Per-Antenna Constant Envelope Precoding for Secure Transmission in Large-Scale MISO Systems

Jun Zhu[†], Ning Wang[§†], and Vijay K. Bhargava[†]

[†]Department of Electrical and Computer Engineering, The University of British Columbia, Vancouver, Canada

[§]School of Information Engineering, Zhengzhou University, Zhengzhou, China

Abstract—Secure transmission in large-scale MISO systems employing artificial noise (AN) is studied under the per-antenna constant envelope (CE) constraint. Achievable secrecy rate of the per-antenna CE precoding scheme for large-scale MISO is analyzed and compared with that of the matched filter linear precoding. A two-stage per-antenna CE precoding scheme for joint signal-plus-AN transmission is proposed. The first stage determines the per-antenna CE precoding for the information-bearing signal. A properly generated AN using an iteration algorithm is incorporated into the transmit signal in the second stage such that the combined signal-plus-AN satisfies the per-antenna CE constraint and the AN is orthogonal to the user channel. It is shown that compared to conventional per-antenna CE transmission, this joint signal-plus-AN secure transmission scheme does not require additional transmit power. An alternative low-complexity AN generation scheme which uses a separate antenna to cancel the AN leakage to the intended user introduced by randomly generated AN is also proposed.

I. INTRODUCTION

Multiple-input-multiple-output (MIMO) antenna system is a promising technology to exploit spatial diversity and improve radio spectral efficiency. This is especially important to the design of future high data rate wireless communication systems where the scarce of spectra is becoming a critical limitation. The MIMO technology has been extensively studied in the literature and has been incorporated into concurrent wireless communication standards such as LTE and the latest versions of Wi-Fi. However, as wireless technologies are evolving, small portable devices, e.g. smartphones, will lead the mobile IP traffic growth [1]. Because it is in general not practical to implement multiple antennas and the associated complex hardware/software on such small devices due to the size and energy constraints, advantages of the MIMO technology are greatly forfeited in such scenarios.

Large-scale MIMO, or massive MIMO, is an emerging revolutionary base station (BS) technology based on MIMO to mitigate the above discrepancies [2] [3]. It uses a large excess of (typically hundreds of) very low power (in the order of mW) antenna units at the BS to serve low-complexity single-antenna mobile terminals (MT). Remarkable improvements in rates as well as in spectral and power efficiency can be achieved by focusing the radiating power into the ever-smaller MT spots with the very large antenna array. Massive MIMO is therefore capable of achieving robust performance at low signal-to-interference-plus-noise ratio (SINR) with highly efficient and inexpensive implementations.

Equipping large antenna array in massive MIMO systems requires each antenna element and its associated radio-frequency (RF) electronics, e.g. power amplifiers (PAs), to be inexpensive and power-efficient. However, cheaply manufactured PAs are in general non-linear devices, which suffer from linearity issues when processing signals with large amplitude-variations. A per-antenna constant envelope (CE) nonlinear precoding was

considered in single-user massive MIMO systems in [4]. It was shown that under the per-antenna CE constraint at the BS transmitter, an equivalent single-input-single-output (SISO) model over additive white Gaussian noise (AWGN) is obtained for multiple-input-single-output (MISO) system where we have a single-user equipped with a single-antenna [4]. When sufficiently large number of antennas are used, the corresponding achievable rate under per-antenna CE constraint is close to the capacity of the MISO channel under the average-only power constraint in high-power regime. More recently, the idea of per-antenna CE precoding has been extended to multi-user massive MIMO systems over flat and frequency-selective fading channels [5] [6].

Information security is a critical concern in communication system design. It is particularly important to wireless communications because of the broadcast nature of the open media. The notion of physical-layer (PHY) security has been attracting increasing attention from both academia and industry. As a complement to cryptography-based security strategies, the PHY-based approach improves security of the communication from the *perfect secrecy* perspective. In the case of passive attacks, i.e. eavesdropping, to MIMO systems, it has been shown that simultaneously transmitting both the information-bearing signal and properly designed artificial noise (AN) is an efficient way to improve the secrecy rate [7]. The application of AN-based secure transmissions for multi-cell massive MIMO systems has been recently studied in [8], [9]. However, design and performance of such security enhancing strategies under the per-antenna CE constraint have yet been investigated.

In this work, we present our recent investigations of incorporating AN-based PHY security strategies into large-scale MISO systems under the per-antenna CE constraint. Different AN generation strategies are considered; the corresponding improvement to the secrecy capacity is studied.

II. SYSTEM MODEL

A. Constant Envelope Precoding for Large-Scale MISO

In a MISO system with N_t transmit (Tx) antennas and one single receive (Rx) antenna, the complex channel gain between the ith Tx antenna and the Rx antenna is h_i, $i = 1, \ldots, N_t$. The total channel vector is $\mathbf{h} = [h_1, \ldots, h_{N_t}]$. Given the complex transmit signal from the ith antenna be x_i, the complex received signal of the user is

$$y = \mathbf{h}\mathbf{x} + n = \sum_{i=1}^{N_t} h_i x_i + n, \qquad (1)$$

where $\mathbf{x} = [x_1, \ldots, x_{N_t}]^T$ is the vector form of the Tx signal, and $n \sim \mathcal{CN}(0, \sigma^2)$ is a zero-mean circular-symmetric additive white Gaussian noise (AWGN) at the receiver with variance σ^2.

With conventional linear matched filter (MF) precoder, the Tx signal $\mathbf{x}$ is the information-bearing signal s multiplied by an MF beamforming vector $\mathbf{w} \in \mathcal{C}^{N_t}$

$$\mathbf{x}_{MF} = \sqrt{P_T}\mathbf{w}s = \sqrt{P_T}\frac{\mathbf{h}^\dagger}{\|\mathbf{h}\|}s, \qquad (2)$$

where average-only power constraint P_T is adopted. $(\cdot)^\dagger$ is the conjugate transpose operator, and $\|\cdot\|$ denotes the 2-norm. Under the per-antenna CE constraint, as in [4], each antenna transmits at a constant power $\frac{P_T}{N_t}$. The Tx signal x_i is in the form $x_i = \sqrt{\frac{P_T}{N_t}}e^{j\theta_i^u}$, where $\theta_i^u \in (-\pi, \pi]$ is the information-bearing phase of the ith Tx antenna. The received signal (1) then becomes

$$y = \sqrt{\frac{P_T}{N_t}}\sum_{i=1}^{N_t} h_i e^{j\theta_i^u} + n. \qquad (3)$$

When perfect channel state information (CSI) is available at both the transmitter and the receiver, the received signal y reduces to the output of a SISO system

$$y = \sqrt{P_T}\, u + n, \qquad (4)$$

where $u = \frac{\sum_{i=1}^{N_t} h_i e^{j\theta_i^u}}{\sqrt{N_t}}$ is the noise-free information signal expected by the intended receiver. The per-antenna CE precoding maps the information symbol u to the information-bearing transmit phases θ_i^u, $i = 1, \ldots, N_t$, based on the channel $\mathbf{h}$. The resulting transmit signal has a constant envelop $\sqrt{\frac{P_T}{N_t}}$ on every antenna branch. The objective of per-antenna CE precoding is to determine $\Theta^u = [\theta_1^u, \ldots, \theta_{N_t}^u]$ given the intended received signal u and the channel $\mathbf{h}$, i.e. the parameterized mapping

$$\Phi(u; \mathbf{h}) \triangleq \Theta^u. \qquad (5)$$

Given the channel $\mathbf{h}$, all possible noise-free received signal u in (4) of the per-antenna CE transmission lie in the set

$$\mathcal{M}(\mathbf{h}) \triangleq \left\{ \frac{1}{\sqrt{N}}\sum_{i=1}^{N_t} h_i e^{j\theta_i}, \ \theta_i \in (-\pi, \pi], \ i = 1, \ldots, N_t \right\}. \qquad (6)$$

The set $\mathcal{M}(\mathbf{h})$ was shown to have a doughnut-like shape on the complex plain [4]. The key properties of $\mathcal{M}(\mathbf{h})$ include

1) The set $\mathcal{M}(\mathbf{h})$ is circular symmetric, i.e. $z \in \mathcal{M}(\mathbf{h})$ also implies $ze^{j\varphi} \in \mathcal{M}(\mathbf{h})$ for all $\varphi \in (-\pi, \pi]$.
2) The maximum value of $|u|$ for $u \in \mathcal{M}(\mathbf{h})$ is

$$M(\mathbf{h}) = \frac{1}{\sqrt{N_t}}\sum_{i=1}^{N_t} |h_i| = \frac{1}{\sqrt{N_t}}\|\mathbf{h}\|_1. \qquad (7)$$

3) The minimum value of $|u|$ for $u \in \mathcal{M}(\mathbf{h})$, denoted by $m(\mathbf{h})$, is greater than zero and is upper bounded by

$$m(\mathbf{h}) \leq \frac{1}{\sqrt{N_t}}\max_{i=1,\ldots,N_t} |h_i| = \frac{1}{\sqrt{N_t}}\|\mathbf{h}\|_\infty. \qquad (8)$$

B. AN-Based Secure Transmission

Security of the single-cell single-user MISO downlink is considered in flat-fading. The BS has size N_t antenna array while the MT has only a single antenna. A single-antenna eavesdropper (Eve) is randomly located in the cell region. The study can be extended to eavesdropping scenarios where the eavesdropper is

Fig. 1. The single-user massive MIMO system with a passive eavesdropper.

equipped with $N_e < N_t$ antennas. The eavesdropper aims to retrieve the information transmitted to the mobile terminal.

As a starting point, we first focus on the single-eavesdropper single-antenna case which is shown by Fig. 1. We still use h_i to denote the complex channel gain between the ith BS antenna and the MT; g_i is the complex channel gain between the ith BS antenna and the eavesdropper. $\mathbf{h} \in \mathcal{C}^{N_t}$ represents the channel gain row vector between the BS and the MT with h_i as its ith entry. Similarly, $\mathbf{g} \in \mathcal{C}^{N_t}$ is the channel gain row vector between the BS and the eavesdropper. The BS then can use up to $(N_t - 1)$ degrees of freedom of the antenna array for AN transmission to degrade Eve's ability of decoding the user message [7].

We now illustrate the concept of AN-based secure transmission in conventional linear precoding system where the average-only power constraint is considered. The transmitted signal-plus-AN is

$$\begin{aligned} \mathbf{x} &= \sqrt{\eta P_T}\mathbf{w}s + \sqrt{(1-\eta)P_T}\mathbf{V}\mathbf{z} \\ &= \sqrt{\eta P_T}\mathbf{w}s + \sum_{k=1}^{N_t-1} \sqrt{(1-\eta)P_T}\mathbf{v}_k z_k \end{aligned} \qquad (9)$$

where $\eta \in [0, 1]$ is the average Tx power allocation factor for user information, $\mathbf{z} = [z_1, \ldots, z_{N_t-1}]^T \in \mathcal{CN}(\mathbf{0}_{N_t-1}, \mathbf{I}_{N_t-1})$ is the AN vector, and $\mathbf{V} = [\mathbf{v}_1, \ldots, \mathbf{v}_{N_t-1}] \in \mathcal{C}^{N_t \times (N_t-1)}$ is an AN shaping matrix with $\|\mathbf{v}_k\| = 1$, $k = 1, \ldots, N_t - 1$. The received signal at the mobile terminal is then given by

$$y_r = \mathbf{h}(\sqrt{\eta P_T}\mathbf{w}s + \sqrt{(1-\eta)P_T}\mathbf{V}\mathbf{z}) + n_r \qquad (10)$$

where $n_r \sim \mathcal{CN}(0, \sigma_r^2)$ is a circular symmetric complex AWGN. The eavesdropper's received signal, on the other hand, is

$$y_e = \mathbf{g}(\sqrt{\eta P_T}\mathbf{w}s + \sqrt{(1-\eta)P_T}\mathbf{V}\mathbf{z}) + n_e \qquad (11)$$

where $n_e \sim \mathcal{CN}(0, \sigma_e^2)$ is a circular symmetric complex AWGN at the eavesdropper. The ideal AN shaping matrix $\mathbf{V}$ is chosen such that it lies in the null-space of the user channel $\mathbf{h}$, i.e. $\mathbf{h}\mathbf{V} = \mathbf{0}^{N_t-1}$. Therefore the precoded AN term $\mathbf{V}\mathbf{z}$ will not affect the user reception. Conversely, an additional noise term is "seen" by the eavesdropper, which degrades her effective signal-to-noise ratio (SNR). As a consequence, the eavesdropper's capacity is reduced, which results in an improvement of the secrecy capacity between the BS and the intended user MT.

III. SECURITY ANALYSIS OF PER-ANTENNA CE PRECODING

In this section, we study secrecy capacity of the per-antenna CE precoding and MF precoding. For MF precoding as given by (2), the ergodic capacity of the legitimate channel between the BS and the intended receiving MT is

$$C_{MF} = \mathbb{E}_{\mathbf{h}}\left[1 + \frac{P_T}{\sigma^2}\|\mathbf{h}\|^2\right], \tag{12}$$

where the expectation is over the distribution of $\mathbf{h}$. By assumption, all elements of $\mathbf{h}$ are independent and identically distributed (i.i.d.) complex Gaussian random variables (RVs) with zero mean and unit variance. Then $z_h = \|\mathbf{h}\|^2 = \sum_{i=1}^{N_t} h_i^2$ is the sum of N_t i.i.d. exponential RVs with parameter $\lambda = 1$, which follows Gamma distribution with shape parameter N_t and scale parameter 1. The ergodic capacity in (12) is then evaluated as [10]

$$\begin{aligned}
C_{MF} &= \int_0^\infty \log_2\left(1 + \frac{P_T}{\sigma^2}z\right)\frac{\exp(-z)z^{N_t-1}}{\Gamma(N_t)}dz \\
&= \frac{1}{\ln 2}\exp\left(\frac{\sigma^2}{P_T}\right)\sum_{n=1}^{N_t} E_n\left(\frac{\sigma^2}{P_T}\right),
\end{aligned} \tag{13}$$

where $E_n(\cdot)$ is the generalized exponential integral [11] $E_n(x) = \int_1^\infty \frac{\exp(-xt)}{t^n}dt$. On the other hand, the ergodic capacity of the eavesdropper channel is

$$C_{MF-Eve} = \mathbb{E}_{\mathbf{g},\mathbf{h}}\left[\log_2\left(1 + \frac{P_T}{\sigma^2}\left|\mathbf{g}\frac{\mathbf{h}^\dagger}{\|\mathbf{h}\|}\right|^2\right)\right]. \tag{14}$$

Since $\frac{\mathbf{h}^\dagger}{\|\mathbf{h}\|}$ is a normalized vector with i.i.d. complex Gaussian entries and it is independent from $\mathbf{g}$, the RV $z_g = \mathbf{g}\frac{\mathbf{h}^\dagger}{\|\mathbf{h}\|}$ has the same distribution as elements of $\mathbf{g}$, i.e. $z_g \sim \mathcal{CN}(0,1)$. As a consequence, $|z_g|^2$ is exponentially distributed with parameter $\lambda = 1$, and the ergodic capacity of the eavesdropper channel is derived as

$$C_{MF-Eve} = \frac{1}{\ln 2}\exp\left(\frac{\sigma^2}{P_T}\right)E_1\left(\frac{\sigma^2}{P_T}\right). \tag{15}$$

The resulting ergodic secrecy capacity of MF precoding is

$$\begin{aligned}
C_{sec-MF} &= [C_{MF} - C_{MF-Eve}]^+ \\
&= \left[\frac{1}{\ln 2}\exp\left(\frac{\sigma^2}{P_T}\right)\sum_{k=2}^{N_t} E_k\left(\frac{\sigma^2}{P_T}\right)\right]^+,
\end{aligned} \tag{16}$$

where $[\cdot]^+$ denotes the max operation $\max\{0,\cdot\}$.

Under the per-antenna CE constraint at the BS transmitter, the achievable rate of the doughnut channel of the legitimate user, given the channel coefficient $\mathbf{h}$, is shown to be tightly lower bounded by [4]

$$\begin{aligned}
C_{CE|\mathbf{h}} &\geq \log_2\left(1 + \frac{P_T}{\sigma^2}\frac{M(\mathbf{h}) - m(\mathbf{h})}{e}\right) \\
&\geq \log_2\left(1 + \frac{P_T}{\sigma^2}\frac{\|\mathbf{h}\|_1^2 - \|\mathbf{h}\|_\infty^2}{Ne}\right).
\end{aligned} \tag{17}$$

By taking expectation of (17) over the distribution of the channel $\mathbf{h}$, we can evaluate the lower bound of the ergodic capacity of the doughnut channel as

$$C_{CE} \geq \mathbb{E}_{\mathbf{h}}\left[\log_2\left(1 + \frac{P_T}{\sigma^2}\frac{\|\mathbf{h}\|_1^2 - \|\mathbf{h}\|_\infty^2}{Ne}\right)\right]. \tag{18}$$

Unfortunately, a closed-form expression for (18) is difficult to obtain. Numerical techniques need to be used to evaluate the ergodic capacity lower bound (18). Similar to (3), with per-antenna CE precoding, the received signal at the eavesdropper is given by

$$y_g = \sqrt{\frac{P_T}{N_t}}\sum_{i=1}^{N_t} g_i e^{j\theta_i^u} + n. \tag{19}$$

Because θ_i^u, $i = 1,\ldots,N_t$, are designed according to the mapping (5), they are uniformly distributed phases and are independent of the eavesdropper channel $\mathbf{g}$. The RV y_g can thus be written in the form

$$y_g = \sqrt{\frac{P_T}{N_t}}\sum_{i=1}^{N_t} g_i' + n = \sqrt{P_T}\sum_{i=1}^{N_t}\frac{g_i'}{\sqrt{N_t}} + n, \tag{20}$$

where g_i' have the same distribution as g_i because they are obtained by giving a uniformly distributed random phase rotation to g_i. It is straightforward to show that the summation term $g_s = \sum_{i=1}^{N_t}\frac{g_i'}{\sqrt{N_t}}$ has the same distribution as g_i, i.e. zero-mean unit variance complex Gaussian distribution. Then $|g_s|^2$ follows exponential distribution with parameter $\lambda = 1$. The ergodic eavesdropper channel capacity for per-antenna CE transmission is therefore

$$\begin{aligned}
C_{CE-Eve} &= \mathbb{E}_{g_s}\left[\log_2\left(1 + \frac{P_T}{\sigma^2}|g_s|^2\right)\right] \\
&= \frac{1}{\ln 2}\exp\left(\frac{\sigma^2}{P_T}\right)E_1\left(\frac{\sigma^2}{P_T}\right),
\end{aligned} \tag{21}$$

which is identical to the ergodic eavesdropper channel capacity for MF transmission at the BS given by (14). The ergodic secrecy capacity of the per-antenna CE precoding scheme can then be determined by using (18) and (21) as

$$C_{sec-CE} = [C_{CE} - C_{CE-Eve}]^+. \tag{22}$$

It is shown in [4] that the per-antenna CE transmission, by putting more stringent power constraint to the transmit signal, suffers from a performance loss in capacity compared with matched filtering beamforming with average-only power constraint. As $C_{CE-Eve} = C_{MF-Eve}$, the MF precoding will still outperform per-antenna CE precoding in terms of secrecy capacity of the system. However, we are going to show that by adding a carefully designed artificial noise, significant improvement in secrecy capacity can be obtained without violating the stringent per-antenna CE power constraint. The benefit of per-antenna CE precoding in less complex RF hardware design is retained.

IV. PER-ANTENNA CE PRECODING FOR JOINT SIGNAL-PLUS-AN SECURE TRANSMISSION

A. General Problem Formulation

We adopt the per-antenna CE constraint to the general AN-based secure transmission model in Section II-B. The transmit signal of the ith antenna then has the following general form

$$x_i = \sqrt{\frac{P_T}{N_t}}\left(\alpha_i e^{j\theta_i} + \beta_i e^{j\phi_i}\right) = \sqrt{\frac{P_T}{N_t}}e^{j\theta_i^u}, \quad i = 1,\ldots,N_t, \tag{23}$$

where α_i and θ_i are the amplitude and phase of the user information part of the per-antenna CE signal on the ith antenna,

Fig. 2. The general per-antenna CE transmit signal for secure transmission enabled by AN.

β_i and ϕ_i are the amplitude and phase of the corresponding AN part transmitted by the same antenna. θ_i, ϕ_i, and θ_i^u are phase angles within the range $(-\pi, \pi]$. In order to guarantee the second equality in (23) such that the per-antenna CE constraint holds, we must have the following trigonometric relation

$$\alpha_i^2 + \beta_i^2 + 2\alpha_i\beta_i \cos(\theta_i - \phi_i) = 1 \tag{24}$$

for all $i = 1, \ldots, N_t$. The relationship (24) is illustrated by Fig. 2, where the unit circle represents the normalized per-antenna CE signal envelope.

Ideally the AN part of the transmit signal (23) is "invisible" to the user, which requires

$$\sqrt{\frac{P_T}{N_t}} \sum_{i=1}^{N_t} h_i \beta_i e^{j\phi_i} = 0. \tag{25}$$

On the other hand, the noise-free user information part of the received signal, denoted

$$u = \sqrt{\frac{1}{N_t}} \sum_{i=1}^{N_t} \alpha_i h_i e^{j\theta_i}, \tag{26}$$

is in the alphabet $\mathcal{U}$ of the information-bearing symbol expected by the receiver. In addition, given the power allocation factor η for joint signal and AN transmission, the parameters α_i and β_i should also satisfy the equality condition

$$\frac{\sum_{i=1}^{N_t} \alpha_i^2}{\sum_{i=1}^{N_t} \beta_i^2} = \frac{\eta}{1 - \eta}. \tag{27}$$

The general problem for joint signal-plus-AN secure transmission in such a per-antenna CE system is to determine the parameters (α_i, θ_i) and (β_i, ϕ_i) for all N_t antenna branches such that the secrecy capacity of the system with respect to the eavesdropper as in Section II-B is maximized.

However, because the parameter pairs (α_i, θ_i) and (β_i, ϕ_i) are coupled through the nonlinear CE constraint characterized by the relationships (24) and (27), the problem cannot easily be transformed into a well-formulated per-antenna CE precoding problem as in [4]. Some techniques must be employed to decouple the information-bearing signal and the artificial noise while achieving the design objective. We will address this problem in our proposed design.

B. Two-Stage Per-Antenna CE Precoding for Joint Signal-plus-AN Transmission

A straightforward way to decouple the information-bearing signal and the artificial noise is to design one part first based on certain criteria and then determine the other accordingly such that the CE constraint holds. In a communication system we first need to focus on the user information which should meet certain requirements. Conversely requirement for the AN is usually loose. We only try to introduce as much extra noise to the eavesdropper as possible while minimizing the AN's impact on user information reception. The aggregate AN at the receiver should sum to zero such that (25) holds. Therefore we propose to determine the user signal first, which is then used to determine the AN to be transmitted according to the per-antenna CE constraint.

As illustrated in Section II-B, ideally the AN shaping matrix $\mathbf{V}$ should be in the null-space of the user channel such that the aggregate AN at the receiver is equal to zero, regardless the random noise $\mathbf{z}$. However, this constraint is too stringent for AN-based secure transmission in single-user large-scale MISO systems. Note that the generated AN is deterministic for each transmission. Therefore the null-space requirement is not necessary. All we need is (25), which requires the aggregate AN at the receiver is zero.

We consider per-antenna CE precoding for the user information as in [4], i.e. we set $\alpha_i = 1$ for all $i = 1, \ldots, N_t$. The precoder mapping $\Phi(u) = \Theta^u$ proposed in [4] is employed to find θ_i's. It was illustrated in [4] that with large number of transmit antennas, which is the case of massive MIMO, there are low-complexity gradient-based algorithms which gives Θ^u with small error norms $\left| u - \sum_{i=1}^{N_t} h_i e^{j\theta_i} \sqrt{N_t} \right|^2$.

With $\alpha_i = 1, \forall\, i$, (24) is simplified to

$$\beta_i^2 + 2\beta_i \cos(\theta_i - \phi_i) = 0 \xrightarrow{\beta_i \neq 0} \beta_i = -2\cos(\theta_i - \phi_i). \tag{28}$$

Accordingly, the "invisible" condition (25) is rewritten as (by ignoring the scaling factors)

$$\sum_{i=1}^{N_t} h_i \cos(\theta_i - \phi_i) e^{j\phi_i} = 0, \tag{29}$$

in which $\phi_i, i = 1, \ldots, N_t$ is the only variable, given that $\theta_i, i = 1, \ldots, N_t$ have already been found based on the precoder mapping $\Phi(u) = \Theta^u$. With sufficiently large N_t, we can always find a set of $\phi_i, i = 1, \ldots, N_t$ satisfying the "invisible" condition given in (25). In this case, we obtain a "free" secrecy improvement from the power consumption perspective, as the AN is designed to meet the trigonometric relationship in (24).

C. Random-Phase AN Generation and AN Leakage Cancellation

Design of an optimal CE precoding mapping for the AN generation scheme proposed in Section IV-B, from the secrecy rate perspective, is nontrivial. Complexity of the algorithm therefore may become a big issue in practical implementations. In this subsection, we propose an alternative scheme with low complexity, which is enabled by one single additional antenna element employing more sophisticated hardware.

A uniform AN phase ϕ_i is generated after determining the signal phase θ_i. The AN amplitude which preserves the per-antenna CE property of the combined transmit symbol is calcu-

Fig. 3. The random-phase AN generation and amplitude adjustment for per-antenna CE transmission.

lated accordingly. This is named the random-phase AN scheme, and the general idea of random-phase AN generation and the amplitude adjustment for per-antenna CE transmission is shown in Fig. 3.

As in the joint signal-plus-AN per-antenna CE secure transmission scheme in Section IV-B, the signal part is designed by adopting the per-antenna CE precoding. The AN phase ϕ_i is randomly generated and uniformly distributed on $(-\pi, \pi]$. The AN amplitude is determined by the phase difference between the per-antenna CE signal and the random AN phase, as illustrated in Fig. 3. The aggregated AN at the intended receiver, given by

$$y_{rAN1} = \sqrt{\frac{P_T}{N_t}} \sum_{i=1}^{N_t} h_i \beta_i e^{j\phi_i}, \tag{30}$$

is most likely non-zero. AN leakage will thus occur, which degrades the secrecy capacity. Note that (30) is simply a scalar. Therefore we can always add one single transmit antenna with user channel gain h_0 and transmit an additional AN signal

$$x_0 = \frac{-y_{rAN}}{h_0} = \beta_0 e^{j\phi_0} \tag{31}$$

such that the overall aggregate AN at the receiver is equal to zero

$$\sqrt{\frac{P_T}{N_t}} \sum_{i=0}^{N_t} h_i \beta_i e^{j\phi_i} = h_0 x_0 + y_{rAN} = 0. \tag{32}$$

That is, we need only one extra antenna which does not satisfy the per-antenna CE constraint in the system to completely cancel the AN leakage due to the random-phase AN and CE constraint on the other N_t antennas.

D. Secrecy Rate Evaluation

By assuming per-antenna CE information signals, the legitimate user's rate expression is the same as that in [4]. Therefore, when calculating the achievable secrecy rate in this work, the key is in how to evaluate the eavesdropper capacity. We next show an upper bound of the eavesdropper capacity by taking the correlation between two RVs, i.e. the information power and the AN power into account. This upper bound is non-trivial for the AN cancellation scheme given in Section IV-C (denoted Scheme II), but becomes trivial for the scheme of Section IV-B (denoted Scheme I). More effective ways to evaluate the eavesdropper capacity under the nonlinear per-antenna CE constraint, which remains an open problem, will be investigated in the journal version.

For both AN generation schemes, the eavesdropper's received signal can be expressed as

$$y_{\mathrm{eve}} = \sqrt{\frac{P_T}{N_t}} \sum_{i=1}^{N_t} g_i e^{j\theta_i} + \sqrt{\frac{P_T}{N_t}} \sum_{i=0}^{N_t} \beta_i g_i e^{j\phi_i} + n \tag{33}$$

$$= \sqrt{P_T} u_{\mathrm{eve}} + n_{\mathrm{AN}} + n,$$

where we define $u_{\mathrm{eve}} = \sqrt{\frac{1}{N_t}} \sum_{i=1}^{N_t} g_i e^{j\theta_i}$ and $n_{\mathrm{AN}} = \sqrt{\frac{P_T}{N_t}} \sum_{i=0}^{N_t} \beta_i g_i e^{j\phi_i}$. The term n is the AWGN, which has zero mean and variance σ^2. For Scheme I, we have $\beta_0 = 0$.

The above eavesdropper channel model (33) is similar to the equivalent SISO channel model for the legitimate MISO system demonstrated in [4]. The eavesdropper capacity is thus given by

$$C_{CE,E} = \sup_u I(u; u_{\mathrm{eve}}), \tag{34}$$

where the function $I(\cdot; \cdot)$ gives the mutual information between two RVs. According to the eavesdropper's equivalent SISO model (33), we have the following Markov relationship

$$u \leftrightarrow \Theta \leftrightarrow y_{\mathrm{eve}} \leftrightarrow u_{\mathrm{eve}}. \tag{35}$$

By the data processing inequality [12], we must have $I(u; u_{\mathrm{eve}}) \le I(\Theta; y_{\mathrm{eve}})$. Therefore we have the following upper bound of the eavesdropper capacity

$$\begin{aligned} C_{CE,E} &= \sup_u I(u; u_{\mathrm{eve}}) \\ &\le \sup_\Theta I(\Theta; y_{\mathrm{eve}}) \le \log_2 \left(1 + \frac{P_{u_{\mathrm{eve}}}}{P_{n_{\mathrm{AN}}} + \sigma^2} \right), \end{aligned} \tag{36}$$

where $P_{n_{\mathrm{AN}}} = \mathbb{E}_{\Theta, \Phi} \left[(u_{\mathrm{eve}} + n_{\mathrm{AN}})^2 \right] - \mathbb{E}_\Theta \left[u_{\mathrm{eve}}^2 \right]$ and $P_{u_{\mathrm{eve}}} = \mathbb{E}_\Theta \left[u_{\mathrm{eve}}^2 \right]$. Note that the above power splitting approach over-estimates the information signal power, which results in an upper bound on Eve capacity. By redefining the power terms in (36) as $P_{u_{\mathrm{eve}}} = \mathbb{E}_{\Theta, \Phi} \left[(u_{\mathrm{eve}} + n_{\mathrm{AN}})^2 \right] - \mathbb{E}_\Theta \left[n_{\mathrm{AN}}^2 \right]$ and $P_{n_{\mathrm{AN}}} = \mathbb{E}_\Theta \left[n_{\mathrm{AN}}^2 \right]$, a lower bound on the eavesdropper capacity can be obtained instead.

It can be shown that based on the above eavesdropper capacity upper bound and the corresponding signal-AN power splitting, the approximate power terms for Scheme I are given as

$$P_{u_{\mathrm{eve}}} = P_T \|\mathbf{g}\|^2 / N_t, \quad P_{n_{\mathrm{AN}}} = 0, \tag{37}$$

which completely ignores the AN power and therefore reduces to a trivial upper bound. By substituting (37) into (36), the capacity expression is identical to that for per-antenna CE precoding (without AN), given in Section III.

The power terms for the eavesdropper capacity upper bound with Scheme II can be calculated in a similar way.

$$P_{u_{\mathrm{eve}}} = P_T \|\mathbf{g}\|^2 / N_t, \tag{38}$$

$$P_{n_{\mathrm{AN}}} = \frac{P_T}{N_t} \cdot \mathbb{E}_{\Theta, \Phi} \left[\left(g_0 \cdot \frac{\sum_{i=1}^{N_t} h_i \beta_i e^{j\theta_i}}{h_0} \right)^2 \right]. \tag{39}$$

Fig. 4. Ergodic secrecy capacity v.s. P_T/σ^2 for i.i.d. Rayleigh fading with $N_t = 100$.

In both schemes, u_{eve} are zero-mean Gaussian distributed with variance $P_{u_{\text{eve}}}$. As $N_t \to \infty$, according to the Central Limit Theorem (CLT), we have

$$\sqrt{\frac{P_T}{N_t}} \cdot \frac{g_0 \sum_{i=1}^{N_t} h_i \beta_i e^{j\theta_i}}{h_0} \xrightarrow{N_t \to \infty} \mathcal{N}(0, P_{n_{\text{AN}}}). \qquad (40)$$

The resulting eavesdropper capacity upper bound for Scheme II is thus non-trivial.

V. NUMERICAL RESULTS

In this section, we evaluate the performance of the proposed secure constant envelope large-scale MISO system in terms of ergodic secrecy capacity as a function of average channel SNR, $\frac{P_T}{\sigma^2}$. In Fig. 4, the curves achieved by MF precoding (MF without AN in Fig. 4) and per-antenna CE precoding (CE without AN in Fig. 4) are calculated based on (16) and (22), respectively. For the curves achieved by AN-based schemes, including MF precoding with AN and optimal power allocation for the maximization of secrecy capacity (MF with AN in Fig. 4), and Scheme II (CE with random AN plus cancellation, discussed in Section IV-C) are obtained by Monte-Carlo simulations.

According to Fig. 4, we first observe that the performance for linear MF and per-antenna CE transmission (without AN) saturate at high-$\frac{P_T}{\sigma^2}$ regime, which motivates the AN-based transmission scheme for security improvement. In contrast, Scheme II described in Section IV-C results in a significantly higher secrecy capacity, especially in the high-$\frac{P_T}{\sigma^2}$ regime. The antenna element for leakage cancellation serves as an additional source of AN to the eavesdropper to mask the legitimate communication. The proposed method leads to comparable secrecy capacity performance with conventional MF precoded transmission with AN (optimal power allocation between data and AN [10]). We consider it a non-trivial observation, as with the absence of AN, the secrecy capacity gap between MF precoding and per-antenna CE precoding is fairly large, especially in the high-$\frac{P_T}{\sigma^2}$ regime. It indicates that with the proposed AN generation scheme, the cheaper and more power efficient CE implementation of large-scale MIMO can achieve secure transmission with performance

very close to linear MF precoder with AN. The only cost is one extra antenna violating the per-antenna CE constraint. Although not shown in our preliminary work, Scheme I of Section IV-B is expected to achieve a similar performance as Scheme II, with an expense of N_t iterations to find a group of ϕ_i's satisfying (25).

VI. CONCLUSIONS

In this work, we have investigated secure transmission in large-scale MISO systems under the per-antenna constant envelope constraint. Based on a security analysis of the per-antenna CE precoding scheme for large-scale MISO, we have proposed to use joint signal-plus-artificial-noise transmission to improve security in systems under the per-antenna CE constraint. A two-stage per-antenna CE precoding framework for joint signal-plus-AN transmission was proposed. In the first stage we determine the per-antenna CE precoding for the information-bearing signal. A properly generated artificial noise is incorporated into the transmit signal such that the combined signal-plus-AN satisfies the CE constraint and the AN part is "invisible" to the legitimate user. It is shown that compared to conventional per-antenna CE transmission, the joint signal-plus-AN secure transmission schemes do not require additional transmit power. A low-complexity AN generation scheme which requires an additional antenna element to cancel the AN leakage to the intended user introduced by randomly generated AN was also investigated.

REFERENCES

[1] (2015, Feb.) Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update 2014–2019 White Paper, [Online] Available: http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-in

[2] T. L. Marzetta, "Noncooperative cellular wireless with unlimited numbers of BS antennas," *IEEE Trans. Wireless Commun.*, vol. 9, no. 11, pp. 3590–3600, Nov. 2010.

[3] F. Rusek, D. Persson, B. K. Lau, E. G. Larsson, T. L. Marzetta, O. Edfors, and F. Tufvesson, "Scaling up MIMO: Opportunities and challenges with very large arrays," *IEEE Signal Process. Mag.*, vol. 30, no. 1, pp. 40C60, Jan. 2013.

[4] S. K. Mohammed and E. G. Larsson, "Single-user beamforming in large-scale MISO systems with per-antenna constant-envelope constraints: The doughnut channel," *IEEE Trans. Wireless Commun.*, vol. 11, pp. 3992–4005, Nov. 2012.

[5] S. K. Mohammed and E. G. Larsson, "Per-antenna constant envelope precoding for large multi-user MIMO systems," *IEEE Trans. Commun.*, vol. 61, pp. 1059–1071, Mar. 2013.

[6] S. K. Mohammed and E. G. Larsson, "Constant-envelope multi-usetr precoding for frequency-selective massive MIMO systems," *IEEE Wireless Commun. Letters*, vol.2, pp. 547–550, Oct. 2013.

[7] S. Goel, and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, pp. 2180–2189, Jun. 2008.

[8] J. Zhu, R. Schober, and V. K. Bhargava, "Secure transmission in multi-cell massive MIMO systems," *IEEE Trans. Wireless Commun.*, vol. 13, pp. 4766–4781, Sep. 2014.

[9] J. Zhu, R. Schober, and V. K. Bhargava, "Linear precoding of data and artificial noise in secure massive MIMO systems", *IEEE Trans. Wireless Commun.*, submitted, Mar., 2015. Available: http://arxiv.org/pdf/1505.00330v2.pdf

[10] X. Zhou and M. R. McKay, "Secure transmission with artificial noise over fading channels: Achievable rate and optimal power allocation," *IEEE Trans. Veh. Technol.*, vol. 59, pp. 3831–3842, Jul. 2010.

[11] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series And Products*, 7th Ed., Academic Press, Burlington, MA, 2007.

[12] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, 2nd Ed. Wiley, Hoboken, NJ, 2006.