Power Allocation for Artificial-Noise Secure MIMO Precoding Systems

Shang-Ho Tsai, *Senior Member, IEEE*, and H. Vincent Poor, *Fellow, IEEE*

***Abstract*—This paper investigates the power allocation problem for artificial noise (AN) secure precoding systems, and proposes closed-form solutions for maximizing the achievable secrecy rate. It is assumed that the transmitter knows the full channel information at the legitimate receiver, and knows only the statistics of the channel information at the eavesdropper. Lower bounds are derived for the secrecy rates in multiple-input single-output channels with single or multiple eavesdroppers and multiple-input multiple-output channels with multiple eavesdroppers. When the number of transmit antennas is sufficiently large, the bounds are tight, and closed-form solutions can be derived from these bounds. The analytical results suggest simple and yet informative solutions as follows: Let the numbers of receive antennas at the legitimate receiver and at the eavesdropper be N_r and $N_{r,e}$, respectively. The system should distribute $N_{r,e}/(N_r + N_{r,e})$ of the power to AN in the high SNR regime, and distribute zero power to AN in the low SNR regime; the rate loss due to the eavesdropper is $-N_r \log(N_r/(N_r + N_{r,e})) - N_{r,e} \log(N_{r,e}/(N_r + N_{r,e}))$ bits/sec/Hz in the high SNR regime and nearly negligible in the low SNR regime. The derived results also show that equal power and water-filling power allocations lead to similar solutions and rate loss. Simulation results corroborate the theoretical results.**

***Index Terms*—Artificial noise, beamforming, MIMOME, MISOME, physical layer security, power distribution, precoding, secrecy capacity, wire-tap channel.**

I. Introduction

MULTIPLE-INPUT MULTIPLE-OUTPUT (MIMO) techniques are widely used in contemporary communication systems owing to their ability to increase channel capacity and diversity gain. Recently considerable research has been conducted into the potential use of multiple-antenna techniques for achieving security in the wireless physical layer.

In 1949, Shannon introduced an information theoretic formulation of communication security in his work [1]. Subsequently, Wyner in [2] formulated the transmission secrecy problem, in which a transmitter sends information to a legitimate receiver which is also intercepted by an eavesdropper via the so called wire-tap channel. He defined and analyzed the secrecy capacity using Shannon's theory, and these ideas have since been widely used in research on physical layer security. Notably the authors in [3] considered the secrecy capacity for multiple-input single-output (MISO) channels assuming that the CSI (channel state information) of both the legitimate receiver and the eavesdropper is known to the transmitter. In this case, the capacity is achieved by beamforming/precoding toward a direction that is as orthogonal to the eavesdropper as possible, while simultaneously being as close to the legitimate receiver as possible. This result was extended by the same authors to a 2×2 MIMO channel in [4]. The secrecy capacity of MIMO channels has been further widely treated, e.g., [5]–[11]. The authors in [12] considered the secrecy capacity for MISO channels with multiple eavesdroppers, i.e., so-called MISOME (multiple-input, single-output, multiple-eavesdropper) channels. A bound on the capacity of MISOME channels was derived assuming that the CSI from both the legitimate receiver and the eavesdropper is known to the transmitter. The MIMOME (MIMO, multiple-eavesdropper) channels were investigated by the same authors in [8].

When the CSI of the legitimate receiver and the eavesdropper is known to the transmitter, several studies have investigated the optimal transmit covariance matrix and the corresponding characteristics for maximizing the secrecy capacity. For example, in [13] transmitting signals in the positive directions of the difference channel has been shown to be a necessary condition for optimality. Also, an explicit closed-form solution for full-rank covariance matrices was proposed, while in [14], the full-rank solution was extended by the same authors to a rank-deficient case, where the null space of the direct channel is in the null space of the indirect channel. The authors in [14] also considered the situation in which only limited CSI of the eavesdropper is known to the transmitter. The authors in [15] independently proved that full rank is a necessary and sufficient condition for the optimal transmit covariance using a different approach. In addition, they also showed that when the covariance is deficient, there exists an equivalent set of channels and a full-rank transmit covariance matrix that achieve the same secrecy capacity.

The use of artificial noise (AN) to impair the receive quality of the eavesdropper was proposed in [16]. This scheme is also called "masked beamforming" in MISO channels [12], and "masked precoding" in MIMO channels [8]. We will call this method "AN precoding" in this work. AN precoding systems assume that the eavesdropper is passive, and that the CSI of the eavesdropper is unknown to the transmitter. For a total transmit power P, AN precoding systems use partial power, say θP, to transmit data, and allocate the residual power, $(1 - \theta)P$, to

Manuscript received October 23, 2013; revised January 17, 2014 and April 05, 2014; accepted May 19, 2014. Date of publication June 05, 2014; date of current version June 17, 2014. The associate editor coordinating the review of this manuscript and approving it for publication was Prof. Rui Zhang. This work was supported in part by the National Science Council (NSC), Taiwan under Grants NSC 102-2918-I-009-010 and NSC 102-2221-E-009-017-MY3, and by the U.S. National Science Foundation under Grant CCF-1016671.

S.-H. Tsai is with the Department of Electrical Engineering, National Chiao Tung University, Hsinchu, Taiwan (e-mail: shanghot@alumni.usc.edu).

H. V. Poor is with the Department of Electrical Engineering, Princeton University, Princeton, NJ 08540 USA (e-mail: poor@princeton.edu).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TSP.2014.2329273

transmit the artificial noise, where $0 \leq \theta \leq 1$. The authors of [16] have shown that the AN precoding scheme guarantees a positive secrecy rate even if the noise variance of the eavesdropper approaches zero, i.e., under the situation in which the eavesdropper is very close to the transmitter. The performance of AN precoding systems with limited feedback was evaluated in [17]. A generalized scheme based on the AN precoding system for MISOSE (MISO single-eavesdropper) channels was proposed in [19], where the AN can be transmitted in the signal direction, not necessarily in the null space of the direct channel. The authors in [12] also analyzed the performance of AN precoding systems in MISOME channels, and showed that it is close to optimal in MISOME channels when the number of transmit antennas is large and the SNR is high; the performance for MIMOME channels was analyzed in [8].

Although the authors in [8], [12] and [16] have derived performance bounds for AN precoding systems, it is still unclear how to allocate the power between the transmit data and the artificial noise to maximize the average secrecy rate. In [17], the authors showed by simulation that when only limited feedback is available, the AN precoding scheme sometimes performs worse than the conventional precoding scheme (without AN precoding) [18]. Thus it is not clear whether or not one should add artificial noise if one is not sure about the appropriate value of θ. Inappropriate power allocation in AN precoding schemes can lead to a serious degradation of secrecy rate. Although simulation may be used to determine suitable values of θ, this is time consuming and different parameter settings such as changing SNR and numbers of antennas lead to different optimal values of θ. Thus if closed-form solutions for optimal values of θ were available, it would help us gain greater insight into AN precoding systems. The discussions above motivate us to investigate the following questions: 1) are there closed-form optimal (or approximately optimal) solutions for θ for maximizing the secrecy rate? 2) What is the maximum rate loss due to the eavesdropper in such systems, i.e., the difference between the secrecy rate of AN precoding systems and the traditional MISO/MIMO achievable rate without eavesdroppers?

In this paper, we investigate the average secrecy rates of AN precoding systems in MISOSE, MISOME and MIMOME channels with large numbers of transmit antennas and moderate numbers of receiver antennas. Systems with large numbers of antennas are usually regarded as massive MIMO systems, and have attracted considerable research attention recently, e.g., see [20]–[22]. In massive MIMO systems, base stations are equipped with very large numbers of antennas, possibly tens to hundreds of antennas [22]. We derive theoretical lower bounds on the average secrecy rate in MISOSE, MISOME and MIMOME channels. The bounds become tight as the number of transmit antennas increases; thanks to the tight low bounds, closed-form solutions for θ to maximize the average secrecy rate are available. From the suggested solutions, we have the following interesting findings:

First, for MISOSE channels, the suggested solution of θ is 1/2 in the high SNR regime, and is 1 in the low SNR regime; the corresponding average rate loss due to the eavesdropper, i.e., the difference between the secrecy rate of the AN precoding system and the traditional achievable rate without the eavesdropper, is 2 bits/sec/Hz in the high SNR regime, and is nearly negligible in the low SNR regime. Moreover, for MISOME and MIMOME channels, the suggested solution is $\theta = N_r/(N_r + N_{r,e})$, in the high SNR regime, and is $\theta = 1$ in the low SNR regime, where N_r and $N_{r,e}$ are the numbers of receive antennas at the legitimate receiver and the eavesdropper, respectively; the corresponding average rate loss due to the eavesdropper is $-N_r \log(N_r/(N_r + N_{r,e})) - N_{r,e} \log(N_{r,e}/(N_r + N_{r,e}))$ bits/sec/Hz in the high SNR regime, and is nearly negligible in the low SNR regime. It is interesting to note that in the low SNR regime the proposed θ is 1, and the corresponding rate loss for MISOSE, MISOME and MIMOME channels are all negligible. Thus, there may be no need to use AN precoding in the low SNR regime. On the other hand, although the results for MISOSE and MIMOME channels are not the same in the high SNR regime, they still have some similarities. To see this, if $N_r = N_{r,e}$ in MIMOME channels, the suggested solution is $\theta = 1/2$ and the corresponding rate loss is $N_r + N_{r,e} = 2N_r$. Although the rate loss increases linearly with N_r, if one considers that the achievable rate of the legitimate receiver also increases linearly with N_r, this loss is reasonable; normalizing the rate loss by N_r, it becomes 2 bits/sec/Hz, which is the rate loss in MISOSE channels. Furthermore, in MIMOME channels, we evaluate equal power allocation and water-filling power allocation. These two power allocations are commonly used in traditional MIMO communications. We find that both schemes have similar solutions for θ and rate loss due to the eavesdropper. Note that the optimal power allocations may be obtained via optimization methods if certain conditions are available to the transmitter. Finally, simulation results are provided to demonstrate the accuracy of the theoretical results. We also learn from the results that inappropriate values of θ indeed seriously degrade the performance.

The rest of this paper is organized as follows. The system model and problem formulation are presented in Section II. The secrecy rate, the proposed power allocation and the maximum rate loss for MISOSE, MISOME and MIMOME channels are analyzed respectively in Section III and Section IV. More specifically, for MIMOME channels, equal power allocation and water-filling power allocation are considered separately in Section IV-A and Section IV-B. Simulation results are provided in Section V. Our conclusions are summarized in Section VI.

Notation: Boldfaced lowercase letters and boldfaced uppercase letters denote vectors and matrices, respectively. $\mathbb{E}\{x\}$ and σ_x^2 denote, respectively, the mean and variance of the random variable x. $\mathbf{A}^*$ denotes the conjugate of the matrix $\mathbf{A}$, while $\mathbf{A}^\dagger$ is the conjugate-transpose of $\mathbf{A}$. $\Re\{x\}$ and $\Im\{x\}$ denote respectively the real and the imaginary parts of the complex number x. $\det(\mathbf{A})$ is the determinant of $\mathbf{A}$, and $\mathrm{Tr}(\mathbf{A})$ is the trace of $\mathbf{A}$. $\mathrm{diag}(\cdot)$ forms a diagonal matrix with the elements inside the brace. $(x)^+ = \max(x, 0)$ for a real variable x. $\|\mathbf{A}\|$ is the Frobenius norm of $\mathbf{A}$.

II. System Model and Problem Formulation

This work considers downlink transmission, in which the transmitter (Alice) has N_t transmit antennas, the legitimate receiver (Bob) has N_r receive antennas, and the eavesdropper (Eve) has $N_{r,e}$ receive antennas. We assume that the transmitter knows full CSI of Bob, but only channel statistics of Eve. We further assume that N_t is large, and in particular is much larger

than N_r and $N_{r,e}$. To maximize the achievable rate, the transmitter sends N_r data streams. Let $\mathbf{x}$ be an $N_r \times 1$ data vector. $\mathbf{x}$ is precoded by an $N_t \times N_r$ precoding matrix $\mathbf{F}$, and then transmitted to the legitimate receiver via an $N_r \times N_t$ MIMO channel $\mathbf{H}$. The signal is also received by the eavesdropper via an $N_{r,e} \times N_t$ wire-tap channel $\mathbf{H}_e$. The elements in $\mathbf{H}$ and $\mathbf{H}_e$ are assumed to be independent and identically distributed (i.i.d.) complex Gaussian with distribution $\mathcal{CN}(0,2)$, where the variance 2 is to reflect that each of the real and the imaginary parts has unit variance. In this paper, we adopt the scheme proposed in [16], where partial transmit power is used for the artificial noise. The artificial noise lies in the null space of $\mathbf{H}$. Let the $N_t \times (N_t - N_r)$ null space be $\mathbf{Z}$, such that $\mathbf{HZ} = \mathbf{0}$. The artificial noise is represented as $\mathbf{Zv}$, where $\mathbf{v}$ is an $(N_t - N_r) \times 1$ complex Gaussian noise vector with covariance matrix $\sigma_v^2\mathbf{I}$. For the legitimate receiver, the received signal can be expressed as

$$\mathbf{y} = \mathbf{HFx} + \mathbf{n}, \tag{1}$$

where $\mathbf{n}$ is an independent $N_r \times 1$ Gaussian noise vector with covariance matrix $\sigma_n^2\mathbf{I}$. For the eavesdropper, the received signal is given by

$$\mathbf{y}_e = \mathbf{H}_e\mathbf{Fx} + \mathbf{H}_e\mathbf{Zv} + \mathbf{e}, \tag{2}$$

where $\mathbf{e}$ is an independent $N_{r,e} \times 1$ Gaussian noise vector with covariance matrix $\sigma_e^2\mathbf{I}$. Let the covariance matrix of $\mathbf{x}$ be $\mathbf{K}_x$. The maximum achievable rate of the legitimate receiver is given by [24]

$$C = \log\det\left(\mathbf{I}_{N_r} + \frac{1}{\sigma_n^2}\mathbf{HFK}_x\mathbf{F}^\dagger\mathbf{H}^\dagger\right). \tag{3}$$

The maximum achievable rate of the eavesdropper can be expressed as [16], [24], [28]

$$C_e = \log\det\left(\sigma_e^2\mathbf{I}_{N_{r,e}} + \mathbf{H}_e\mathbf{FK}_x\mathbf{F}^\dagger\mathbf{H}_e^\dagger + \mathbf{H}_e\mathbf{ZZ}^\dagger\mathbf{H}_e^\dagger\sigma_v^2\right) - \log\det\left(\sigma_e^2\mathbf{I}_{N_{r,e}} + \mathbf{H}_e\mathbf{ZZ}^\dagger\mathbf{H}_e^\dagger\sigma_v^2\right). \tag{4}$$

From (3) and (4), the following secrecy rate can be achieved:

$$C_{se} \doteq C - C_e. \tag{5}$$

The goal is to maximize the average secrecy rate, i.e., $\mathbb{E}\{C_{se}\} = \mathbb{E}\{C\} - \mathbb{E}\{C_e\}$, where the expectations are with respect to the precoder and random channels. Since the eavesdropper is passive, the channel information of $\mathbf{H}_e$ is not available to the transmitter. Under this situation, it is reasonable to use the N_r singular vectors corresponding to the N_r largest singular values of $\mathbf{H}$ as the precoder [3], [16]. Thus the goal becomes to determine how to distribute the power between $\mathbf{K}_x$ and σ_v^2 to maximize C_{se}. Let the total transmit power be P. The problem can thus be formulated as follows:

$$\max_{\mathbf{K}_x,\sigma_v^2} \mathbb{E}\{C_{se}\} \quad s.t. \quad \mathbb{E}\{\mathbf{x}^\dagger\mathbf{x}\} + (N_t - N_r)\sigma_v^2 \le P. \tag{6}$$

The AN precoding systems in MISOSE, MISOME and MIMOME channels are analyzed in the following sections.

III. Achievable Rate in MISOSE Channels

This section analyzes the achievable rate for MISOSE channels. Similar procedures will be used for analyzing MISOME and MIMOME channels. In MISOSE channels, $N_r = 1$ and $\mathbf{K}_x$ becomes σ_x^2, which is the average power of the transmit data. Since the artificial noise vector is of dimension $(N_t - 1) \times 1$, the power constraint becomes $\sigma_x^2 + (N_t - 1)\sigma_v^2 \le P$. On letting θP be the power for data transmission, and $(1-\theta)P$ be that for the artificial noise, we have $\sigma_x^2 = \theta P$ and $\sigma_v^2 = (1-\theta)P/(N_t - 1)$. Let $\mathbf{h}^\dagger$ be the $1 \times N_t$ MISO channel of the legitimate receiver, and $\mathbf{h}_e^\dagger$ be the $1 \times N_t$ wire-tap channel of the eavesdropper. The precoder is

$$\mathbf{f} = \frac{\mathbf{h}}{\|\mathbf{h}\|}. \tag{7}$$

Define $\mathrm{SNR} = P/\sigma_n^2$ and $\mathrm{SNR}_e = P/\sigma_e^2$. From (3) and (4), the achievable rate of the legitimate receiver becomes

$$C = \log\left(1 + \frac{\theta P}{\sigma_n^2}|\mathbf{h}^\dagger\mathbf{f}|^2\right) = \log\left(1 + \theta\mathrm{SNR}|\mathbf{h}^\dagger\mathbf{f}|^2\right), \tag{8}$$

and the achievable rate of the eavesdropper becomes

$$C_e = \log\left(1 + \frac{\theta P\left|\mathbf{h}_e^\dagger\mathbf{f}\right|^2}{\sigma_e^2 + \frac{(1-\theta)P}{N_t-1}\left\|\mathbf{h}_e^\dagger\mathbf{Z}\right\|^2}\right) = \log\left(1 + \frac{\theta\mathrm{SNR}_e\left|\mathbf{h}_e^\dagger\mathbf{f}\right|^2}{1 + (1-\theta)\mathrm{SNR}_e\frac{\left\|\mathbf{h}_e^\dagger\mathbf{Z}\right\|^2}{N_t-1}}\right). \tag{9}$$

To analyze C and C_e, we need the statistics of $|\mathbf{h}^\dagger\mathbf{f}|^2$, $|\mathbf{h}_e^\dagger\mathbf{f}|^2$ and $\|\mathbf{h}_e^\dagger\mathbf{Z}\|^2$. The following lemmas will help in the analysis.

Lemma 1: When the precoder in (7) is used, the value of $|\mathbf{h}^\dagger\mathbf{f}|^2$ converges in probability to $2N_t$ as N_t approaches ∞.

Proof: Please see Appendix A. ∎

Lemma 2: The random variable $\|\mathbf{H}_e\mathbf{f}\|^2$ has the χ^2 distribution with $2N_{r,e}$ degrees of freedom.

Proof: Please see Appendix B. ∎

Lemma 3: When N_t approaches ∞, the achievable rate of the eavesdropper C_e can be approximated by a concave function of the random variable $|\mathbf{h}_e^\dagger\mathbf{f}|^2$, and $\mathbb{E}\{C_e\}$ can be approximately upper bounded by

$$\mathbb{E}\{C_e\} \lessapprox \log\left(1 + \frac{2\theta\mathrm{SNR}_e}{1 + 2(1-\theta)\mathrm{SNR}_e}\right). \tag{10}$$

Proof: The following equation is useful in the derivations for MISO and MIMO channels:

$$\|\mathbf{H}_e\|^2 = \|\mathbf{H}_e\mathbf{F}\|^2 + \|\mathbf{H}_e\mathbf{Z}\|^2, \tag{11}$$

where the columns of $\mathbf{F} \in \mathbb{C}^{N_t \times N_r}$ are the N_r right singular vectors corresponding to the maximum N_r singular values of $\mathbf{H}$ and $\mathbf{Z} \in \mathbb{C}^{N_t \times (N_t - N_r)}$ is the null space of $\mathbf{H}$ such that $\mathbf{HZ} = \mathbf{0}$. (11) can be easily proved by first noting that $\mathbf{FF}^\dagger + \mathbf{ZZ}^\dagger = \mathbf{I}$,

since $\mathbf{F}$ and $\mathbf{Z}$ form an orthonormal basis. Then (11) is obtained by left and right multiplying by $\mathbf{H}_e$ and taking the trace. From (9) and (11), we have

$$C_e = \log\left(1 + \frac{\theta \mathrm{SNR}_e \left|\mathbf{h}_e^\dagger \mathbf{f}\right|^2}{1 + (1-\theta)\mathrm{SNR}_e \frac{\left(\left\|\mathbf{h}_e^\dagger\right\|^2 - \left|\mathbf{h}_e^\dagger \mathbf{f}\right|^2\right)}{N_t - 1}}\right). \quad (12)$$

Using arguments similar to those used for proving Lemma 1, $\left\|\mathbf{h}_e^\dagger\right\|^2 \approx 2N_t$ as $N_t \to \infty$. Hence (12) can be approximated by

$$C_e \approx \log\left(1 + \frac{\theta \mathrm{SNR}_e \left|\mathbf{h}_e^\dagger \mathbf{f}\right|^2}{1 + (1-\theta)\mathrm{SNR}_e \frac{\left(2N_t - \left|\mathbf{h}_e^\dagger \mathbf{f}\right|^2\right)}{N_t - 1}}\right). \quad (13)$$

From Lemma 2, $\left\|\mathbf{h}_e^\dagger \mathbf{f}\right\|^2$ has the χ^2 distribution with two degrees of freedom, and its mean is $\mathbb{E}\{\left|\mathbf{h}_e^\dagger \mathbf{f}\right|^2\} = 2$. Thus, it is reasonable to say $2N_t \gg \left|\mathbf{h}_e^\dagger \mathbf{f}\right|^2$ because $N_t \gg 1$. Hence, we can further approximate (13) by

$$C_e \approx \log\left(1 + \frac{\theta \mathrm{SNR}_e \left|\mathbf{h}_e^\dagger \mathbf{f}\right|^2}{1 + 2(1-\theta)\mathrm{SNR}_e}\right), \quad (14)$$

which is a concave function of $|\mathbf{H}_e \mathbf{f}|^2$. Applying Jensen's Inequality to (14) leads to the result in (10). ■

Theorem 1: When N_t approaches ∞, the average secrecy rate for MISOSE channels can be approximately lower bounded by

$$\mathbb{E}\{C_{se}\} \gtrapprox \log(1 + 2N_t\theta\mathrm{SNR}) - \log\left(1 + \frac{2\theta\mathrm{SNR}_e}{1 + 2(1-\theta)\mathrm{SNR}_e}\right). \quad (15)$$

Proof: From (8) and Lemma 1, we have

$$\mathbb{E}\{C\} \approx \log(1 + 2N_t\theta\mathrm{SNR}). \quad (16)$$

Together with Lemma 3, this theorem is proved. ■

Discussion 1: Accuracy of Theorem 1: Please note that the approximate bound in (15) is a true bound when N_t is sufficiently large so that the approximation in (16) is accurate. When N_t is not sufficiently large, the bound in (15) may no longer be exact and it should be considered, instead, to be an approximation.

In general, however, the approximation in (16) is quite accurate. Consequently, the confidence in saying that (15) is indeed a bound is high. To see this more clearly, we discuss $\mathbb{E}\{C\}$ and $\mathbb{E}\{C_e\}$ respectively as follows: For $\mathbb{E}\{C\}$, some numerically feasible closed-form solutions can be found in [25] and [26]. More specifically, from (8) and [26]

$$\mathbb{E}\{C\} = \frac{e^{-2\theta\mathrm{SNR}}}{\ln(2)} \sum_{i=0}^{N_t-1} E_{i+1}\left(\frac{1}{2\theta\mathrm{SNR}}\right), \quad (17)$$

where $E_n(x)$ is the nth order exponential integral given by

$$E_n(x) = \int_1^\infty \frac{e^{-xt}}{t^n} dt.$$

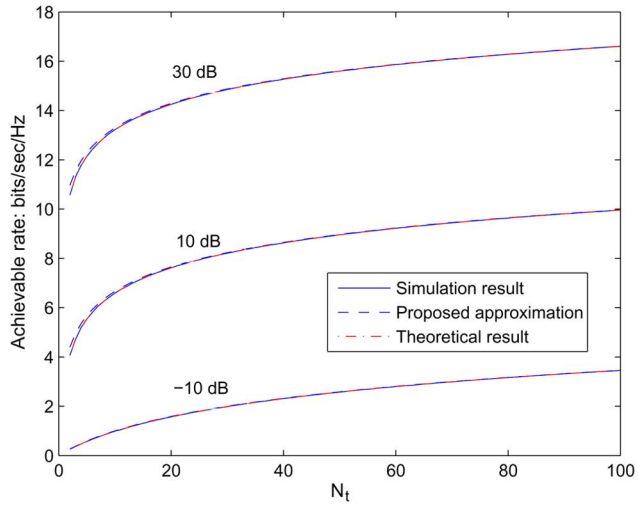

Fig. 1. Comparisons among the theoretical, simulation, and approximation results.

Let $\theta = 1/2$ and $\mathrm{SNR} = -10$, 10 and 30 dB. Fig. 1 shows the Monte Carlo simulation result, proposed approximation in (16), and the theoretical result in (17) for $\mathbb{E}\{C\}$. From the figure, the approximation in (16) is generally accurate; for instance, for $N_t > 6$, the rate difference between the approximation in (16) and the theoretical result in (17) is less than 0.1 bits/sec/Hz.

Now let us investigate $\mathbb{E}\{C_e\}$, which is defined as

$$\mathbb{E}\{C_e\} = \mathbb{E}_{\mathbf{h}_e}\left\{\mathbb{E}_{\mathbf{f}}\{C_e\}\right\}. \quad (18)$$

That is, the expected value is obtained by averaging over different precoding vectors and channels. Let us first assume the channel between the transmitter and the eavesdropper is fixed and analyze $\mathbb{E}_{\mathbf{f}}\{C_e\}$. This situation may apply in fixed communications, in which both the transmitter and the eavesdropper do not move so that the indirect channel stays unchanged for a long period. Define $a_1 = 1 + \frac{2N_t(1-\theta)\mathrm{SNR}}{N_t - 1}$, $a_2 = \frac{\mathrm{SNR}(\theta N_t - 1)}{N_t - 1}$, $a_3 = \frac{(1-\theta)\mathrm{SNR}}{N_t - 1}$, and $b = \frac{a_1(a_2 - a_3)}{2a_2a_3}$. We have the following corollary:

Corollary 1: When $\left|\mathbf{h}_e^\dagger \mathbf{f}\right|^2 < b$ and $\left\|\mathbf{h}_e^\dagger\right\|^2$ is fixed, C_e in (12) is a concave function of $\left|\mathbf{h}_e^\dagger \mathbf{f}\right|^2$, and hence $\mathbb{E}_{\mathbf{f}}\{C_e\}$ can be upper bounded by

$$\mathbb{E}_{\mathbf{f}}\{C_e\} \le \log\left(1 + \frac{2\theta\mathrm{SNR}_e}{1 + (1-\theta)\mathrm{SNR}_e \frac{\left(\left\|\mathbf{h}_e^\dagger\right\|^2 - 2\right)}{N_t - 1}}\right). \quad (19)$$

Proof: Let $x = \left|\mathbf{h}_e^\dagger \mathbf{f}\right|^2$. From (12), we have

$$C_e = \log\left(\frac{a_1 + a_2 x}{a_1 - a_3 x}\right). \quad (20)$$

It is obvious that $a_1, a_3 > 0$ for $N_t > 1$. Also, $a_2 > 0$ for $\theta > 1/N_t$. From (20), taking the first derivative of C_e yields

$$\frac{\partial C_e}{\partial x} = \frac{1}{\ln(2)}\left(\frac{a_2}{a_1 + a_2 x} + \frac{a_3}{a_1 - a_3 x}\right). \quad (21)$$

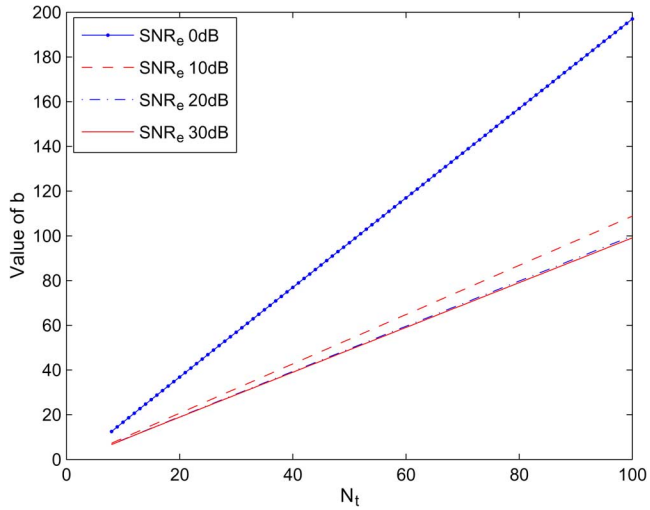

Fig. 2. Value of b.

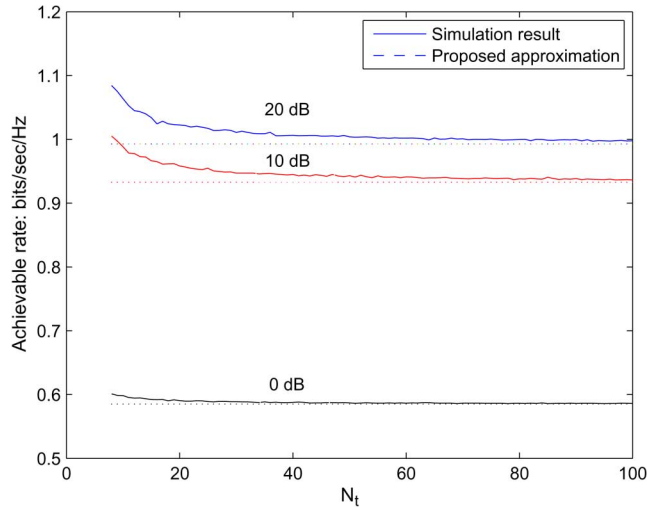

Fig. 3. Comparisons between the simulation and approximate results for C_e.

From (21), when $x < a_1/a_3$, $\frac{\partial C_e}{\partial x} > 0$; in this case, C_e is a monotonically increasing function of x. Taking the second derivative of C_e leads to

$$\frac{\partial^2 C_e}{\partial x^2} = \frac{1}{\ln(2)}\left(\frac{-a_2^2}{(a_1+a_2x)^2} + \frac{a_3^2}{(a_1-a_3x)^2}\right). \quad (22)$$

From (22), when $x < \frac{a_1(a_2-a_3)}{2a_2a_3} \equiv b$, $\frac{\partial^2 C_e}{\partial x^2} < 0$; in this case, C_e is a concave function of $\left|\mathbf{h}_e^\dagger \mathbf{f}\right|^2$, and one can apply Jensen's Inequality to (12) and obtain (19). ■

Now let us evaluate the probability that $x < b$ so that C_e is a concave function of x, and (19) is exactly an upper bound. Let $\theta = 1/2$ and $\left\|\mathbf{h}_e^\dagger\right\|^2 = 2N_t$. The value of b as a function of N_t for different values of SNR_e is shown in Fig. 2. Observe that as the value of SNR_e decreases, the value of b increases. Also, we see that b tends to be unchanged when the value of SNR_e increases to a certain level. The larger the value of b is, the higher probability that the bound in (19) holds. For example, when $\mathrm{SNR}_e = 10$ dB, $b = 7.25$ for $N_t = 8$, and $b = 16.25$ for $N_t = 16$. Since x has the χ^2 distribution with two degrees of freedom, the probability $\Pr\{x < b\}$ is 0.9734 for $N_t = 8$, and 0.9997 for $N_t = 16$, respectively.

If the indirect channel is not fixed, from (19), the average rate $\mathbb{E}\{C_e\} = \mathbb{E}_{\mathbf{h}_e}\{\mathbb{E}_{\mathbf{f}}\{C_e\}\}$ is upper bounded by

$$\mathbb{E}\{C_e\} \le \mathbb{E}_{\mathbf{h}_e}\left\{\log\left(1 + \frac{2\theta \mathrm{SNR}_e}{1+(1-\theta)\mathrm{SNR}_e \frac{\left(\left\|\mathbf{h}_e^\dagger\right\|^2 - 2\right)}{N_t - 1}}\right)\right\}, \quad (23)$$

where $\left\|\mathbf{h}_e^\dagger\right\|^2$ has the χ^2 distribution with $2N_t$ degrees of freedom. To the authors' knowledge, a simple closed-form solution for (23) is not available. Let $\theta = 1/2$. Fig. 3 shows the proposed approximate bound, i.e., $\mathbb{E}\{C_e\}$ in (10), and the Monte Carlo simulation results for (23). Observe that the approximate error is less than 0.1 bits/sec/Hz. Also, the error decreases as N_t increases because $\left\|\mathbf{h}_e^\dagger\right\|^2$ converges in probability to $2N_t$ when N_t approaches ∞. Moreover, the approximation is more accurate in the low SNR regime than in the high SNR regime. From the discussion above, we conclude

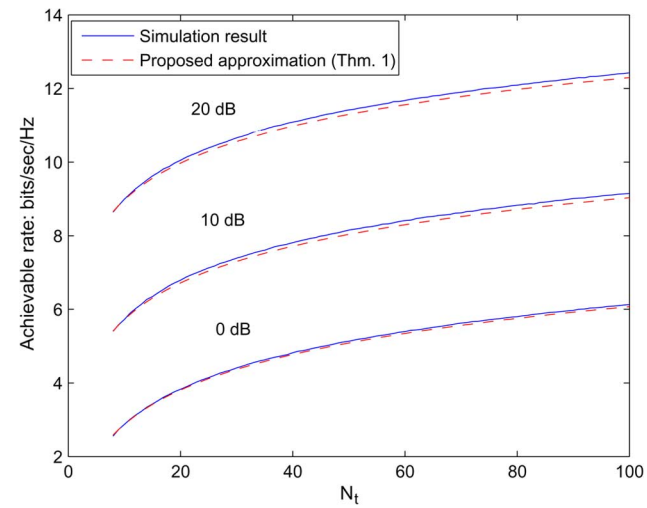

Fig. 4. Comparisons between the simulation and approximate results for C_{se}.

that the proposed approximations for $\mathbb{E}\{C\}$ and $\mathbb{E}\{C_e\}$ in Theorem 1 are generally accurate.

To compare the ergodic secrecy rate $C_{se} = C - C_e$, we assume for convenience of presentation $\sigma_n^2 = \sigma_e^2$. Fig. 4 shows the approximate result for $\mathbb{E}\{C_{se}\}$ proposed in (15) and the corresponding Monte Carlo simulation result (by using (8) and (9)). Observe from the figure, that the approximate result is generally a lower bound when N_t is sufficiently large.

Let C_0 be the achievable rate without considering the eavesdroppers; that is, C_0 can be obtained by letting $\theta = 1$ in C. To gain greater insight into the results in Theorem 1, we continue to assume that $\sigma_n^2 = \sigma_e^2$, which results in $\mathrm{SNR} = \mathrm{SNR}_e$, to have the following corollaries and remark.

Corollary 2: In the high SNR regime ($\mathrm{SNR} \gg 1$), as $N_t \to \infty$, the rate loss due to the eavesdropper in MISOSE channels, i.e., the difference between the secrecy rate and the achievable rate without the eavesdropper, can be approximately upper bounded by

$$\mathbb{E}\{C_0\} - \mathbb{E}\{C_{se}\} \lessapprox 2 \text{ bits/sec/Hz}.$$

The proposed value of θ is $\theta_0 = 1/2$.

Proof: When $\mathrm{SNR} \gg 1$, the bound in (15) can be approximately bounded by

$$\begin{aligned}\mathbb{E}\{C_{se}\} &\gtrsim \log(2N_t\theta\mathrm{SNR}) - \log\left(1+\frac{\theta}{1-\theta}\right)\\ &= \log(2N_t\mathrm{SNR}) + \log\left(\theta(1-\theta)\right). \end{aligned} \tag{24}$$

Since log is an increasing function, the value of $\log x$ is maximized when x is maximized. Hence taking the derivative of $\theta(1-\theta)$ in (15) in terms of θ, and letting it be zero, the optimal value of θ is $\theta_0 = 1/2$. This solution meets the constraint that $0 \le \theta \le 1$. Substituting θ_0 into (24) and because $C_0 \approx \log(2N_t\mathrm{SNR})$, this corollary is proved. ∎

Corollary 3: In the low SNR regime, as $N_t \to \infty$, the rate loss due to the eavesdropper in MISOSE channels, i.e., the difference between the secrecy rate and the achievable rate without the eavesdropper, can be approximated by

$$\mathbb{E}\{C_0\} - \mathbb{E}\{C_{se}\} \approx 0.$$

The proposed value of θ is $\theta_0 = 1$.

Proof: Since the denominator of $\frac{2\theta\mathrm{SNR}}{1+2(1-\theta)\mathrm{SNR}}$ is greater or equal to 1, we have

$$\frac{2\theta\mathrm{SNR}}{1+2(1-\theta)\mathrm{SNR}} \le 2\theta\mathrm{SNR}. \tag{25}$$

Since $N_t \gg 1$, the following inequalities hold:

$$2N_t\theta\mathrm{SNR} \gg 2\theta\mathrm{SNR} \ge \frac{2\theta\mathrm{SNR}}{1+2(1-\theta)\mathrm{SNR}}. \tag{26}$$

From (15) and (26), the secrecy rate is approximated by

$$\mathbb{E}\{C_{se}\} \approx \log(1+2N_t\theta\mathrm{SNR}), \tag{27}$$

where the maximum value occurs when $\theta = 1$. In this case, there is nearly no rate loss. ∎

Remark 1: From Corollaries 2–3, it is interesting to note that for AN precoding systems in MISOSE channels, the approximate rate loss is either 0 or 2 bits/sec/Hz. From the discussion above, a simple rule for the values of θ in MISOSE channels is letting $\theta_0 = 1/2$ for $\mathrm{SNR} \gg 1$ and letting $\theta_0 = 1$ for $\mathrm{SNR} \ll 1$.

Corollary 3 suggests that when the number N_t of transmit antennas is large and the SNR is small, AN precoding only slightly affects the performance. Thus, the power should all be allocated for signal transmission. It is worth pointing out that when N_t is small, the generalized AN precoding for MISOSE channels in [19] suggested not to allocate the AN power in the null space of the direct channel. Instead, most of the AN power should be allocated in the signal direction. When N_t grows, according to [19], the performance improvement due to the generalized AN decreases. That is, when N_t is sufficiently large, the generalized AN and the conventional AN precoding should achieve comparable performance.

IV. Achievable Rate in MISOME and MIMOME Channels

The MISOME channels may be regarded as a special case of MIMOME channels by letting $N_r = 1$. Thus we discuss MIMOME channels directly. In MIMOME channels, the transmitter submits N_r data streams to maximize the achievable rate of the legitimate receiver. We discuss two popular power allocation methods in MIMO communications, namely the equal power and the water-filling power allocations. Note that if the transmitter knows the statistics of the channel between the transmitter and the eavesdropper and the channel is not i.i.d., the transmitter may use the information of the covariance matrix of the channels at the eavesdropper to design the precoder, using ideas similar to those used for single-user MIMO without an eavesdropper considered in [27]. For the equal power and the water-filling power allocations, when the SNR is high, the equal power allocation achieves comparable performance to the water-filling power allocation [28]. These two power allocations schemes are discussed separately as follows.

A. Equal Power Allocation

For MIMO systems with equal power allocation, the covariance matrix of the data vector is $\mathbf{K}_x = \sigma_x^2\mathbf{I}_{N_r}$. For notational convenience, we define

$$\mathbf{A} = \mathbf{H}_e\mathbf{F}\mathbf{F}^\dagger\mathbf{H}_e^\dagger, \quad \text{and} \quad \mathbf{B} = \mathbf{H}_e\mathbf{Z}\mathbf{Z}^\dagger\mathbf{H}_e^\dagger, \tag{28}$$

where recall that the precoding matrix $\mathbf{F}$ consists of the right singular vectors corresponding to the maximum N_r singular values of $\mathbf{H}$. Also, let $\mathbf{h}_{i,e}^\dagger$ be the ith row of $\mathbf{H}_e$. Since

$$N_r\sigma_x^2 + (N_t - N_r)\sigma_v^2 \le P,$$

letting $\sigma_x^2 = \theta P/N_r$ and $\sigma_v^2 = (1-\theta)P/(N_t - N_r)$, we can rewrite (4) as

$$\begin{aligned}C_e = \log\det&\left(\sigma_e^2\mathbf{I}_{N_{r,e}} + \frac{\theta P}{N_r}\mathbf{A} + \frac{(1-\theta)P}{N_t-N_r}\mathbf{B}\right)\\ &- \log\det\left(\sigma_e^2\mathbf{I}_{N_{r,e}} + \frac{(1-\theta)P}{N_t-N_r}\mathbf{B}\right). \end{aligned} \tag{29}$$

Again, letting $\mathrm{SNR} = P/\sigma_n^2$ and $\mathrm{SNR}_e = P/\sigma_e^2$ yields

$$\begin{aligned}C_e = \log\det&\left(\mathbf{I}_{N_{r,e}} + \frac{\theta\mathrm{SNR}_e}{N_r}\mathbf{A} + \frac{(1-\theta)\mathrm{SNR}_e}{N_t-N_r}\mathbf{B}\right)\\ &- \log\det\left(\mathbf{I}_{N_{r,e}} + \frac{(1-\theta)\mathrm{SNR}_e}{N_t-N_r}\mathbf{B}\right). \end{aligned} \tag{30}$$

The statistics of the two determinant terms in (30) are discussed in the following lemmas.

Lemma 4: When $N_t \to \infty$ and $N_t \gg N_r$, the last term in (30) can be approximated by

$$\det\left(\mathbf{I}_{N_{r,e}} + \frac{(1-\theta)\mathrm{SNR}_e}{N_t-N_r}\mathbf{B}\right) \approx \prod_{i=1}^{N_{r,e}}\left(1+\frac{(1-\theta)\mathrm{SNR}_e}{N_t-N_r}[\mathbf{B}]_{ii}\right), \tag{31}$$

where

$$[\mathbf{B}]_{ii} \approx 2N_t - \left\|\mathbf{h}_{i,e}^\dagger\mathbf{F}\right\|^2. \tag{32}$$

Proof: Please see Appendix C. ∎

Discussion 2: Accuracy of Determinant Approximation: Consider further the determinant approximation in (31). According to [29], given a Hermitian matrix $\mathbf{M}$, its diagonal matrix $\mathbf{D}$ and off-diagonal matrix $\mathbf{O}$, the normalized error for

the determinant approximation depends on the radius of the matrix $\rho \equiv \rho(\mathbf{D}^{-1}\mathbf{O})$, and is bounded by

$$0 < \frac{\det(\mathbf{D}) - \det(\mathbf{M})}{\det(\mathbf{D})} \leq N_{r,e}\rho^2, \quad \text{if } \rho < \frac{1}{N_{r,e}^2}. \tag{33}$$

From (31), let

$$\mathbf{M} = \mathbf{I}_{N_{r,e}} + \frac{(1-\theta)\mathrm{SNR}_e}{N_t - N_r}(\mathbf{B}_d + \mathbf{B}_o) = \mathbf{D} + \mathbf{O},$$

where $\mathbf{B}_d$ and $\mathbf{B}_o$ are the diagonal and the off-diagonal matrices of $\mathbf{B}$ respectively, and

$$\mathbf{D} = \mathbf{I}_{N_{r,e}} + \frac{(1-\theta)\mathrm{SNR}_e}{N_t - N_r}\mathbf{B}_d \quad \text{and} \quad \mathbf{O} = \frac{(1-\theta)\mathrm{SNR}_e}{N_t - N_r}\mathbf{B}_o. \tag{34}$$

From (32), when $N_t \gg N_r$, $[\mathbf{B}]_{ii} \approx 2N_t$. Hence, $\mathbf{D}^{-1}\mathbf{O}$ can be approximated by

$$\begin{aligned}\mathbf{D}^{-1}\mathbf{O} &\approx \frac{(1-\theta)\mathrm{SNR}_e}{(N_t - N_r)\left(1 + 2(1-\theta)\mathrm{SNR}_e\right)}\mathbf{B}_o \\ &\approx \begin{cases} \frac{1}{2(N_t - N_r)}\mathbf{B}_o, & \mathrm{SNR}_e \gg 1; \\ \frac{(1-\theta)\mathrm{SNR}_e}{N_t - N_r}\mathbf{B}_o, & \mathrm{SNR}_e \ll 1. \end{cases}\end{aligned} \tag{35}$$

In the proof of Lemma 4, since $[\mathbf{B}]_{ij} \sim \mathcal{CN}(0, 2(N_t - N_r))$ (see (67)), the elements of $\mathbf{D}^{-1}\mathbf{O}$ are distributed as follows:

$$[\mathbf{D}^{-1}\mathbf{O}]_{ij} \sim \begin{cases} \mathcal{CN}\left(0, \frac{1}{2(N_t - N_r)}\right), & \mathrm{SNR}_e \gg 1; \\ \mathcal{CN}\left(0, \frac{2(1-\theta)^2\mathrm{SNR}_e^2}{N_t - N_r}\right), & \mathrm{SNR}_e \ll 1. \end{cases} \tag{36}$$

The radius ρ of a matrix is the absolute value of its maximum eigenvalue. Taking $N_r = N_{r,e} = 2$ for instance, the eigenvalue of $\mathbf{D}^{-1}\mathbf{O}$ is $\pm\sqrt{[\mathbf{D}^{-1}\mathbf{O}]_{12}^*[\mathbf{D}^{-1}\mathbf{O}]_{21}}$. In this case, ρ has the Rayleigh distribution [23], i.e.,

$$\rho \sim \begin{cases} \mathcal{R}ayleigh\left(\frac{1}{2}\sqrt{\frac{1}{N_t - N_r}}\right), & \mathrm{SNR}_e \gg 1; \\ \mathcal{R}ayleigh\left(\sqrt{\frac{1}{N_t - N_r}(1-\theta)\mathrm{SNR}_e}\right), & \mathrm{SNR}_e \ll 1. \end{cases} \tag{37}$$

From (37), the radius is highly affected by N_t in both high and low SNR regimes. For example, when $\mathrm{SNR}_e \gg 1$, $\Pr\{\rho < 1/N_{r,e}^2 = 1/4\} \geq 0.9996$, for $N_t \geq 64$. Thus, when $N_t \geq 64$, the second condition in (33) that $\rho < 1/N_{r,e}^2$ holds with very high probability. When $N_t \gg N_r$ the ρ will be near its mean value $\bar{\rho}$ with high probability. If a realization of ρ is $\bar{\rho} = \sigma\sqrt{\frac{\pi}{2}} = \frac{1}{2}\sqrt{\frac{1}{N_t - 2}\frac{\pi}{2}}$, the normalized error is bounded by $N_{r,e}\bar{\rho}^2 \lessapprox 8.014 \times 10^{-3}$ for $N_t = 100$. If the true determinant value is, for instance 128, the corresponding rate is $\log(128) = 7$; the approximate determinant value is bounded by $128 + 128 \times 8.014 \times 10^{-3}$, which results in an achievable rate being 7.0115.

Lemma 5: The first term in (30) can be upper bounded by

$$\begin{aligned}&\det\left(\mathbf{I}_{N_{r,e}} + \frac{\theta\mathrm{SNR}_e}{N_r}\mathbf{A} + \frac{(1-\theta)\mathrm{SNR}_e}{N_t - N_r}\mathbf{B}\right) \\ &\quad\leq \prod_{i=1}^{N_{r,e}}\left(1 + \frac{\theta\mathrm{SNR}_e}{N_r}[\mathbf{A}]_{ii} + \frac{(1-\theta)\mathrm{SNR}_e}{N_t - N_r}[\mathbf{B}]_{ii}\right),\end{aligned} \tag{38}$$

where

$$[\mathbf{A}]_{ii} = \left\|\mathbf{h}_{i,e}^\dagger\mathbf{F}\right\|^2. \tag{39}$$

Proof: Please see Appendix D. ∎

Lemma 6: When N_t approaches ∞, the achievable rate of the eavesdropper C_e can be approximated by a sum of $N_{r,e}$ concave functions of the random variables $\|\mathbf{h}_{i,e}^\dagger\mathbf{F}\|^2$, where $1 \leq i \leq N_{r,e}$. In addition, $\mathbb{E}\{C_e\}$ can be approximately upper bounded by

$$\mathbb{E}\{C_e\} \lessapprox N_{r,e}\log\left(1 + \frac{2\theta\mathrm{SNR}_e}{1 + 2(1-\theta)\mathrm{SNR}_e}\right). \tag{40}$$

Proof: From (30) and Lemmas 4–5, C_e can be approximately bounded by (41), shown at the bottom of the page. Since $\|\mathbf{h}_{i,e}^\dagger\mathbf{F}\|^2$ has the χ^2 distribution with $2N_r$ degrees of freedom, its mean is $2N_r$. Thus, when $N_t \gg N_r$, it is reasonable to say $2N_t \gg \|\mathbf{h}_{i,e}^\dagger\mathbf{F}\|^2$. Hence (41) can be further approximated by

$$C_e \lessapprox \sum_{i=1}^{N_{r,e}}\log\left(1 + \frac{\theta\mathrm{SNR}_e\frac{\|\mathbf{h}_{i,e}^\dagger\mathbf{F}\|^2}{N_r}}{1 + 2(1-\theta)\mathrm{SNR}_e}\right), \tag{42}$$

which is a sum of $N_{r,e}$ concave functions of $\|\mathbf{h}_{i,e}^\dagger\mathbf{F}\|^2$. By using Jensen's Inequality, the mean value of C_e can be approximately bounded by (40), which completes the proof. ∎

Next let us discuss the statistics of the achievable rate of the legitimate receiver. The following lemma is used to approximate the achievable rate.

Lemma 7: Extreme Eigenvalue Approximations [30]: When N_t approaches ∞, the maximum eigenvalue λ_{max} of $\mathbf{H}\mathbf{H}^\dagger$ converges in probability as follows:

$$\frac{\lambda_{max}}{N_t} \xrightarrow{p} 2\left(1 + \sqrt{\frac{N_r}{N_t}}\right)^2, \tag{43}$$

and the minimum eigenvalue λ_{min} of $\mathbf{H}\mathbf{H}^\dagger$ converges in probability as follows:

$$\frac{\lambda_{min}}{N_t} \xrightarrow{p} 2\left(1 - \sqrt{\frac{N_r}{N_t}}\right)^2. \tag{44}$$

$$C_e \lessapprox \log\prod_{i=1}^{N_{r,e}}\left(\frac{1 + \theta\mathrm{SNR}_e\frac{\|\mathbf{h}_{i,e}^\dagger\mathbf{F}\|^2}{N_r} + (1-\theta)\mathrm{SNR}_e\frac{2N_t - \|\mathbf{h}_{i,e}^\dagger\mathbf{F}\|^2}{N_t - N_r}}{1 + (1-\theta)\mathrm{SNR}_e\frac{2N_t - \|\mathbf{h}_{i,e}^\dagger\mathbf{F}\|^2}{N_t - N_r}}\right) = \log\prod_{i=1}^{N_{r,e}}\left(1 + \frac{\theta\mathrm{SNR}_e\frac{\|\mathbf{h}_{i,e}^\dagger\mathbf{F}\|^2}{N_r}}{1 + (1-\theta)\mathrm{SNR}_e\frac{2N_t - \|\mathbf{h}_{i,e}^\dagger\mathbf{F}\|^2}{N_t - N_r}}\right). \tag{41}$$

Lemma 8: When $N_t \to \infty$ and $N_t \gg N_r$, the achievable rate of the legitimate receiver can be approximated by

$$C \approx N_r \log\left(1 + \frac{2N_t\theta\mathrm{SNR}}{N_r}\right). \quad (45)$$

Proof: Please see Appendix E. ∎

It is worth mentioning that the same approximate result as in (45) can be obtained by using the property that $\det(\mathbf{I}+\mathbf{AB}) = \det(\mathbf{I}+\mathbf{BA})$, and the asymptotic property that $\mathbf{H}^\dagger\mathbf{H}$ converges to $2N_t\mathbf{I}_{N_r}$ as $N_t \to \infty$, mentioned in [31].

Theorem 2: When N_t approaches ∞ and $N_t \gg N_r$, the average secrecy rate for MIMOME channels can be approximately lower bounded by

$$\mathbb{E}\{C_{se}\} \gtrapprox N_r \log\left(1 + \frac{2N_t\theta\mathrm{SNR}}{N_r}\right) - N_{r,e}\log\left(1 + \frac{2\theta\mathrm{SNR}_e}{1+2(1-\theta)\mathrm{SNR}_e}\right). \quad (46)$$

Proof: The theorem is a direct result of Lemma 6 and Lemma 8. ∎

To gain greater insight into the results in Theorem 2, again, we assume $\sigma_n^2 = \sigma_e^2$, which leads to $\mathrm{SNR} = \mathrm{SNR}_e$, to have the following corollaries and remark.

Corollary 4: In the high SNR regime ($\mathrm{SNR} \gg 1$), as $N_t \to \infty$, the rate loss due to the eavesdropper in MIMOME channels, i.e., $\mathbb{E}\{C_0\} - \mathbb{E}\{C_{se}\}$, the difference between the secrecy rate and the achievable rate without the eavesdropper, can be approximately upper bounded by

$$-N_r\log\left(\frac{N_r}{N_r+N_{r,e}}\right) - N_{r,e}\log\left(\frac{N_{r,e}}{N_r+N_{r,e}}\right) \text{ bits/sec/Hz}.$$

The proposed value of θ is

$$\theta_0 \approx \frac{N_r}{N_r+N_{r,e}}.$$

Proof: When $\mathrm{SNR} \gg 1$, the bound in (46) can be approximately bounded by

$$\mathbb{E}\{C_{se}\} \gtrapprox N_r\log\left(\frac{2N_t\theta\mathrm{SNR}}{N_r}\right) - N_{r,e}\log\left(1+\frac{\theta}{1-\theta}\right) = N_r\log\left(\frac{2N_t\mathrm{SNR}}{N_r}\right) + \log\left(\theta^{N_r}(1-\theta)^{N_{r,e}}\right). \quad (47)$$

The first term in (47) is irrelevant to θ. Since log is an increasing function, the value of $\log x$ is maximized whenever x is maximized. Taking the derivative of $\theta^{N_r}(1-\theta)^{N_{r,e}}$ in (47) in terms of θ, and letting it be zero, the optimal value of θ is $\theta_0 = N_r/(N_r+N_{r,e})$. This solution meets the constraint that $0 \le \theta \le 1$. Substituting θ_0 into (47) and using the fact that $C_0 \approx N_r\log\left(\frac{2N_t\mathrm{SNR}}{N_r}\right)$, this corollary is proved. ∎

Corollary 5: In the low SNR regime, as $N_t \to \infty$, the rate loss due to the eavesdropper in MIMOME channels, i.e., $\mathbb{E}\{C_0\} - \mathbb{E}\{C_{se}\}$, the difference between the secrecy rate and the achievable rate without the eavesdropper, can be approximated by

$$\mathbb{E}\{C_0\} - \mathbb{E}\{C_{se}\} \approx N_{r,e}\log(1+2\mathrm{SNR}).$$

The proposed value of θ is $\theta_0 = 1$.

Proof: From the last log term in (46), when $\mathrm{SNR} \ll 1$, the value $(1+2(1-\theta)\mathrm{SNR}) \lessapprox 1$. This approximation leads to the following inequality:

$$1 + \frac{2\theta\mathrm{SNR}}{1+2(1-\theta)\mathrm{SNR}} = \frac{1+2\mathrm{SNR}}{1+2(1-\theta)\mathrm{SNR}} \lessapprox 1+2\mathrm{SNR}. \quad (48)$$

The approximate bound in (46) becomes

$$\mathbb{E}\{C_{se}\} \gtrapprox N_r\log\left(1+\frac{2N_t\theta\mathrm{SNR}}{N_r}\right) - N_{r,e}\log(1+2\mathrm{SNR}). \quad (49)$$

From (49), $\mathbb{E}\{C_{se}\}$ is maximized when $\theta = 1$. In this case, the rate loss is given by

$$\mathbb{E}\{C_0\} - \mathbb{E}\{C_{se}\} \approx N_{r,e}\log(1+2\mathrm{SNR}). \quad (50)$$

Note that from (49), when $N_r \approx N_{r,e}$ and $\theta = 1$, the rate loss in (50) is negligible because

$$N_r\log\left(1+2\mathrm{SNR}\frac{N_t}{N_r}\right) \gg N_{r,e}\log(1+2\mathrm{SNR}),$$

due to the fact that $N_t \gg N_r$. In this case, it is reasonable to say that there is nearly no rate loss. ∎

Remark 2: According to Theorems 1–2 and Corollaries 2–5, in the low SNR regime, the proposed value of θ is 1 and there is nearly no rate loss when precoding systems are used in both MISOME and MIMOME channels. On the other hand, in the high SNR regime, the results for MIMOME channels depend on N_r and $N_{r,e}$. However, when $N_r = N_{r,e}$, the resulting value of θ for MIMOME channels is the same as that for MISOSE channels, i.e., $\theta_0 = 1/2$; also the rate loss for MIMOME channels is $N_r + N_{r,e} = 2N_r$, which increases linearly with N_r. It is worth mentioning that the results for MISOSE channels can be regarded as a special case of MIMOME channels by letting $N_r = N_{r,e} = 1$.

B. Water-Filling Power Allocation

Since the CSI at the eavesdropper is not available to the transmitter, the power allocation is determined solely by the CSI at the legitimate receiver. Recall that $\mathbf{x}$ is of dimension $N_r \times 1$, and the average transmit power σ_x^2 is given by

$$\sigma_x^2 = \frac{1}{N_r}\mathbb{E}\{\mathbf{x}^\dagger\mathbf{x}\}. \quad (51)$$

Let the covariance matrix of the transmitted signal be

$$\mathbf{K}_x = \mathrm{diag}\left(\sigma_{x_1}^2\sigma_{x_1}^2\cdots\sigma_{x_{N_r}}^2\right) = \sigma_x^2\mathrm{diag}(\alpha_1\alpha_2\cdots\alpha_{N_r}), \quad (52)$$

where α_i is a power allocation coefficient such that $\sigma_{x_i}^2 = \alpha_i\sigma_x^2$. From (51) and (52), we have

$$\mathrm{Tr}(\mathbf{K}_x) = \sigma_x^2\sum_{i=1}^{N_r}\alpha_i = \mathbb{E}\{\mathbf{x}^\dagger\mathbf{x}\} = N_r\sigma_x^2. \quad (53)$$

From (53), we have

$$\frac{1}{N_r}\sum_{i=1}^{N_r}\alpha_i = 1. \quad (54)$$

Because $\mathbb{E}\{\mathbf{x}^\dagger\mathbf{x}\} = \theta P$, from (51), $\sigma_x^2 = \frac{\theta P}{N_r}$. With water-filling power allocation, the achievable rate of the legitimate receiver is given by [28]

$$C = \sum_{i=1}^{N_r} \log\left(1 + \frac{\sigma_{x_i}^2}{\sigma_n^2}\lambda_i\right) = \sum_{i=1}^{N_r} \log\left(1 + \alpha_i \frac{\theta P}{N_r}\frac{1}{\sigma_n^2}\lambda_i\right) = \sum_{i=1}^{N_r} \log\left(1 + \frac{\theta \mathrm{SNR}}{N_r}\alpha_i\lambda_i\right), \quad (55)$$

where λ_i is the ith eigenvalue of $\mathbf{H}\mathbf{H}^\dagger$, and $\sigma_{x_i}^2$ with water-filling power allocation is

$$\sigma_{x_i}^2 = \left(\mu - \frac{\sigma_n^2}{\lambda_i}\right)^+, \quad (56)$$

with μ chosen to satisfy the power constraint $\sum_{i=1}^{N_r}\sigma_{x_i}^2 = \theta P$. α_i is available when $\sigma_{x_i}^2$ is obtained.

Lemma 9: When N_t approaches ∞, the achievable rate of the eavesdropper C_e can be approximated by a sum of $N_{r,e}$ concave functions of the random variables $\sum_{j=1}^{N_r}\alpha_i|\mathbf{h}_{i,e}^\dagger\mathbf{f}_j|^2$, where $1 \le i \le N_{r,e}$. Also, $\mathbb{E}\{C_e\}$ can be approximately upper bounded by

$$\mathbb{E}\{C_e\} \lessapprox N_{r,e}\log\left(1 + \frac{2\theta\mathrm{SNR}_e}{1 + 2(1-\theta)\mathrm{SNR}_e}\right). \quad (57)$$

Proof: From (4), (28), (30) and (52), allocating power only affects the matrix $\mathbf{A}$. Now $\mathbf{A} = \mathbf{H}_e\mathbf{F}\mathbf{D}_x\mathbf{F}^\dagger\mathbf{H}_e^\dagger$, where $\mathbf{D}_x = \mathrm{diag}(\alpha_1\alpha_2\cdots\alpha_{N_r})$. Hence the elements of $\mathbf{A}$ are

$$[\mathbf{A}]_{ij} = \begin{cases} \sum_{j=1}^{N_r}\alpha_i\left|\mathbf{h}_{i,e}^\dagger\mathbf{f}_j\right|^2, & i = j; \\ \sum_{k=1}^{N_r}\alpha_i\left(\mathbf{h}_{i,e}^\dagger\mathbf{f}_k\right)\left(\mathbf{h}_{j,e}^\dagger\mathbf{f}_k\right)^*, & i \ne j. \end{cases} \quad (58)$$

The random variable α_i is correlated with the eigenvalues λ_i. By using the new definition of $\mathbf{A}$ in (58), C_e can be represented by (30). Using arguments similar to those in Lemmas 4–6, C_e can be approximately bounded by

$$C_e \lessapprox \sum_{i=1}^{N_{r,e}}\log\left(1 + \frac{\theta\mathrm{SNR}_e\frac{\sum_{j=1}^{N_r}\alpha_i|\mathbf{h}_{i,e}^\dagger\mathbf{f}_j|^2}{N_r}}{1 + 2(1-\theta)\mathrm{SNR}_e}\right), \quad (59)$$

which is a sum of $N_{r,e}$ concave functions of $\sum_{j=1}^{N_r}\alpha_i|\mathbf{h}_{i,e}^\dagger\mathbf{f}_j|^2$. By using Jensen's Inequality and from (59), the mean value of C_e is bounded by

$$\mathbb{E}\{C_e\} \lessapprox \sum_{i=1}^{N_{r,e}}\log\left(1 + \frac{\theta\mathrm{SNR}_e\frac{\sum_{j=1}^{N_r}\mathbb{E}\left\{\alpha_i|\mathbf{h}_{i,e}^\dagger\mathbf{f}_j|^2\right\}}{N_r}}{1 + 2(1-\theta)\mathrm{SNR}_e}\right). \quad (60)$$

According to [32], the singular values are distributed independently of the corresponding right singular vectors. Hence, α_i is distributed independently of $\mathbf{f}_i$. From (54), $\mathbb{E}\{\alpha_i\} = 1$, we have the following equality:

$$\mathbb{E}\left\{\alpha_i\left|\mathbf{h}_{i,e}^\dagger\mathbf{f}\right|^2\right\} = \mathbb{E}\{\alpha_i\}\mathbb{E}\left\{\left|\mathbf{h}_{i,e}^\dagger\mathbf{f}\right|^2\right\} = 2. \quad (61)$$

Using (60) and (61) leads to the result in (57). ■

Theorem 3: When N_t approaches ∞ and $N_t \gg N_r$, the average secrecy rate for MIMOME channels with water-filling power allocation can be approximated by (62), shown at the bottom of the page, where γ is defined as

$$\gamma = \sum_{i=1}^{N_r}\mathbb{E}\{\alpha_i\lambda_i\}. \quad (63)$$

Proof: From (40) and (57), it is interesting to note that $\mathbb{E}\{C_e\}$ with equal power and water-filling power allocations is theoretically bounded by the same form. Thus the difference in $\mathbb{E}\{C_{se}\}$ between these two power allocations is mainly determined by $\mathbb{E}\{C\}$. In the high SNR regime, using equal power allocation achieves nearly the same value of $\mathbb{E}\{C\}$ with that obtained by using water-filling power allocation [28]. Hence, $\mathbb{E}\{C_e\}$ with water-filling power allocation is nearly the same as that with equal power allocation.

For low SNRs, substituting the approximation $\log(1+x) \approx x\log e$ into (55) and (57) yields the result in (62). ■

Using arguments and derivations similar to those in Corollaries 4–5, and assuming $\sigma_n^2 = \sigma_e^2$, we have the following two corollaries.

Corollary 6: Using water-filling power allocation in the high SNR regime, as $N_t \to \infty$, the rate loss due to the eavesdropper in MIMOME channels, i.e., $\mathbb{E}\{C_0\} - \mathbb{E}\{C_{se}\}$, the difference between the secrecy rate and the achievable rate without the eavesdropper, can be approximately upper bounded by

$$-N_r\log\left(\frac{N_r}{N_r + N_{r,e}}\right) - N_{r,e}\log\left(\frac{N_{r,e}}{N_r + N_{r,e}}\right) \text{ bits/sec/Hz}.$$

The proposed value of θ is

$$\theta_0 \approx \frac{N_r}{N_r + N_{r,e}}.$$

Corollary 7: Using water-filling power allocation in the low SNR regime, as $N_t \to \infty$, the rate loss due to the eavesdropper in MIMOME channels, i.e., the difference between the secrecy rate and the achievable rate without the eavesdropper, can be approximated by

$$\mathbb{E}\{C_0\} - \mathbb{E}\{C_{se}\} \approx 2N_{r,e}\mathrm{SNR}\log e.$$

$$\mathbb{E}\{C_{se}\} \approx \begin{cases} \theta\left(\frac{\gamma\mathrm{SNR}}{N_r} - \frac{2N_{r,e}\mathrm{SNR}_e}{1+2(1-\theta)\mathrm{SNR}_e}\right)\log e \text{ bits/sec/Hz}, & \mathrm{SNR}N_t \ll 1 \text{ and } \mathrm{SNR}_e \ll 1; \\ N_r\log\left(1 + \frac{2N_t\theta\mathrm{SNR}}{N_r}\right) - N_{r,e}\log\left(1 + \frac{2\theta\mathrm{SNR}_e}{1+2(1-\theta)\mathrm{SNR}_e}\right) \text{ bits/sec/Hz}, & \text{otherwise}, \end{cases} \quad (62)$$

The proposed value of θ is $\theta_0 = 1$. The rate loss is negligible when $N_t \gg N_r \approx N_{r,e}$.

From Corollaries 2 and 6, in the high SNR regime, the rate loss with and without water-filling power allocation is nearly the same. This is reasonable because water-filling power allocation tends to be equal power allocation as SNR grows [28]. On the other hand, in the low SNR regime, the rate loss with and without water-filling power allocation is also close according to Corollaries 3 and 7. This is also reasonable because the achievable rate of the legitimate receiver is much larger than that of the eavesdropper regardless of whether or not water-filling power allocation is applied. Consequently, AN precoding only slightly affects the secrecy rate, and all power should be allocated for signal transmission in the low SNR regime.

V. Simulation Results

In this section, simulation results are provided to verify the accuracy of the theoretical results as well as demonstrate how the proposed values of θ improve the performance. The theoretical results are plotted according to the proposed theorems and corollaries. Again, for convenience of presentation, we let $\sigma_n^2 = \sigma_e^2$ and thus $\mathrm{SNR} = \mathrm{SNR}_e$. The simulation results are obtained by conducting Monte Carlo simulation for 10^5 different channel realizations. The number of transmit antennas $N_t = 100$ is used if it is not otherwise specifically mentioned.

Example 1: Theoretical and Simulation Results in MISOSE Channels: Let $N_r = N_{r,e} = 1$. The average secrecy rates for MISOSE channels are shown in Fig. 5, where the achievable rate without considering Eve, i.e., $\mathbb{E}\{C_0\}$, is also shown to serve as a performance benchmark. Observe that the simulation results match well with the theoretical results. First, the average secrecy rate does obey Theorem 1. Second, when $\mathrm{SNR} \gg 1$, the optimal value of θ is around 1/2 and the corresponding rate loss is around 2 bits/sec/Hz, which corroborates the results in Corollary 2. Third, when the SNR decreases, the rate loss decreases; the optimal value of θ is around 1 and the corresponding rate loss is negligible when $\mathrm{SNR} \ll 1$ (see the curve with $\mathrm{SNR} = -20$ dB), which corroborates the results in Corollary 3. Moreover, we also see from the figure that the rate loss is large if an inappropriate value of θ is applied. As for the proposed value $\theta = 1/2$, although the optimal value of θ is not exactly at 1/2, the achievable rate obtained by the optimal value of θ using simulation is very close to that obtained by the proposed value of θ. To see this more clearly, Fig. 6 shows the achievable rates obtained by simulation and the proposed values of θ as functions of SNR. Observe that the proposed values of θ achieves comparable rates to those obtained via simulation (see the circles and dots). This shows that the proposed values of θ are indeed good solutions for AN precoding systems.

Example 2: Theoretical and Simulation Results in MISOME and MIMOME Channels: This example shows the average secrecy rates for MISOME and MIMOME channels. For MISOME channels, let $N_r = 1$ and $N_{r,e} = 2$. For MIMOME channels, let $N_r = 4$ and $N_{r,e} = 4$. The average secrecy rates for MISOME and MIMOME channels are shown in Figs. 7 and 8, respectively, where the achievable rates without considering Eve, i.e., $\mathbb{E}\{C_0\}$, are also provided to serve as performance benchmarks. Performance trends similar to those in Example 1

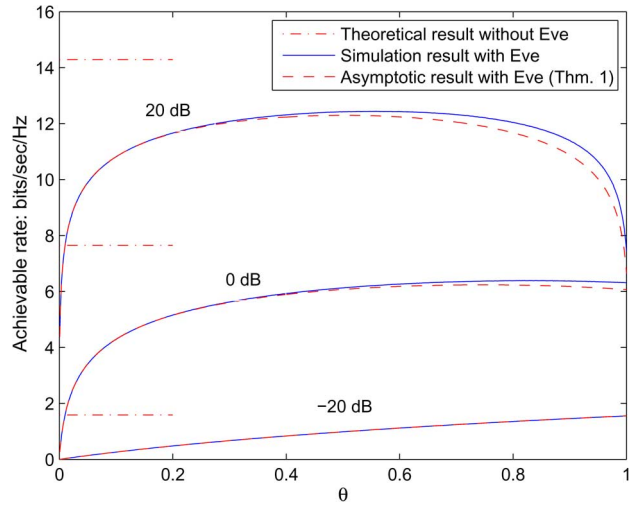

Fig. 5. $\mathbb{E}\{C_{se}\}$ as a function of θ for MISOSE channels; $N_t = 100$, $N_r = N_{r,e} = 1$.

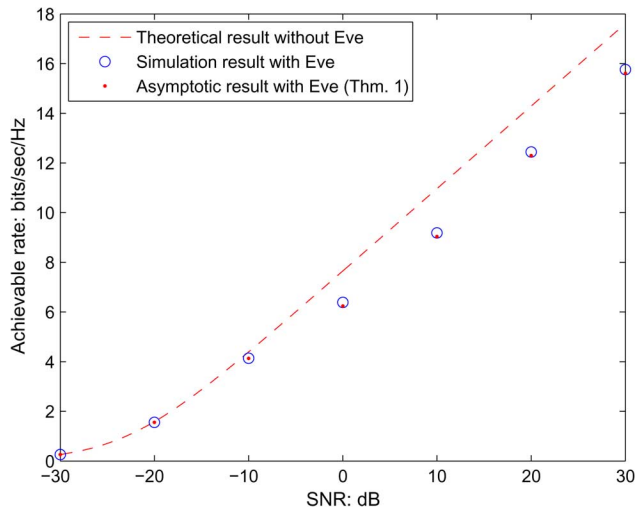

Fig. 6. $\mathbb{E}\{C_{se}\}$ as a function of SNR for MISOSE channels; $N_t = 100$, $N_r = N_{r,e} = 1$.

are observed from these two figures. First, the average secrecy rate indeed fellows Theorem 2 well. Second, when $\mathrm{SNR} \gg 1$, the optimal value of θ is around $N_r/(N_r + N_{r,e})$ (1/3 in Fig. 7, and 1/2 in Fig. 8) and the corresponding rate loss is around $-N_r \log\left(\frac{N_r}{N_r+N_{r,e}}\right) - N_{r,e} \log\left(\frac{N_{r,e}}{N_r+N_{r,e}}\right)$ bits/sec/Hz (2.755 in Fig. 7, and 8 in Fig. 8), which corroborates the results in Corollary 4. Third, when the SNR decreases, the rate loss decreases; the optimal value of θ is around 1 and the corresponding rate loss is negligible when $\mathrm{SNR} \ll 1$ (see the curves with $\mathrm{SNR} = -20$ dB in these two figures), which corroborates the results in Corollary 5. As for the proposed value of θ, although it is not exactly the optimal value, the achievable rate obtained by the optimal value of θ via simulation is very close to that obtained by the proposed value of θ. To see this more clearly, Figs. 9 and 10 show the achievable rates obtained by simulation and the proposed values of θ as functions of SNR for MISOME and MIMOME channels, respectively. Observe that the proposed values of θ achieve rates comparable to those obtained by simulation (see the circles and dots in the two

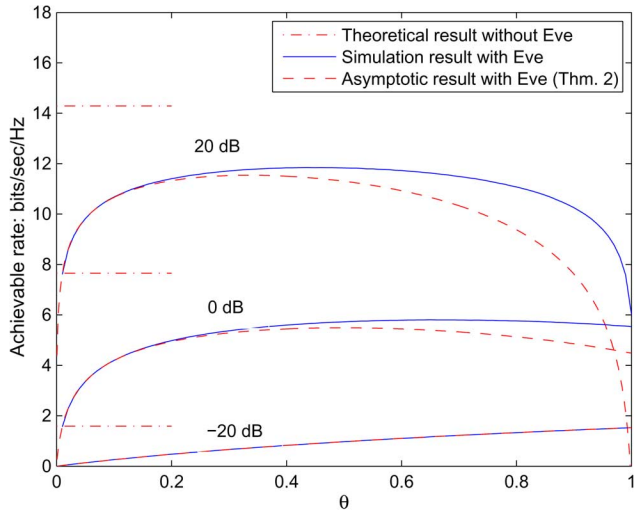

Fig. 7. $\mathbb{E}\{C_{se}\}$ as a function of θ for MISOME channels; $N_t = 100, N_r = 1$ and $N_{r,e} = 2$.

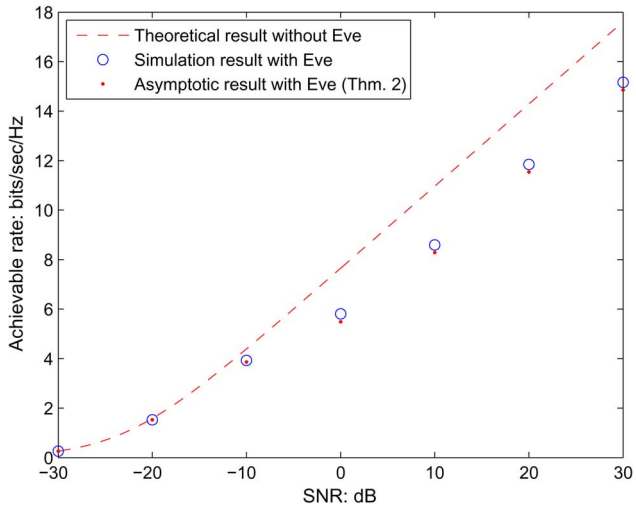

Fig. 9. $\mathbb{E}\{C_{se}\}$ as a function of SNR for MISOME channels; $N_t = 100$, $N_r = 1$ and $N_{r,e} = 2$.

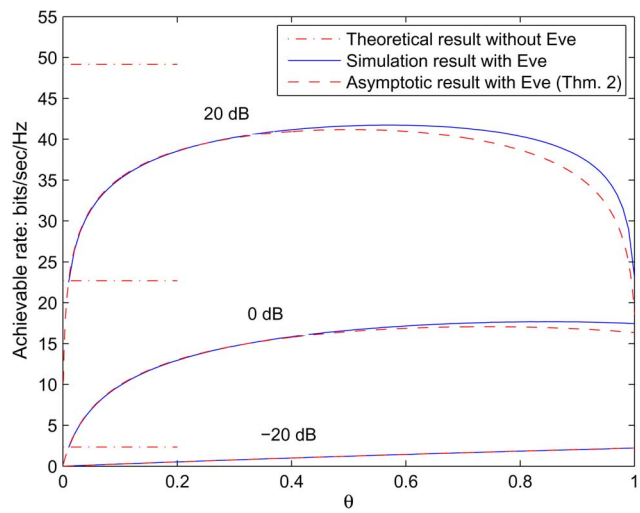

Fig. 8. $\mathbb{E}\{C_{se}\}$ as a function of θ for MIMOME channels; $N_t = 100, N_r = 4$ and $N_{r,e} = 4$.

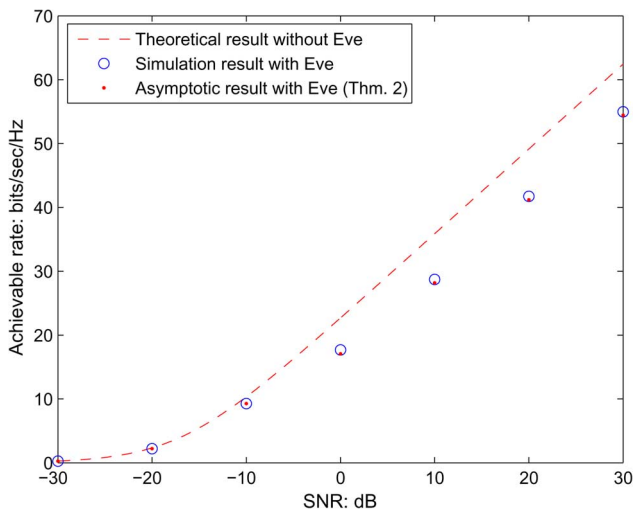

Fig. 10. $\mathbb{E}\{C_{se}\}$ as a function of SNR for MIMOME channels; $N_t = 100$, $N_r = 4$ and $N_{r,e} = 4$.

figures). This again shows that the proposed values of θ are indeed good solutions for AN precoding systems in MISOME and MIMOME channels. Finally, it is worth pointing out that in the high SNR regime, the gap between the simulation and the theoretical results is more pronounced when the value of θ is close to 1, see e.g., the curves with $\mathrm{SNR} = 20$ dB in Fig. 7. This is reasonable because referring to (38), when the value of θ and SNR increase, the matrix $\mathbf{A}$ affects the approximation significantly. For $N_r \neq 1$, the approximation is more accurate for $N_r \geq N_{r,e}$ than for $N_r < N_{r,e}$. Fortunately, when $N_{r,e}$ increases, the optimal value of θ tends to be small according to Corollary 4, and the proposed approximation is accurate for small values of θ. As a result, the proposed values of θ can still lead to achievable rates comparable to those obtained via simulations (see the circles and dots in Fig. 9).

Example 3: Proposed Values of θ for Different SNRs: Letting $N_r = 2$, the proposed value of θ as a function of the SNR is evaluated for different values of $N_{r,e}$, and is shown in Fig. 11 for

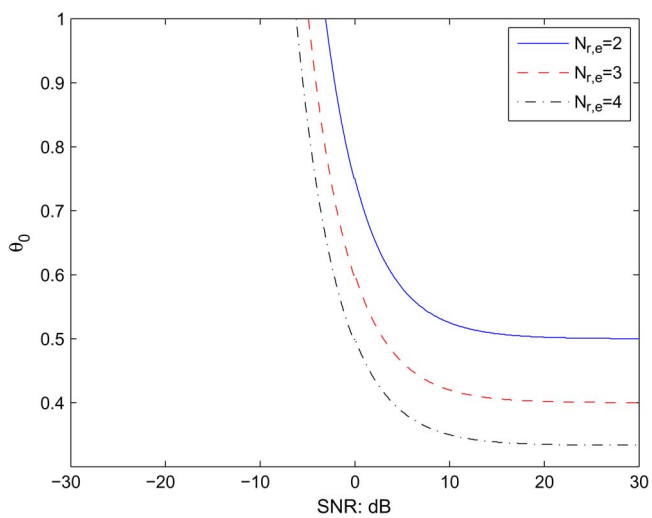

Fig. 11. Optimal value of θ for MIMO channels; $N_t = 100, N_r = 2$.

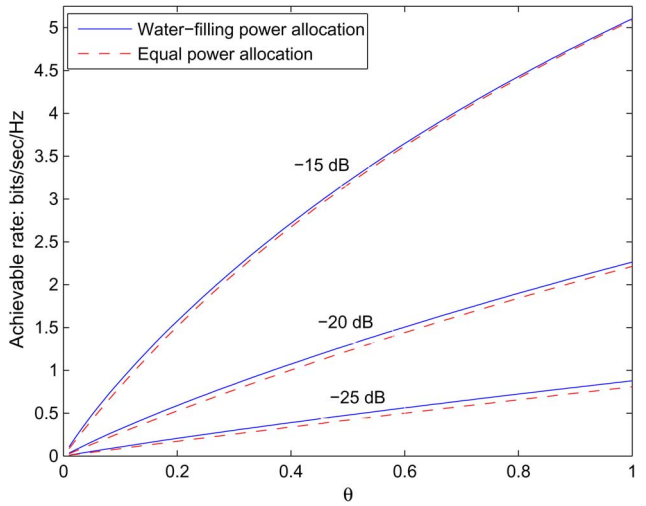

Fig. 12. Comparison of equal power and water-filling power allocations; $N_t = 100$, $N_r = 4$ and $N_{r,e} = 4$.

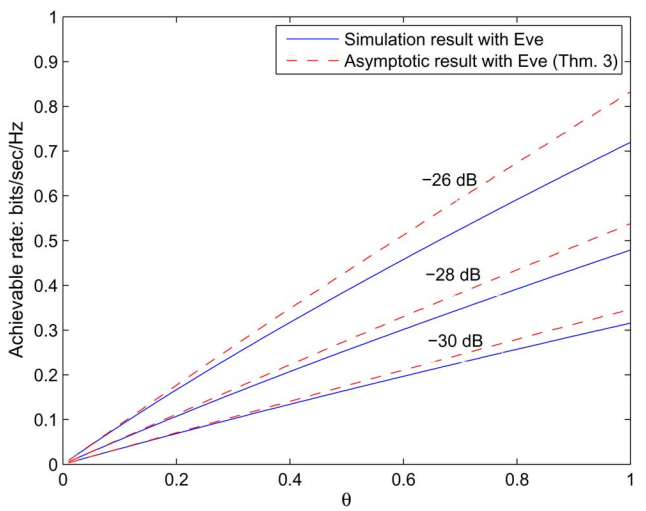

Fig. 13. Simulation and theoretical results with water-filling power allocations; $N_t = 100$, $N_r = 4$ and $N_{r,e} = 4$.

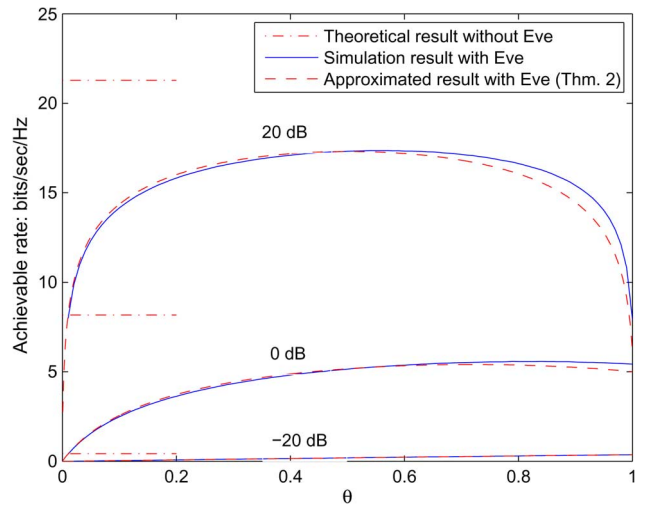

Fig. 14. $\mathbb{E}\{C_{se}\}$ as a function of θ for MIMOME channels; $N_t = 16$, $N_r = 2$ and $N_{r,e} = 2$.

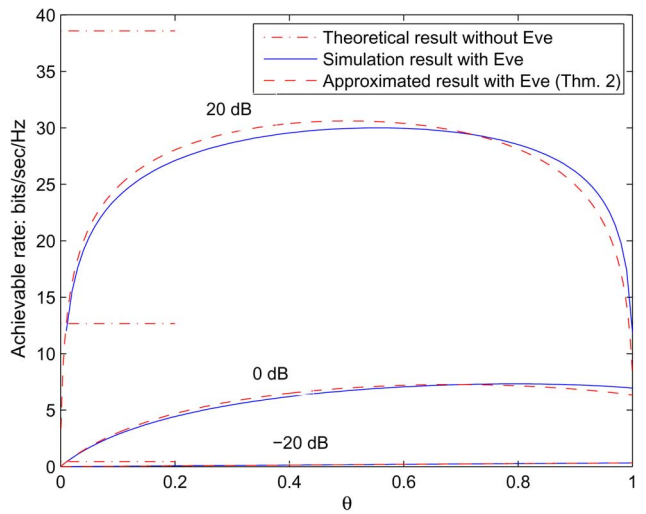

Fig. 15. $\mathbb{E}\{C_{se}\}$ as a function of θ for MIMOME channels; $N_t = 16$, $N_r = 4$ and $N_{r,e} = 4$.

MIMOME channels. Observe that as SNR increases, the value of θ drops quickly from 1 to $N_r/(N_r + N_{r,e})$. The rapid transition explains why the suggested values of θ in the high and low SNR regimes, i.e., $N_r/(N_r + N_{r,e})$ and 1 work well and can nearly achieve the performance of the optimal solution of θ as observed in Examples 1 and 2.

Example 4: Comparison of Equal Power and Water-Filling Power Allocations: Let $N_r = N_{r,e} = 4$. This example compares the performance of AN precoding with equal power and water-filling power allocations. The simulation results are shown in Fig. 12. Observe that the water-filling power allocation outperforms the equal power allocation in the low SNR regime. The performance improvement of the water-filling power allocation becomes less pronounced when the SNR increases. This is not surprising because we have shown in Theorem 3 that in the high SNR regime the secrecy rates for the water-filling power and the equal power allocations are bounded by the same form. Hence the theoretical results derived for the equal power allocation can be applied for the water-filling power allocation in the high SNR regime. Fig. 13 shows the theoretical and simulation results for water-filling power allocation in the low SNR regime. From the figure, we can see that the theoretical result in Theorem 3 becomes accurate when the SNR decreases.

Example 5: Accuracy of Approximations for Moderate Numbers of Transmit Antennas: This example investigates the accuracy of the approximations when N_t is not sufficiently large for the asymptotics to hold. Let $N_t = 16$, which is an acceptable number of antennas with current technology. The secrecy rates as functions of θ are shown in Figs. 14 and 15, respectively. Observe that the proposed values of θ can still provide reasonable solutions in this case. Also note that when N_t is not sufficiently large, the theoretical result is no longer a lower bound because the approximations in (16) and (45) are no longer accurate. Under this situation, the lower bounds in the theorems may be considered, instead, to be approximations.

VI. Conclusion

We have analyzed the secrecy rates and derived lower bounds for AN precoding systems in MISOSE, MISOME and MIMOME channels. When the number N_t of transmit antennas is sufficiently large, e.g., $N_t = 100$ in the examples, the derived bounds are tight. When the value of N_t is moderate, e.g., $N_t = 16$, the proposed power allocation can still provide a reasonable solution. Closed-form solutions for the nearly optimal power allocation were obtained from these bounds. We have made several interesting findings as follows: In the low SNR regime, we should distribute zero power to artificial noise in MISOSE, MISOME and MIMOME channels. The corresponding rate loss due to the eavesdropper is negligible. This result suggests that there may be no need to use AN precoding in the low SNR regime, because the effect due to the eavesdropper is minor. If the numbers of receive antennas at the legitimate receiver and the eavesdropper are comparable, i.e., $N_r \approx N_{r,e}$, in the high SNR regime, we should distribute half of the power to artificial noise for both MISOSE and MIMOME channels; the corresponding rate loss due to the eavesdropper normalized by N_r is 2 bits/sec/Hz. Moreover, the theoretical results have shown that equal power and water-filling power allocations have similar trends in the optimal values of θ and the rate loss. The simulation results have confirmed the accuracy of the theoretical results.

Appendix

A. Proof of Lemma 1

Using the property that the sample mean equals to the ergodic mean, i.e., the weak law of large numbers, we have $|\mathbf{h}^\dagger \mathbf{f}|^2 = \sum_{i=1}^{N_t} |h(i)|^2 \approx N_t \mathbb{E}\{|h(i)|^2\}$ as $N_t \to \infty$, where $h(i)$ is the ith element of the vector $\mathbf{h}$. Since $h(i)$ is with $\mathcal{CN}(0,2)$, $|h(i)|^2$ has the χ^2 distribution with two degrees of freedom. Thus $\mathbb{E}\{|h(i)|^2\} = 2$ (see [23]). This proves the lemma.

B. Proof of Lemma 2

$\|\mathbf{H}_e \mathbf{f}\|^2 = \sum_{i=1}^{N_{r,e}} \left|\mathbf{h}_{i,e}^\dagger \mathbf{f}\right|^2$, where $\mathbf{h}_{i,e}^\dagger$ is the ith row of $\mathbf{H}_e$. Because the elements of $\mathbf{H}_{i,e}$ are i.i.d. Gaussian, $\mathbf{h}_{i,e}^\dagger \mathbf{f}$ are i.i.d. Gaussian with zero mean and variance $\mathbb{E}\{|\mathbf{h}_{i,e}^\dagger \mathbf{f}|^2\} = 2$ for $i = 1, 2, \cdots N_{r,e}$, i.e., $\mathbf{h}_{i,e}^\dagger \mathbf{f} \sim \mathcal{CN}(0,2)$. Therefore $\|\mathbf{H}_e \mathbf{f}\|^2$ has the χ^2 distribution with $2N_{r,e}$ degrees of freedom.

C. Proof of Lemma 4

This approximation is proved by arguing that $\mathbf{B}$ is approximately diagonal, i.e., $[\mathbf{B}]_{ii} \gg [\mathbf{B}]_{ij}$. From (28) and (11), the ith diagonal element of $\mathbf{B}$ is

$$[\mathbf{B}]_{ii} = \left\|\mathbf{h}_{i,e}^\dagger \mathbf{Z}\right\|^2 = \|\mathbf{h}_{i,e}\|^2 - \left\|\mathbf{h}_{i,e}^\dagger \mathbf{F}\right\|^2. \tag{64}$$

From Lemma 1, $\|\mathbf{h}_{i,e}\|^2 \approx 2N_t$ as $N_t \to \infty$. Hence (64) can be rewritten as (32).

The elements of the $1 \times N_r$ vector $\mathbf{h}_{i,e}^\dagger \mathbf{F}$ are i.i.d. $\mathcal{CN}(0,2)$ random variables, because the columns of $\mathbf{F}$ are orthonormal. Thus $\left\|\mathbf{h}_{i,e}^\dagger \mathbf{F}\right\|^2$ has the χ^2 distribution with $2N_r$ degrees of freedom, and its mean value $\mathbb{E}\{\left\|\mathbf{h}_{i,e}^\dagger \mathbf{F}\right\|^2\} = 2N_r$. Therefore, when $N_t \gg N_r$, we can approximate (32) by

$$[\mathbf{B}]_{ii} \approx 2N_t. \tag{65}$$

The off-diagonal element of $\mathbf{B}$ at the ith row and the jth column is

$$[\mathbf{B}]_{ij} = \mathbf{h}_{i,e}^\dagger \mathbf{Z}\mathbf{Z}^\dagger \mathbf{h}_{j,e}. \tag{66}$$

The elements of the $1 \times (N_t - N_r)$ vector $\mathbf{h}_{i,e}^\dagger \mathbf{Z}$ are i.i.d. $\mathcal{CN}(0,2)$ random variables, because the columns of $\mathbf{Z}$ are orthonormal. Hence $\mathbf{h}_{i,e}^\dagger \mathbf{Z}\mathbf{Z}^\dagger \mathbf{h}_{j,e}$ is the sum of $N_t - N_r$ i.i.d. complex Gaussian product variables. Applying the Central Limit Theorem, $\mathbf{h}_{i,e}^\dagger \mathbf{Z}\mathbf{Z}^\dagger \mathbf{h}_{j,e}$ is approximately complex Gaussian distributed with zero mean and variance $2(N_t - N_r)$, i.e.,

$$[\mathbf{B}]_{ij} \sim \mathcal{CN}\left(0, 2(N_t - N_r)\right). \tag{67}$$

From (65) and (67), $[\mathbf{B}]_{ii}$ is frequently much greater than the real and the imaginary parts of $[\mathbf{B}]_{ij}$. For example, let $N_t = 100$ and $N_r = 4$, from (67), the probability that $\Re[\mathbf{B}]_{ij}$ or $\Im[\mathbf{B}]_{ij}$ is larger than 2.58σ is smaller than 1%. Here, $[\mathbf{B}]_{ii} \approx 2N_t = 200$ and this value is indeed much greater than $\Re[\mathbf{B}]_{ij}$ or $\Im[\mathbf{B}]_{ij}$, which is approximately $2.58\sqrt{N_t - N_r} \approx 25.3$. That is, $\Pr\{\Re[\mathbf{B}]_{ij} \text{ or } \Im[\mathbf{B}]_{ij} > 25.3\sigma\} < 0.01$.

D. Proof of Lemma 5

The bound in (38) can be obtained by using the Hadamard Inequality, where the equality holds when $\mathbf{A}$ and $\mathbf{B}$ are both diagonal matrices. Using a procedure similar to that in Lemma 4, it is easy to show that $[\mathbf{A}]_{ii} = \left\|\mathbf{h}_{i,e}^\dagger \mathbf{F}\right\|^2$, which is χ^2 distributed with $2N_r$ degrees of freedom. Also, $[\mathbf{A}]_{ij} = \mathbf{h}_{i,e}^\dagger \mathbf{F}\mathbf{F}^\dagger \mathbf{h}_{j,e}$ is the sum of N_r i.i.d. complex Gaussian products. Since it is not appropriate to apply the Central Limit Theorem for $[\mathbf{A}]_{ii}$ and $[\mathbf{A}]_{ij}$ when N_r is not sufficiently large, we use a bound rather than an approximation in this lemma.

E. Proof of Lemma 8

The precoding and the postcoding matrices are the right and left singular vectors corresponding to the largest N_r singular values. Applying the precoding at the transmitter side and the postcoding at the receiver side, the achievable rate of the legitimate receiver in (3) can be expressed as [28]

$$C = \sum_{i=1}^{N_r} \log\left(1 + \frac{\theta \mathrm{SNR}}{N_r} \lambda_i\right), \tag{68}$$

where λ_i is the ith eigenvalue of $\mathbf{H}\mathbf{H}^\dagger$. Pair the N_r non-zero singular values as follows:

$$C = \sum_{i=1}^{\frac{N_r}{2}} \log\left(1 + \frac{\theta \mathrm{SNR}}{N_r} \lambda_i\right) + \log\left(1 + \frac{\theta \mathrm{SNR}}{N_r} \lambda_{N_r - i + 1}\right). \tag{69}$$

According to [30], the smaller the value N_r/N_t is, the less spread the eigenvalues is. Hence we may approximate the pairs in (69) by the pair with the maximum and the minimum eigenvalues. From Lemma 7, we approximate (69) by

$$\begin{aligned} C &\approx \frac{N_r}{2}\log\left(1+\frac{2N_t\theta\mathrm{SNR}}{N_r}\left(1+\sqrt{\frac{N_r}{N_t}}\right)^2\right) \\ &\quad+\frac{N_r}{2}\log\left(1+\frac{2N_t\theta\mathrm{SNR}}{N_r}\left(1-\sqrt{\frac{N_r}{N_t}}\right)^2\right) \\ &\approx \frac{N_r}{2}\log\left(1+\frac{4N_t\mathrm{SNR}\theta}{N_r}+\left(\frac{2N_t\mathrm{SNR}\theta}{N_r}\right)^2\right), \quad (70) \end{aligned}$$

where the last approximation is due to the assumption that $N_t \gg N_r$. The last equation in (70) leads to (45). Please note that in (70), we have used a linear approximation for approximating the sum of the eigenvalues. For $N_t \gg N_r$, this linear approximation is generally satisfactory. The reason is that from Lemma 7, when N_r/N_t decreases, the difference between the maximum and the minimum eigenvalues decreases. That is, the dynamic range of the eigenvalues decreases. Hence, when $N_t \gg N_r$, the linear approximation may still lead to a satisfactory result.

ACKNOWLEDGMENT

The authors would like to thank the anonymous reviewers for their constructive suggestions, which have significantly improved the quality of this work.

REFERENCES

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

[2] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, pp. 1355–1387, 1975.

[3] S. Shafiee and S. Ulukus, "Achievable rates in Gaussian MISO channels with secrecy constraints," in *Proc. IEEE Int. Symp. Inf. Theory*, Jun. 2007, pp. 2466–2470.

[4] S. Shafiee and S. Ulukus, "Towards the secrecy capacity of the Gaussian MIMO wire-tap channel: The 2-2-1 channel," *IEEE Trans. Inf. Theory*, vol. 55, no. 9, pp. 4033–4039, Sep. 2009.

[5] R. Bustin, R. Liu, H. V. Poor, and S. Shamai, "An MMSE approach to secrecy capacity of the MIMO Gaussian wiretap channel," *EURASIP J. Wireless Commun. Netw.*, vol. 2009, 2009, Article ID 370970, 8 pages.

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

[7] R. Liu, T. Liu, H. V. Poor, and S. Shamai, "Multiple-input multiple-output Gaussian broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 56, pp. 4215–4227, Sep. 2010.

[8] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas—Part II: The MIMOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 11, pp. 5515–5532, Nov. 2010.

[9] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *IEEE Trans. Inf. Theory*, vol. 57, no. 8, pp. 4961–4972, Aug. 2011.

[10] S. A. A. Fakoorian and A. L. Swindlehurst, "MIMO interference channel with confidential messages: Achievable secrecy rates and precoder design," *IEEE Trans. Inf. Forens. Secur.*, vol. 6, pp. 640–649, Sep. 2011.

[11] R. Liu, T. Liu, H. V. Poor, and S. Shamai, "New results on multiple-input multiple-output broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 59, no. 3, pp. 1346–1359, Mar. 2013.

[12] 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, Jul. 2010.

[13] S. Loyka and C. D. Charalambous, "On optimal signaling over secure MIMO channels," in *Proc. IEEE Int. Symp. Inf. Theory*, Jul. 2012, pp. 443–447.

[14] S. Loyka and C. D. Charalambous, "Further results on optimal signaling over secure MIMO channels," in *Proc. IEEE Int. Symp. Inf. Theory*, Jul. 2013, pp. 2019–2023.

[15] S. A. A. Fakoorian and A. L. Swindlehurst, "Full rank solutions for the MIMO Gaussian wiretap channel with an average power constraint," *IEEE Trans. Signal Process.*, vol. 61, no. 10, pp. 2620–2631, May 2013.

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

[17] S. Bashar, Z. Ding, and G. Y. Li, "On secrecy of codebook-based transmission beamforming under receiver limited feedback," *IEEE Trans. Wireless Commun.*, vol. 10, no. 4, pp. 1212–1223, Apr. 2011.

[18] D. J. Love, R. W. Heath, and T. Strohmer, "Grassmannian beamforming for multiple-input multiple-output wireless systems," *IEEE Trans. Inf. Theory*, vol. 49, no. 10, pp. 2735–2747, Oct. 2003.

[19] P.-H. Lin, S.-H. Lai, S.-C. Lin, and H.-J. Su, "On secrecy rate of the generalized artificial-noise assisted secure beamforming for wiretap channels," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1728–1740, Sep. 2013.

[20] E. G. Larsson, F. Tufvesson, S. O. Edfors, and T. L. Marzetta, "Massive MIMO for next generation wireless systems," 2013, arXiv:1304.6690 [cs.IT], submitted for publication.

[21] J. Hoydis, S. T. Brink, and M. Debbah, "Massive MIMO in the UL/DL of cellular networks: How many antennas do we need?," *IEEE J. Sel. Areas Commun.*, vol. 31, pp. 160–171, Feb. 2013.

[22] *CFP IEEE J. Select. Topics Signal Process.: Special Issue on Signal Processing for Large-Scale MIMO Communications*.

[23] A. Papoulis and S. U. Pillai, *Probability, Random Variables and Stochasitic Process*. New York, NY, USA: McGraw-Hill, 2002.

[24] E. Telatar, "Capacity of multi-antenna Gaussian channels," AT&T-Bell Labs, Internal Tech. Memo., 1995.

[25] C. K. Au-Yeung and D. J. Love, "On the performance of random vector quantization limited feedback beamforming in a MISO system," *IEEE Trans. Wireless Commun.*, vol. 6, no. 2, pp. 458–462, Feb. 2007.

[26] M.-S. Alouini and A. J. Goldsmith, "Capacity of rayleigh fading channels under different adaptive transmission and diversity-combining techniques," *IEEE Trans. Veh. Technol.*, vol. 49, no. 4, pp. 1165–1181, Jul. 1999.

[27] E. Visotsky and U. Madhow, "Space-time transmit precoding with imperfect feedback," *IEEE Trans. Inf. Theory*, vol. 47, no. 9, pp. 2632–2639, Sep. 2001.

[28] D. Tse and P. Viswanath, *Fundamentals of Wireless Communication*. Cambridge, U.K.: Cambridge Univ. Press, 2005.

[29] I. C. F. Ipsen and D. J. Lee, *Determinant Approximations*. New York, NY, USA: Wiley, 2005.

[30] A. Edelman, "Eigenvalues and condition numbers of random matrices," *SIAM J. Matrix Anal. Appl.*, vol. 9, pp. 543–560, Oct. 1988.

[31] B. M. Hochwald, T. L. Marzetta, and V. Tarokh, "Multiple-antenna channel hardening and its implications for rate feedback and scheduling," *IEEE Trans. Inf. Theory*, vol. 50, no. 9, pp. 1893–1909, Sep. 2004.

[32] T. W. Anderson, *An Introduction to Multivariate Statistical Analysis*, 2nd ed. New York, NY, USA: Wiley, 1984.

Shang-Ho (Lawrence) Tsai (SM'12) was born in Kaohsiung, Taiwan, 1973. He received the Ph.D. degree in Electrical Engineering from the University of Southern California (USC), in August 2005.

From June 1999 to July 2002, he was with the Silicon Integrated Systems Corp. (SiS), where he participated the VLSI design for DMT-ADSL systems. From September 2005 to January 2007, he was with the MediaTek Inc. (MTK) and participated the VLSI design for MIMO-OFDM systems. From June 2013 to December 2013, he was a visiting fellow in the Department of Electrical Engineering at the Princeton University. Since February 2007, he joined the Department of Electrical and Control Engineering (now Department of Electrical Engineering) at the National Chiao Tung University where he is now an associate professor. His research interests are in the areas of signal processing for communications, statistical signal processing, and signal processing for VLSI designs.

Dr. Tsai was awarded a government scholarship for overseas study from the Ministry of Education, Taiwan, in 2002–2005.

H. Vincent Poor (S'72–M'77–SM'82–F'87) received the Ph.D. degree in EECS from Princeton University in 1977.

From 1977 until 1990, he was on the faculty of the University of Illinois at Urbana-Champaign. Since 1990 he has been on the faculty at Princeton, where he is the Michael Henry Strater University Professor of Electrical Engineering and Dean of the School of Engineering and Applied Science. His research interests are in the areas of stochastic analysis, statistical signal processing, and information theory, and their applications in wireless networks and related fields such as social networks and smart grid. Among his publications in these areas are the recent books *Principles of Cognitive Radio* (Cambridge University Press, 2013) and *Mechanisms and Games for Dynamic Spectrum Allocation* (Cambridge University Press, 2014).

Dr. Poor is a member of the National Academy of Engineering and the National Academy of Sciences, and a foreign member of Academia Europaea and the Royal Society. He is also a fellow of the American Academy of Arts and Sciences, the Royal Academy of Engineering (U.K.), and the Royal Society of Edinburgh. He received the Technical Achievement and Society Awards of the IEEE Signal Processing Society in 2007 and 2011, respectively. Recent recognition of his work includes the 2014 URSI Booker Gold Medal, and honorary doctorates from Aalborg University, the Hong Kong University of Science and Technology, and the University of Edinburgh.