Correlation-Based Power Allocation for Secure Transmission with Artificial Noise

Shihao Yan[†], Xiangyun Zhou[†], Nan Yang[†], Biao He[‡], and Thushara D. Abhayapala[†]
[†]Research School of Engineering, The Australian National University, Canberra, ACT 0200, Australia
[‡]Department of Electronic and Computer Engineering, Hong Kong University of Science and Technology, Hong Kong
Emails: {shihao.yan, xiangyun.zhou, nan.yang, thushara.abhayapala}@anu.edu.au, eebiaohe@ust.hk

***Abstract*—We examine for the first time the impact of transmitter-side correlation on the secure transmission with artificial noise (AN), based on which a new power allocation strategy for AN is devised for physical layer security enhancement. Specifically, we design a correlation-based power allocation (CPA) for AN, of which the optimality in terms of achieving the minimum secrecy outage probability is analytically proved in the large system regime with the number of transmit antennas approaching infinity. Our numerical results demonstrate that the CPA is nearly optimal and can significantly outperform the widely-used uniform power allocation (UPA) even for a moderate (finite) number of correlated transmit antennas. Our numerical results also reveal a fundamental difference between the secrecy performance of the CPA and that of the UPA. When the number of correlated transmit antennas increases, we find that the secrecy outage probability of the CPA always reduces while the secrecy outage probability of the UPA suffers from a saturation point.**

I. Introduction

A. Background and Motivation

As wireless devices are becoming increasingly ubiquitous, crucial concerns on the security of wireless communication are emerging since a large amount of confidential information is conveyed by the open medium. Besides the traditional cryptographic techniques, physical layer security has recently become another key mechanism for safeguarding wireless communications and thus attracted a high level of research interest due to its two noticeable advantages [1–3]. First, physical layer security can guarantee information secrecy regardless of an eavesdropper's computational capability, which leads to the fact that perfect secrecy can be achieved on the physical layer only. Second, physical layer security eliminates the centralized key distribution and management requested by cryptographic techniques, thus facilitating the management and improving the efficiency of wireless communications. In pioneering studies, e.g., [4, 5], a wiretap channel was proposed as the fundamental model of physical layer security, in which an eavesdropper (Eve) wiretaps the wireless communication from a transmitter (Alice) to an intended receiver (Bob).

Motivated by multiple-input multiple-output (MIMO) techniques, physical layer security in MIMO wiretap channels has attracted considerable research interest in the past decade (e.g., [6–8]). In this context, an increasing amount of research effort has been devoted to the secure transmission with artificial noise (AN) due to its robustness and desirable performance (e.g., [9–15]). The utilization of AN to enhance physical layer security was proposed in [9], where AN is isotropically transmitted in the null space of the main channel (i.e., the channel between Alice and Bob) in order to possibly reduce the quality of the eavesdropper's channel (i.e., the channel between Alice and Eve) without causing interference to Bob. Following [9] the secure transmission with AN has been well investigated in uncorrelated fading channels. However, it is often in practical scenarios that correlation exists among multiple antennas at one transceiver due to limited separation between antenna elements or poor scattering conditions. To the best knowledge of the authors, in the context of physical layer security the study on antenna correlation is still in its infancy. The impact of *receiver-side correlation* at Bob and Eve on the system performance was examined in [16] and [17], while the impact of the *transmitter-side correlation* has never been examined in the literature. This leaves an important gap in our understanding on the performance of the secure transmission with AN, and closing this gap forms the core of this work.

B. Our Contributions

In this work, we first detail the secure transmission with AN in wiretap channels with transmitter-side correlation, based on which we determine the optimal power allocation (OPA) for AN that minimizes the secrecy outage probability as an $(N_t - 1)$-dimensional numerical search problem (where N_t is the number of antennas at Alice). Then, focusing on the large system regime with $N_t \to \infty$ we derive a closed-form solution to the optimal power allocation, named the correlation-based power allocation (CPA), in which Alice allocates all the AN power to one specific direction determined by the transmitter-side correlation matrix and the channel state information (CSI) of the main channel. We further analytically prove that the CPA maximizes the average interference power to Eve for arbitrary number of correlated transmit antennas. In addition, based on the conducted analysis we draw useful insights on the comparison between the proposed CPA and the widely-used uniform power allocation (UPA), in which AN is isotropically transmitted in the null space of the main channel [9–15].

We present numerical results to characterize the secrecy performance of the CPA with UPA as the benchmark. Our results first demonstrate that a moderate level of antenna correlation already allows the CPA to achieve the nearly optimal secrecy performance even with a small number of transmit antennas. In such a situation, the CPA significantly

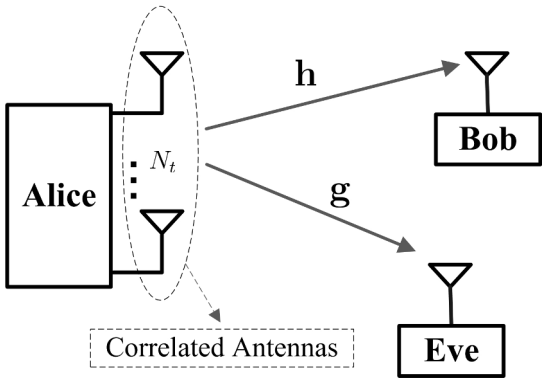

Fig. 1. Illustration of the wiretap channel of interest where Alice is equipped with N_t correlated antennas.

outperforms the UPA. Our results also reveal a fundamental difference between the CPA and UPA. That is when the number of correlated transmit antennas (i.e., N_t) increases, the secrecy outage probability achieved by the CPA always decreases, while the secrecy outage probability achieved by the UPA suffers from a saturation point.

II. System Model

A. Channel Model

The wiretap channel of interest is illustrated in Fig. 1, where Alice is equipped with N_t antennas, Bob is equipped with a single antenna, and Eve is equipped with a single antenna. We assume that all the wireless channels within our system model are subject to quasi-static Rayleigh fading, and the average fading power is normalized to one. Specifically, we adopt the separable correlation model and thus the $1 \times N_t$ main channel (i.e., the channel between Alice and Bob) vector is given by

$$\mathbf{h} = \mathbf{h}_s \mathbf{T}^{1/2}, \tag{1}$$

where $\mathbf{h}_s \in \mathcal{C}^{1\times N_t}$ has independent and identically distributed (i.i.d.) circularly-symmetric complex Gaussian entries (i.e., the entries are i.i.d circularly symmetric complex Gaussian random variables with zero-mean and unit-variance), $\mathbf{T}$ is the transmitter-side correlation matrix, and $\mathbf{T}^{1/2}$ denotes the *cholesky square root* of $\mathbf{T}$. Without loss of generality, we assume that $\mathbf{T}$ is a positive symmetric matrix. Thus, its singular value decomposition (SVD) can be written as $\mathbf{T} = \mathbf{U}_T \mathbf{\Lambda} \mathbf{U}_T^\dagger$, where $\mathbf{U}_T$ is a unitary matrix and $\mathbf{\Lambda} = \text{diag}[\lambda_1, \cdots, \lambda_{N_t}]$ is the diagonal matrix with λ_i as the i-th singular value of $\mathbf{T}$. Then, we can rewrite (1) as $\mathbf{h} = \mathbf{h}_s \sqrt{\mathbf{\Lambda}} \mathbf{U}_T^\dagger$, where each element of $\sqrt{\mathbf{\Lambda}}$ is the square root of the corresponding element of $\mathbf{\Lambda}$. In this work, we assume $\mathbf{h}$ is perfectly known at all transceivers.

The eavesdropper's channel is subject to the same transmitter-side correlation as the main channel and thus the $1 \times N_t$ eavesdropper's channel vector is given by

$$\mathbf{g} = \mathbf{g}_s \mathbf{T}^{1/2} = \mathbf{g}_s \sqrt{\mathbf{\Lambda}} \mathbf{U}_T^\dagger, \tag{2}$$

where $\mathbf{g}_s \in \mathcal{C}^{1\times N_t}$ has i.i.d circularly-symmetric complex Gaussian entries. We consider a passive eavesdropping scenario, where Alice does not know $\mathbf{g}$, but knows $\mathbf{T}$ due to the fact that $\mathbf{T}$ is determined by Alice's antenna geometry.

B. Secure Transmission with Artificial Noise

We next detail the secure transmission with AN in the wiretap channel of interest. In this secure transmission scheme, Alice transmits an information signal s_I in conjunction with an $(N_t - 1) \times 1$ AN signal vector $\mathbf{s}_N$ [9–15], where s_I and each entry of $\mathbf{s}_N$ have unit variance. We denote the total transmit power of Alice by P_A. The fraction of the power allocated to s_I is α ($0 < \alpha \leq 1$), and the remaining power $(1-\alpha)P_A$ is allocated to $\mathbf{s}_N$. In order to transmit s_I and $\mathbf{s}_N$, Alice designs an $N_t \times N_t$ beamforming matrix $\mathbf{V}$ given by

$$\mathbf{V} = [\mathbf{v}_I \ \mathbf{V}_N], \tag{3}$$

where $\mathbf{v}_I \in \mathcal{C}^{N_t \times 1}$ is used to transmit s_I and $\mathbf{V}_N \in \mathcal{C}^{N_t \times (N_t-1)}$ is used to transmit $\mathbf{s}_N$. The aim of $\mathbf{v}_I$ is to maximize the instantaneous SNR of the main channel, and thus we have $\mathbf{v}_I = \frac{\mathbf{h}^\dagger}{\|\mathbf{h}\|}$. Meanwhile, $\mathbf{V}_N$ is to degrade the quality of the eavesdropper's channel by transmitting $\mathbf{s}_N$ while perfectly avoiding interference to Bob. As such, $\mathbf{V}_N$ consists of $N_t - 1$ orthonomal column vectors in the nullspace of $\mathbf{h}^\dagger$. Then, the $N_t \times 1$ transmitted signal vector at Alice, $\mathbf{x}$, is given by

$$\begin{aligned}\mathbf{x} &= [\mathbf{v}_I \ \mathbf{V}_N] \begin{bmatrix} \sqrt{\alpha P_A}, & 0 \\ 0, & \sqrt{\frac{(1-\alpha)P_A}{N_t-1}}\sqrt{\mathbf{\Omega}} \end{bmatrix} \begin{bmatrix} s_I \\ \mathbf{s}_N \end{bmatrix} \\ &= \sqrt{\alpha P_A}\mathbf{v}_I s_I + \sqrt{\frac{(1-\alpha)P_A}{N_t-1}}\mathbf{V}_N\sqrt{\mathbf{\Omega}}\mathbf{s}_N, \end{aligned} \tag{4}$$

where $\mathbf{\Omega} \in \mathcal{C}^{(N_t-1)\times(N_t-1)}$ is the power allocation matrix for $\mathbf{s}_N$ satisfying $\text{tr}(\mathbf{\Omega}) = N_t - 1$.

Following (4) and noting $\mathbf{h}\mathbf{V}_N = 0$, the received signal at Bob is given by

$$y = \mathbf{h}\mathbf{x} + n_B = \sqrt{\alpha P_A}\mathbf{h}\mathbf{v}_I s_I + n_B, \tag{5}$$

where n_B is the additive white Gaussian noise (AWGN) at Bob satisfying $\mathbb{E}\left[n_B n_B^\dagger\right] = \sigma_B^2$. Based on (5), the instantaneous SNR at Bob is given by

$$\gamma_B = \alpha\overline{\gamma}_B \|\mathbf{h}\|^2 = \alpha\overline{\gamma}_B \sum_{i=1}^{N_t} \lambda_i |\mathbf{h}_s(i)|^2, \tag{6}$$

where $\overline{\gamma}_B = P_A/\sigma_B^2$. We note that γ_B is a function of $\mathbf{\Lambda}$ but not a function of $\mathbf{U}_T$.

Following (4), the received signal at Eve is given by

$$\begin{aligned} z &= \mathbf{g}\mathbf{x} + n_E \\ &= \sqrt{\alpha P_A}\mathbf{g}\mathbf{v}_I s_I + \sqrt{\frac{(1-\alpha)P_A}{N_t-1}}\mathbf{g}\mathbf{V}_N\sqrt{\mathbf{\Omega}}\mathbf{s}_N + n_E, \end{aligned} \tag{7}$$

where n_E is the AWGN at Eve satisfying $\mathbb{E}\left[n_E n_E^\dagger\right] = \sigma_E^2$. It is crucial to clarify that although Eve knows $\mathbf{h}$ and $\mathbf{V}$,

she cannot eliminate the interference caused by $\mathbf{V}_N\mathbf{s}_N$ due to $N_t > 1$. Following (7), the instantaneous SINR at Eve is given by

$$\gamma_E = \alpha \mathbf{g}\mathbf{v}_I \left(\frac{1-\alpha}{N_t - 1} \mathbf{g}\mathbf{V}_N \mathbf{\Omega} \mathbf{V}_N^\dagger \mathbf{g}^\dagger + \frac{1}{\overline{\gamma}_E} \right)^{-1} \mathbf{v}_I^\dagger \mathbf{g}^\dagger, \quad (8)$$

where $\overline{\gamma}_E = P_A/\sigma_E^2$. We note that γ_E is a function of $\mathbf{\Lambda}$ but not of $\mathbf{U}_T$ (the proof is similar to that of Lemma 2 in [18] and omitted here). Noting γ_B is a function of $\mathbf{\Lambda}$ but not of $\mathbf{U}_T$ as well, we can conclude that only the singular values of the correlation matrix $\mathbf{T}$ have impact on the secure communication with AN, while the eigenvectors of $\mathbf{T}$ (i.e., $\mathbf{U}_T$) have no impact.

C. Secrecy Performance Metric

An important assumption in this work is that the instantaneous CSI of the main channel is available at Alice. As such, the capacity of the main channel, $C_B = \log_2(1+\gamma_B)$, is known by Alice. On the other hand, Alice does not know the capacity of the eavesdropper's channel, $C_E = \log_2(1+\gamma_E)$, due to the fact that she cannot access the instantaneous CSI of the eavesdropper's channel. Therefore, we adopt the secrecy outage probability as our key performance metric, which is defined as the probability that the target rate of a secure transmission is larger than the secrecy capacity. The secrecy outage probability is given by [19]

$$P_{so}(R_s) = \Pr(C_s < R_s) = \Pr(C_B - R_s < C_E), \quad (9)$$

where R_s is the target rate of a secure transmission and $C_s = [C_B - C_E]^+$ is the secrecy capacity, where $[x]^+ = \max\{0, x\}$. In order to facilitate the secure transmission design under a given main channel condition, we study the secrecy outage probability in (9) for a given C_B, and this outage is solely caused by the uncertainty of C_E. We also note that if $R_s \geq C_B$ the main channel cannot support such a secure transmission (i.e., the secrecy outage probability is one).

III. Power Allocation for Artificial Noise

In this section, we first present the OPA for AN in the secure transmission that minimizes the secrecy outage probability in the wiretap channel with transmitter-side correlation. Then, focusing on the large system regime with $N_t \to \infty$, we derive a closed-form solution to the optimal power allocation based on the correlation matrix, named CPA. In addition, we discuss the UPA in the wiretap channel with transmitter-side correlation as a benchmark in this section.

A. Optimal Power Allocation

Utilizing the secrecy outage probability as the objective function, the optimization problem of power allocation for AN can be written as

$$\min_{\mathbf{\Omega}} \quad P_{so}(R_s), \quad \text{s.t.} \quad \text{tr}(\mathbf{\Omega}) = N_t - 1. \quad (10)$$

The optimization problem presented in (10) involves the determination of $(N_t-1)^2$ complex entries of the power allocation matrix $\mathbf{\Omega}$ (i.e., $2(N_t-1)^2$ real numbers), which is of high complexity. We have the following lemma to simplify (10) as a (N_t-1)-dimensional numerical search problem. For the sake of clear presentation, we define a positive definite Hermitian matrix as

$$\mathbf{Q} = \mathbf{V}_N^\dagger \mathbf{T} \mathbf{V}_N, \quad (11)$$

and its SVD can be written as

$$\mathbf{Q} = \mathbf{W} \Theta \mathbf{W}^\dagger, \quad (12)$$

where $\mathbf{W}$ is a unitary matrix and $\Theta = \text{diag}[\theta_1, \ldots, \theta_{N_t-1}]$ is the diagonal matrix with θ_m as the m-th singular value of $\mathbf{Q}$ with $\theta_1 \geq \theta_2 \geq \cdots \geq \theta_{N_t-1}$. We now present Lemma 1 based on the SVD of $\mathbf{Q}$.

Lemma 1: The optimization problem presented in (10) can be simplified as

$$\begin{aligned} \min_{\mathbf{\Phi}} \quad & P_{so}(R_s), \\ \text{s.t.} \quad & \mathbf{\Omega} = \mathbf{W}\mathbf{\Phi}, \quad \text{tr}(\mathbf{\Phi}) = N_t - 1, \\ & \mathbf{\Phi} = \text{diag}\left[\phi_1, \phi_2, \ldots, \phi_{N_t-1}\right], \end{aligned} \quad (13)$$

where $\phi_1, \phi_2, \ldots, \phi_{N_t-1}$ are non-negative real numbers.

Proof: We note that the selection of $\mathbf{\Omega}$ affects $P_{so}(R_s)$ only through $\mathbf{g}\mathbf{V}_N\mathbf{\Omega}\mathbf{V}_N^\dagger\mathbf{g}^\dagger$ involved in γ_E given in (8). Based on the definition of $\mathbf{g}$ given in (2), we have $\mathbf{V}_N^\dagger\mathbf{g}^\dagger \sim \mathcal{CN}(\mathbf{0}, \mathbf{Q})$. Then we know that $\mathbf{g}\mathbf{V}_N\mathbf{W}$ has i.i.d circularly-symmetric complex Gaussian entries. As proved in [20], $\mathbf{g}\mathbf{V}_N\mathbf{W}\mathbf{\Phi}\mathbf{W}^\dagger\mathbf{V}_N^\dagger\mathbf{g}^\dagger$ is equal in distribution to $\mathbf{g}\mathbf{V}_N\mathbf{\Omega}\mathbf{V}_N^\dagger\mathbf{g}^\dagger$ for general $\mathbf{\Phi}$ and $\mathbf{\Omega}$. This completes the proof of Lemma 1. ■

We note that the optimization problem presented in (13) is much less complex than that provided in (10). This is due to the fact that in (10) there are $2(N_t-1)^2$ real numbers to determine for $\mathbf{\Omega}$ while we only have to determine $N_t - 1$ real numbers for $\mathbf{\Phi}$ in (13). We also note that analytical solution to (13) is still mathematically intractable. This is mainly due to the fact that $P_{so}(R_s)$ cannot be derived in a closed-form expression for a general $\mathbf{\Phi}$. The difficulty lies in the fact that in the expression of γ_E given in (8) $\mathbf{g}\mathbf{V}_N\mathbf{W}\mathbf{\Phi}\mathbf{W}^\dagger\mathbf{V}_N^\dagger\mathbf{g}^\dagger$ and $|\mathbf{g}\mathbf{v}_I|^2$ are correlated, which leads to that the probability density function (pdf) of γ_E is mathematically intractable. Therefore, the optimization problem given in (13) can only be solved through numerical simulations, which is of high complexity and time-consuming for large N_t. As such, in the following we develop a sub-optimal but much simpler power allocation, and analytically prove its optimality in the large system regime with $N_t \to \infty$.

B. Correlation-Based Power Allocation

Now, we propose the CPA, which is optimal in terms of minimizing $P_{so}(R_s)$ in the large system regime with $N_t \to \infty$, in the following theorem.

Theorem 1: As $N_t \to \infty$, the optimal solution to $\mathbf{\Omega}$ that minimizes $P_{so}(R_s)$ is given by

$$\mathbf{\Omega}^* = (N_t - 1)\mathbf{w}_I, \quad (14)$$

where $\mathbf{w}_I$ is the principal eigenvector corresponding to the largest singular value of $\mathbf{Q}$ (i.e., $\mathbf{\Omega}^* = \mathbf{W}\mathbf{\Phi}^*$ and $\mathbf{\Phi}^* = \text{diag}\,[N_t - 1, 0, \ldots, 0]$).

Proof: Due to the distance concentration phenomenon [21], when $N_t \to \infty$ both $|\mathbf{g}\mathbf{v}_I|^2$ and $\|\mathbf{g}\mathbf{V}_N\mathbf{W}\sqrt{\mathbf{\Phi}}\|^2$ involved in γ_E approach their mean values. As such, γ_E approaches its mean and its variance approaches zero as $N_t \to \infty$. It follows that the minimization of the secrecy outage probability $P_{so}(R_s)$ is equivalent to minimizing the mean of γ_E. We note that $\mathbf{\Phi}$ only varies the value of $\|\mathbf{g}\mathbf{V}_N\mathbf{W}\sqrt{\mathbf{\Phi}}\|^2$ (i.e., $|\mathbf{g}\mathbf{v}_I|^2$ is not a function of $\mathbf{\Phi}$). Therefore, $\mathbf{\Phi}$ is to maximize the mean of $\|\mathbf{g}\mathbf{V}_N\mathbf{W}\sqrt{\mathbf{\Phi}}\|^2$ in order to minimize $P_{so}(R_s)$ as per the expression of γ_E given in (8). As mentioned in the proof of Lemma 1, $\mathbf{g}\mathbf{V}_N\mathbf{W}$ has i.i.d entries, and thus we have

$$\|\mathbf{g}\mathbf{V}_N\mathbf{W}\sqrt{\mathbf{\Phi}}\|^2 = \sum_{m=1}^{N_t-1} \phi_m\theta_m|\mathbf{g}_I(m)|^2, \tag{15}$$

where $\mathbf{g}_I = \mathbf{g}\mathbf{V}_N\mathbf{W}\left(\sqrt{\Theta}\right)^{-1}$ has i.i.d circularly-symmetric complex Gaussian entries with unit variance. Then, the mean of $\|\mathbf{g}\mathbf{V}_N\mathbf{W}\sqrt{\mathbf{\Phi}}\|^2$ is given by

$$\mathbb{E}\left[\|\mathbf{g}\mathbf{V}_N\mathbf{W}\sqrt{\mathbf{\Phi}}\|^2\right] = \sum_{m=1}^{N_t-1} \phi_m\theta_m. \tag{16}$$

Noting $\theta_1 \geq \theta_2 \geq \cdots \geq \theta_{N_t-1}$, in order to maximize $\mathbb{E}[\|\mathbf{g}\mathbf{V}_N\mathbf{W}\sqrt{\mathbf{\Omega}}\|^2]$ subject to $\text{tr}(\mathbf{\Phi}) = N_t - 1$ (i.e., $\phi_1 + \phi_2 + \cdots + \phi_{N_t-1} = N_t - 1$), we have to set $\phi_1^* = N_t - 1$ and $\phi_k^* = 0$ for $k = 2, 3, \ldots, N_t - 1$ (i.e., $\mathbf{\Phi}^* = \text{diag}\,[N_t - 1, 0, \ldots, 0]$). We note that for $\mathbf{\Phi}^* = \text{diag}\,[N_t - 1, 0, \ldots, 0]$ we have $\mathbf{\Omega}^* = \mathbf{W}\mathbf{\Phi}^* = (N_t - 1)\mathbf{w}_I$. This completes the proof of Theorem 1. ∎

We note that the CPA allocates all the AN power to the direction corresponding to the largest singular value of $\mathbf{Q}$, which is similar to the beamforming strategy based on $\mathbf{Q}$. The intuitive meaning of the CPA is that Alice first maps the N_t-dimensional eavesdropper's channel vector into the $(N_t - 1)$-dimensional nullspace of the main channel by applying $\mathbf{V}_N$ and then transmits AN along the average strongest direction of the effective eavesdropper's channel vector $\mathbf{g}\mathbf{V}_N$. This is due to the fact that $\mathbf{Q} = \mathbf{V}_N^\dagger\mathbf{T}\mathbf{V}_N$ is the covariance matrix of $\mathbf{g}\mathbf{V}_N$ and thus $\mathbf{w}_I$ corresponds to the average strongest direction of $\mathbf{g}\mathbf{V}_N$.

The following corollary states another important property of the CPA.

***Corollary** 1:* The CPA (i.e., $\mathbf{\Omega}^* = (N_t - 1)\mathbf{w}_I$) achieves the maximum average interference to Eve for all values of N_t, which is given by

$$\mathbb{E}\left[|\mathbf{g}\mathbf{V}_N\sqrt{\mathbf{\Omega}^*}|^2\right] = (N_t - 1)\theta_1. \tag{17}$$

Proof: Based on Lemma 1, we know that $\mathbb{E}\left[\|\mathbf{g}\mathbf{V}_N\sqrt{\mathbf{\Omega}}\|^2\right] = \mathbb{E}\left[\|\mathbf{g}\mathbf{V}_N\mathbf{W}\sqrt{\mathbf{\Phi}}\|^2\right]$. Then, based on the discussion after (16) in the proof of Theorem 1 we can conclude that the CPA maximizes the average interference to Eve (i.e., maximizes $\mathbb{E}\left[\|\mathbf{g}\mathbf{V}_N\sqrt{\mathbf{\Omega}}\|^2\right]$). Finally, substituting $\mathbf{\Omega}^* = \mathbf{W}\mathbf{\Phi}^* = (N_t - 1)\mathbf{w}_I$ into (16) we achieve the result given in (17). ∎

As per Theorem 1, the instantaneous SINR at Eve of the CPA for a given α is given by

$$\gamma_E^c = \frac{\alpha\overline{\gamma}_E|\mathbf{g}\mathbf{v}_I|^2}{(1-\alpha)\overline{\gamma}_E|\mathbf{g}\mathbf{V}_N\mathbf{w}_I|^2 + 1}. \tag{18}$$

C. Uniform Power Allocation

In this subsection, we present the UPA as a benchmark to clarify the benefits of our proposed CPA. In the UPA, Alice isotropically allocates the transmit power for the AN among all entries of $\mathbf{s}_N$, i.e., $\mathbf{\Omega} = \mathbf{I}_{N_t-1}$. Following (8), the SINR at Eve of the UPA for a given α is given by [14]

$$\gamma_E^u = \frac{\alpha\overline{\gamma}_E|\mathbf{g}\mathbf{v}_I|^2}{\frac{(1-\alpha)\overline{\gamma}_E}{N_t-1}\|\mathbf{g}\mathbf{V}_N\|^2 + 1}. \tag{19}$$

Following a similar procedure for obtaining (15), we have

$$\|\mathbf{g}\mathbf{V}_N\|^2 = \sum_{m=1}^{N_t-1} \theta_m|\mathbf{g}_I(m)|^2. \tag{20}$$

Then, the average interference to Eve achieved by the UPA is given by

$$\mathbb{E}\left[\|\mathbf{g}\mathbf{V}_N\|^2\right] = \sum_{m=1}^{N_t-1} \theta_m. \tag{21}$$

We note that the UPA is widely adopted in the literature in wiretap channels without correlation. This is due to the fact that Alice cannot access the instantaneous CSI of the eavesdropper's channel and has no information on $\mathbf{g}$ other than its distribution. With regard to the comparison between the UPA and CPA, we have the following remarks.

- The UPA maximizes the average interference to Eve in wiretap channels without correlation (i.e., $\mathbb{E}\left[\|\mathbf{g}\mathbf{V}_N\|^2\right] \geq \mathbb{E}\left[\mathbf{g}\mathbf{V}_N\mathbf{\Omega}\mathbf{V}_N^\dagger\mathbf{g}^\dagger\right]$ when $\mathbf{T} = \mathbf{I}_{N_t}$). We note that our proposed CPA achieves the same average interference to Eve as the UPA when $\mathbf{T} = \mathbf{I}_{N_t}$ (i.e., $(N_t - 1)\theta_1 = \sum_{m=1}^{N_t-1}\theta_m$ when $\mathbf{T} = \mathbf{I}_{N_t}$ due to $\theta_1 = \theta_2 = \cdots = \theta_{N_t-1}$ for $\mathbf{T} = \mathbf{I}_{N_t}$).
- Comparing (17) and (21) we can see that the CPA leads to a larger average interference to Eve than the UPA in wiretap channels with transmitter-side correlation. This is due to $\theta_1 \geq \theta_2 \geq \cdots \geq \theta_{N_t-1}$, which leads to $(N_t - 1)\theta_1 \geq \sum_{m=1}^{N_t-1}\theta_m$.
- Following the proof of Theorem 1, we know that as $N_t \to \infty$ these average interferences to Eve of the CPA and UPA as given in (17) and (21), respectively, determine the secrecy outage probabilities of the CPA and UPA, respectively. As such, we can conclude that in the large system regime with $N_t \to \infty$ the CPA leads to a lower $P_{so}(R_s)$ relative to the UPA in wiretap channels with transmitter-side correlation.
- The gap between θ_1 and $\frac{1}{N_t-1}\sum_{m=1}^{N_t-1}\theta_m$ increases as the correlation becomes more severe. As such, our proposed CPA is more desirable in wiretap channels with high transmitter-side correlation.

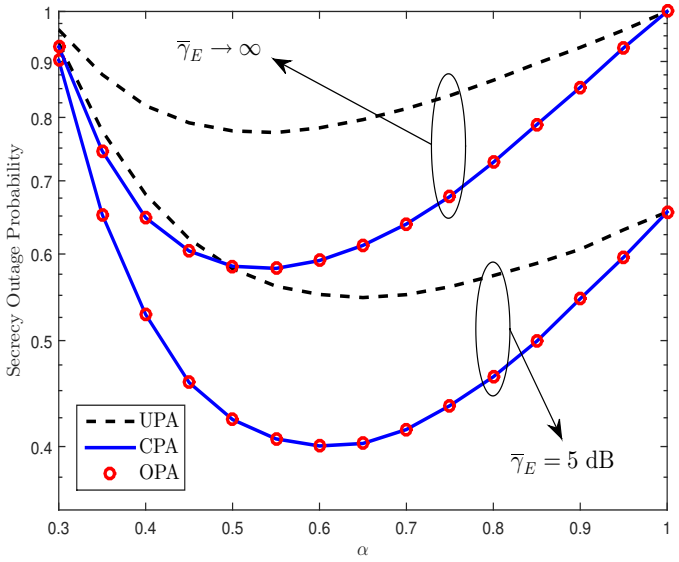

Fig. 2. Secrecy outage probabilities of the OPA, CPA, and UPA versus different values of α for $N_t = 4$, $R_s = 2$, $\overline{\gamma}_B = 5$ dB, $\mathbf{\Lambda} = \text{diag}[2.8, 0.7, 0.3, 0.2]$, and $\mathbf{h}_s = [0.1104 - 0.6619i, -0.6677 + 1.2432i, 0.7588 + 0.9201i, 1.0196 + 0.4098i]$.

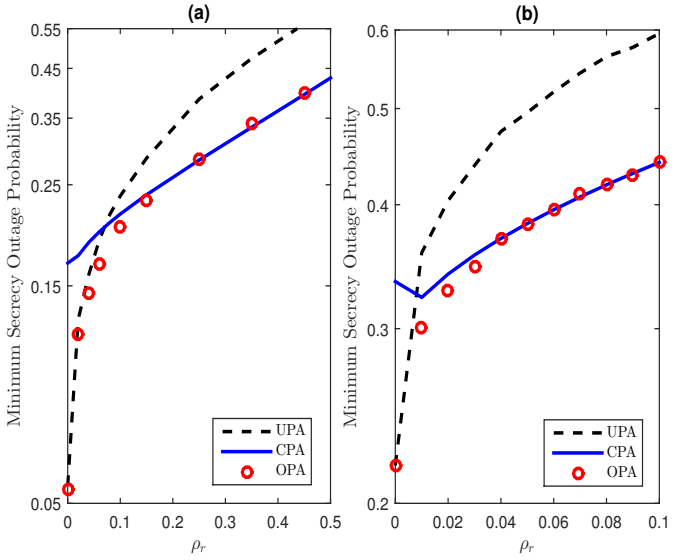

Fig. 3. Minimum secrecy outage probabilities of OPA, CPA, and UPA versus different values of ρ_r for $N_t = 3$, $L = 0.5$m, $R_s = 1$, $\overline{\gamma}_B = 10$ dB, $\overline{\gamma}_E \to \infty$, and (a) $\mathbf{h}_s = [-0.1470 + 0.1876i, -0.3905 + 1.0675i, -0.5091 - 0.8150i]$, (b) $\mathbf{h}_s = [-0.0845 + 0.5064i, 0.1612 + 0.0330i, -0.7529 + 0.0282i]$.

IV. Numerical Results

In this section, we first provide numerical comparison among the OPA, CPA, and UPA. Based on the comparison we draw useful insights on the CPA and the impact of transmitter-side correlation on the secure transmission with AN.

In Fig. 2 we plot the secrecy outage probabilities of the secure transmission with OPA, CPA, and UPA. Surprisingly, we first observe that our proposed CPA achieves almost identical secrecy outage probabilities with the OPA, which demonstrates that the proposed CPA is nearly optimal in terms of minimizing the secrecy outage probability under the adopted specific simulation settings (which are detailed in the caption of this figure[1]). Noting $N_t = 4$ for Fig. 2, we can conclude that our proposed CPA is nearly optimal even for a finite number of transmit antennas with moderate correlation. We note that as we have proved in Theorem 1 the CPA is optimal in the large system regime with $N_t \to \infty$. In this figure, we also observe that the proposed CPA achieves much lower secrecy outage probabilities than the UPA, which shows one advantage of the CPA relative to the UPA. Finally, we note that the optimal value of α that minimizes the secrecy outage probability for the CPA is different from that for the UPA.

In Fig. 3 we plot the minimum secrecy outage probabilities of the OPA, CPA, and UPA, which are obtained through setting α as its optimal values that minimizing the secrecy outage probabilities of the OPA, CPA, and UPA, respectively. Although our analysis is valid for an arbitrary correlation matrix, in this figure and the following figure we adopt an *exponential correlation model*, in which the (i, j)-th entry of $\mathbf{T}$ is given by $t_{ij} = \rho_r^{\delta_{ij}}$, where $\rho_r \in [0, 1]$ is the correlation parameter specified by system settings (e.g., signal frequency) and δ_{ij} is the distance between the i-th and j-th antennas at Alice. We note that a larger ρ_r indicates a larger correlation for a fixed δ_{ij}, where $\rho_r = 0$ serves as the uncorrelated case and $\rho_r = 1$ represents the fully correlated case. We also adopt the *uniform linear array* as Alice's antenna configuration and the array length is denoted as L in this figure and the following figures. In Fig. 3 (a) for the specific adopted $\mathbf{h}_s$ we observe that all the minimum secrecy outage probabilities increase as ρ_r increases. This is due to the fact that as $\rho_r \to 1$ the null space of the main channel disappears and Alice cannot create interference to Eve while perfectly avoiding the interference to Bob. In Fig. 3 (b) for the specific adopted $\mathbf{h}_s$ we observe that the minimum secrecy outage probability of the CPA first decreases and then increases as ρ_r increases. The decrease can be explained by the fact that the initial increase in the correlation (i.e., ρ_r) offers useful information of the eavesdropper's channel while does not significantly affect the null space of the specific $\mathbf{h}_s$, which leads to the reduction in the secrecy outage probability. The following increase in the minimum secrecy outage probability of the CPA can be explained by the fact that the offered information on the eavesdropper's channel by the increase in ρ_r cannot counteract the decay of the null space caused by the increase in ρ_r. We conducted hundreds of simulations for different realizations of $\mathbf{h}_s$ and all the results are similar to either Fig. 3 (a) or Fig. 3 (b). In both Fig. 3 (a) and Fig. 3 (b) we observe that the CPA outperforms the UPA when ρ_r is larger than some specific value, which only corresponds to a small correlation.

As we mentioned in Section II-C, we have focused on the secrecy outage probability for a given value of C_B in

[1]As we mentioned in Section II-B, $\mathbf{U}_T$ does not affect the performance of the secure transmission with AN. Thus, we only presented the adopted $\mathbf{\Lambda}$ for this figure.

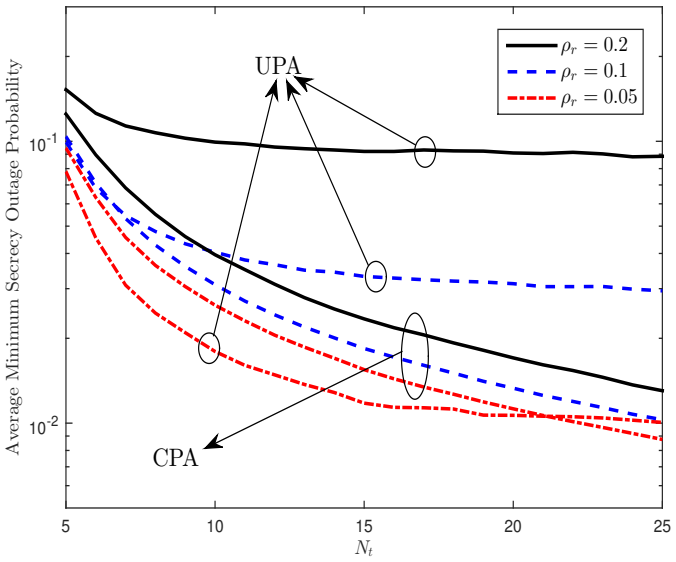

Fig. 4. Average minimum secrecy outage probabilities of CPA and UPA versus different values of N_t for $L = 0.5$m, $R_s = 1$, $\overline{\gamma}_B = 10$ dB, and $\overline{\gamma}_E \to \infty$.

order to study the AN power allocation design based on a given main channel realization. Now, we also present the secrecy outage probability averaged over all main channel realizations. In Fig. 4, we plot the average minimum secrecy outage probabilities of the CPA and UPA (denoted by $\overline{P_{so}^{c*}}(R_s)$ and $\overline{P_{so}^{u*}}(R_s)$, respectively) versus different values of N_t for fixed array length L, which are obtained through averaging the minimum secrecy outage probabilities of the CPA and UPA over $\mathbf{h}$, respectively. In this figure, we first observe that $\overline{P_{so}^{u*}}(R_s)$ first decreases and then keeps nearly constant as N_t increases. This indicates that N_t suffers from a saturation point in improving the secrecy performance of the UPA, which can be explained by the fact that as N_t increases for a fixed L the correlation among these transmit antennas becomes stronger. On the contrary, we observe that $\overline{P_{so}^{s*}}(R_s)$ continuously decreases as N_t increases without such a saturation point. This demonstrates another advantage of our proposed CPA relative to the UPA, which is that when N_t is large the CPA outperforms the UPA even in the wiretap channel with very low transmitter-side correlation. This advantage is confirmed by the observation that $\overline{P_{so}^{c*}}(R_s)$ becomes lower than $\overline{P_{so}^{u*}}(R_s)$ for $\rho_r = 0.05$ when N_t is larger than 21. Also, this observation can be explained by our Theorem 1, in which we have proved that the CPA is optimal in the large system-regime. Finally, we observe that the gap between $\overline{P_{so}^{c*}}(R_s)$ and $\overline{P_{so}^{u*}}(R_s)$ increases as N_t increases. This is caused by the fact that $\overline{P_{so}^{u*}}(R_s)$ suffers from a saturation point as N_t increases, but $\overline{P_{so}^{s*}}(R_s)$ does not.

V. Conclusion

In this work, we devised the CPA for AN in the wiretap channel with transmitter-side correlation and theoretically proved its optimality in terms of achieving the minimum secrecy outage probability in the large system regime with $N_t \to \infty$. Our analysis showed that the proposed CPA maximizes the average interference to Eve for arbitrary N_t. The conducted numerical results demonstrated that the CPA is nearly optimal and significantly outperforms the UPA even for finite N_t.

Acknowledgments

This work was supported by the Australian Research Council's Discovery Projects (DP150103905).

References

[1] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge University Press, 2011.
[2] X. Zhou, L. Song, and Y. Zhang, *Physical Layer Security in Wireless Communications*, CRC Press, 2013.
[3] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, and M. Di Renzo, "Safeguarding 5G wireless communication networks using physical layer security," *IEEE Commun. Mag.*, vol. 53, no. 4, pp. 20-27, Apr. 2015.
[4] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Techn. J.*, vol. 28, no. 4, pp. 656–715, Oct. 1949.
[5] A. Wyner, "The wire-tap channel," *Bell Syst. Techn. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.
[6] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennasPart II: The MIMOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 11, pp. 5515–5532, Nov. 2010.
[7] A. Mukherjee and A. L. Swindlehurst, "Robust beamforming for secrecy in MIMO wiretap channels with imperfect CSI," *IEEE Trans. Signal Process.*, vol. 59, no. 1, pp. 351–361, Jan. 2011.
[8] S. Yan, N. Yang, R. Malaney, and J. Yuan, "Transmit antenna selection with Alamouti coding and power allocation in MIMO wiretap channels," *IEEE Trans. Wireless Commun.*, vol. 13, no. 3, pp. 1656–1667, Mar. 2014.
[9] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, Jun. 2008.
[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, no. 8, pp. 3831–3842, Oct. 2010.
[11] X. Zhang, X. Zhou, and M. R. McKay, "On the design of artificial-noise-aided secure multi-antenna transmission in slow fading channels," *IEEE Trans. Veh. Technol.*, vol. 62, no. 5, pp. 2170–2181, Jun. 2013.
[12] G. Zheng, I. Krikidis, J. Li, A. P. Petropulu, and B. Ottersten, "Improving physical layer secrecy using full-duplex jamming receivers," *IEEE Trans. Signal Process.*, vol. 61, no. 20, pp. 4962–4974, Oct. 2013.
[13] X. Zhang, M. R. McKay, X. Zhou, and R. W. Heath Jr., "Artificial-noise-aided secure multi-antenna transmission with limited feedback," *IEEE Trans. Wireless Commun.*, vol. 14, no. 5, pp. 2742–2754, May. 2015.
[14] N. Yang, S. Yan, J. Yuan, R. Malaney, R. Subramanian, and I. Land, "Artificial noise: Transmission optimization in multi-input single-output wiretap channels," *IEEE Trans. Commun.*, vol. 63, no. 5, pp. 1771–1783, May 2015.
[15] N. Yang, M. Elkashlan, T. Q. Duong, J. Yuan, and R. Malaney, "Optimal transmission with artificial noise in MISOME wiretap channels," *IEEE Trans. Veh. Technol.*, accepted to appear.
[16] N. Yang, H. A. Suraweera, I. B. Collings, and C. Yuen, "Physical layer security of TAS/MRC with antenna correlation," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 1, pp. 254–259, Jan. 2013.
[17] B. He, X. Zhou, and T. D. Abhayapala, "Achieving secrecy without knowing the number of eavesdropper antennas," *IEEE Trans. Wireless Commun.*, vol. 14, no. 12, pp. 7030–7043, Dec. 2015.
[18] L. Hanlen and A. Grant, "Capacity analysis of correlated MIMO channels," *IEEE Trans. Inf. Theory*, vol. 58, no. 11, pp. 6773–6787, Nov. 2012.
[19] M. Bloch, J. Barros, M. Rodrigues, and S. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, Jun. 2008.
[20] S. A. Jafar and A. Goldsmith, "Transmitter optimization and optimality of beamforming for multiple antenna systems," *IEEE Trans. Wireless Commun.*, vol. 3, no. 4, pp. 1165–1175, Jul. 2004.
[21] D. Franҫois, V. Wertz, and M. Verleysen, "The concentration of fractional distances," *IEEE Trans. Knowl. Data. Eng.*, vol. 19, no. 7, pp. 873–886, Jul. 2007.