Achieving secrecy of MISO fading wiretap channels via jamming and precoding with imperfect channel state information

Xiong, Qi; Gong, Yi; Liang, Ying-Chang; Li, Kwok Hung

2014

Xiong, Q., Gong, Y., Liang, Y.-C., & Li, K. H. (2014). Achieving secrecy of MISO fading wiretap channels via jamming and precoding with imperfect channel state information. *IEEE wireless communications letters*, 3(4), 357-360.

<https://hdl.handle.net/10356/103628>

<https://doi.org/10.1109/LWC.2014.2317194>

© 2014 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works. The published version is available at: [<http://dx.doi.org/10.1109/LWC.2014.2317194>].

Downloaded on 26 Apr 2023 19:47:32 SGT

Achieving Secrecy of MISO Fading Wiretap Channels Via Jamming and Precoding With Imperfect Channel State Information

Qi Xiong, Yi Gong, Ying-Chang Liang, and Kwok Hung Li

Abstract—In this letter, we consider physical layer security in multiple-input single-output (MISO) fading wiretap channels, where the transmitter utilizes a jamming-aided precoding transmission strategy to maximize the achievable secrecy rate of the channel. The instantaneous channel state information (CSI) of the eavesdropper's channel is considered unavailable at the transmitter. We derive the closed-form expression of the ergodic secrecy rate, based on which we find that there exists an optimal power allocation ratio between the information signal and the jamming signal. Asymptotic analysis shows that the optimal power ratio depends on the number of antennas as well as the available transmit power at Alice.

Index Terms—Physical layer security, MISO, precoding, jamming, imperfect CSI

I. INTRODUCTION

Due to the broadcast nature of wireless medium, secure transmission in wireless networks is a fundamental challenge. Physical layer security has been used to protect the confidentiality of transmission via the information-theoretic perspective [1]. In the past few years, many research efforts have been made to study physical layer security over various antenna deployment and channel state information (CSI) situations [2]. In [3] and [4], the transmitter (Alice) was equipped with multiple antennas while the intended receiver (Bob) was only equipped with a single antenna. Their results show that the optimal transmission strategy is precoding or beamforming of the information signal. The idea is to increase the signal-to-noise ratio (SNR) as much as possible at Bob. This precoding strategy is referred to as *conventional precoding*. On the other hand, because of the randomness of eavesdropper (Eve)'s position, Eve may experience a better channel than Bob. As a result, it is difficult to always achieve positive secrecy rate, especially when Eve's CSI is unknown at Alice. To address this problem, a precoding strategy based on jamming has been proposed in [5], where part of the available power at Alice was used to transmit artificial noise in an intended way to jam Eve. The essence of this strategy is to not only increase SNR at Bob's side, but also intend to degrade Eve's channel as much as possible. This strategy is referred to as *jamming-aided precoding* (JP), where the power ratio between the information signal and the jamming signal should be optimized

in order to maximize the achievable secrecy rate. In [6], it is shown that Alice could obtain the near-optimal secrecy rate with equal power allocation when the available power at Alice was sufficiently large. Note that this finding is based on the assumption of a simplified scenario where no noise is experienced at Eve (i.e., the worst case).

In this letter, we consider MISO fading wiretap channels where Eve's instantaneous CSI is unknown at Alice. Our interest is to study how to achieve the maximum secrecy rate by designing the optimal JP strategy. The main contributions of this letter are: when the noise power is considered, we can obtain the closed-form expression of the ergodic secrecy rate, and statistically find the optimal power allocation ratio that leads to the maximum secrecy rate. This power ratio depends on the number of antennas as well as the available transmit power at Alice. In particular, we show that when the available power at Alice is small, most of the power should be allocated to the information signal. When the power increases, more power should be allocated to the jamming signal. When the power is sufficiently large, the optimal power allocation ratio will approach a constant that is only dependent on the number of antennas at Alice.

II. SYSTEM MODEL AND PROBLEM FORMULATION

Consider a wiretap channel where there are one transmitter (Alice) with N ($N > 1$) antennas, one receiver (Bob) and one eavesdropper (Eve), both with a single antenna. Alice intends to send precoded signal vector $\mathbf{x} \in \mathbb{C}^{N \times 1}$ to Bob, where the time index of $\mathbf{x}$ is omitted. The signals received at Bob and Eve are given by $Y_b = \mathbf{h}_b^H \mathbf{x} + R_b$ and $Y_e = \mathbf{h}_e^H \mathbf{x} + R_e$, respectively, where $\mathbf{h}_b, \mathbf{h}_e \in \mathbb{C}^{N \times 1}$ represent the CSI of Bob's channel and Eve's channel, respectively. Each element of $\mathbf{h}_b$ and $\mathbf{h}_e$ is independently and identically distributed as a circular symmetric complex Gaussian (CSCG) random variable with zero mean and unit variance. R_b and R_e represent the white Gaussian noise at Bob and Eve with variance $\sigma_b^2 = \sigma_e^2 = 1$. It is assumed that $\mathbf{h}_b$ is available at Alice while $\mathbf{h}_e$ is known at Eve but unknown to Alice. The transmitted signal $\mathbf{x}$ is subject to power constraint $\text{Tr}\{\mathbf{x}\mathbf{x}^H\} \leq P$, where P represents the total available power at Alice.

A. Conventional Precoding

With conventional precoding, the transmitted signal vector $\mathbf{x} = \mathbf{s} \cdot u$, where u is the information codeword from Gaussian codebook with zero mean and unit variance and $\mathbf{s} \in \mathbb{C}^{N \times 1}$ is the precoder for u . Clearly, we have $\text{Tr}\{\mathbf{s}\mathbf{s}^H\} \leq P$ and the secrecy capacity can be expressed as

$$C_1 = \max_{\text{Tr}(\mathbf{S}) \leq P} \{\log_2(1 + \mathbf{h}_b^H \mathbf{S} \mathbf{h}_b) - \log_2(1 + \mathbf{h}_e^H \mathbf{S} \mathbf{h}_e)\} \quad (1)$$

where $\mathbf{S} \triangleq \mathbf{s}\mathbf{s}^H$ is positive semi-definite.

Manuscript received February 3, 2014. The associate editor coordinating the review of this letter and approving it for publication was Z. Ding.

Q. Xiong and K. H. Li are with the School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore (e-mail: qxiong1@e.ntu.edu.sg, ekhli@ntu.edu.sg).

Y. Gong is with the Department of Electrical and Electronic Engineering, South University of Science and Technology of China, Shenzhen, China (e-mail: gong.y@sustc.edu.cn).

Y.-C. Liang is with the Institute for Infocomm Research, A*STAR, Singapore (e-mail: ycliang@i2r.a-star.edu.sg).

Digital Object Identifier 10.1109/LCOMM.2014.XXXXXX.XXXXXX

B. Jamming-aided Precoding

With the JP strategy, the transmitted signal $\mathbf{x}$ consists of information signal $\mathbf{s} \cdot \mathbf{u}$ and jamming signal $\mathbf{w} \in \mathbb{C}^{N \times 1}$, i.e., $\mathbf{x} = \mathbf{s} \cdot \mathbf{u} + \mathbf{w}$. Letting ρ denote the ratio of the power allocated to the information signal, we have $\text{Tr}\{\mathbf{s}\mathbf{s}^H\} \leq \rho P$. The secrecy capacity is now expressed as

$$C_2 = \max_{\text{Tr}(\mathbf{S} + \mathbf{W}) \leq P} \left\{ \log_2 \left(1 + \frac{\mathbf{h}_b^H \mathbf{S} \mathbf{h}_b}{\mathbf{h}_b^H \mathbf{W} \mathbf{h}_b + 1} \right) - \log_2 \left(1 + \frac{\mathbf{h}_e^H \mathbf{S} \mathbf{h}_e}{\mathbf{h}_e^H \mathbf{W} \mathbf{h}_e + 1} \right) \right\} \quad (2)$$

where $\mathbf{W} \triangleq \mathbb{E}\{\mathbf{w}\mathbf{w}^H\}$ is the jamming signal covariance matrix, which is positive semi-definite. Since $\mathbf{h}_e$ is unknown to Alice, we follow the original design of $\mathbf{w}$ and $\mathbf{s}$ in [5]. That is, $\mathbf{s} = \sqrt{\rho P}(\mathbf{h}_b / \|\mathbf{h}_b\|)$ and $\mathbf{S} = \rho P(\mathbf{h}_b / \|\mathbf{h}_b\|)(\mathbf{h}_b / \|\mathbf{h}_b\|)^H$. The jamming signal is allocated to the null space of $\mathbf{h}_b$ in order to ensure the jamming signal not to interfere Bob. By choosing $\mathbf{Z} = \text{null}(\mathbf{h}_b^H)$ as the orthonormal basis of the null space of $\mathbf{h}_b$, where $\mathbf{Z} \in \mathbb{C}^{N \times (N-1)}$, it follows that $\mathbf{w} = \mathbf{Z}\mathbf{v}$, where $\mathbf{v} \in \mathbb{C}^{(N-1) \times 1}$ is a complex Gaussian noise vector with each element being zero mean and variance of σ_v^2 . Since the jamming signal power $(1 - \rho)P$ is uniformly allocated to the $N - 1$ elements, we get $\sigma_v^2 = (1 - \rho)P / (N - 1)$. Therefore, (2) can be rewritten as

$$C_2 = \max_{0 < \rho \leq 1} \left\{ \log_2(1 + \rho P \mathbf{h}_b^H \mathbf{h}_b) - \log_2 \left(1 + \frac{\rho P \mathbf{h}_{eb}^H \mathbf{h}_{eb}}{\frac{(1-\rho)}{N-1} P \mathbf{h}_{ez}^H \mathbf{h}_{ez} + 1} \right) \right\} \quad (3)$$

where $\mathbf{h}_{eb} = (\mathbf{h}_b / \|\mathbf{h}_b\|)^H \mathbf{h}_e$ and $\mathbf{h}_{ez} = \mathbf{Z}^H \mathbf{h}_e$.

C. JP Strategy with $\mathbf{h}_e$ Known at Alice

Before we proceed to find the optimal JP strategy when Eve's channel $\mathbf{h}_e$ is unknown to Alice, let us briefly review the optimal JP strategy when Eve's channel is known at Alice. Based on the work in [4], it is easy to show that with known $\mathbf{h}_e$, the optimal solution is to allocate all the available power to the information signal (i.e., $\rho = 1$). Therefore, the JP strategy in this case reduces to the conventional precoding. The optimal beamformer $\mathbf{s}$ for the information signal is the unit-norm generalized eigenvector corresponding to the largest generalized eigenvalue of the matrix pencil $(\mathbf{I} + P \mathbf{h}_b \mathbf{h}_b^H, \mathbf{I} + P \mathbf{h}_e \mathbf{h}_e^H)$.

III. OPTIMAL JP STRATEGY WITH UNKNOWN $\mathbf{h}_e$

In this section, after deriving the closed-form expression of the ergodic secrecy rate, we study how to design the optimal JP strategy that achieves the maximal ergodic secrecy rate when $\mathbf{h}_e$ is unknown at Alice.

Our main result is summarized in the theorem below.

Theorem 1: When $\mathbf{h}_e$ is unknown to Alice, the optimal power allocation ratio maximizing the ergodic secrecy rate is found to be dependent on P and N only. In the low power region ($P \rightarrow 0$), most of the power should be allocated to the information signal (i.e., $\rho \rightarrow 1$), while in the high power region ($P \rightarrow \infty$), the optimal power ratio should approach a constant that is only dependent on N .

A. Proof of Theorem 1

The ergodic secrecy rate in this case is defined as

$$\tilde{C}_2 \triangleq \tilde{C}_{2\text{-AB}} - \tilde{C}_{2\text{-AE}} \triangleq E_{x_1} \{ \log_2(1 + \rho P x_1) \} - E_{x_2, x_3} \{ \log_2(1 + \frac{\rho P x_2}{\frac{1-\rho}{N-1} P x_3 + 1}) \} \quad (4)$$

where $\tilde{C}_{2\text{-AB}}$ and $\tilde{C}_{2\text{-AE}}$ represent the ergodic channel rate of the legitimate channel and the illegitimate channel, respectively. Moreover, $x_1 \triangleq \|\mathbf{h}_b\|^2$, $x_2 \triangleq \|\mathbf{h}_{eb}\|^2$, and $x_3 \triangleq \|\mathbf{h}_{ez}\|^2$ follow gamma distribution, i.e., $x_1 \sim \Gamma(N, 1)$, $x_2 \sim \Gamma(1, 1)$, and $x_3 \sim \Gamma(N - 1, 1)$.

Firstly, the ergodic channel rate between Alice and Bob can be expressed as

$$\begin{aligned} \tilde{C}_{2\text{-AB}} &= \frac{1}{\ln 2} \int_0^\infty \left[\ln(1 + \rho P x_1) x_1^{N-1} \frac{\exp(-x_1)}{\Gamma(N)} \right] dx_1 \\ &= \frac{1}{\ln 2} \exp\left(\frac{1}{\rho P}\right) \sum_{i=1}^N G_i\left(\frac{1}{\rho P}\right) \end{aligned} \quad (5)$$

where $G_i(\cdot)$ is the generalized exponential integral [8].

Next, we derive the ergodic channel rate between Alice and Eve. By denoting $x = \rho P x_2 / (\frac{1-\rho}{N-1} P x_3 + 1)$, it is easy to show that x is equivalent to the signal-to-interference-plus-noise ratio (SINR) of a single-branch MMSE diversity combiner with $N - 1$ interferers [7]. The complementary cumulative distribution function (CCDF) of x is given by

$$R(x) = \frac{\exp(-ax)}{(1 + bx)^{N-1}} \quad (6)$$

where $a = 1/(\rho P)$ and $b = (1 - \rho)/((N - 1)\rho)$. Accordingly, $\tilde{C}_{2\text{-AE}}$ becomes

$$\begin{aligned} \tilde{C}_{2\text{-AE}} &= \int_0^\infty [\log_2(1 + x) f(x)] dx \\ &= \frac{1}{\ln 2} \int_0^\infty \frac{\exp(-ax)}{(1 + x)(1 + bx)^{N-1}} dx \end{aligned} \quad (7)$$

where (7) is obtained through integration by parts. Generally, it is not straightforward to obtain the closed-form expression of (7). Through the partial fraction decomposition [8], it can be shown that

$$\begin{aligned} \frac{1}{(1 + x)(1 + bx)^{N-1}} &= \frac{a_1}{(1 + bx)} + \frac{a_2}{(1 + bx)^2} + \dots \\ &\quad + \frac{a_{N-1}}{(1 + bx)^{N-1}} + \frac{a_N}{(1 + x)} \end{aligned} \quad (8)$$

where the calculation of coefficients a_i ($1 \leq i \leq N$) is omitted due to space limit. Therefore, (7) is rewritten as

$$\tilde{C}_{2\text{-AE}} = \frac{1}{\ln 2} \int_0^\infty \left[\sum_{j=1}^{N-1} \frac{a_j e^{-ax}}{(1 + x)(1 + bx)^j} + \frac{a_N e^{-ax}}{1 + x} \right] dx \quad (9)$$

From [8], we get the following integral evaluations

$$\int_0^\infty \frac{\exp(-\mu x)}{x + \beta} dx = -\exp(\beta \mu) E_i(-\mu \beta) \quad (10)$$

$$\begin{aligned} \int_0^\infty \frac{\exp(-\mu x)}{(x + \beta)^n} dx &= \frac{1}{(n-1)!} \sum_{k=1}^{n-1} (k-1)! (-\mu)^{n-k-1} \beta^{-k} \\ &\quad - \frac{\mu^{n-1}}{(n-1)!} \exp(\beta \mu) E_i(-\mu \beta) \quad (\mu \geq 0, \beta \geq 0, n \geq 2) \end{aligned} \quad (11)$$

where $E_i(\cdot)$ is the exponential integral [8]. Based on (10) and (11), we obtain the expression of $\tilde{C}_{2\text{-AE}}$ as

$$\tilde{C}_{2\text{-AE}} = \frac{1}{\ln 2} \left\{ \sum_{i=2}^{N-1} \left[\frac{a_i}{b^i(i-1)!} \sum_{k=1}^{i-1} (k-1)!(-a)^{i-k-1} b^k \right. \right. \\ \left. \left. - \frac{a^{i-1}}{(i-1)!} e^{\frac{a}{b}} E_i\left(-\frac{a}{b}\right) \right] - \frac{a_1}{b} e^{\frac{a}{b}} E_i\left(-\frac{a}{b}\right) - a_N e^a E_i(-a) \right\} \quad (12)$$

With (4), (5) and (12), the ergodic secrecy rate $\tilde{C}_2$ is now expressed in closed-form, which involves ρ , N and P only. This suggests that the optimal ρ , denoted as ρ^* , depends on N and P only, and numerical methods can be used to find ρ^* .

When the available power is sufficiently large (i.e., $P \rightarrow \infty$), we can ignore the noise at Eve's side by letting $\sigma_e^2 = 0$. Therefore, the CCDF of x can be rewritten as

$$R(x) = \frac{1}{(1+bx)^{N-1}} \quad (13)$$

and the ergodic secrecy rate in this case can be found as [6]

$$\tilde{C}_2 = \frac{1}{\ln 2} \left[\exp\left(\frac{1}{\rho P}\right) \sum_{i=1}^N E_i\left(\frac{1}{\rho P}\right) - \frac{\rho}{\rho-1} {}_2F_1\left(1, 1; N; \frac{1-\rho N}{\rho-1}\right) \right]^+ \quad (14)$$

where the ${}_2F_1(\cdot)$ is the Gauss hyper-geometric function. Note that when the power is not sufficiently large, (14) actually reflects the ergodic secrecy rate in the worst-case scenario (i.e., no noise is experienced at Eve's side). The case of $\sigma_e^2 = 1$ is referred to as the general-case scenario in the sequel. When $P \rightarrow \infty$, (14) can be shown to be

$$\lim_{P \rightarrow \infty} \tilde{C}_2 = \frac{1}{\ln 2} \left[\sum_{i=2}^N \left(\frac{1}{1-i} \right) + \left(\frac{N\rho - \rho}{N\rho - 1} \right)^{N-1} \cdot \left(\ln\left(\frac{N\rho - \rho}{1 - \rho}\right) - \sum_{j=1}^{N-2} \frac{1}{j} \left(\frac{N\rho - 1}{N\rho - \rho} \right)^j \right) \right]^+ \quad (15)$$

Based on (15), it is found that the optimal ρ , which leads to the maximal secrecy rate, is dependent on N only. Note that (15) is not an upper bound for $\tilde{C}_2$ when $P \rightarrow \infty$. In fact, with the optimal ρ , $\tilde{C}_2$ keeps increasing with P ; however, with the increasing P , the optimal ρ will approach a constant related to N only.

Next, we consider the low power region ($P \rightarrow 0$). Using $\log_2(1+x) \approx x/\ln 2$ at $x \rightarrow 0$ yields

$$\begin{aligned} \lim_{P \rightarrow 0} \tilde{C}_2 &= \lim_{P \rightarrow 0} \left\{ E_{x_1} \{ \log_2(1 + \rho P x_1) \} \right. \\ &\quad \left. - E_{x_2, x_3} \{ \log_2(1 + \rho P x_2 + \frac{1-\rho}{N-1} P x_3) \} \right. \\ &\quad \left. + E_{x_3} \{ \log_2(1 + \frac{1-\rho}{N-1} P x_3) \} \right\} \\ &\approx E_{x_1, x_2, x_3} \{ \rho P x_1 - [\rho P x_2 \\ &\quad + \frac{1-\rho}{N-1} P x_3] + \frac{1-\rho}{N-1} P x_3 \} / \ln 2 \\ &= \rho P E_{x_1, x_2} \{ x_1 - x_2 \} / \ln 2 \\ &= \rho P (N-1) / \ln 2. \end{aligned} \quad (16)$$

which clearly suggests that in the low power region ($P \rightarrow 0$), most of the transmit power should be used to precode the information signal, i.e., $\rho \rightarrow 1$. This completes the proof.

B. Discussions

Remark 1: In the worst-case scenario (i.e., $\sigma_e^2 = 0$), it can be shown that when P decreases, more power should be allocated to the jamming signal, though this may not be directly observable from (14).

In the following, we illustrate this trend by considering a special case of the low power region ($P \rightarrow 0$). In this case, with $\sigma_e^2 = 0$, (4) can be rewritten as

$$\begin{aligned} \tilde{C}_2 &= E_{x_1, x_2, x_3} \left\{ \log_2 \left(\frac{1 + \rho P x_1}{1 + \frac{(N-1)\rho x_2}{(1-\rho)x_3}} \right) \right\} \\ &\approx E_{x_2, x_3} \left\{ -\log_2 \left(1 + \frac{(N-1)\rho x_2}{(1-\rho)x_3} \right) \right\}. \end{aligned} \quad (17)$$

Clearly, $\tilde{C}_2$ is monotonically decreasing with ρ , suggesting that more power should be allocated for jamming. This is opposite to our earlier result for the general-case scenario in (16), where more power should be allocated to the information signal.

Furthermore, it can be shown that when P increases, more power should be allocated to the jamming signal in the general-case scenario ($\sigma_e^2 = 1$). This is different from the result for the worst-case scenario ($\sigma_e^2 = 0$) where when P increases, less power should be allocated to the jamming signal [6]. However, in both scenarios, when N increases, more power should be allocated to the information signal.

Remark 2: When P increases, the ergodic secrecy rate achieved by conventional precoding is upper bounded by

$$\begin{aligned} \lim_{P \rightarrow \infty} \tilde{C}_1 &= \lim_{P \rightarrow \infty} E_{x_1, x_2} \left\{ \log_2 \left(\frac{1 + P x_1}{1 + P x_2} \right) \right\} \\ &\approx E_{x_1, x_2} \{ \log_2(x_1) - \log_2(x_2) \} \\ &= (\psi(N) - \psi(1)) / \ln 2 \end{aligned} \quad (18)$$

where $\psi(N)$ represents the poly-gamma function [8] with parameter N and $\psi(1)/\ln 2 = 0.8327$. On the other hand, as mentioned earlier, with the optimal ρ^* , the secrecy rate of the JP strategy keeps increasing with P and $\tilde{C}_2$ is unbounded. This clearly indicates that when $\mathbf{h}_e$ is unknown to Alice, conventional precoding is no longer the optimal strategy and it is always optimal to allocate part of the power for jamming. In particular, when P increases or N decreases, more power should be allocated to the jamming signal.

IV. NUMERICAL RESULTS

In this section, we provide numerical results to illustrate the performance of the JP strategy with $\mathbf{h}_e$ unknown to Alice. The elements of $\mathbf{h}_b$ and $\mathbf{h}_e$ are generated from independent CSCG random variables distributed as $CN(0, 1)$.

Figure 1 displays the ergodic secrecy rate of the JP strategy via both simulation and analysis, where the analytical result is based on its closed-form expression. Figure 1 clearly shows that the analytical and simulation results match very well under different antenna deployment and variable power supply. It

Fig. 1. Ergodic secrecy rate versus P with optimal ρ .

verifies the accuracy of the closed-form expression. Figure 1 also shows that the achievable ergodic secrecy rate increases with more antennas and larger power supply at Alice.

The ergodic secrecy rate achieved by JP as well as conventional precoding is shown in Fig. 2, where it is observed that in the low power region, there is little difference between the conventional precoding and JP (with ρ^*) strategies. This is because in this case, ρ^* approaches 1 and therefore JP reduces to conventional precoding. However, when P increases, their difference becomes more and more significant. For conventional precoding, it is limited by the upper bound given in (18), while for JP with ρ^* , the ergodic secrecy rate is unbounded and keeps increasing with P . Figure 2 also shows that employing more antennas at Alice helps to improve the secrecy rate.

The optimal power allocation ratio for the JP strategy is shown in Fig. 3. We observe opposite behaviors of the general-case and worst-case scenarios, which are consistent with our analytical results in Section III. In the former scenario, ρ^* decreases with P and eventually converges to a constant; while in the latter scenario, ρ^* increases with P and eventually converges to the same constant. It should be noted that in practice, the worst-case scenario can only be justified under a large power assumption. It is observed from Fig. 3 that ρ^* is around 0.5 at various N when $P > 20$ dB. Figure 3 also shows that employing more antennas at Alice results in a larger ρ^* . This is expected since when N increases, with the same ρ , the capacity of the legitimate channel increases faster than that of the illegitimate channel by observing (3). Therefore, ρ should also increase to further improve the secrecy rate.

V. CONCLUSION

In this letter, we studied achievable secrecy rate of MISO fading wiretap channels through jamming and precoding. With unknown Eve's channel, we find that there exists an optimal power allocation ratio between the information signal and the jamming signal and that this power ratio depends on the number of antennas as well as the available transmit power. In particular, when the available transmit power increases or the

Fig. 2. Ergodic secrecy rate versus P .

Fig. 3. Optimal power ratio ρ for JP strategy.

number of antennas at Alice decreases, more power should be allocated to the jamming signal.

REFERENCES

- [1] A. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, Vol.54, No.8, pp. 1355-1387, Oct. 1975.
- [2] N.-E. Wu and H.-J. Li, "Effect of feedback delay on secure cooperative networks with joint relay and jammer selection," *IEEE Wireless Commun. Lett.*, vol. 2, no. 4, pp. 415-418, Aug. 2013.
- [3] S. Shafiee and S. Ulukus, "Achievable rates in Gaussian MISO channels with secrecy constraints," *IEEE Int. Symp. Inf. Theory*, pp. 2466-2470, June 2007.
- [4] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas I: the MISOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 7, pp. 3088-3104, July 2010.
- [5] S. Goel and R. Negi, "Secret communications using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180-2189, June 2008.
- [6] X. Zhou and M. R. McKay, "Secret communication with artificial noise over fading channels: achievable rate and optimal power allocation," *IEEE Trans. Veh. Technology*, vol. 59, no. 8, pp. 3831-3842, Oct. 2010.
- [7] H. Gao, P. J. Smith, and M. V. Clark, "Theoretical reliability of MMSE linear diversity combining in Rayleigh-fading additive interference channels," *IEEE Trans. Commun.*, vol. 46, no. 5, pp. 666-672, May 1998.
- [8] I. S. Gradshteyn and I. M. Ryzhik, *Tables of Integrals, Series, and Products*, 7th ed. New York: Academic, 2007.