Artificial-Noise-Aided Secure Transmission in Wiretap Channels With Transmitter-Side Correlation

Shihao Yan, *Member, IEEE*, Xiangyun Zhou, *Member, IEEE*, Nan Yang, *Member, IEEE*, Biao He, *Member, IEEE*, and Thushara D. Abhayapala, *Senior Member, IEEE*

***Abstract*— This paper, for the first time, examines the impact of transmitter-side correlation on the artificial-noise (AN)-aided secure transmission, 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. In order to fully reveal the benefits of the CPA, we derive easy-to-evaluate expressions for the secrecy outage probability achieved by the CPA. Our study demonstrates that the CPA is nearly optimal and significantly outperforms the widely used uniform power allocation (UPA) even for a moderately small number of correlated transmit antennas. Furthermore, our numerical results reveal a fundamental difference between the CPA and UPA. That is when the number of correlated transmit antennas increases, the secrecy outage probability of the CPA always reduces while the secrecy outage probability of the UPA suffers from a saturation point.**

***Index Terms*— Physical layer security, transmitter-side correlation, artificial noise, power allocation.**

I. Introduction

A. Background and Motivation

CRUCIAL concerns on the security of wireless communication are emerging due to the fact that a large amount of confidential information (e.g., email/bank account information and password, credit card details) is currently conveyed by the wireless medium. Apart from 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]. The first one lies in the fact that physical layer security can guarantee information secrecy regardless of an eavesdropper's computational capability, which leads to that perfect secrecy can be achieved at the physical layer alone. 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., [5], [6], 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., [7], [8]). In this context, an increasing amount of research effort has been devoted to the artificial-noise-aided secure transmission due to its robustness and desirable performance (e.g., [10]–[17]). The utilization of artificial noise (AN) to enhance physical layer security was proposed in [10], where the 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. In [11], an achievable secrecy rate was derived in a closed-form expression, based on which the authors optimized the power allocation between the information signal and the AN. It was shown that equal power allocation is a near-optimal strategy in terms of maximizing the secrecy rate. Instead of transmitting AN isotropically, [12] considered joint optimization of the covariance matrices of the information signal and the AN for secrecy rate optimization. It was shown that transmit beamforming is optimal for secrecy rate maximization, which has been proved as optimal without using AN in [18]. Besides transmitting AN by Alice, a full-duplex Bob can also transmit AN in order to create interference to Eve, and this strategy is highly desirable in some specific practical scenarios (e.g., where Eve is close to Bob but far from Alice) [14]. In [17], practical transmission schemes (e.g., on-off transmission) with AN were examined and associated system parameters were optimized to maximize the effective secrecy rate. Meanwhile, massive MIMO is emerging as a key technology enabler for future 5G wireless networks, and thus physical layer security in the context of massive MIMO is attracting increasing research interests. For example, in [19] the secure downlink transmission in a multicell massive MIMO system was examined, in which two AN shaping matrices were considered. The opportunities and challenges of physical layer security in the context of massive MIMO were discussed in [20], in which active pilot contamination attacks

Manuscript received April 22, 2016; revised August 8, 2016; accepted September 20, 2016. Date of publication September 27, 2016; date of current version December 8, 2016. This work was supported by the Australian Research Council's Discovery Projects under Grant DP150103905. This work was presented at the IEEE Globecom, December 2016 [4]. The associate editor coordinating the review of this paper and approving it for publication was W. Mow.

S. Yan, X. Zhou, N. Yang, and T. D. Abhayapala are with the Research School of Engineering, Australian National University, Canberra, ACT, Australia (e-mail: shihao.yan@anu.edu.au; xiangyun.zhou@anu.edu.au; nan.yang@anu.edu.au; thushara.abhayapala@anu.edu.au).

B. He is with the Department of Electronic and Computer Engineering, The Hong Kong University of Science and Technology, Hong Kong (e-mail: eebiaohe@ust.hk).

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/TWC.2016.2613860

1536-1276 © 2016 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission.
See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

Authorized licensed use limited to: Centrale Supelec. Downloaded on October 22,2020 at 09:37:01 UTC from IEEE Xplore. Restrictions apply.

were revealed to be difficult to detect but of high harmfulness. A most recent work [21] investigated different precoding strategies of data and AN in secure massive MIMO systems and the impact of channel estimation, pilot contamination, multicell interference, and path-loss was examined as well.

In many practical scenarios, correlation exists among the multiple antennas at one transceiver due to limited separation between antenna elements or poor scattering conditions. This motivates the intensive investigation of how the antenna correlation affects the capacity of traditional MIMO systems without secrecy constraints (see [22] and reference therein). For example, in [22] it was shown that the transmit antenna correlation may increase capacity while the receive antenna correlation always leads to capacity reduction. It was proved in [23] that the link capacity is independent of the eigenvectors of correlation matrices and the capacity of a MIMO channel with channel state information (CSI) at the receiver increases almost surely as the number of transmit antennas increases. However, in the context of physical layer security the study on correlation is still in its infancy. The impact of receiver-side correlation at Bob and Eve on the transmit antenna selection (TAS) at Alice was investigated in wiretap channels [24]. It was shown that the receiver-side correlation enhances secrecy performance of TAS in the low average signal-to-noise ratio (SNR) regime of the main channel, but leads to performance degradation in the medium and high average SNR regimes [24]. Furthermore, spatial receiver-side correlation was introduced into wiretap channels in order to study physical layer security without knowing the number of eavesdropper's antennas [25]. However, the impact of the *transmitter-side correlation* has never been examined in the context of physical layer security, not to mention the AN-aided secure transmission. This leaves an important gap in our understanding on the performance of the AN-aided secure transmission, and closing this gap forms the core of this work.

B. Our Main 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 CSI of the main channel. We further analytically prove that the CPA maximizes the average interference power to Eve for any finite number of correlated transmit antennas. In order to fully understand the benefits of our proposed CPA, we derive easy-to-evaluate expressions for the secrecy outage probability achieved by the CPA, based on which we determine the optimal power allocation between the information signal and AN. 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 [10]–[17].

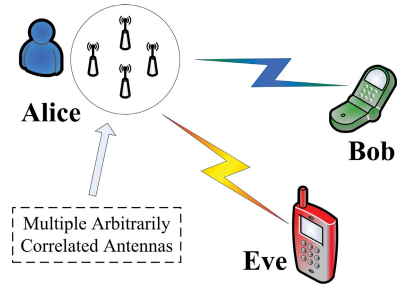


Fig. 1. Illustration of the wiretap channel of interest where Alice is equipped with multiple arbitrarily correlated antennas.

We present numerical results to characterize the secrecy performance of the CPA with the OPA and UPA as the benchmarks. 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 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. Furthermore, our numerical studies show that the transmitter-side correlation decreases the performance of the AN-aided secure transmission, which is mainly due to the fact that the null space of the main channel disappears as transmit antennas become fully correlated.

C. Paper Organization and Notation

The rest of this paper is organized as follows. Section II details our system model and the AN-aided secure transmission in correlated fading channels. Section III presents the three power allocations (i.e., OPA, CPA, and UPA), analytically proves the optimality of the CPA in the large system regime, and clarifies the benefits of the CPA relative to the UPA. Section IV derives the secrecy outage probability achieved by the CPA and optimizes the power allocation between the information signal and AN in the AN-aided secure transmission with CPA. Section V provides numerical results to confirm our analysis and provide useful insights on the impact of transmit antenna correlation. Section VI draws concluding remarks.

Notations: Scalar variables are denoted by italic symbols. Vectors and matrices are denoted by lower-case and upper-case boldface symbols, respectively. Given a complex number z, $|z|$ denotes the modulus of z. Given a complex vector $\mathbf{x}$, $\|\mathbf{x}\|$ denotes the Euclidean norm and $\mathbf{x}^\dagger$ denotes the conjugate transpose of $\mathbf{x}$. The $L \times L$ identity matrix is referred to as $\mathbf{I}_L$ and $\mathbb{E}[\cdot]$ denotes expectation.

II. System Model

A. Channel Model

The wiretap channel of interest is illustrated in Fig. 1, where Alice is equipped with N_t correlated antennas, Bob is equipped with a single antenna, and Eve is equipped with a single

Authorized licensed use limited to: Centrale Supelec. Downloaded on October 22,2020 at 09:37:01 UTC from IEEE Xplore. Restrictions apply.

antenna. This consideration can be justified in the scenarios where Alice is a multi-antenna access point or base station while both Bob and Eve are single-antenna user terminals in the network (and Alice transmits confidential information to Bob which should not be intercepted by Eve). 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 (i.e., Kronecker model) and thus the $1 \times N_t$ main channel (i.e., the channel between Alice and Bob) vector is given by [26]

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

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 $\mathbf{T}$. We note that the transmitter-side correlation matrix $\mathbf{T}$ in the Kronecker model is determined by the signal frequency, transmitter-side antenna geometry, and transmitter-side scattering characteristics [26]–[28]. As such, in this work we assume that $\mathbf{T}$ is known by Alice and the eavesdropper's channel is subject to the same transmit antenna correlation as the main channel. Without loss of generality, we assume that $\mathbf{T}$ is a positive symmetric matrix. Thus, its singular value decomposition (SVD) can be written as $\mathbf{T} = \mathbf{U}_T \Lambda \mathbf{U}_T^\dagger$, where $\mathbf{U}_T$ is a unitary matrix and $\Lambda = \mathrm{diag}[\lambda_1, \cdots, \lambda_{N_t}]$ is the diagonal matrix with λ_i as the i-th singular value of $\mathbf{T}$. Then, we can rewrite (1) as $\mathbf{h} = \mathbf{h}_s \sqrt{\Lambda} \mathbf{U}_T^\dagger$, where each element of $\sqrt{\Lambda}$ is the square root of the corresponding element of Λ. We note that in most practical scenarios, Alice will send pilots *a priori* or together with data to enable the estimation of $\mathbf{h}$ at Bob, and then Alice acquires the estimated CSI of the main channel through requesting feedback from Bob. The obtained CSI may suffer from the channel estimation and quantization errors. However, if sufficient resources are available for the channel estimation and feedback (e.g., transmit power and/or time slots are enough for accurate channel estimation), these errors can be made negligible. As such, we assume that $\mathbf{h}$ is perfectly known at all transceivers in this work, since Eve may eavesdrop on the feedback from Bob to Alice to obtain $\mathbf{h}$.

Since the eavesdropper's channel is also subject to the transmitter-side correlation matrix $\mathbf{T}$, the $1 \times N_t$ eavesdropper's channel vector in the Kronecker model is given by

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

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 have the full knowledge of $\mathbf{g}$.

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 $\mathbf{s}_N$ [10]–[17], 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

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

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

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 $\mathbb{E}[n_B n_B^\dagger] = \sigma_B^2$. Based on (5), the instantaneous SNR at Bob is given by

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

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

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

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

where n_E is the AWGN at Eve satisfying $\mathbb{E}[n_E n_E^\dagger] = \sigma_E^2$. 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 [11]

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

where $\mu_E = P_A/\sigma_E^2$. We note that γ_E is a function of Λ but not of $\mathbf{U}_T$ (the proof is similar to that of Lemma 2 in [22] and omitted here). Noting γ_B is a function of Λ 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.

Authorized licensed use limited to: Centrale Supelec. Downloaded on October 22,2020 at 09:37:01 UTC from IEEE Xplore. Restrictions apply.

C. Secrecy Performance Metric

Since the CSI of the main channel is assumed to be known by Alice, the capacity of the main channel, $C_B = \log_2(1+\gamma_B)$, is available at 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 CSI of the eavesdropper's channel. Considering quasi-static fading channels, 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 [29], [30]

$$P(R_s) = \Pr(C_s < R_s) = \Pr(C_B - R_s < C_E), \tag{9}$$

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 (i.e., optimal power allocation) 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 (i.e., correlation-based power allocation). In addition, we discuss the UPA (i.e., uniform power allocation) 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

$$\begin{aligned} \min_{\Omega} \quad & P(R_s), \\ \text{s.t.} \quad & \mathrm{tr}(\Omega) = N_t - 1. \end{aligned} \tag{10}$$

The optimization problem presented in (10) involves the determination of $(N_t-1)^2$ complex entries of the power allocation matrix Ω (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

$$\mathbf{Q} = \mathbf{V}_N^\dagger \mathbf{T} \mathbf{V}_N, \tag{11}$$

and its SVD can be written as

$$\mathbf{Q} = \mathbf{W}\Theta\mathbf{W}^\dagger, \tag{12}$$

where $\mathbf{W}$ is a unitary matrix and $\Theta = \mathrm{diag}[\theta_1, \ldots, \theta_{N_t-1}]$ 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

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

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

Proof: We note that the selection of Ω affects $P(R_s)$ only through $\mathbf{g}\mathbf{V}_N\Omega\mathbf{V}_N^\dagger\mathbf{g}^\dagger$ 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 [31, Th. 1 and Lemma 1], $\mathbf{g}\mathbf{V}_N\mathbf{W}\Phi\mathbf{W}^\dagger\mathbf{V}_N^\dagger\mathbf{g}^\dagger$ is equal in distribution to $\mathbf{g}\mathbf{V}_N\Omega\mathbf{V}_N^\dagger\mathbf{g}^\dagger$ for general Φ and Ω. 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 Ω while we only have to determine $N_t - 1$ real numbers for Φ in (13). We also note that analytical solution to (13) is still mathematically intractable. This is mainly due to the fact that $P(R_s)$ cannot be derived in a closed-form expression for a general Φ. The difficulty lies in the fact that $\mathbf{g}\mathbf{V}_N\mathbf{W}\Phi\mathbf{W}^\dagger\mathbf{V}_N^\dagger\mathbf{g}^\dagger$ and $|\mathbf{g}\mathbf{v}_I|^2$ are correlated in the expression of γ_E given in (8), 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 $P(R_s)$ 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 Ω that minimizes $P(R_s)$ is given by

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

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

Proof: Due to the distance concentration phenomenon [32], when $N_t \to \infty$ both $|\mathbf{g}\mathbf{v}_I|^2$ and $\|\mathbf{g}\mathbf{V}_N\mathbf{W}\sqrt{\Phi}\|^2$ involved in γ_E approach their mean values.

We note that the mean of $\|\mathbf{g}\mathbf{V}_N\mathbf{W}\sqrt{\Phi}\|^2$ is positive and $\mu_E \geq 0$. As such, we can conclude that γ_E approaches its mean as $N_t \to \infty$ based on the quotient rule for limits, which states that the limit of a quotient of two functions is the quotient of their limits, provided the limit of the denominator is not zero [33]. It follows that the minimization of the secrecy outage probability $P(R_s)$ is equivalent to minimizing the mean of γ_E. We note that Φ only varies the value of $\|\mathbf{g}\mathbf{V}_N\mathbf{W}\sqrt{\Phi}\|^2$ (i.e., $|\mathbf{g}\mathbf{v}_I|^2$ is not a function of Φ). Therefore, Φ is to maximize the mean of $\|\mathbf{g}\mathbf{V}_N\mathbf{W}\sqrt{\Phi}\|^2$ in order to minimize $P(R_s)$ as per the expression of γ_E given in (8). As mentioned

Authorized licensed use limited to: Centrale Supelec. Downloaded on October 22,2020 at 09:37:01 UTC from IEEE Xplore. Restrictions apply.

in the proof of Lemma 1, $\mathbf{g}\mathbf{V}_N\mathbf{W}$ has i.i.d entries, and thus we have

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

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

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

Noting $\theta_1 \geq \theta_2 \geq \cdots \geq \theta_{N_t-1}$, in order to maximize $\mathbb{E}[\|\mathbf{g}\mathbf{V}_N\mathbf{W}\sqrt{\Omega}\|^2]$ subject to $\mathrm{tr}(\Phi) = N_t - 1$ (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., $\Phi^* = \mathrm{diag}[N_t - 1, 0, \ldots, 0]$). We note that for $\Phi^* = \mathrm{diag}[N_t - 1, 0, \ldots, 0]$ we have $\Omega^* = \mathbf{W}\Phi^*\mathbf{W}^\dagger = (N_t - 1)\mathbf{w}_I\mathbf{w}_I^\dagger$. 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 $\mathbf{g}\mathbf{V}_N$. We also note that this is the first work studying the impact of transmitter-side correlation on the design of secure transmission. As such, we focus more on the transmitter side and considered a simple baseline model for receivers, in which Bob and Eve are both single-antenna devices. Moreover, we clarify that our Theorem 1 is still valid when Eve is equipped with multiple (i.e., N_e) uncorrelated antennas.

The following corollary states another important property of the CPA.

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

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

Proof: Based on Lemma 1, we know that $\mathbb{E}[\|\mathbf{g}\mathbf{V}_N\sqrt{\Omega}\|^2] = \mathbb{E}[\|\mathbf{g}\mathbf{V}_N\mathbf{W}\sqrt{\Phi}\|^2]$. 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 $\mathbb{E}[\|\mathbf{g}\mathbf{V}_N\sqrt{\Omega}\|^2]$). Finally, substituting $\Omega^* = \mathbf{W}\Phi^*\mathbf{W}^\dagger = (N_t - 1)\mathbf{w}_I\mathbf{w}_I^\dagger$ 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

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

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., $\Omega = \mathbf{I}_{N_t-1}$. Following (8), the SINR at Eve of the UPA for a given α is given by [17]

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

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 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., $\mathbb{E}[\|\mathbf{g}\mathbf{V}_N\|^2] \geq \mathbb{E}[\mathbf{g}\mathbf{V}_N\Omega\mathbf{V}_N^\dagger\mathbf{g}^\dagger]$ 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 $P(R_s)$ 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.

IV. Secrecy Performance Analysis of the Correlation-Based Power Allocation

In this section we analyze the secrecy performance of the AN-aided secure transmission with CPA in order to fully understand the benefits of the proposed CPA for AN. As mentioned in Section II-C, we study the secrecy outage probability for a given main channel realization in order to facilitate the channel-dependent transmission design. Specifically, we derive easy-to-evaluate expressions for the secrecy outage probabilities of the CPA. Based on these expressions, we determine the optimal power allocation between the information signal and

Authorized licensed use limited to: Centrale Supelec. Downloaded on October 22,2020 at 09:37:01 UTC from IEEE Xplore. Restrictions apply.

the AN. We note that in practice we may not be able to know the receiver noise level at Eve (i.e., σ_E^2), and thus we first derive the secrecy outage probability for $\sigma_E^2 = 0$ (referred to as the asymptotic secrecy outage probability) and then derive the secrecy outage probability for arbitrary known values of σ_E^2 with $\sigma_E^2 > 0$ (referred to as the exact secrecy outage probability). We would like to clarify that the asymptotic secrecy outage probability is not a special case of the exact secrecy outage probability.

A. Asymptotic Secrecy Outage Probability

For $\sigma_E^2 = 0$ (i.e., $\mu_E \to \infty$) , following (18) the SINR at Eve is given by

$$\gamma_E^{\infty} = \frac{\alpha|\mathbf{g}\mathbf{v}_I|^2}{(1-\alpha)|\mathbf{g}\mathbf{V}_N\mathbf{w}_I|^2}. \tag{22}$$

We next derive the asymptotic secrecy outage probability achieved by the CPA for $\sigma_E^2 = 0$ in the following theorem. We note that we have $\alpha < 1$ for $\sigma_E^2 = 0$ in order to guarantee the asymptotic secrecy outage probability to be less than one (i.e., the asymptotic secrecy outage probability equals one for $\alpha = 1$).

Theorem 2: The asymptotic secrecy outage probability achieved by the CPA is given by

$$P_{\infty}(R_s) = 1 - \frac{\sigma_n^2(1-\rho)}{\sigma_d^2}\sum_{k=0}^{\infty}\frac{(2k+1)!\sigma_n^{2k}\rho^k}{(k!)^2\sigma_d^{2k}}\sum_{i=0}^{k}\frac{\binom{k}{i}\left(-\frac{\sigma_n^2}{\sigma_d^2}\right)^{k-i}}{i-2k-1} \times\left[\left(\frac{\gamma_B+1}{2^{R_s}} - 1 + \frac{\sigma_n^2}{\sigma_d^2}\right)^{i-2k-1} - \left(\frac{\sigma_n^2}{\sigma_d^2}\right)^{i-2k-1}\right], \tag{23}$$

where

$$\rho = \frac{\alpha(1-\alpha)|\mathbf{v}_I^{\dagger}\mathbf{T}\mathbf{V}_N\mathbf{w}_I|^2}{4\sigma_n^2\sigma_d^2}, \tag{24}$$

$$\sigma_n = \sqrt{\frac{\alpha}{2}\mathbf{v}_I^{\dagger}\mathbf{T}\mathbf{v}_I}, \tag{25}$$

$$\sigma_d = \sqrt{\frac{1-\alpha}{2}\mathbf{w}_I^{\dagger}\mathbf{V}_N^{\dagger}\mathbf{T}\mathbf{V}_N\mathbf{w}_I}. \tag{26}$$

Proof: Following (9), the asymptotic secrecy outage probability of the CPA is given by

$$P_{\infty}(R_s) = \Pr\left(\gamma_E^{\infty} > \frac{\gamma_B+1}{2^{R_s}} - 1\right) = 1 - F_{\gamma_E^{\infty}}\left(\frac{\gamma_B+1}{2^{R_s}} - 1\right), \tag{27}$$

where $F_{\gamma_E^{\infty}}(\cdot)$ is the cumulative distribution function (cdf) of γ_E^{∞}. In order to derive the expression of $P_{\infty}(R_s)$, we next derive $F_{\gamma_E^{\infty}}(\cdot)$. We can rewrite γ_E^{∞} as $\gamma_E^{\infty} = \chi_n/\chi_d$, where

$$\chi_n = \alpha|\mathbf{g}\mathbf{v}_I|^2, \tag{28}$$

$$\chi_d = (1-\alpha)|\mathbf{g}\mathbf{V}_N\mathbf{w}_I|^2. \tag{29}$$

The correlation coefficient between χ_n and χ_d is ρ. We note that $\rho = 0$ if $\mathbf{T} = \mathbf{I}_{N_t}$ (i.e., uncorrelated fading channels) due to the fact that $\mathbf{v}_I$ and $\mathbf{V}_N$ are orthogonal. We also note that $\mathbf{v}_I$, $\mathbf{V}_N$, and $\mathbf{w}_I$ are known and deterministic since the CSI of the main channel $\mathbf{h}$ and the correlation matrix $\mathbf{T}$ are assumed to be fixed and known. As such, $\mathbf{g}\mathbf{v}_I$ and $\mathbf{g}\mathbf{V}_N\mathbf{w}_I$ are both complex Gaussian random variables (for given deterministic $\mathbf{v}_I$, $\mathbf{V}_N$, and $\mathbf{w}_I$), which leads to that χ_n and χ_d are independent when $\rho = 0$. We next focus on the case where $\rho \neq 0$ since we are interested in correlated fading channels in this work. Again, since $\mathbf{g}\mathbf{v}_I$ and $\mathbf{g}\mathbf{V}_N\mathbf{w}_I$ are both complex Gaussian random variables (for given deterministic $\mathbf{v}_I$, $\mathbf{V}_N$, and $\mathbf{w}_I$), the joint pdf of χ_n and χ_d is given by [35]

$$f_{\chi_n,\chi_d}(x,y) = \frac{e^{-\frac{1}{2(1-\rho)}\left(\frac{x}{\sigma_n^2}+\frac{y}{\sigma_d^2}\right)}}{4\sigma_n^2\sigma_d^2(1-\rho)} I_0\left(\frac{\sqrt{\rho}}{1-\rho}\frac{\sqrt{xy}}{\sigma_n\sigma_d}\right), \tag{30}$$

where $I_0(\cdot)$ is the zero-order modified Bessel function of the first kind, which can be expanded as

$$I_0(t) = \sum_{k=0}^{\infty}\frac{t^{2k}}{2^{2k}(k!)^2}. \tag{31}$$

Then, the pdf of γ_E^{∞} is derived as

$$\begin{aligned} f_{\gamma_E^{\infty}}(z) &= \int_0^{\infty} y f_{\chi_n,\chi_d}(zy,y)dy \\ &\overset{a}{=} \frac{1}{4\sigma_n^2\sigma_d^2(1-\rho)}\sum_{k=0}^{\infty}\frac{\left(\frac{\sqrt{\rho}}{1-\rho}\frac{\sqrt{z}}{\sigma_n\sigma_d}\right)^{2k}}{2^{2k}(k!)^2} \\ &\quad\times\int_0^{\infty} y^{2k+1}e^{-\frac{1}{2(1-\rho)}\left(\frac{z}{\sigma_n^2}+\frac{1}{\sigma_d^2}\right)y}dy \\ &\overset{b}{=} \frac{1}{4\sigma_n^2\sigma_d^2(1-\rho)}\sum_{k=0}^{\infty}\frac{\left(\frac{\sqrt{\rho}}{1-\rho}\frac{\sqrt{z}}{\sigma_n\sigma_d}\right)^{2k}}{2^{2k}(k!)^2} \\ &\quad\times(2k+1)!\left[\frac{1}{2(1-\rho)}\left(\frac{z}{\sigma_n^2}+\frac{1}{\sigma_d^2}\right)\right]^{-(2k+2)} \\ &= \frac{\sigma_n^2(1-\rho)}{\sigma_d^2}\sum_{k=0}^{\infty}\frac{(2k+1)!\sigma_n^{2k}\rho^k}{(k!)^2\sigma_d^{2k}}\frac{z^k}{\left(z+\frac{\sigma_n^2}{\sigma_d^2}\right)^{2k+2}}, \end{aligned} \tag{32}$$

where $\overset{a}{=}$ is achieved by substituting (31) into (30) and $\overset{b}{=}$ is obtained based on the following identify [36, eq. (3.351.3)]

$$\int_0^{\infty} x^n e^{-\tau x}dx = n!\tau^{-n-1}. \tag{33}$$

Then, following (32) the cdf of γ_E^{∞} can be derived as

$$\begin{aligned} F_{\gamma_E^{\infty}}(z) &= \int_0^z f_{\gamma_E^{\infty}}(x)dx \\ &\overset{c}{=} \frac{\sigma_n^2(1-\rho)}{\sigma_d^2}\sum_{k=0}^{\infty}\frac{(2k+1)!\sigma_n^{2k}\rho^k}{(k!)^2\sigma_d^{2k}} \\ &\quad\times\int_{\frac{\sigma_n^2}{\sigma_d^2}}^{z+\frac{\sigma_n^2}{\sigma_d^2}} y^{-(2k+2)}\left(y-\frac{\sigma_n^2}{\sigma_d^2}\right)^k dy \\ &\overset{d}{=} \frac{\sigma_n^2(1-\rho)}{\sigma_d^2}\sum_{k=0}^{\infty}\frac{(2k+1)!\sigma_n^{2k}\rho^k}{(k!)^2\sigma_d^{2k}}\sum_{i=0}^{k}\frac{\binom{k}{i}\left(-\frac{\sigma_n^2}{\sigma_d^2}\right)^{k-i}}{i-2k-1} \\ &\quad\times\left[\left(z+\frac{\sigma_n^2}{\sigma_d^2}\right)^{i-2k-1} - \left(\frac{\sigma_n^2}{\sigma_d^2}\right)^{i-2k-1}\right], \end{aligned} \tag{34}$$

Authorized licensed use limited to: Centrale Supelec. Downloaded on October 22,2020 at 09:37:01 UTC from IEEE Xplore. Restrictions apply.

where $\overset{c}{=}$ is achieved by exchanging variables (i.e., setting $y = x + \sigma_n^2/\sigma_d^2$) and $\overset{d}{=}$ is obtained by applying the following identity [36, eq. (1.111)]

$$(x-t)^n = \sum_{i=0}^{n} \binom{n}{i} x^i (-t)^{n-i}. \tag{35}$$

Then, the secrecy outage probability given in (23) is achieved by substituting (34) into (27). ■

We note that although the expression of the secrecy outage probability given in (23) involves an infinite series (i.e., $\sum_{k=0}^{\infty}$), it can be approximated by its finite truncation accurately (e.g., utilizing the first K terms, $\sum_{k=0}^{K}$, as an approximation of $\sum_{k=0}^{\infty}$). This is due to the fact that (23) is convergent since the infinite series involved in (23) arises from the series expansion of the zero-order modified Bessel function of the first kind given in (31), which is convergent.

B. Exact Secrecy Outage Probability

In some scenarios, the receiver noise level at Eve (i.e., σ_E^2) is possible to be known by Alice. For example, Eve could be a normal user served by Alice, but secure communication between Alice and Bob is requested while treating Eve as an eavesdropper. As such, in this subsection we derive the exact secrecy outage probability achieved by the CPA for $\sigma_E^2 > 0$, which is presented in the following theorem.

Theorem 3: The exact secrecy outage probability achieved by the CPA is given by

$$P(R_s) = \begin{cases} e^{-\dfrac{\frac{\gamma_B+1}{2^{R_s}}-1}{\mu_E \mathbf{v}_I^\dagger \mathbf{T} \mathbf{v}_I}}, & \alpha = 1, \\ P_{so}^{\alpha}(R_s), & 0 < \alpha < 1, \end{cases} \tag{36}$$

where

$$\begin{aligned} P_{so}^{\alpha}(R_s) = 1 &- \frac{e^{\frac{1}{2(1-\rho)s_d^2}}}{4s_n^2 s_d^2 (1-\rho)} \sum_{k=0}^{\infty} \frac{\rho^k (1-\rho)^{-k}}{2^k (k!)^2 s_d^{2k}} \sum_{i=0}^{k} \frac{\binom{k}{i}}{(-1)^{i-k}} \\ &\times \sum_{j=0}^{k+i+1} \frac{(k+i+1)!}{j!\left[2(1-\rho)s_n^2\right]^{j-i-2}} \sum_{m=0}^{k} \binom{k}{m} \left(-\frac{s_n^2}{s_d^2}\right)^{k-m} \\ &\times \left[\Gamma\left(k+i-j-m+1, \frac{1}{2(1-\rho)s_n^2}, \frac{\gamma_B+1}{2^{R_s}} - 1 + \frac{s_n^2}{s_d^2}\right) - \Gamma\left(k+i-j-m+1, \frac{1}{2(1-\rho)s_n^2}, \frac{s_n^2}{s_d^2}\right)\right], \end{aligned} \tag{37}$$

$$s_n = \sqrt{\frac{\alpha \mu_E}{2} \mathbf{v}_I^\dagger \mathbf{T} \mathbf{v}_I}, \tag{38}$$

$$s_d = \sqrt{\frac{(1-\alpha)\mu_E}{2} \mathbf{w}_I^\dagger \mathbf{V}_N^\dagger \mathbf{T} \mathbf{V}_N \mathbf{w}_I}, \tag{39}$$

$$\Gamma(n,p,x) = \begin{cases} p^n \gamma(-n, px), & n < 0, \\ \mathbf{Ei}(-px), & n = 0, \\ \dfrac{p^n \mathbf{Ei}(-px)}{n!(-1)^n} - \dfrac{e^{-px}}{x^n} \sum_{k=0}^{n-1} \dfrac{(-1)^k p^k x^k}{n(n-1)\ldots(n-k)}, & n > 0, \end{cases} \tag{40}$$

$\gamma(\cdot,\cdot)$ is the incomplete gamma function, and $\mathbf{Ei}(\cdot)$ is the exponential integral function.

Proof: Following (9), the exact secrecy outage probability of the CPA is given by

$$P(R_s) = \Pr\left(\gamma_E > \frac{\gamma_B+1}{2^{R_s}} - 1\right) = 1 - F_{\gamma_E}\left(\frac{\gamma_B+1}{2^{R_s}} - 1\right), \tag{41}$$

where $F_{\gamma_E}(\cdot)$ is the cdf of γ_E. In order to derive the expression of $P(R_s)$, we next derive $F_{\gamma_E}(\cdot)$. We can rewrite γ_E as $\gamma_E = \psi_n/\psi_d$, where

$$\psi_n = \alpha \mu_E |\mathbf{g}\mathbf{v}_I|^2, \tag{42}$$

$$\psi_d = (1-\alpha)\mu_E |\mathbf{g}\mathbf{V}_N \mathbf{w}_I|^2 + 1. \tag{43}$$

When $\alpha = 1$, $\gamma_E = \mu_E |\mathbf{g}\mathbf{v}_I|^2$, and thus the cdf of γ_E for $\alpha = 1$ is given by

$$F_{\gamma_E}(z) = 1 - e^{-\frac{z}{\mu_E \mathbf{v}_I^\dagger \mathbf{T} \mathbf{v}_I}}. \tag{44}$$

As such, $P(R_s)$ for $\alpha = 1$ is derived as given in (36). We note that $\mathbf{g}\mathbf{v}_I$ and $\mathbf{g}\mathbf{V}_N\mathbf{w}_I$ are both complex Gaussian random variables (for given deterministic $\mathbf{v}_I$, $\mathbf{V}_N$, and $\mathbf{w}_I$). As such, for $0 < \alpha < 1$ the joint pdf of ψ_n and ψ_d is given by [35]

$$f_{\psi_n,\psi_d}(x,y) = \frac{e^{-\frac{1}{2(1-\rho)}\left(\frac{x}{s_n^2} + \frac{y-1}{s_d^2}\right)}}{4s_n^2 s_d^2 (1-\rho)} I_0\left(\frac{\sqrt{\rho}}{1-\rho} \frac{\sqrt{x(y-1)}}{s_n s_d}\right). \tag{45}$$

Then, the pdf of γ_E for $0 < \alpha < 1$ is derived as

$$\begin{aligned} f_{\gamma_E}(z) &= \int_0^{\infty} y f_{\psi_n,\psi_d}(zy, y) dy \\ &\overset{e}{=} \frac{e^{\frac{1}{2(1-\rho)s_d^2}}}{4s_n^2 s_d^2 (1-\rho)} \sum_{k=0}^{\infty} \frac{\left(\frac{\sqrt{\rho}}{1-\rho}\frac{\sqrt{z}}{s_n s_d}\right)^{2k}}{2^{2k}(k!)^2} \\ &\quad \times \int_1^{\infty} y^{k+1}(y-1)^k e^{-\frac{1}{2(1-\rho)}\left(\frac{z}{s_n^2} + \frac{1}{s_d^2}\right)y} dy \\ &\overset{f}{=} \frac{e^{\frac{1}{2(1-\rho)s_d^2}}}{4s_n^2 s_d^2 (1-\rho)} \sum_{k=0}^{\infty} \frac{\left(\frac{\sqrt{\rho}}{1-\rho}\frac{\sqrt{z}}{s_n s_d}\right)^{2k}}{2^{2k}(k!)^2} \sum_{i=0}^{k} \binom{k}{i} (-1)^{k-i} \\ &\quad \times \int_1^{\infty} y^{k+i+1} e^{-\frac{1}{2(1-\rho)}\left(\frac{z}{s_n^2} + \frac{1}{s_d^2}\right)y} dy \\ &\overset{g}{=} \frac{e^{\frac{1}{2(1-\rho)s_d^2}}}{4s_n^2 s_d^2 (1-\rho)} \sum_{k=0}^{\infty} \frac{\left(\frac{\sqrt{\rho}}{1-\rho}\frac{\sqrt{z}}{s_n s_d}\right)^{2k}}{2^{2k}(k!)^2} \sum_{i=0}^{k} \frac{\binom{k}{i}}{(-1)^{i-k}} \end{aligned}$$

Authorized licensed use limited to: Centrale Supelec. Downloaded on October 22,2020 at 09:37:01 UTC from IEEE Xplore. Restrictions apply.

$$\times \sum_{j=0}^{k+i+1} \frac{(k+i+1)!}{j!} \frac{e^{-\frac{1}{2(1-\rho)}\left(\frac{z}{s_n^2}+\frac{1}{s_d^2}\right)}}{\left[\frac{1}{2(1-\rho)}\left(\frac{z}{s_n^2}+\frac{1}{s_d^2}\right)\right]^{k+i-j+2}}, \tag{46}$$

where $\overset{e}{=}$ is achieved by noting $\psi_d \in [1, \infty)$, $\overset{f}{=}$ is obtained by applying (35), and $\overset{g}{=}$ is gained by utilizing the following identify

$$\int_1^\infty x^n e^{-\tau x} dx = e^{-\tau} \sum_{j=0}^{n} \frac{n!}{j!} \tau^{-n-j+1}. \tag{47}$$

Following (46), the cdf of γ_E for $0 < \alpha < 1$ is derived as

$$\begin{aligned}
F_{\gamma_E}(z) &= \int_0^z f_{\gamma_E}(x) dx \\
&= \frac{e^{\frac{1}{2(1-\rho)s_d^2}}}{4s_n^2 s_d^2 (1-\rho)} \sum_{k=0}^{\infty} \frac{\rho^k (1-\rho)^{-k}}{2^k (k!)^2 s_d^{2k}} \sum_{i=0}^{k} \frac{\binom{k}{i}}{(-1)^{i-k}} \\
&\quad \times \sum_{j=0}^{k+i+1} \frac{(k+i+1)!}{j! \left[2(1-\rho)s_n^2\right]^{j-i-2}} \\
&\quad \times \int_0^z x^k \left(x + \frac{s_n^2}{s_d^2}\right)^{-(k+i-j+2)} e^{-\frac{1}{2(1-\rho)s_n^2}\left(x+\frac{s_n^2}{s_d^2}\right)} dx \\
&\overset{h}{=} \frac{e^{\frac{1}{2(1-\rho)s_d^2}}}{4s_n^2 s_d^2 (1-\rho)} \sum_{k=0}^{\infty} \frac{\rho^k (1-\rho)^{-k}}{2^k (k!)^2 s_d^{2k}} \sum_{i=0}^{k} \frac{\binom{k}{i}}{(-1)^{i-k}} \\
&\quad \times \sum_{j=0}^{k+i+1} \frac{(k+i+1)!}{j! \left[2(1-\rho)s_n^2\right]^{j-i-2}} \sum_{m=0}^{k} \binom{k}{m} \left(-\frac{s_n^2}{s_d^2}\right)^{k-m} \\
&\quad \times \int_{\frac{s_n^2}{s_d^2}}^{z+\frac{s_n^2}{s_d^2}} y^{m-k-i+j-2} e^{-\frac{1}{2(1-\rho)s_n^2} y} dy \\
&\overset{i}{=} \frac{e^{\frac{1}{2(1-\rho)s_d^2}}}{4s_n^2 s_d^2 (1-\rho)} \sum_{k=0}^{\infty} \frac{\rho^k (1-\rho)^{-k}}{2^k (k!)^2 s_d^{2k}} \sum_{i=0}^{k} \frac{\binom{k}{i}}{(-1)^{i-k}} \\
&\quad \times \sum_{j=0}^{k+i+1} \frac{(k+i+1)!}{j! \left[2(1-\rho)s_n^2\right]^{j-i-2}} \sum_{m=0}^{k} \binom{k}{m} \left(-\frac{s_n^2}{s_d^2}\right)^{k-m} \\
&\quad \times \left[\Gamma\left(k+i-j-m+1, \frac{1}{2(1-\rho)s_n^2}, z + \frac{s_n^2}{s_d^2}\right) \right. \\
&\quad \left. - \Gamma\left(k+i-j-m+1, \frac{1}{2(1-\rho)s_n^2}, \frac{s_n^2}{s_d^2}\right) \right],
\end{aligned} \tag{48}$$

where the incomplete gamma function $\gamma(\cdot, \cdot)$ is given by

$$\gamma(n, x) = \int_0^x e^{-t} t^{n-1} dt, \tag{49}$$

and the exponential integral function $\mathbf{Ei}(\cdot)$ is given by

$$\mathbf{Ei}(x) = -\int_{-x}^{\infty} \frac{e^{-t}}{t} dt = \int_{-\infty}^{x} \frac{e^t}{t} dt, \quad [x < 0]. \tag{50}$$

We note that $\overset{h}{=}$ in (48) is achieved by exchanging random variable (i.e., $y = x + s_n^2/s_d^2$) and $\overset{i}{=}$ is gained with the aid of the following two identities

$$\int_0^\tau x^n e^{-px} dx = p^{-n-1} \gamma(n+1, p\tau), \quad [n \geq 0], \tag{51}$$

$$\int_\tau^\infty \frac{e^{-px} dx}{x^{n+1}} = \frac{p^n \mathbf{Ei}(-p\tau)}{n!(-1)^{n+1}} - \frac{e^{-p\tau}}{\tau^n} \sum_{k=0}^{n-1} \frac{(-1)^k p^k \tau^k}{n(n-1)\ldots(n-k)}, \quad [n > 0]. \tag{52}$$

Then, the secrecy outage probability given in (37) is achieved by substituting (48) into (41). ■

Comparing (36) and (23), we know that the expression for the exact secrecy outage probability is much more complicated than that for the asymptotic secrecy outage probability. Similar to (23), the infinite series involved in (37) can be approximated by its finite truncation accurately due to the convergence of this infinite series. As per (36), we can draw the conclusion that when $\alpha = 1$ the exact secrecy outage probability averaged over all realizations of $\mathbf{h}$ increases as the correlation becomes more severe. This is due to the following two facts. Firstly, based on (6) the average value of γ_B does not vary with the correlation matrix $\mathbf{T}$. Secondly, $\mathbf{v}_I^\dagger \mathbf{T} \mathbf{v}_I^\dagger$ increases on average as the correlation becomes more severe due to the fact that if $\mathbf{h}_s^\dagger \mathbf{h}_s = \mathbf{I}_{N_t}$ we have $\mathbf{v}_I^\dagger \mathbf{T} \mathbf{v}_I^\dagger = \lambda_1$ and λ_1 increases as the correlation becomes more severe. The detrimental effect of correlation can be intuitively understood as follows. As correlation increases, the eavesdropper's channel becomes more aligned with the main channel and thus the SNR at Eve improves in the absence of AN (since $\alpha = 1$). As we will confirmed later in Section V, this conclusion also holds with AN, i.e., when α is optimized.

C. Optimization of the Power Allocation Parameter α

In order to guarantee the secrecy outage probability of a secure transmission is less than one, we have to guarantee $C_B > R_s$. As such, the lower bound on the power allocation parameter α is given by

$$\alpha_l = \frac{2^{R_s} - 1}{\mu_B \|\mathbf{h}\|^2}. \tag{53}$$

The optimal value of power allocation parameter α that minimizes the asymptotic secrecy outage probability given in (23) can be obtained through

$$\alpha_\infty^* = \text{argmin}_{\alpha_l < \alpha < 1} P_\infty(R_s), \tag{54}$$

and we denote $P_\infty^*(R_s)$ as the minimum asymptotic secrecy outage probability achieved by setting $\alpha = \alpha_\infty^*$ in the asymptotic secrecy outage probability $P_\infty(R_s)$.

The optimal value of power allocation parameter α that minimizes the exact secrecy outage probability given in (36) can be obtained through

$$\alpha^* = \text{argmin}_{\alpha_l < \alpha \leq 1} P(R_s), \tag{55}$$

and we denote $P^*(R_s)$ as the minimum exact secrecy outage probability achieved by setting $\alpha = \alpha^*$ in the exact secrecy outage probability $P(R_s)$.

Authorized licensed use limited to: Centrale Supelec. Downloaded on October 22,2020 at 09:37:01 UTC from IEEE Xplore. Restrictions apply.

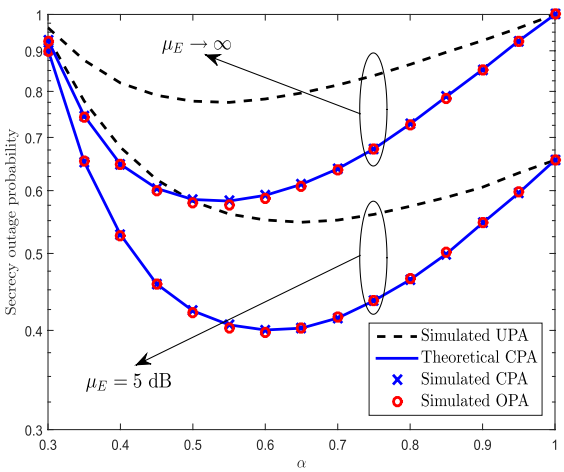


Fig. 2. Secrecy outage probabilities of the AN-aided secure transmission with OPA, CPA, and UPA versus different values of α for $N_t = 4$, $R_s = 2$, $\mu_B = 5$ dB, $\Lambda = \text{diag}[2.8, 0.7, 0.3, 0.2]$, and $\mathbf{h}_s = [0.1104 - 0.6619i, -0.6677 + 1.2432i, 0.7588 + 0.9201i, 1.0196 + 0.4098i]$.

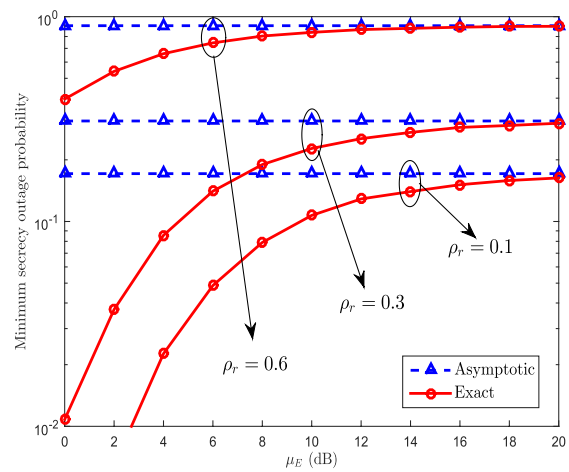


Fig. 3. Minimum secrecy outage probabilities achieved by the CPA versus different values of μ_E for $N_t = 3$, $L = 0.5$m (i.e., $\delta_{1,2} = \delta_{2,3} = 0.25$m and $\delta_{1,3} = 0.5$m), $R_s = 1$, $\mu_B = 10$ dB, and $\mathbf{h}_s = [0.0234 + 0.2351i, -0.0788 - 0.4619i, -0.5344 + 1.0582i]$.

V. Numerical Results

In this section, we first provide numerical comparison among the OPA, CPA, and UPA, based on which we observe that our proposed CPA is nearly optimal in terms of minimizing the secrecy outage probability even for finite N_t. We also examine the impact of transmitter-side correlation on the AN-aided secure transmission. Finally, based on our numerical studies we draw useful insights on the effect of system parameters (e.g., N_t) on the AN-aided secure transmission with different power allocations.

In Fig. 2 we plot the asymptotic (i.e., for $\mu_E \to \infty$) and exact (i.e., for $\mu_E = 5$ dB) secrecy outage probabilities of the AN-aided secure transmission with OPA, CPA, and UPA. In this figure we first observe that the theoretic secrecy outage probabilities achieved by the CPA precisely match its simulated secrecy outage probabilities. This confirms the correctness of the results presented in Theorem 2 and Theorem 3. We note that in the calculation of our theoretic secrecy outage probabilities (i.e., $P_\infty(R_s)$ and $P(R_s)$) we truncate the infinite series $\sum_{k=0}^{\infty}$ at $k = 15$. As such, the exact match between the theoretic and simulated secrecy outage probabilities as shown in this figure also indicates that the theoretic $P_\infty(R_s)$ and $P(R_s)$ can be approximated accurately by closed-form expressions (i.e., the involved infinite series can be accurately approximated by a finite series). Surprisingly, we also observe that our proposed CPA achieves almost identical secrecy outage probabilities as 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 smaller than that for the UPA (for $\mu_E \to \infty$ the gap is tiny, but when μ_E is finite, e.g., $\mu_E = 5$ dB, this gap is noticeable). This is mainly due to the fact that under the specific system settings the CPA utilizes AN more efficiently relative to the UPA (i.e., by using the same transmit power of AN, the CPA leads to more interference to Eve on average than the UPA). For $\mu_E \to \infty$, the optimal values of α are already low (considerable transmit power is allocated to AN) and thus the gap is relatively minor. For finite μ_E, the optimal values of α are relatively high and thus the gap becomes noticeable.

In Fig. 3 we plot the minimum asymptotic and exact secrecy outage probabilities of the CPA (i.e., $P^*_\infty(R_s)$ and $P^*(R_s)$) versus different values of μ_E. Although our analysis is valid for an arbitrary correlation matrix, in this figure and the following figures 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 this figure we first observe that $P^*(R_s)$ approaches $P^*_\infty(R_s)$ as μ_E increases and they are almost equal when $\mu_E \geq 20$ dB. This demonstrates that $P^*_\infty(R_s)$ can be a good approximation of $P^*(R_s)$ even for a finite μ_E (e.g., 20 dB). We also observe that for the adopted $\mathbf{h}_s$, both $P^*_\infty(R_s)$ and $P^*(R_s)$ increase as ρ_r increases, which means that the secrecy performance of the CPA decreases as the correlation of transmit antennas becomes more severe. This is mainly caused by the fact that as the correlation increases the null space of the main

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

Authorized licensed use limited to: Centrale Supelec. Downloaded on October 22,2020 at 09:37:01 UTC from IEEE Xplore. Restrictions apply.

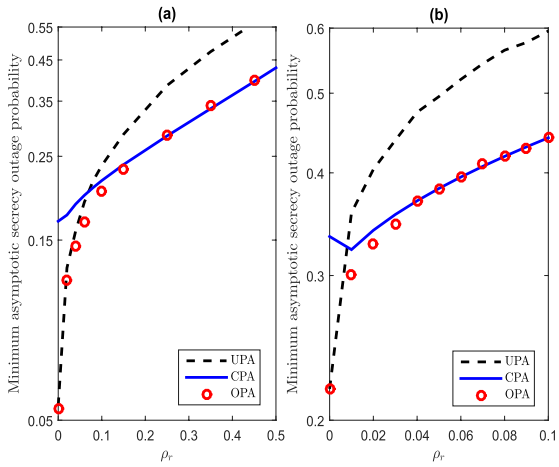


Fig. 4. Minimum asymptotic secrecy outage probabilities achieved by the OPA, CPA, and UPA versus different values of ρ_r for $N_t = 3$, $L = 0.5$m, $R_s = 1$, $\mu_B = 10$ dB, and (a) $\mathbf{h}_s = [-0.1470 + 0.1876i, -0.3905 + 1.0675i, -0.5091 - 0.8150i]$, (b) $\mathbf{h}_s = [-0.0845 + 0.5064i, 0.1612 + 0.0330i, -0.7529 + 0.0282i]$.

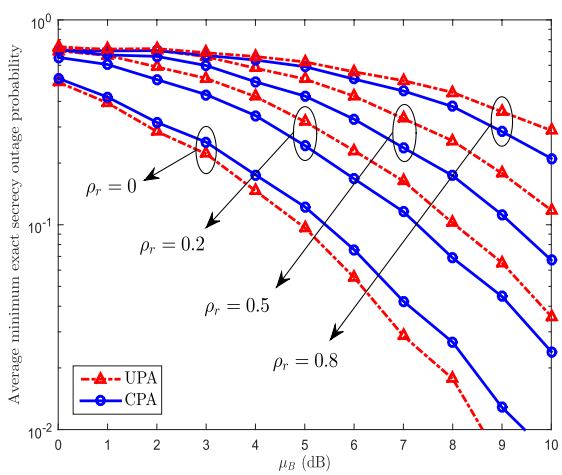


Fig. 5. Expected minimum exact secrecy outage probabilities achieved by the CPA and UPA versus different values of μ_B for $N_t = 3$, $L = 0.5$m, $R_s = 1$, $\mu_E = 5$ dB.

channel shrinks. As this null space shrinks, the probability that the eavesdropper's channel lies in the null space decreases. As such, transmitting AN in the null space leads to less interference to Eve on average as the correlation increases. We note that as the transmit antenna correlation increases the statistical CSI can better represent the instantaneous CSI [37]. As we assume the statistical information on the eavesdropper's channel is known, the increase in the correlation offers more information on the instantaneous eavesdropper's channel. This seems to be in contradiction with the observation that both $P^*_\infty(R_s)$ and $P^*(R_s)$ increase as ρ_r increases. The main reason is that the additional information offered by the increased correlation cannot counteract the decay in the null space of the main channel. We will further examine the impact of the transmitter-side correlation on the performance of the CPA in Fig. 4 and Fig. 5, in which we will see that the increased correlation may decrease the secrecy outage probability of the CPA.

In Fig. 4 we plot the minimum asymptotic secrecy outage probabilities achieved by the UPA, CPA, and OPA versus different values of ρ_r. In Fig. 4 (a) for the specific adopted $\mathbf{h}_s$ we observe that all the three minimum asymptotic 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 avoid the interference to Bob. In Fig. 4 (b) for the specific adopted $\mathbf{h}_s$ we observe that the minimum asymptotic secrecy outage probability achieved by the CPA first decreases and then increases as ρ_r increases. This initial 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 asymptotic secrecy outage probability achieved by 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. 4 (a) or Fig. 4 (b). In both Fig. 4 (a) and Fig. 4 (b) we also observe that the minimum asymptotic secrecy outage probability achieved by the CPA is lower than that achieved by 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 main channel realization in 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. 5 we plot the average minimum exact secrecy outage probabilities achieved by the CPA and UPA, which are obtained through averaging the minimum exact secrecy outage probabilities over $\mathbf{h}$ obtained by the CPA and UPA, respectively. As expected, in this figure we first observe that the average minimum exact secrecy outage probability achieved by the CPA is higher than that achieved by the UPA for the uncorrelated case (i.e., $\rho_r = 0$). This is due to the fact that for $\rho_r = 0$ the variance of the interference to Eve for the CPA is larger than that for the UPA while the mean of the interference to Eve for these two power allocations is the same. We also observe that the average minimum exact secrecy outage probability achieved by the CPA is lower than that achieved by the UPA for the most of the correlated cases (e.g., for $\rho_r \geq 0.2$). This can be explained by the fact that on average the CPA leads to a much larger average interference to Eve relative to the UPA. The aforementioned two observations again demonstrate that our proposed CPA can outperform the UPA in correlated fading channels. Finally, as expected we observe that both these two average minimum exact secrecy outage probabilities decrease as μ_B increases, which caused by the increasing quality of the main channel.

Continuing with Fig. 5, we plot the average minimum asymptotic secrecy outage probabilities achieved by the CPA and UPA versus different values of N_t for fixed array length L in Fig. 6 (Alice is equipped with uniform linear array with N_t elements and the array length is L). In this figure, we first observe that the average minimum asymptotic secrecy

Authorized licensed use limited to: Centrale Supelec. Downloaded on October 22,2020 at 09:37:01 UTC from IEEE Xplore. Restrictions apply.

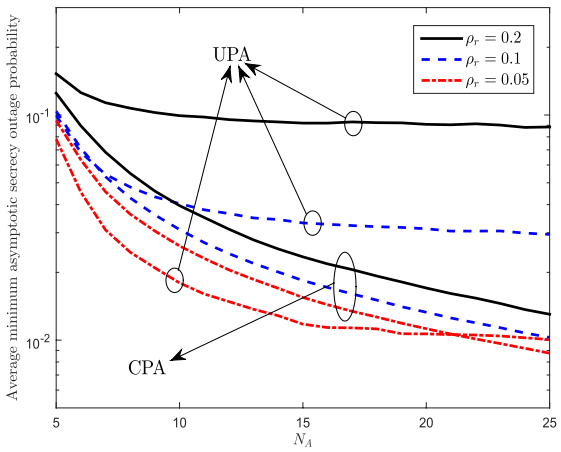


Fig. 6. Average minimum asymptotic secrecy outage probabilities achieved by the CPA and UPA versus different values of N_t for $L = 0.5$m, $R_s = 1$, $\mu_B = 10$ dB, and $\mu_E = 5$ dB.

outage probability achieved by the UPA 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 the average minimum asymptotic secrecy outage probability achieved by the CPA 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 the average minimum asymptotic secrecy outage probability achieved by the CPA becomes lower than that achieved by the UPA 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 these two average minimum asymptotic secrecy outage probabilities increases as N_t increases.

VI. 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 asymptotic and exact secrecy outage probabilities of the CPA for arbitrary N_t were derived in easy-to-evaluate expressions, based on which we optimized the power allocation between the information signal and AN in the AN-aided secure transmission with CPA. The conducted numerical results demonstrated that the CPA is nearly optimal and significantly outperforms the UPA even for finite N_t in the wiretap channel with transmitter-side correlation. Our study also revealed that the secrecy outage probability achieved by the UPA suffers from a saturation point as N_t increases while the secrecy outage probability obtained by our proposed CPA does not.

References

[1] M. Bloch and J. Barros, *Physical-Layer Security: From Inf. Theory to Security Engineering*. Cambridge, MA, USA: Cambridge Univ. Press, 2011.

[2] X. Zhou, L. Song, and Y. Zhang, *Physical Layer Security Wireless Communication*. Boca Raton, FL, USA: 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] S. Yan, X. Zhou, N. Yang, B. He, and T. D. Abhayapala, "Correlation-based power allocation for secure transmission with artificial noise," in *Proc. IEEE Globecom*, Dec. 2016, pp. 1–6.

[5] C. E. Shannon, "Communication theory of secrecy systems," *Bell Labs Tech. J.*, vol. 28, no. 4, pp. 656–715, Oct. 1949.

[6] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, 1975.

[7] A. Mukherjee and A. L. Swindlehurst, "Robust beamforming for security 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. Yan and R. Malaney, "Location-based beamforming for enhancing secrecy in rician wiretap channels," *IEEE Trans. Wireless Commun.*, vol. 15, no. 4, pp. 2780–2791, Apr. 2016.

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

[11] 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.

[12] Q. Li and W.-K. Ma, "Spatially selective artificial-noise aided transmit optimization for MISO multi-eves secrecy rate maximization," *IEEE Trans. Signal Process.*, vol. 61, no. 10, pp. 2704–2717, May 2013.

[13] 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.

[14] 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.

[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.*, vol. 65, no. 4, pp. 2170–2181, Apr. 2015.

[16] X. Zhang, M. R. McKay, X. Zhou, and R. W. Heath, "Artificial-noise-aided secure multi-antenna transmission with limited feedback," *IEEE Trans. Wireless Commun.*, vol. 14, no. 5, pp. 2742–2754, May 2015.

[17] 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.

[18] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas I: The misome wireltap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 7, pp. 3088–3104, Jul. 2010.

[19] J. Zhu, R. Schober, and V. K. Bhargava, "Secure transmission with multiple antennas I: The misome wiretap channel," *IEEE Trans. Wireless Commun.*, vol. 13, no. 9, pp. 4766–4781, Sep. 2014.

[20] D. Kapetanovic, G. Zheng, and F. Rusek, "Physical layer security for massive MIMO: An overview on passive eavesdropping and active attacks," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 21–27, Jun. 2015.

[21] J. Zhu, R. Schober, and V. K. Bhargava, "Linear precoding of data and artificial noise in secure massive MIMO systems," *IEEE Trans. Wireless Commun.*, vol. 15, no. 3, pp. 2245–2261, Mar. 2016.

[22] L. Hanlen and A. Grant, "Capacity analysis of correlated MIMO channels," *IEEE Trans. Inf. Theory*, vol. 58, no. 11, pp. 6773–6787, Nov. 2012.

[23] S. A. Jafar and A. Goldsmith, "Multiple antenna capacity in correlated rayleigh fading with channel covariance information," *IEEE Trans. Wireless Commun.*, vol. 4, no. 3, pp. 990–997, May 2005.

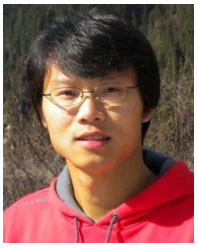
[24] N. Yang, H. A. Suraweera, I. B. Collings, and C. Yuen, "Physical layer security of TAS/MRC with antenna correlation," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 1, pp. 254–259, Jan. 2013.

[25] 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.

Authorized licensed use limited to: Centrale Supelec. Downloaded on October 22,2020 at 09:37:01 UTC from IEEE Xplore. Restrictions apply.

[26] J.-P. Kermoal, L. Schumacher, K. I. Pedersen, P. E. Mogensen, and F. Frederiksen, "A stochastic MIMO radio channel model with experimental validation," *IEEE J. Sel. Areas Commun.*, vol. 20, no. 6, pp. 1211–1226, Aug. 2002.
[27] A. Abdi and M. Kaveh, "A space-time correlation model for multi-element antenna systems in mobile fading environments," *IEEE J. Sel. Areas Commun.*, vol. 20, no. 3, pp. 550–560, Apr. 2002.
[28] G. J. Byers and F. Takawira, "Spatially and temporally correlated MIMO channels: Modeling and capacity analysis," *IEEE Trans. Veh. Technol.*, vol. 53, no. 3, pp. 634–643, May 2004.
[29] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, Jun. 2008.
[30] S. Yan, N. Yang, G. Geraci, R. Malaney, and J. Yuan, "Optimization of code rates in sisome wiretap channels," *IEEE Trans. Wireless Commun.*, vol. 14, no. 11, pp. 6377–6388, Nov. 2015.
[31] 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.
[32] D. Francois, V. Wertz, and M. Verleysen, "The concentration of fractional distances," *IEEE Trans. Knowl. Data Eng.*, vol. 19, no. 7, pp. 873–886, Jul. 2007.
[33] D. Voiculescu, "Limit laws for random matrices and free products," *Inventiones Mathematicae*, vol. 104, pp. 201–220, Dec. 1991.
[34] H. Gao, P. J. Smith, and M. V. Clark, "Theoretical reliability of mmse linear diversity combining in rayleigh-fading additive interference channels," *IEEE Trans. Commun.*, vol. 46, no. 5, pp. 666–672, May 1998.
[35] R. K. Mallik, "On multivariate rayleigh and exponential distributions," *IEEE Trans. Inf. Theory*, vol. 49, no. 6, pp. 1499–1515, Jun. 2003.
[36] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series and Products*, 7th ed. San Diego, CA, USA: Academic, 2007.
[37] J. Wang, S. Jin, X. Gao, K.-K. Wong, and E. Au, "Statistical eigenmode-based sdma for two-user downlink," *IEEE Trans. Signal Process.*, vol. 60, no. 10, pp. 5371–5383, Oct. 2012.

Shihao Yan (S'11–M'15) received the B.S. degree in communication engineering and the M.S. degree in communication and information systems from Shandong University, Jinan, China, in 2009 and 2012, respectively, and the Ph.D. degree in electrical engineering from the University of New South Wales, Sydney, NSW, Australia, in 2015. He was a visiting Ph.D. student with The University of South Australia, Adelaide, SA, Australia, in 2014. He is currently a Post-doctoral Research Fellow with the Research School of Engineering, Australian National University, Canberra, Australia. His current research interests are in the areas of wireless communications and statistical signal processing, including physical layer security, location verification, and localization algorithms.



Xiangyun Zhou (M'11) received the Ph.D. degree in telecommunications engineering from the Australian National University (ANU) in 2010. From 2010 to 2011, he was a Post-Doctoral Fellow with the University Graduate Center, University of Oslo, Norway. Since 2011, he has been a Senior Lecturer with ANU. His research interests are in the fields of communication theory and wireless networks. He is a recipient of the Best Paper Award at ICC'11. He currently serves on the editorial board of the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS and the IEEE COMMUNICATION LETTERS. He also served as a Guest Editor of the IEEE *Communication Magazine*'s feature topic on wireless physical layer security in 2015 and *EURASIP Journal on Wireless Communications and Networking*'s special issue on energy harvesting wireless communications in 2014. He has also served as the symposium/track/workshop co-chair for major IEEE conferences. He was the Chair of the ACT Chapter of the IEEE Communications Society and Signal Processing Society, from 2013 to 2014.

Nan Yang (S'09–M'11) received the Ph.D. degree in electronic engineering from the Beijing Institute of Technology in 2011. He was a Post-Doctoral Research Fellow with the University of New South Wales from 2012 to 2014 and a Post-doctoral Research Fellow with the Commonwealth Scientific and Industrial Research Organization from 2010 to 2012. He is currently a Future Engineering Research Leadership Fellow and a Lecturer with the Research School of Engineering, Australian National University. His research interests include heterogeneous networks, massive multi-antenna systems, millimeter wave communications, cyber-physical security, and molecular communications. He is currently serving on the editorial board of the IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY and the *Transactions on Emerging Telecommunications Technologies*. He received the Exemplary Reviewer Award of the IEEE TRANSACTIONS ON COMMUNICATIONS and the Top Reviewer Award from the IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY in 2015, the IEEE ComSoc Asia-Pacific Outstanding Young Researcher Award and the Exemplary Reviewer Award of the IEEE WIRELESS COMMUNICATIONS LETTERS in 2014, the Exemplary Reviewer Award of the IEEE COMMUNICATIONS LETTERS in 2013 and 2012, and the Best Paper Award at the IEEE 77th Vehicular Technology Conference in 2013.

Biao He (M'16) received the B.E. degree (Hons.) from Australian National University (ANU) and the Beijing Institute of Technology in 2012 and the Ph.D. degree from ANU in 2016. He is currently a Post-Doctoral Fellow with the Department of Electronic and Computer Engineering, The Hong Kong University of Science and Technology. His research interests include physical layer security and wireless communications.

Thushara D. Abhayapala (M'00–SM'08) received the B.E. degree (Hons.) in engineering and the Ph.D. degree in telecommunications engineering from Australian National University (ANU), Canberra, in 1994 and 1999, respectively. He is currently the Deputy Dean of the College of Engineering and Computer Science, ANU. He was the Director of the Research School of Engineering with ANU from 2010 to 2014 and the Leader of the Wireless Signal Processing Program with the National ICT Australia from 2005 to 2007. He has supervised over 30 Ph.D. students and co-authored over 200 peer reviewed papers. His research interests are in the areas of spatial audio and acoustic signal processing, multi-channel signal processing, and spatial aspects of wireless communications. He is a member of the Audio and Acoustic Signal Processing Technical Committee (from 2011 to 2016) of the IEEE Signal Processing Society. He is a fellow of the Engineers Australia. He is an Associate Editor of the IEEE/ACM TRANSACTIONS ON AUDIO, SPEECH, AND LANGUAGE PROCESSING.

Authorized licensed use limited to: Centrale Supelec. Downloaded on October 22,2020 at 09:37:01 UTC from IEEE Xplore. Restrictions apply.