Artificial Noise Assisted Secure Massive MIMO Transmission Exploiting Statistical CSI

Wenjin Wang, *Member, IEEE*, Xu Chen, Li You, *Member, IEEE*, Xinping Yi, *Member, IEEE*, and Xiqi Gao, *Fellow, IEEE*

***Abstract*—For the single-cell massive multiple-input multiple-output (MIMO) downlink transmission, we investigate an artificial noise (AN) assisted secure transmission strategy where the base station has only access to statistical channel state information (CSI) of the legitimate user terminals and the eavesdropper. By maximizing a lower bound of the ergodic secrecy sum rate, we figure out the eigenvectors of the optimal secrecy signal and AN transmit covariance matrices in the closed-form. Notably, such a solution reveals that it is more favorable to transmit both the secrecy signals and the AN in the beam domain, by which we translate the original problem into a simpler power allocation problem in the beam domain. Building on the approaches of sequential optimization and the deterministic equivalent, we further propose an iterative algorithm for power allocation with guaranteed convergence to a local optimum. Numerical results show the superior performance of the proposed approach compared with the traditional one without AN.**

***Index Terms*—Massive MIMO, secure transmission, artificial noise, beam domain, statistic CSI.**

I. Introduction

Wireless transmission is facing a critical threat of leaking information to potential eavesdroppers owing to the broadcast propagation nature of wireless medium. Utilizing the inherent wireless channel propagation properties to enhance data confidentiality, physical layer security has received extensive attention [1]. Massive multiple-input multiple-output (MIMO) is deemed a promising technology to improve physical layer security thanks to the ability of generating sharp beams at the base station (BS) towards targeted user terminals (UTs) [2], [3]. As the number of BS antennas increases, spatially separated channels become more and more orthogonal, for which UTs' transmission with sharp beams orthogonal to the eavesdropper's channel could protect information from eavesdropping. Albeit promising from a theoretical viewpoint, this approach requires accurate knowledge of instantaneous channel state information at the transmitter (CSIT), which is rather challenging in massive MIMO especially when channel reciprocity does not hold. As such, utilizing the slowly-changing statistical CSIT for secure transmission seems more appealing. However, the orthogonality is not maintained for statistical CSI any more, so auxiliary approaches are required to guarantee security.

To this end, we consider downlink transmission in massive MIMO provided that only the statistical CSI is available at the BS. To ensure secure communication, we adopt the artificial noise (AN) based physical-layer security approach to prevent the possible eavesdropping [4]. Introducing a lower bound of the ergodic secrecy sum rate for the sake of tractability, we could discover that it is favorable to perform AN assisted secure transmission in the beam domain. Guided by this insight, we translate the challenging ergodic rate maximization problem with respect to transmit covariance matrices to a simpler power allocation problem in the beam domain, and propose a concave-convex procedure (CCCP) based iterative power allocation algorithm with guaranteed convergence to a stationary point. To further reduce the computational complexity, we take the advantage of the deterministic equivalents (DEs) calculation of the objectives in each iteration. Numerical results demonstrate the performance gain of our proposed AN assisted approach in contrast to the traditional one without AN injection.

II. System Model

Consider a single-cell massive MIMO secure downlink transmission system including one M-antenna BS, K legitimate UTs, with N_k receive antennas at UT k, and one eavesdropper with N_{e} receive antennas. Denote by $\mathbf{x}_k \in \mathbb{C}^{M\times 1}$ the transmitted signal from the BS to the kth UT with mean $\mathbf{0}$ and covariance $\mathbf{Q}_k$, and by $\mathbf{x}_{\mathrm{AN}} \in \mathbb{C}^{M\times 1}$ the AN vector which is independent of $\mathbf{x}_k$ $(\forall k)$ with mean $\mathbf{0}$ and covariance $\mathbf{Q}_{\mathrm{AN}}$, respectively. Then the received signal at UT k is

$$\mathbf{y}_k = \mathbf{H}_k\mathbf{x}_k + \sum\nolimits_{i\neq k}\mathbf{H}_k\mathbf{x}_i + \mathbf{H}_k\mathbf{x}_{\mathrm{AN}} + \mathbf{n}_k \in \mathbb{C}^{N_k\times 1}, \quad (1)$$

and the received signals at the eavesdropper is

$$\mathbf{y}_{\mathrm{e}} = \sum\nolimits_{i=1}^{K}\mathbf{H}_{\mathrm{e}}\mathbf{x}_i + \mathbf{H}_{\mathrm{e}}\mathbf{x}_{\mathrm{AN}} + \mathbf{n}_{\mathrm{e}} \in \mathbb{C}^{N_{\mathrm{e}}\times 1}, \quad (2)$$

where $\mathbf{n}_k$ and $\mathbf{n}_{\mathrm{e}}$ are the additive white Gaussian noise with covariance $\mathbf{I}_{N_k}$ and $\mathbf{I}_{N_{\mathrm{e}}}$, respectively.

With the number of BS antennas M tending to infinity, the downlink channel matrices $\mathbf{H}_k$ in (1) and $\mathbf{H}_{\mathrm{e}}$ in (2) can be well approximated as [5], [6]

$$\mathbf{H}_k \overset{M\to\infty}{=} \mathbf{U}_k\mathbf{G}_k\mathbf{V}^H,\ \mathbf{H}_{\mathrm{e}} \overset{M\to\infty}{=} \mathbf{U}_{\mathrm{e}}\mathbf{G}_{\mathrm{e}}\mathbf{V}^H, \quad (3)$$

where $\mathbf{U}_k \in \mathbb{C}^{N_k\times N_k}$, $\mathbf{U}_{\mathrm{e}} \in \mathbb{C}^{N_{\mathrm{e}}\times N_{\mathrm{e}}}$, and $\mathbf{V} \in \mathbb{C}^{M\times M}$ are all deterministic unitary matrices. We point out that $\mathbf{V}$ is

Manuscript received August 9, 2019; revised September 15, 2019; accepted October 11, 2019. Date of publication XXXX, 2019; date of current version XXXX, 2019. This work was supported in part by the National Key R&D Program of China under Grant 2018YFB1801103, the National Natural Science Foundation of China under Grants 61761136016, 61801114, and 61631018, the Natural Science Foundation of Jiangsu Province under Grant BK20170688, and the Fundamental Research Funds for the Central Universities. The associate editor coordinating the review of this manuscript and approving it for publication was Prof. Yansha Deng. *(Corresponding author: Wenjin Wang.)*

W. Wang, X. Chen, L. You, and X. Q. Gao are with the National Mobile Communications Research Laboratory, Southeast University, Nanjing 210096, China, and also with the Purple Mountain Laboratories, Nanjing 211100, China (e-mail: wangwj@seu.edu.cn; chen_xu@seu.edu.cn; liyou@seu.edu.cn; xqgao@seu.edu.cn).

X. Yi is with the Department of Electrical Engineering and Electronics, University of Liverpool, Liverpool L69 3BX, U.K. (e-mail: xinping.yi@liverpool.ac.uk).

Digital Object Identifier

independent of the locations of UTs and is only related to the BS antenna array geometry [5], [7]. For instance, given the uniform linear array (ULA) with antenna spacing of half-wavelength, it has been shown in [5] that the discrete Fourier transform matrix is a good approximation of $\mathbf{V}$. Note that we usually refer to $\mathbf{G}_k$ and $\mathbf{G}_{\mathrm{e}}$ in (3) as the beam domain channel matrices with independently distributed elements [5]. The statistical CSI of $\mathbf{G}_k$ and $\mathbf{G}_{\mathrm{e}}$ can be modeled as [8]

$$\mathbf{\Omega}_k = \mathbb{E}\left\{\mathbf{G}_k \odot \mathbf{G}_k^*\right\},\ \mathbf{\Omega}_{\mathrm{e}} = \mathbb{E}\left\{\mathbf{G}_{\mathrm{e}} \odot \mathbf{G}_{\mathrm{e}}^*\right\}, \quad (4)$$

respectively, where $\odot$ denotes the Hadamard product.

It is assumed that only legitimate UT and the eavesdropper's statistical CSI, i.e., $\mathbf{\Omega}_k$ and $\mathbf{\Omega}_{\mathrm{e}}$ in (4), is known at the BS, and the legitimate UTs and the eavesdropper have access to instantaneous CSI of their own channels with properly designed pilot signals [9], [10]. The interference-plus-noise item $\sum_{i\neq k}\mathbf{H}_k\mathbf{x}_i + \mathbf{n}_k$ in (1) is treated as the Gaussian noise with covariance $\mathbf{K}_k = \mathbf{I}_{N_k} + \sum_{i\neq k}\mathbb{E}\left\{\mathbf{H}_k\mathbf{Q}_i\mathbf{H}_k^H\right\} \in \mathbb{C}^{N_k\times N_k}$ at each legitimate UT k. By assuming the worst-case scenario that the eavesdropper could be able to cancel the interfering signals of all UTs other than the one of interest [11], we have the ergodic secrecy rate of the kth UT

$$\mathcal{R}_k^{\mathrm{sec}} = \left[\mathcal{R}_k - \mathcal{R}_{\mathrm{e},k}\right]^+, \quad (5)$$

where $\mathcal{R}_k$ is the ergodic rate of the kth UT, i.e.,

$$\begin{aligned}\mathcal{R}_k =& \mathbb{E}\left\{\mathrm{logdet}\left(\overline{\mathbf{K}}_k + \mathbf{G}_k\mathbf{V}^H\left(\mathbf{Q}_k + \mathbf{Q}_{\mathrm{AN}}\right)\mathbf{V}\mathbf{G}_k^H\right)\right\}\\ &- \mathbb{E}\left\{\mathrm{logdet}\left(\overline{\mathbf{K}}_k + \mathbf{G}_k\mathbf{V}^H\mathbf{Q}_{\mathrm{AN}}\mathbf{V}\mathbf{G}_k^H\right)\right\}, \quad (6)\end{aligned}$$

and $\mathcal{R}_{\mathrm{e},k}$ represents the ergodic rate of the eavesdropper, which attempts to eavesdrop the signal for the kth UT, i.e.,

$$\begin{aligned}\mathcal{R}_{\mathrm{e},k} =& \mathbb{E}\left\{\mathrm{logdet}\left(\mathbf{I}_{N_{\mathrm{e}}} + \mathbf{G}_{\mathrm{e}}\mathbf{V}^H\left(\mathbf{Q}_k + \mathbf{Q}_{\mathrm{AN}}\right)\mathbf{V}\mathbf{G}_{\mathrm{e}}^H\right)\right\}\\ &- \mathbb{E}\left\{\mathrm{logdet}\left(\mathbf{I}_{N_{\mathrm{e}}} + \mathbf{G}_{\mathrm{e}}\mathbf{V}^H\mathbf{Q}_{\mathrm{AN}}\mathbf{V}\mathbf{G}_{\mathrm{e}}^H\right)\right\}, \quad (7)\end{aligned}$$

and $\overline{\mathbf{K}}_k$ in (6) can be expressed as

$$\overline{\mathbf{K}}_k = \mathbf{I}_{N_k} + \sum_{i\neq k}^{K}\mathbb{E}\left\{\mathbf{G}_k\mathbf{V}^H\mathbf{Q}_i\mathbf{V}\mathbf{G}_k^H\right\} \in \mathbb{C}^{N_k\times N_k}. \quad (8)$$

We consider the AN assisted secure transmission strategy, with the objective to design the transmit covariance matrices $\mathbf{Q} \triangleq \{\mathbf{Q}_{\mathrm{AN}}, \mathbf{Q}_1, \cdots, \mathbf{Q}_K\}$ maximizing (5), as follows

$$\begin{aligned}\underset{\mathbf{Q}}{\arg\max}\quad & \mathcal{R}^{\mathrm{sec}} \triangleq \sum_{k=1}^{K}\left[\mathcal{R}_k - \mathcal{R}_{\mathrm{e},k}\right]\\ \text{subject to}\quad & \sum_{k=1}^{K}\mathrm{tr}\left(\mathbf{Q}_k\right) + \mathrm{tr}\left(\mathbf{Q}_{\mathrm{AN}}\right) \leq P_{\max}\\ & \mathbf{Q}_{\mathrm{AN}} \succeq \mathbf{0},\ \mathbf{Q}_k \succeq \mathbf{0},\ \forall k, \quad (9)\end{aligned}$$

where $P_{\max}$ denotes the BS power budget. Note that in the objective of (9) we omit the operator $[\cdot]^+$ without loss of optimality as $\mathbf{Q}_k = \mathbf{0}$ leads to a zero secrecy rate of UT k for arbitrary k, and any feasible point with the secrecy rate being negative will not be the optimal solution.

Due to the nonconcavity of the ergodic secrecy sum rate $\mathcal{R}^{\mathrm{sec}}$ in (9) over $\mathbf{Q}$ and the involved expectation operation, it is in general challenging to identify the optimal solution to the transmit covariance matrices. For the sake of tractability, a lower bound on the ergodic secrecy sum rate is firstly introduced as

$$\mathcal{R}^{\mathrm{sec,lb}} \triangleq \sum_{k=1}^{K}\left[\mathcal{R}_k^{\mathrm{lb}} - \mathcal{R}_{\mathrm{e},k}^{\mathrm{ub}}\right], \quad (10)$$

where $\mathcal{R}_k^{\mathrm{lb}}$ is a lower bound of $\mathcal{R}_k$, and $\mathcal{R}_{\mathrm{e},k}^{\mathrm{ub}}$ is an upper bound of $\mathcal{R}_{\mathrm{e},k}$. Both of them can be obtained from Jensen's inequality as

$$\begin{aligned}\mathcal{R}_k^{\mathrm{lb}} =& \mathbb{E}\left\{\mathrm{logdet}\left(\overline{\mathbf{K}}_k + \mathbf{G}_k\mathbf{V}^H\left(\mathbf{Q}_k + \mathbf{Q}_{\mathrm{AN}}\right)\mathbf{V}\mathbf{G}_k^H\right)\right\}\\ &- \mathrm{logdet}\left(\overline{\mathbf{K}}_k + \mathbb{E}\left\{\mathbf{G}_k\mathbf{V}^H\mathbf{Q}_{\mathrm{AN}}\mathbf{V}\mathbf{G}_k^H\right\}\right), \quad (11)\\ \mathcal{R}_{\mathrm{e},k}^{\mathrm{ub}} =& \mathrm{logdet}\left(\mathbf{I}_{N_{\mathrm{e}}} + \mathbb{E}\left\{\mathbf{G}_{\mathrm{e}}\mathbf{V}^H\left(\mathbf{Q}_k + \mathbf{Q}_{\mathrm{AN}}\right)\mathbf{V}\mathbf{G}_{\mathrm{e}}^H\right\}\right)\\ &- \mathbb{E}\left\{\mathrm{logdet}\left(\mathbf{I}_{N_{\mathrm{e}}} + \mathbf{G}_{\mathrm{e}}\mathbf{V}^H\mathbf{Q}_{\mathrm{AN}}\mathbf{V}\mathbf{G}_{\mathrm{e}}^H\right)\right\}, \quad (12)\end{aligned}$$

respectively. We will demonstrate the tightness of the lower bound presented in (10) in Section IV. With the lower bound in (10) being the objective function, the problem in (9) can be reformulated as

$$\begin{aligned}\underset{\mathbf{Q}}{\arg\max}\quad & \mathcal{R}^{\mathrm{sec,lb}}\\ \text{subject to}\quad & \text{constraints in (9)}. \quad (13)\end{aligned}$$

III. AN Assisted Secure Transmission Design

To figure out the optimal AN assisted secure transmission design in (13), we first decompose the transmit covariance matrices into $\mathbf{Q}_k = \mathbf{\Psi}_k\mathbf{\Lambda}_k\mathbf{\Psi}_k^H, \forall k$ and $\mathbf{Q}_{\mathrm{AN}} = \mathbf{\Psi}_{\mathrm{AN}}\mathbf{\Lambda}_{\mathrm{AN}}\mathbf{\Psi}_{\mathrm{AN}}^H$ by eigenvalue decomposition, with $\mathbf{\Psi}_k$ and $\mathbf{\Psi}_{\mathrm{AN}}$ representing the subspaces in which the transmit secrecy signals and the AN fall, respectively. Note that the elements of diagonal matrices $\mathbf{\Lambda}_k$ and $\mathbf{\Lambda}_{\mathrm{AN}}$ represent the power assigned to each dimension/direction of the subspace for the transmit secrecy signals and the AN, respectively. By doing so, we identify the eigenmatrices (i.e., the matrices consist of all eigenvectors) of the transmit covariance of the secrecy signals and the AN.

Proposition 1: The corresponding eigenmatrices of the optimal transmit covariance $\mathbf{Q}_k$ for all k and $\mathbf{Q}_{\mathrm{AN}}$ to problem (13) are all given by the eigenmatrix $\mathbf{V}$ of the transmit correlation matrices, i.e., $\mathbf{\Psi}_k = \mathbf{V}\,(\forall k)$ and $\mathbf{\Psi}_{\mathrm{AN}} = \mathbf{V}$.

Proof: The nth diagonal element of $\mathbb{E}\left\{\mathbf{G}_k\mathbf{X}\mathbf{G}_k^H\right\}$ can be calculated by $\left[\mathbb{E}\left\{\mathbf{G}_k\mathbf{X}\mathbf{G}_k^H\right\}\right]_{n,n} = \sum_{m=1}^{M}\left[\mathbf{\Omega}_k\right]_{n,m}\left[\mathbf{X}\right]_{m,m}$ according to (4), and then the off-diagonal entries of $\mathbf{X}$ will not affect the value of $\mathbb{E}\left\{\mathbf{G}_k\mathbf{X}\mathbf{G}_k^H\right\}$. Thus, the values of $\overline{\mathbf{K}}_k(\forall k)$ in (8) are not related to the off-diagonal elements of $\mathbf{V}^H\mathbf{Q}_{k'}\mathbf{V}(\forall k')$. Then, using a proof approach similar to that in [12], we can show that $\mathbf{V}^H\mathbf{Q}_k\mathbf{V}(\forall k)$ and $\mathbf{V}^H\mathbf{Q}_{\mathrm{AN}}\mathbf{V}$ should be all diagonal to maximize $\mathcal{R}^{\mathrm{sec,lb}}$ in (10). Moreover, the transmit power $\sum_{k=1}^{K}\mathrm{tr}\left(\mathbf{Q}_k\right) + \mathrm{tr}\left(\mathbf{Q}_{\mathrm{AN}}\right)$ is only related to the diagonal entries of $\mathbf{V}^H\mathbf{Q}_k\mathbf{V}\,(\forall k)$ and $\mathbf{V}^H\mathbf{Q}_{\mathrm{AN}}\mathbf{V}$. Thus, in order to maximize the objective of problem (13) under the given constraints, we can conclude that $\mathbf{V}^H\mathbf{Q}_k\mathbf{V}\,(\forall k)$ and $\mathbf{V}^H\mathbf{Q}_{\mathrm{AN}}\mathbf{V}$ should be all diagonal. ■

Proposition 1 reveals that, to maximize the objective in (13), the transmit directions of both the secrecy signals and the AN should be aligned with the eigenvectors of the transmit correlation matrices of the downlink channels. The result in Proposition 1 indicates that the transmission of all secrecy signals and the AN in secure massive MIMO favors the beam domain. By Proposition 1, we can therefore simplify and replace the original optimization problem in (13) by optimizing the eigenvalues of the transmit covariance matrices of the secrecy signals and the AN, i.e.,

$$\begin{aligned} \underset{\boldsymbol{\Lambda} \triangleq \{\boldsymbol{\Lambda}_{\mathrm{AN}}, \boldsymbol{\Lambda}_1, \cdots, \boldsymbol{\Lambda}_K\}}{\arg\max} \quad & \mathcal{R}^{\mathrm{sec,lb}}(\boldsymbol{\Lambda}) = \sum_{k=1}^{K} \left(f_k(\boldsymbol{\Lambda}) - g_k(\boldsymbol{\Lambda})\right) \\ \text{subject to} \quad & \sum_{k=1}^{K} \mathrm{tr}(\boldsymbol{\Lambda}_k) + \mathrm{tr}(\boldsymbol{\Lambda}_{\mathrm{AN}}) \le P_{\max} \\ & \boldsymbol{\Lambda}_{\mathrm{AN}} \succeq \mathbf{0}, \ \boldsymbol{\Lambda}_k \succeq \mathbf{0}, \ \forall k, \end{aligned} \tag{14}$$

where

$$\begin{aligned} f_k(\boldsymbol{\Lambda}) \triangleq\, & \mathbb{E}\left\{\mathrm{logdet}\left(\overline{\mathbf{K}}_k(\boldsymbol{\Lambda}) + \mathbf{G}_k(\boldsymbol{\Lambda}_k + \boldsymbol{\Lambda}_{\mathrm{AN}})\mathbf{G}_k^H\right)\right\} \\ & + \mathbb{E}\left\{\mathrm{logdet}\left(\mathbf{I}_{N_\mathrm{e}} + \mathbf{G}_\mathrm{e}\boldsymbol{\Lambda}_{\mathrm{AN}}\mathbf{G}_\mathrm{e}^H\right)\right\}, \end{aligned} \tag{15}$$

$$\begin{aligned} g_k(\boldsymbol{\Lambda}) \triangleq\, & \mathrm{logdet}\left(\overline{\mathbf{K}}_k(\boldsymbol{\Lambda}) + \mathbb{E}\left\{\mathbf{G}_k\boldsymbol{\Lambda}_{\mathrm{AN}}\mathbf{G}_k^H\right\}\right) \\ & + \mathrm{logdet}\left(\mathbf{I}_{N_\mathrm{e}} + \mathbb{E}\left\{\mathbf{G}_\mathrm{e}(\boldsymbol{\Lambda}_k + \boldsymbol{\Lambda}_{\mathrm{AN}})\mathbf{G}_\mathrm{e}^H\right\}\right). \end{aligned} \tag{16}$$

Noting that $f_k(\boldsymbol{\Lambda})$ and $g_k(\boldsymbol{\Lambda})$ in (14) for all k are all concave over $\boldsymbol{\Lambda}$, we then adopt the iterative CCCP approach [13] to address this problem. To reduce the computational complexity of the expectation operation, we calculate the DEs of $f_k(\boldsymbol{\Lambda})$ for all k in each iteration instead of averaging over the channel realizations [14]. Specifically, the DE of $f_k(\boldsymbol{\Lambda})$ is given by (17) at the top of the next page where

$$\begin{aligned} & \boldsymbol{\Gamma}_k = \boldsymbol{\Pi}_k\left(\widetilde{\boldsymbol{\Phi}}_k^{-1}\overline{\mathbf{K}}_k^{-1}\right), \ \boldsymbol{\Gamma}_\mathrm{e} = \boldsymbol{\Pi}_\mathrm{e}\left(\widetilde{\boldsymbol{\Phi}}_\mathrm{e}^{-1}\right), \\ & \widetilde{\boldsymbol{\Gamma}}_k = \boldsymbol{\Xi}_k\left(\boldsymbol{\Phi}_k^{-1}(\boldsymbol{\Lambda}_k + \boldsymbol{\Lambda}_{\mathrm{AN}})\right), \ \widetilde{\boldsymbol{\Gamma}}_\mathrm{e} = \boldsymbol{\Xi}_\mathrm{e}\left(\boldsymbol{\Phi}_\mathrm{e}^{-1}\boldsymbol{\Lambda}_{\mathrm{AN}}\right), \\ & \widetilde{\boldsymbol{\Phi}}_k = \mathbf{I} + \boldsymbol{\Xi}_k\left(\boldsymbol{\Phi}_k^{-1}(\boldsymbol{\Lambda}_k + \boldsymbol{\Lambda}_{\mathrm{AN}})\right)\overline{\mathbf{K}}_k^{-1}, \\ & \widetilde{\boldsymbol{\Phi}}_\mathrm{e} = \mathbf{I} + \boldsymbol{\Xi}_\mathrm{e}\left(\boldsymbol{\Phi}_\mathrm{e}^{-1}\boldsymbol{\Lambda}_{\mathrm{AN}}\right), \\ & \boldsymbol{\Phi}_k = \mathbf{I} + \boldsymbol{\Pi}_k(\boldsymbol{\Phi}_k^{-1}\overline{\mathbf{K}}_k^{-1})(\boldsymbol{\Lambda}_k + \boldsymbol{\Lambda}_{\mathrm{AN}}), \\ & \boldsymbol{\Phi}_\mathrm{e} = \mathbf{I} + \boldsymbol{\Pi}_\mathrm{e}\left(\boldsymbol{\Phi}_\mathrm{e}^{-1}\right)\boldsymbol{\Lambda}_{\mathrm{AN}}, \\ & \boldsymbol{\Pi}_k(\mathbf{X}) \triangleq \mathbb{E}\left\{\mathbf{G}_k^H\mathbf{X}\mathbf{G}_k\right\}, \ \boldsymbol{\Pi}_\mathrm{e}(\mathbf{X}) \triangleq \mathbb{E}\left\{\mathbf{G}_\mathrm{e}^H\mathbf{X}\mathbf{G}_\mathrm{e}\right\}, \\ & \boldsymbol{\Xi}_k(\mathbf{X}) \triangleq \mathbb{E}\left\{\mathbf{G}_k\mathbf{X}\mathbf{G}_k^H\right\}, \ \boldsymbol{\Xi}_\mathrm{e}(\mathbf{X}) \triangleq \mathbb{E}\left\{\mathbf{G}_\mathrm{e}\mathbf{X}\mathbf{G}_\mathrm{e}^H\right\}. \end{aligned} \tag{18}$$

Via utilizing CCCP and replacing $f_k(\boldsymbol{\Lambda})$ with its DE $\overline{f}_k(\boldsymbol{\Lambda})$, the problem in (14) is converted to a sequence of convex sub-problems as (19) on the top of the next page, where $\boldsymbol{\Lambda}^{(\ell)} \triangleq \{\boldsymbol{\Lambda}_{\mathrm{AN}}^{(\ell)}, \boldsymbol{\Lambda}_1^{(\ell)}, \ldots, \boldsymbol{\Lambda}_K^{(\ell)}\}$, the gradients of $g_k(\boldsymbol{\Lambda})$ over $\boldsymbol{\Lambda}_a\,(\forall a)$ and $\boldsymbol{\Lambda}_{\mathrm{AN}}$ are all diagonal matrices. The mth entries of the gradient matrices are given by (20) and (21), respectively, on the top of the next page, and $\boldsymbol{\Lambda}_{\setminus k}^{(\ell)} = \sum_{i \neq k}^{K} \boldsymbol{\Lambda}_i^{(\ell)}$. Our proposed AN assisted secure transmission design with statistical CSI is formally presented in Algorithm 1.

Each sub-problem generated by CCCP is a concave problem. From [13], the solution sequence $\left\{\boldsymbol{\Lambda}^{(\ell)}\right\}_{\ell=0}^{\infty}$ converges monotonically to a stationary point of the original problem in (14). In addition, the DE expression $\overline{f}_k(\boldsymbol{\Lambda})$ is still concave over $\boldsymbol{\Lambda}$, and is a quite good approximation of $f_k(\boldsymbol{\Lambda})$. Then, each sub-problem in (19) is still concave, and the solution sequence still converges to the stationary point.

IV. Numerical Results

Numerical analysis is presented to evaluate the performance of our proposed AN assisted approach. The QuaDRiGa channel model with a suburban macro cell scenario [15] is adopted throughout the simulations. The signal-to-noise-ratio (SNR) is defined as $P_{\max}$. In the simulations, $K = 8$ legitimate UTs, each with $N_k = 4$ antennas, and one eavesdropper with $N_\mathrm{e} = 4$ antennas are randomly distributed in the cell sector. The BS is equipped with $M = 128$ antennas. The antenna array topology ULA is adopted for the BS, legitimate UTs and the eavesdropper, with half-wavelength antenna spacing.

The convergence behavior of the proposed iterative Algorithm 1 at different SNRs is firstly presented in Fig. 1. We can observe that the proposed AN assisted algorithm has quick convergence performance in a wide range of SNRs. Furthermore, the algorithm converges more slowly when SNR goes higher, which indicates that in the high SNR region, the proposed algorithm could be able to provide performance gains for secure transmission.

Fig. 2 compares the secrecy transmission rate performance of the AN assisted approach with that of the conventional approach where AN is not injected [7]. We can observe that the exploitation of AN yields performance gains over the

Algorithm 1 Iterative Power Allocation Algorithm for AN Assisted Secure Massive MIMO

Input: Statistical CSI $\boldsymbol{\Omega}_k\,(\forall k)$ and $\boldsymbol{\Omega}_\mathrm{e}$, an initial power allocation matrix $\boldsymbol{\Lambda}^{(0)}$, the iterative threshold ϵ

Output: Power allocation matrix $\boldsymbol{\Lambda}$

Initialize the iteration index $\ell = -1$ and $\overline{\mathcal{R}}\left(\boldsymbol{\Lambda}^{(\ell)}\right) = 0$

repeat

  $\ell = \ell + 1$

  Calculate $\overline{\mathcal{R}}\left(\boldsymbol{\Lambda}^{(\ell)}\right) = \sum_{k=1}^{K}\left(\overline{f}_k\left(\boldsymbol{\Lambda}^{(\ell)}\right) - g_k\left(\boldsymbol{\Lambda}^{(\ell)}\right)\right)$

  Calculate $\boldsymbol{\Lambda}^{(\ell+1)}$ by solving (19) with $\boldsymbol{\Lambda}^{(\ell)}$

until $\left|\overline{\mathcal{R}}\left(\boldsymbol{\Lambda}^{(\ell)}\right) - \overline{\mathcal{R}}\left(\boldsymbol{\Lambda}^{(\ell-1)}\right)\right| \le \epsilon$

Return $\boldsymbol{\Lambda} = \boldsymbol{\Lambda}^{(\ell)}$

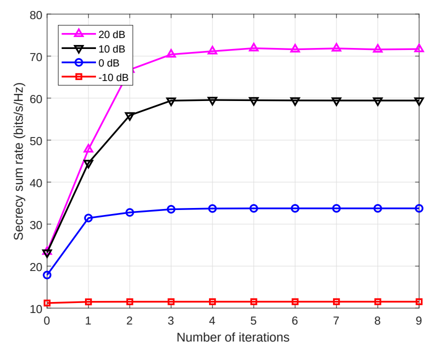

Fig. 1. The convergence behavior of secrecy sum rate obtained by Algorithm 1 as the number of iterations increases.

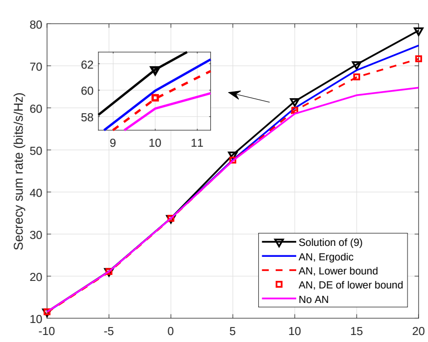

Fig. 2. The performance comparison of secrecy sum rate between our proposed AN assisted approach and the traditional one without AN.

$$
\begin{aligned}
\overline{f}_k(\mathbf{\Lambda}) = &\log\det\left(\mathbf{I}_{N_k} + \mathbf{\Gamma}_k(\mathbf{\Lambda}_k + \mathbf{\Lambda}_{\mathrm{AN}})\right) + \log\det\left(\widetilde{\mathbf{\Gamma}}_k + \overline{\mathbf{K}}_k(\mathbf{\Lambda})\right) - \mathrm{tr}\left(\mathbf{I}_{N_k} - \widetilde{\mathbf{\Phi}}_k^{-1}\right) \\
&+ \log\det\left(\mathbf{I}_{N_\mathrm{e}} + \mathbf{\Gamma}_\mathrm{e}\mathbf{\Lambda}_{\mathrm{AN}}\right) + \log\det\left(\widetilde{\mathbf{\Gamma}}_\mathrm{e} + \mathbf{I}_{N_\mathrm{e}}\right) - \mathrm{tr}\left(\mathbf{I}_{N_\mathrm{e}} - \widetilde{\mathbf{\Phi}}_\mathrm{e}^{-1}\right)
\end{aligned} \tag{17}
$$

$$
\begin{aligned}
\mathbf{\Lambda}^{(\ell+1)} = \arg\max_{\mathbf{\Lambda}} &\sum_{k=1}^{K}\left(\overline{f}_k(\mathbf{\Lambda}) - g_k\left(\mathbf{\Lambda}^{(\ell)}\right) - \sum_{a=1}^{K}\mathrm{tr}\left\{\left(\frac{\partial g_k\left(\mathbf{\Lambda}^{(\ell)}\right)}{\partial \mathbf{\Lambda}_a}\right)^T\left(\mathbf{\Lambda}_a - \mathbf{\Lambda}_a^{(\ell)}\right)\right\} - \mathrm{tr}\left\{\left(\frac{\partial g_k\left(\mathbf{\Lambda}^{(\ell)}\right)}{\partial \mathbf{\Lambda}_{\mathrm{AN}}}\right)^T\left(\mathbf{\Lambda}_{\mathrm{AN}} - \mathbf{\Lambda}_{\mathrm{AN}}^{(\ell)}\right)\right\}\right) \\
\text{subject to } &\sum_{k=1}^{K}\mathrm{tr}\left(\mathbf{\Lambda}_k\right) + \mathrm{tr}\left(\mathbf{\Lambda}_{\mathrm{AN}}\right) \le P_{\max},\ \mathbf{\Lambda}_{\mathrm{AN}} \succeq \mathbf{0},\ \mathbf{\Lambda}_k \succeq \mathbf{0},\ \forall k
\end{aligned} \tag{19}
$$

$$
\left[\frac{\partial g_k\left(\mathbf{\Lambda}^{(\ell)}\right)}{\partial \mathbf{\Lambda}_a}\right]_{m,m} = \begin{cases} \sum\limits_{n=1}^{N_\mathrm{e}} \dfrac{[\mathbf{\Omega}_\mathrm{e}]_{n,m}}{1+\sum\limits_{q=1}^{M}[\mathbf{\Lambda}_k^{(\ell)}+\mathbf{\Lambda}_{\mathrm{AN}}^{(\ell)}]_{q,q}[\mathbf{\Omega}_\mathrm{e}]_{n,q}}, & a = k \\ \sum\limits_{n=1}^{N_k} \dfrac{[\mathbf{\Omega}_k]_{n,m}}{1+\sum\limits_{q=1}^{M}[\mathbf{\Lambda}_{\backslash k}^{(\ell)}+\mathbf{\Lambda}_{\mathrm{AN}}^{(\ell)}]_{q,q}[\mathbf{\Omega}_k]_{n,q}}, & a \neq k \end{cases} \tag{20}
$$

$$
\left[\frac{\partial g_k\left(\mathbf{\Lambda}^{(\ell)}\right)}{\partial \mathbf{\Lambda}_{\mathrm{AN}}}\right]_{m,m} = \sum_{n=1}^{N_k}\frac{[\mathbf{\Omega}_k]_{n,m}}{1+\sum\limits_{q=1}^{M}[\mathbf{\Lambda}_{\backslash k}^{(\ell)}+\mathbf{\Lambda}_{\mathrm{AN}}^{(\ell)}]_{q,q}[\mathbf{\Omega}_k]_{n,q}} + \sum_{n=1}^{N_\mathrm{e}}\frac{[\mathbf{\Omega}_\mathrm{e}]_{n,m}}{1+\sum\limits_{q=1}^{M}[\mathbf{\Lambda}_k^{(\ell)}+\mathbf{\Lambda}_{\mathrm{AN}}^{(\ell)}]_{q,q}[\mathbf{\Omega}_\mathrm{e}]_{n,q}} \tag{21}
$$

conventional approach without utilizing AN. The considerable improvement happens in the high SNR region, indicating that injecting AN is an effective way of secrecy enhancement. We can observe that the exploitation of AN yields performance gains over the conventional approach without utilizing AN. The considerable improvement happens in the high SNR region, indicating that injecting AN is an effective way of secrecy enhancement. Notably, the simulation results demonstrate the tightness of the introduced lower bound and the accuracy of the derived DE in a wide SNR region. We also compare the proposed approach with the numerical one solving (9) and observe that its performance is almost identical with that solving (9) in a wide SNR region.

V. Conclusion

We have investigated the AN assisted secure downlink transmission in massive MIMO systems, in which the BS has only access to the statistical CSI of the legitimate UTs and the eavesdropper. A tight lower bound of the ergodic secrecy sum rate was firstly introduced as the tractable objective of optimization, followed by the closed-form derivation of the optimal secrecy signal and AN transmit directions. Consequently, the secrecy signal and AN transmit strategy design can be reduced to a power allocation problem in the beam domain. A CCCP based iterative algorithm with convergence guarantee was further proposed to solve such a power allocation problem, together with the reduction of computational complexity using deterministic equivalent theory. We demonstrated by numerical results the secrecy improvement of the proposed AN assisted approach over the traditional one without AN injected.

References

[1] D. Kapetanović, 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.

[2] J. Zhu, R. Schober, and V. K. Bhargava, "Secure transmission in multicell massive MIMO systems," *IEEE Trans. Wireless Commun.*, vol. 13, no. 9, pp. 4766–4781, Sep. 2014.

[3] L. You, J. Wang, W. Wang, and X. Q. Gao, "Secure multicast transmission for massive MIMO with statistical channel state information," *IEEE Signal Process. Lett.*, vol. 26, no. 6, pp. 803–807, Jun. 2019.

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

[5] L. You, X. Q. Gao, X.-G. Xia, N. Ma, and Y. Peng, "Pilot reuse for massive MIMO transmission over spatially correlated Rayleigh fading channels," *IEEE Trans. Wireless Commun.*, vol. 14, no. 6, pp. 3352–3366, Jun. 2015.

[6] L. You, X. Q. Gao, A. L. Swindlehurst, and W. Zhong, "Channel acquisition for massive MIMO-OFDM with adjustable phase shift pilots," *IEEE Trans. Signal Process.*, vol. 64, no. 6, pp. 1461–1476, Mar. 2016.

[7] W. Wu, X. Q. Gao, Y. Wu, and C. Xiao, "Beam domain secure transmission for massive MIMO communications," *IEEE Trans. Veh. Technol.*, vol. 67, no. 8, pp. 7113–7127, Aug. 2018.

[8] L. You, X. Q. Gao, G. Y. Li, X.-G. Xia, and N. Ma, "BDMA for millimeter-wave/Terahertz massive MIMO transmission with per-beam synchronization," *IEEE J. Sel. Areas Commun.*, vol. 35, no. 7, pp. 1550–1563, Jul. 2017.

[9] C. Sun, X. Q. Gao, S. Jin, M. Matthaiou, Z. Ding, and C. Xiao, "Beam division multiple access transmission for massive MIMO communications," *IEEE Trans. Commun.*, vol. 63, no. 6, pp. 2170–2184, Jun. 2015.

[10] Y. Wu, R. Schober, D. W. K. Ng, C. Xiao, and G. Caire, "Secure massive MIMO transmission with an active eavesdropper," *IEEE Trans. Inf. Theory*, vol. 62, no. 7, pp. 3880–3900, Jul. 2016.

[11] 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.

[12] A. M. Tulino, A. Lozano, and S. Verdú, "Capacity-achieving input covariance for single-user multi-antenna channels," *IEEE Trans. Wireless Commun.*, vol. 5, no. 3, pp. 662–671, Mar. 2006.

[13] B. K. Sriperumbudur and G. R. G. Lanckriet, "A proof of convergence of the concave-convex procedure using Zangwill's theory," *Neural Comput.*, vol. 24, no. 6, pp. 1391–1407, Jun. 2012.

[14] A.-A. Lu, X. Q. Gao, and C. Xiao, "Free deterministic equivalents for the analysis of MIMO multiple access channel," *IEEE Trans. Inf. Theory*, vol. 62, no. 8, pp. 4604–4629, Aug. 2016.

[15] S. Jaeckel, L. Raschkowski, K. Börner, and L. Thiele, "QuaDRiGa: A 3-D multi-cell channel model with time evolution for enabling virtual field trials," *IEEE Trans. Antennas Propag.*, vol. 62, no. 6, pp. 3242–3256, Jun. 2014.