1 = t. \tag{17}$$

And suppose that

$$\frac{\mathrm{Tr}(R_{g,m}W^*)}{\mathrm{Tr}(R_{g,m}\Sigma^*)+\sigma_{e,m}^2} = t, m \in \mathcal{K}, \tag{18}$$

$$\frac{\mathrm{Tr}(R_{g,m}W^*)}{\mathrm{Tr}(R_{g,m}\Sigma^*)+\sigma_{e,m}^2} < t, m \in \{1,\cdots,M\}/\mathcal{K}, \tag{19}$$

where $\mathcal{K} \subseteq \{1,\cdots,M\}$; $m \in \{1,\cdots,M\}/\mathcal{K}$ means $m \in \{1,\cdots,M\}$, but $m \notin \mathcal{K}$. Let $\mathbb{L}$ denotes the space extended by $\{h, g_m, m \in \mathcal{K}\}$. Then w^*'s projection in the null space of $\mathbb{L}$ is zero, i.e. $w^* \in \mathbb{L}$, and there exist $a \in \mathbb{C}$ and $b_m \in \mathbb{C}$ subject to

$$w^* = ah + \sum_{m\in\mathcal{K}} b_m g_m. \tag{20}$$

Its proof is shown in Appendix I.

Feature 2: The asymptote of $P^*(t)$ for large t is determined as

$$10\log_{10} P^*(t) \approx 10\log_{10}(t) + \gamma 10\log_{10}(2) + 10\log_{10}\frac{\sigma_b^2}{\mathrm{Tr}(R_h)}. \tag{21}$$

The (21) shows that the power consumption of the inner-level problem (14) is a linear function of t in dB when t is large. This is also demonstrated by Fig. 2, where the curve tends to straight in large t, $t \geq 15$ dB. The proof of this feature is given in Appendix II. The (21) also shows that $P^*(t)$ is a linear function of secrecy rate γ when t is large.

IV. Simulation Results

In the simulations, we consider the system described in section II with $N_t = 4$ and $M = 3$. We set $1/\sigma_b^2 = 10$ dB, $1/\sigma_{e,m}^2 = 1/\sigma_v^2 = 10$ dB if not mentioned specifically. The coefficients of h and $g_m, m = 1,\cdots,M$ are generated according to complex Gaussian distribution $\mathcal{CN}(0, I_{N_T}/N_t)$. Problem (11) is solved according to the algorithm in Tab. I.

Figure 3 presents the comparisons between our scheme and the previous scheme of [16]. The required SNR corresponding to various secrecy rate obtained by the optimal solution to the problem (11) is shown, where SNR $= \frac{|w|^2+\mathrm{Tr}(\Sigma)}{\sigma_b^2}$. In the scheme of [16], we assume that Eves' SINR is not larger than -10 dB, 3 dB and 10 dB, respectively, and Bob's SINR is set to achieve the target secrecy rate γbits/s/Hz. One can easily observe that our scheme can achieve more efficient power consumption than that of [16] with the same secrecy rate.

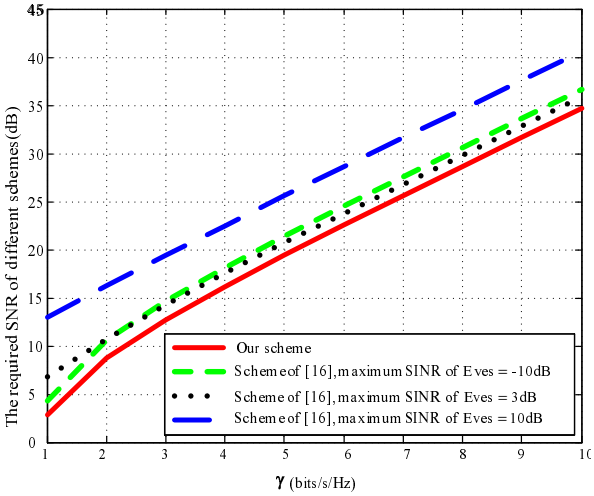

Fig. 3. The required SINR indicated by the optimal solution to the problem (11) with $N_t = 4,\ M = 3,\ 1/\sigma_b^2 = 10$ dB, $1/\sigma_v^2 = 10$ dB.

V. Conclusion

In this paper, we have obtained the optimal power allocation for joint beamforming and artificial noise design to minimize the transmission power subject to a target secrecy rate constraint. A fast convergence algorithm has been proposed to solve problem (11). Some properties of the optimal solution are also provided to illustrate the features of the problem.

Acknowledgement

The authors would like to thank Yang Yan and YanMin Wang for their kind help in the preparation of this paper.

Appendix I
Proof of Feature 1

Proof: If

$$\frac{2^{-\gamma}\mathrm{Tr}(R_h W^*)}{\mathrm{Tr}(R_h\Sigma^*)+\sigma_b^2} + 2^{-\gamma} - 1 > t, \tag{22}$$

One may reduce the amplitude of w^* to obtain a smaller value of the objective function while keeping all constraints hold true. This conflicts with the assumption that w^* is optimal. Therefore, (17) should hold true.

Assume that w^*'s projection in the null space of $\mathbb{L}$ is not zero, and denote it by w_p. Then one can find a small enough δ subject to $w' = w^* + \delta w_p$ satisfies

$$\|w'\| < \|w^*\|, \tag{23}$$

$$\frac{\mathrm{Tr}(R_{g,m}W^*)}{\mathrm{Tr}(R_{g,m}\Sigma^*)+\sigma_{e,m}^2} \leq t, m \in \{1,\cdots,M\}/\mathcal{K}, \tag{24}$$

As w' is changed in the null space of $\mathbb{L}$, so the other constraints are still true. This conflicts with optimality of w^*. So the assumption is false, and w^*'s projection in the null space of $\mathbb{L}$ is zero.

APPENDIX II
PROOF OF FEATURE 2

According to Feature 1, the problem (14) can be written as

$$\begin{aligned} \min_{w,\Sigma} \quad & \mathrm{Tr}(W) + \mathrm{Tr}(\Sigma) \\ \text{s.t.} \quad & \tfrac{2^{-\gamma}\mathrm{Tr}(R_h W)}{\mathrm{Tr}(R_h \Sigma)+\sigma_b^2} + 2^{-\gamma} - 1 = t, \\ & \tfrac{\mathrm{Tr}(R_{g,m} W)}{\mathrm{Tr}(R_{g,m} \Sigma)+\sigma_{e,m}^2} \le t, m = 1, \cdots, M, \\ & W \succeq 0, \quad \mathrm{rank}(W) = 1, \\ & \Sigma \succeq 0, \end{aligned} \tag{25}$$

using the SDR tools. As the first constraint in (25) achieves equality, if Σ becomes larger, W should also be larger. Therefor, with the objective of minimizing $\mathrm{Tr}(W + \Sigma)$. If Σ takes the value of 0, the second constraint maybe false. However, this scenario does not happen for large t and $\Sigma = 0$. So Σ should takes the value of 0. In order to minimize the transmitted power, W should choose the same direction of h, i.e. $w^* = \alpha h$. Then we have

$$\mathrm{Tr}(W^*) = \alpha^2 \|h\|^2 = \frac{2^\gamma t \sigma_b^2 - 2^\gamma + 1}{\mathrm{Tr}(R_h)} \approx \frac{2^\gamma t \sigma_b^2}{\mathrm{Tr}(R_h)}, \tag{26}$$

for large t. By this, the asymptote of (21) is proved.

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. Wyner, "The wire-tap channel," *Bell. Syst Tech J*, vol. 54, no. 8, pp. 1355-1387, Jan. 1975.

[3] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Inform. Theory*, vol.IT-24, no. 3, pp. 339-348, May. 1978.

[4] Z. Li, R. Yates, and W. Trappe, "Securecy capacity of independent parrallel channels," *Proc. IEEE int. Symp. Information Theory(ISIT)*, Seattle, WA, pp. 356-360, Jul. 2006.

[5] Y. Liang, H. V. Poor and S. Shamai(Shitz), "Secure communication over fading channels," *IEEE Trans. Inform. Theory.*, vol. 54, no. 6, pp. 2470-2492, Jun. 2008.

[6] A. Khisti and G. W. Wornell, "Secure communication with multiple antennas: The MISOME wiretap channel," *IEEE Trans. Inform. Theory.*, vol. 56, no. 7, pp. 3088-3104, Jul. 2010.

[7] F. Oggier, and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *Proc. 45th Annu. Allerton Conf. Communication, Control and Computing.*, Monticello, IL, Sept. 2007, pp. 848-855.

[8] T. Liu, and S. Shammai(Shitz), "A note on the secrecy capacity of the multi-antenna wiretap channel," *IEEE Trans. Inform. Theory.*, vol. 55, no. 6, pp. 2547-2553, Jun. 2009.

[9] E. Ekremm, and S. Ulukus, "Gaussian MIMO multi-receiver wiretap channel," *GLOBECOM.*, 2009.

[10] Y. Liang, G. Kramer, H. V. Poor, and S. Shamai (Shitz), "Compound wire-tap channels," *Proc. Allerton Conf. Communication, Control and Computing.*, Monticello, IL, USA, Sept. 2007.

[11] L. Dong, Z. Han, A. Petropulu, and H. V. Poor, "Secure wireless communications via cooperation," *Proc. 46th Annu. Allerton Conf. Commun., Control, Computing.*, Monticello, IL, Sep.-Oct. 2008.

[12] L. Dong, Z. Han, A. Petropulu, and H. V. Poor, "Amplify-and-forward based cooperation for secure wireless communications," in *Proc. IEEE Int. Conf. Acoust., Speech, Signal Process.*, Taipei, Taiwan, Apr. 2009.

[13] L. Dong, Z. Han, A. Petropulu, and H. V. Poor, "Cooperative jamming for wireless physical layer security," in *Proc. IEEE Statistical Signal Processing Workshop.* Cardiff, Wales, U.K., Aug.-Sep. 2009.

[14] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, " Improving wireless physical layer security via cooperative relays," *IEEE Trans. Signal Process.*, vol. 58, no. 3, pp. 1875-1888, Mar. 2010.

[15] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180-2189, June. 2008.

[16] W. C. Liao, T. H. Chang, W. K. Ma, and C. Y. Chi, "Joint transmit beamforming and artificial noise design for QoS discrimination in wireless downlink," *ICASSP 2010.*, Dallas, Texas, USA, pp. 2562-2565, Mar. 2010.

[17] Y. L. Liang, Y. S. Wang, T. H. Chang, Y.-W. P. Hong, and C. Y. Chi, "On the impact of quantized channel feedback in guaranteeing secrecy with artificial noise," *ISIT 2009.*, Seoul, Korea, June-Jul 2009.

[18] J. Strum, "Using SeDuMi 1.02: A MATLAB toolbox for optimization over symmetric cones," *Opt. Methods and Software.*, vol. 11-12, pp. 625-653, 1999, Special issue on Interior Point Methods (CD supplement with software).

[19] M. T. Heath, *Scientific computing: An introductory survey*, McGraw-Hill Companies, pp. 270-273, Jul 2001.