Article

QoS Guaranteed Secure Transmission for Beam Domain Massive MIMO Communications

Wenjin Wang *, Xu Chen, Li You and Xiqi Gao

National Mobile Communications Research Laboratory, Southeast University, Nanjing 210096, China; chen_xu@seu.edu.cn (X.C.); liyou@seu.edu.cn (L.Y.); xqgao@seu.edu.cn (X.G.)

* Correspondence: wangwj@seu.edu.cn; Tel.: +86-025-83790506

Version November 22, 2018 submitted to Electronics

Abstract: This paper considers the secure transmission with the quality of service guarantee for massive MIMO system where only statistical channel state information of all legitimate UTs and eavesdropper are known at the BS. We introduce a lower bound on the achievable ergodic secrecy rate of each legitimate UT, then we adopt system minimum UT's lower bound of ergodic secrecy rate as the optimization goal. We demonstrate it is optimal to transmit signals in the beam domain. Then we simplify the large-dimensional matrix-valued quality of service guaranteed secure transmission design into a beam domain power allocation problem. Based on the minorization-maximization procedure, we utilize large dimensional random matrix theory and derive the deterministic equivalents of the objective in each iteration. Numerical results show the proposed method can guarantee all legitimate UTs have a suitable ergodic secrecy rate.

Keywords: secure transmission, quality of service, massive MIMO, beam domain, statistic channel state information

1. Introduction

Due to the broadcast nature of wireless medium, secure transmission is always considered as a very important issue in wireless communication. Traditionally, the secure transmission has been achieved by utilizing key-based encryption techniques. However, these approaches are potentially vulnerable because they are built on certain assumptions for computational complexity [1]. In addition to key-based encryption techniques, physical layer security has attracted tremendous research interest. As shown in the pioneering work on physical layer security [2], if the legitimate UT's channel conditions is better than the eavesdropper's conditions, the BS can reliably send private message to the legitimate UT. And a typical approach to enhance the security of data transmission is the use of artificial noise (AN) to disturbs the signal to interference-plus-noise ratio (SINR) and the decoding process at the eavesdropper [3]. Much recent research has considered physical layer secure transmission of multi-antenna systems [4]. For MIMO wiretap channels, the work in [5,6] determine the optimal input covariance matrix to maximize the ergodic secrecy rate in the case only statistical channel state information (CSI) is required.

Massive multiple-input multiple-output (MIMO) which employs a large number of antennas at the base stations (BSs) to simultaneously serve a relatively large number of user terminals (UTs) to improve spectral efficiency and power efficiency [7]. And Massive MIMO has been considered as a promising technology to improve the physical layer security, the great number of antennas can not only increase the signal strength towards the legitimate UTs, but also focus the AN energy into direction of eavesdropper [8]. Massive MIMO enables simple UL detection and DL precoding to eliminate the inter-user interference [7,9,10]. There are some works have been dedicated to investigating physical layer security in massive MIMO systems. The work in [8] dedicated to secure downlink transmission in multi-cell massive MIMO system in the presence of a multi-antenna eavesdropper, where only imperfect CSI of the legitimate UTs is available at the BS. Article [11] proposed three secure transmission schemes for single-cell multi-user massive MIMO systems. The research in [12,13] based on the assumption that instantaneous CSI of the single-antenna legitimate UTs is available at the BS.

The accuracy of instantaneous CSI at the BS plays a significant role in most existing works. However, there are some challenges in the acquisition of instantaneous CSI. Exploiting the statistical CSI provides a practical way to overcome this challenge for statistical CSI varies over much larger time scales than instantaneous CSI. Article [14] proposed the method of beam domain transmission only utilize statistic CSI at the BS, and this transmission method was proven optimal for a sum-rate upper bound maximization. The work in [15] was further extended to solve the problem of beam domain secure transmission. It optimized for secure transmission sum-rate lower bound. However, such optimization results may result in some UTs' secrecy ergodic secure rate very small. This is very inapplicable for some scenarios where the quality of service (QoS) is required.

In this paper, we investigate the secure transmission with QoS guarantee for massive MIMO systems with an eavesdropper exists. We assume only the statistical CSI of legitimate UTs and the eavesdropper is acquired at the BS. Jointly correlated MIMO channel model is considered here. We utilize the method of beam domain transmission proposed in [14] to perform secure transmission with QoS guarantee.

The major contributions of our works are summarized as follows:

- In order to guarantee QoS, we use the system minimum UT's secrecy rate as the optimization goal to perform power allocation to the BS transmission signal. And we introduce a lower bound of above optimization goal. Based on this lower bound, we formulate a power allocation problem to maximize the achievable ergodic system minimum secrecy rate.
- We show the closed-form optimal secure transmit directions, i.e., the eigenvectors of transmit signal covariance matrices for secure transmission. We demonstrate that it is optimal to transmit signals in the beam domain.
- We propose an iterative beam domain power allocation algorithm for secure transmission via invoking the minorization-maximization (MM) framework. Our proposed algorithm is guaranteed to converge to a stationary point.
- We employ the large-dimensional random matrix theory to derive the deterministic equivalent of the objectives to further reduce the computational complexity.

The following notations are used. Upper and lower case boldface letters denote matrices and column vectors, respectively. $\mathbb{C}^{M\times N}$ denote the $M\times N$ dimensional complex-valued vector matrix. $\mathbf{I}_M$ denotes the $M\times M$ dimensional identity matrix. $(\cdot)^H$,$(\cdot)^*$ and $(\cdot)^T$ denote conjugate-transpose, conjugate, and transpose operations, respectively. $\odot$ denotes the Hadamard product. The operations $\mathrm{tr}\{\cdot\}$ and $\det\{\cdot\}$ denote the matrix trace and determinant operations, respectively. $[\mathbf{A}]_{m,n}$ denotes the (m,n)th element of matrix $\mathbf{A}$. $\mathbf{A}\succeq\mathbf{0}$ denotes that $\mathbf{A}$ is positive semidefinite. $[x]^+$ represents $\max\{x,0\}$.

2. Massive MIMO Channel Model

Consider secure transmission in a massive MIMO system with one M-antennas BS, K legitimate UTs, each with N_k antennas, and one eavesdropper with N_{eve} antennas. The BS transmits private and independent messages to each legitimate UT. We assume that each UT may be potentially targeted by the eavesdropper.

Let $\mathbf{H}_k\in\mathbb{C}^{N_k\times M}$ and $\mathbf{H}_{\mathrm{eve}}\in\mathbb{C}^{N_{\mathrm{eve}}\times M}$ denote the downlink channel matrices from the BS to legitimate UT $k, k=1,...,K$ and the eavesdropper, respectively. The received signals at the kth UT and at the eavesdropper are given by

$$\mathbf{y}_k = \mathbf{H}_k\mathbf{x}_k + \sum_{i\neq k}\mathbf{H}_k\mathbf{x}_i + \mathbf{n}_k \in \mathbb{C}^{N_k\times 1}, \tag{1}$$

$$\mathbf{y}_{\mathrm{eve}} = \sum_{i=1}^{K}\mathbf{H}_{\mathrm{eve}}\mathbf{x}_i + \mathbf{n}_{\mathrm{eve}} \in \mathbb{C}^{N_{\mathrm{eve}}\times 1}, \tag{2}$$

respectively. $\mathbf{x}_k \in \mathbb{C}^{M\times 1}$ denotes the signal vector transmitted to the kth UT which satisfies $\mathbb{E}\left\{\mathbf{x}_k\right\} = \mathbf{0}$, $\mathbb{E}\left\{\mathbf{x}_k\mathbf{x}_{k'}^H\right\} = 0\,(k\neq k')$, and $\mathbb{E}\left\{\mathbf{x}_k\mathbf{x}_k^H\right\} = \mathbf{Q}_k \in \mathbb{C}^{M\times M}$. $\mathbf{n}_k \in \mathbb{C}^{N_k\times 1}$ and $\mathbf{n}_{\mathrm{eve}} \in \mathbb{C}^{N_{\mathrm{eve}}\times 1}$ are zero-mean circularly symmetric complex Gaussian noise with covariance matrices $\mathbf{I}_{N_r}$ and $\mathbf{I}_{N_{\mathrm{eve}}}$ respectively. Here, without loss of generality, we consider a unit variance and assume that the BS has the power constraint

$$\sum_k \mathrm{tr}\left(\mathbf{Q}_k\right) \leq P, \tag{3}$$

where $P \geq 0$ depends on the BS power budget.

In this work, we consider the joint spatially correlated Rayleigh fading MIMO channel model [16,17] , which captures the joint correlation characteristics between the transmitter and the receiver. In particular, the downlink channel matrices from the BS to legitimate UT k and the eavesdropper in (1) and (2) can be modeled as:

$$\mathbf{H}_k = \mathbf{U}_{r,k}\mathbf{G}_k\mathbf{V}_{t,k}^H \in \mathbb{C}^{N_r\times M}, \tag{4}$$

$$\mathbf{H}_{\mathrm{eve}} = \mathbf{U}_{r,\mathrm{eve}}\mathbf{G}_{\mathrm{eve}}\mathbf{V}_{t,\mathrm{eve}}^H \in \mathbb{C}^{N_{\mathrm{eve}}\times M}, \tag{5}$$

where $\mathbf{U}_{r,k} \in \mathbb{C}^{N_k\times N_k}$, $\mathbf{U}_{r,\mathrm{eve}} \in \mathbb{C}^{N_{\mathrm{eve}}\times N_{\mathrm{eve}}}$, $\mathbf{V}_{t,k} \in \mathbb{C}^{M\times M}$, and $\mathbf{V}_{t,\mathrm{eve}} \in \mathbb{C}^{M\times M}$ are deterministic unitary matrices, $\mathbf{G}_k \in \mathbb{C}^{N_k\times M}$ and $\mathbf{G}_{\mathrm{eve}} \in \mathbb{C}^{N_{\mathrm{eve}}\times M}$ are random matrices with zero-mean independent elements. Note that $\mathbf{G}_k$ and $\mathbf{G}_{\mathrm{eve}}$ are referred to as the downlink beam domain channel matrices between the BS and legitimate UT k and the eavesdropper, respectively [14,18]. The statistical CSI of the beam domain channels $\mathbf{G}_k$ and $\mathbf{G}_{\mathrm{eve}}$ can be described as

$$\mathbf{\Omega}_k = \mathbb{E}\left\{\mathbf{G}_k \odot \mathbf{G}_k^*\right\} \in \mathbb{R}^{N_k\times M}, \tag{6}$$

$$\mathbf{\Omega}_{\mathrm{eve}} = \mathbb{E}\left\{\mathbf{G}_{\mathrm{eve}} \odot \mathbf{G}_{\mathrm{eve}}^*\right\} \in \mathbb{R}^{N_{\mathrm{eve}}\times M}, \tag{7}$$

respectively. The elements of $\mathbf{\Omega}_k$ and $\mathbf{\Omega}_{\mathrm{eve}}$ represent the average power of the corresponding beam domain channel elements. Statistical CSI $\mathbf{\Omega}_k$ and $\mathbf{\Omega}_{\mathrm{eve}}$ vary much slowly than instantaneous $\mathbf{G}_k$ and $\mathbf{G}_{\mathrm{eve}}$. In addition, the channel statistics have been shown to stay constant over a wide frequency interval [19,20]. Therefore, statistical CSI can be obtained via averaging over time and frequency in a wideband wireless transmission system with guaranteed accuracy and can be adopted to facilitate practical wideband transmission.

For massive MIMO channels, as the number of BS antennas M tends to infinity, the eigenvector matrices of the BS correlation matrices of different legitimate UTs and the eavesdropper tend to be equal to a deterministic unitary matrix $\mathbf{V}$, which only depends on the BS array topology [18,21,22]. Thus the channel matrices can be well approximated by

$$\mathbf{H}_k \overset{M\to\infty}{=} \mathbf{U}_{r,k}\mathbf{G}_k\mathbf{V}^H, \tag{8}$$

$$\mathbf{H}_{\mathrm{eve}} \overset{M\to\infty}{=} \mathbf{U}_{r,k}\mathbf{G}_{\mathrm{eve}}\mathbf{V}^H, \tag{9}$$

respectively. Note that the above approximations have been widely adopted in previous works and shown to be quire accurate for a practical number of antennas [14,21,23–26]. Thus, we will adopt the massive MIMO channel model in (8) and (9) in this work.

3. Secure transmission design

We assume that the BS only has statistical CSI of all legitimate UTs as well as the eavesdropper. We also assume that the legitimate UTs and the eavesdropper have instantaneous CSI of their corresponding channel matrices. At each legitimate UT, we treat the aggregate interference-plus-noise $\mathbf{n}'_k = \sum_{i \neq k} \mathbf{H}_k \mathbf{x}_i + \mathbf{n}_k$ as Gaussian noise with covariance matrix

$$\mathbf{K}_k = \mathbf{I}_{N_r} + \sum_{i \neq k} \mathbb{E}\left\{\mathbf{H}_k \mathbf{Q}_i \mathbf{H}_k^H\right\} \in \mathbb{C}^{N_r \times N_r}. \tag{10}$$

Here, we assume the covariance matrix $\mathbf{K}_k$ is known at the kth UT. Besides, we make the pessimistic assumption that, at the eavesdropper, signals of all legitimate UTs can be decoded and cancelled from the received signal $\mathbf{y}_{\text{eve}}$ except the signal transmitted to the UT of interest. Since each UT in the system has the risk of being eavesdropped, the ergodic secrecy rate of UT k can be expressed as [15]

$$R_k^{\text{sec}} = [R_k - C_k^{\text{eve}}]^+ , \tag{11}$$

R_k denotes an achievable ergodic rate between the BS and the kth UT and R_k^{eve} denotes the ergodic capacity between the BS and the eavesdropper, which seeks to decode the private messages intended for the kth UT.

$$\begin{aligned} R_k &= \mathbb{E}\left\{\operatorname{logdet}\left(\mathbf{I}_{N_k} + \mathbf{K}_k^{-1}\mathbf{H}_k\mathbf{Q}_k\mathbf{H}_k^H\right)\right\} \\ &= \mathbb{E}\left\{\operatorname{logdet}\left(\mathbf{K}_k + \mathbf{H}_k\mathbf{Q}_k\mathbf{H}_k^H\right)\right\} - \operatorname{logdet}\left\{\mathbf{K}_k\right\} \\ &\overset{\text{(a)}}{=} \mathbb{E}\left\{\operatorname{logdet}\left(\overline{\mathbf{K}}_k + \mathbf{G}_k\mathbf{V}^H\mathbf{Q}_k\mathbf{V}\mathbf{G}_k^H\right)\right\} - \operatorname{logdet}\left\{\overline{\mathbf{K}}_k\right\}, \end{aligned} \tag{12}$$

and [12]

$$\begin{aligned} C_k^{\text{eve}} &= \mathbb{E}\left\{\operatorname{logdet}\left(\mathbf{I}_{N_{\text{eve}}} + \mathbf{H}_{\text{eve}}\mathbf{Q}_k\mathbf{H}_{\text{eve}}^H\right)\right\} \\ &\overset{\text{(b)}}{=} \mathbb{E}\left\{\operatorname{logdet}\left(\mathbf{I}_{N_{\text{eve}}} + \mathbf{G}_{\text{eve}}\mathbf{V}^H\mathbf{Q}_k\mathbf{V}\mathbf{G}_{\text{eve}}^H\right)\right\}. \end{aligned} \tag{13}$$

Notice that, in practical system, it is difficult to acquire instantaneous $\mathbf{H}_k\mathbf{Q}_i\mathbf{H}_k$ $(i \neq k)$ at the kth UT in massive MIMO system. Thus, we make an assumption that each legitimate UT treats $\mathbf{n}'_k$ as a Gaussian noise and the covariance matrix with expectation over $\mathbf{H}_k$ is known at each UT's side. With this assumption, the matrix $\mathbf{K}_k$ defined in (10) is the covariance matrix of $\mathbf{n}'_k$. Therefore, the ergodic rate defined in (12) is reasonable for practice. In addition, (a) and (b) follows from the massive MIMO channel model in (8) (9), the Sylvester's determinant identity $\det\{\mathbf{I} + \mathbf{AB}\} = \det\{\mathbf{I} + \mathbf{BA}\}$ and the following definition

$$\begin{aligned} \overline{\mathbf{K}}_k &\triangleq \mathbf{U}_{r,k}^H \mathbf{K}_k \mathbf{U}_{r,k} \\ &= \mathbf{I}_{N_k} + \sum_{i \neq k} \mathbb{E}\left\{\mathbf{G}_k\mathbf{V}^H\mathbf{Q}_i\mathbf{V}\mathbf{G}_k^H\right\} \in \mathbb{C}^{N_k \times N_k}, \end{aligned} \tag{14}$$

For notation convenience, we define a matrix-valued function as follows

$$\Xi_k(\mathbf{X}) \triangleq \mathbb{E}\left\{\mathbf{G}_k\mathbf{X}\mathbf{G}_k^H\right\}. \tag{15}$$

Using the beam domain massive MIMO channel properties, it is not difficult to verify that $\Xi_k(\mathbf{X})$ defined in (15) is a diagonal matrix-valued function with the elements given by

$$[\Xi_k(\mathbf{X})]_{i,j} = \begin{cases} \mathrm{tr}\left\{\mathrm{diag}\left\{\left([\mathbf{\Omega}_k]_{i,:}\right)^T\right\}\mathbf{X}\right\}, & i=j, \\ 0, & i \neq j. \end{cases} \tag{16}$$

The system minimum secrecy rate can be expressed as

$$R_{\mathrm{sec}} = \min_k\ R_k^{\mathrm{sec}} = \min_k\ [R_k - C_k^{\mathrm{eve}}]^+. \tag{17}$$

In general, the system minimum secrecy rate given by (17) is a non-concave function with respect to $(\mathbf{Q}_1,...,\mathbf{Q}_K)$. Hence, it is difficult to determine the optimal input covariance matrices to maximize the minimum secrecy rate. From Jensen's inequality, C_k^{eve} in (13) can be upper bounded by

$$\begin{aligned} C_k^{\mathrm{eve}} \leq C_{k,\mathrm{ub}}^{\mathrm{eve}} &= \mathrm{logdet}\left(\mathbf{I}_{N_{\mathrm{eve}}} + \mathbb{E}\left\{\mathbf{G}_{\mathrm{eve}}\mathbf{V}^H\mathbf{Q}_k\mathbf{V}\mathbf{G}_{\mathrm{eve}}^H\right\}\right) \\ &= \mathrm{logdet}\left(\mathbf{I}_{N_{\mathrm{eve}}} + \Xi_{\mathrm{eve}}\left(\mathbf{V}^H\mathbf{Q}_k\mathbf{V}\right)\right). \end{aligned} \tag{18}$$

Thus the lower bound of secrecy rate for UT k can be obtained as

$$R_{k,\mathrm{lb}}^{\mathrm{sec}} = \left[R_k - C_{k,\mathrm{ub}}^{\mathrm{eve}}\right]^+, \tag{19}$$

Then the lower bound of system minimum secrecy rate in (17) can be obtained as follows

$$R_{\mathrm{sec,lb}} = \min_k \left[R_k - C_{k,\mathrm{ub}}^{\mathrm{eve}}\right]^+. \tag{20}$$

Then, we design the secure transmission strategies by optimizing the lower bound of system minimum secrecy rate. Our main objective is to design the input covariance matrices $\mathbf{Q}_1,...,\mathbf{Q}_K$ maximizing (20), which can be formulated as the following optimization problem

$$\begin{aligned} \left[\mathbf{Q}_1^{\mathrm{op}},...,\mathbf{Q}_K^{\mathrm{op}}\right] = \arg\max_{\mathbf{Q}_1,...,\mathbf{Q}_K} &\quad \min_k \left(R_k - C_{k,\mathrm{ub}}^{\mathrm{eve}}\right) \\ \text{subject to} &\quad \mathrm{tr}\left(\sum_{k=1}^K \mathbf{Q}_k\right) \leq P \\ &\quad \mathbf{Q}_k \succeq \mathbf{0}, \quad k = 1,...,K, \end{aligned} \tag{21}$$

where $\mathbf{Q}_1^{\mathrm{op}},...,\mathbf{Q}_K^{\mathrm{op}}$ is the optimal solution of the problem in (21). Because any negative term in the summation could increase to zero by setting the corresponding $\mathbf{Q}_k = \mathbf{0}, k = 1,...,K$, the notation $[\cdot]^+$ is ignored when solving the problem in (21).

Let $\mathbf{Q}_k = \mathbf{\Phi}_k\mathbf{\Lambda}_k\mathbf{\Phi}_k^H$, where $\mathbf{\Phi}_k$ is the eigenmatrix and $\mathbf{\Lambda}_k$ is a diagonal matrix of the corresponding eigenvalues. Note that eigenvectors and the eigenvalues of the transmit covariance matrix have practical engineering meaning. Specifically, the eigenvectors of the transmit covariance matrix represent the directions of the transmit signals, while the eigenvalues represent the powers allocated onto each direction. And for the beam domain transmission proposed in [14], $\mathbf{\Phi}_k$ is set to be $\mathbf{V}, k = 1, ..., K$.

We start our investigation of the optimal transmit covariance $\mathbf{Q}_k, k = 1, ..., K$ by focusing on its eigenvectors. In particular, we present the eigenvectors of the optimal transmit covariance matrix in the following proposition.

Theorem 1. *The eigenvector of the optimal input covariance matrix of each legitimate UT, maximizing the lower bound of system minimum secrecy rate as given by (20) are given by*

$$\mathbf{Q}_k^{\mathrm{op}} = \mathbf{V}\mathbf{\Lambda}_k\mathbf{V}^H, \quad k = 1, ..., K. \tag{22}$$

Proof. Please refer to the Appendix. □

Theorem 1 shows the eigenmatrices of the input signals maximizing the low bound of system minimum secrecy rate are given by the columns of $\mathbf{V}$, which implies that the optimal QoS guaranteed secure transmission should be performed in the beam domain.

Inspired by Theorem 1, we focus on the beam domain secure transmission. Thus the optimization problem in (21) can be simplified to

$$\begin{aligned}
&\underset{\mathbf{\Lambda}=\{\mathbf{\Lambda}_1,...,\mathbf{\Lambda}_K\}}{\arg\max} && \min_k \left(R_k\left(\mathbf{\Lambda}\right) - C_{k,\mathrm{ub}}^{\mathrm{eve}}\left(\mathbf{\Lambda}\right)\right) \\
&\text{subject to} && \mathrm{tr}\left(\sum_{k=1}^{K}\mathbf{\Lambda}_k\right) \leq P \\
& && \mathbf{\Lambda}_k \succeq \mathbf{0}, \quad k = 1, ..., K,
\end{aligned} \tag{23}$$

where

$$R_k\left(\mathbf{\Lambda}\right) = \mathbb{E}\left\{\mathrm{logdet}\left(\overline{\mathbf{K}}_k\left(\mathbf{\Lambda}\right) + \mathbf{G}_k\mathbf{\Lambda}_k\mathbf{G}_k^H\right)\right\} - \mathrm{logdet}\left(\overline{\mathbf{K}}_k\left(\mathbf{\Lambda}\right)\right), \tag{24}$$

$$C_{k,\mathrm{ub}}^{\mathrm{eve}}\left(\mathbf{\Lambda}\right) = \mathrm{logdet}\left(\overline{\mathbf{K}}_{\mathrm{eve},k}\left(\mathbf{\Lambda}\right)\right), \tag{25}$$

and

$$\begin{aligned}
\overline{\mathbf{K}}_k\left(\mathbf{\Lambda}\right) &= \mathbf{I}_{N_k} + \sum_{i\neq k}\mathbb{E}\left\{\mathbf{G}_k\mathbf{\Lambda}_i\mathbf{G}_k^H\right\} \\
&= \mathbf{I}_{N_k} + \sum_{i\neq k}\Xi_k\left(\mathbf{\Lambda}_i\right) \qquad (26) \\
\overline{\mathbf{K}}_{\mathrm{eve},k}\left(\mathbf{\Lambda}\right) &= \mathbf{I}_{N_{\mathrm{eve}}} + \mathbb{E}\left\{\mathbf{G}_{\mathrm{eve}}\mathbf{\Lambda}_k\mathbf{G}_{\mathrm{eve}}^H\right\} \\
&= \mathbf{I}_{N_{\mathrm{eve}}} + \Xi_{\mathrm{eve}}\left(\mathbf{\Lambda}_k\right). \qquad (27)
\end{aligned}$$

We define

$$f_k\left(\mathbf{\Lambda}\right) = \mathbb{E}\left\{\mathrm{logdet}\left(\overline{\mathbf{K}}_k\left(\mathbf{\Lambda}\right) + \mathbf{G}_k\mathbf{\Lambda}_k\mathbf{G}_k^H\right)\right\}, \tag{28}$$

and

$$g_k(\mathbf{\Lambda}) = \text{logdet}\left(\overline{\mathbf{K}}_k(\mathbf{\Lambda})\right) + \text{logdet}\left(\overline{\mathbf{K}}_{\text{eve},k}(\mathbf{\Lambda})\right). \tag{29}$$

Then we can rewrite (23) as follows

$$\begin{aligned} &\underset{\mathbf{\Lambda}=\{\mathbf{\Lambda}_1,...,\mathbf{\Lambda}_K\}}{\arg\max} \quad \min_k \left(f_k(\mathbf{\Lambda}) - g_k(\mathbf{\Lambda})\right) \\ &\text{subject to} \quad \text{tr}\left(\sum_{k=1}^{K}\mathbf{\Lambda}_k\right) \le P \\ &\qquad\qquad\quad \mathbf{\Lambda}_k \succeq \mathbf{0}, \quad k = 1,...,K, \end{aligned} \tag{30}$$

We observe that $f_k(\mathbf{\Lambda})$ and $g_k(\mathbf{\Lambda})$ in the objective function of (30) are both concave functions with respect to $\mathbf{\Lambda}$, then we adopt the minorization-maximization (MM) framework [27,28] to address this problem. The MM framework is a sequential optimization approach to solve difficult maximization problem via solving a sequence of maximization problems that are easy to handle. The key step of MM framework is to construct a surrogate lower-bound function of the objective so that the maximization problems are easy to handle. We construct the surrogate lower-bound function in each iteration by replacing $g_k(\mathbf{\Lambda})$ for $\forall k$ with their first-order Taylor expansions at the current iteration and solve it, which further yields the next iteration. Specifically, the problem in (30) is handled via iteratively solving the following sequence of optimization problems

$$\begin{aligned} \left\{\mathbf{\Lambda}^{(\ell+1)}\right\} = &\underset{\mathbf{\Lambda}}{\arg\max} \quad \min_k \left\{ f_k(\mathbf{\Lambda}) - g_k\left(\mathbf{\Lambda}^{(\ell)}\right) - \sum_{i=1}^{K} \text{tr}\left\{ \left(\frac{\partial}{\partial \mathbf{\Lambda}_i} g_k\left(\mathbf{\Lambda}^{(\ell)}\right)\right)^T \left(\mathbf{\Lambda}_i - \mathbf{\Lambda}_i^{(\ell)}\right)\right\}\right\} \\ &\text{subject to} \quad \text{tr}\left(\sum_{k=1}^{K}\mathbf{\Lambda}_k\right) \le P \\ &\qquad\qquad\quad \mathbf{\Lambda}_k \succeq \mathbf{0}, \quad k = 1,...,K, \end{aligned} \tag{31}$$

where ℓ denotes the iteration index.

Note the composition of $g_k(\mathbf{\Lambda})$ in (29), we can simplify (31) as follows:

$$\begin{aligned} \left\{\mathbf{\Lambda}^{(\ell+1)}\right\} = &\underset{\mathbf{\Lambda}}{\arg\max} \quad \min_k \left\{ f_k(\mathbf{\Lambda}) - g_k\left(\mathbf{\Lambda}^{(\ell)}\right) - \sum_{i\neq k} \text{tr}\left\{ \left(\frac{\partial}{\partial \mathbf{\Lambda}_i} \text{logdet}\left(\overline{\mathbf{K}}_k\right)\right)^T \left(\mathbf{\Lambda}_i - \mathbf{\Lambda}_i^{(\ell)}\right)\right\} \right. \\ &\qquad\qquad \left. - \text{tr}\left\{ \left(\frac{\partial}{\partial \mathbf{\Lambda}_k} \text{logdet}\left(\overline{\mathbf{K}}_{\text{eve},k}\right)\right)^T \left(\mathbf{\Lambda}_k - \mathbf{\Lambda}_k^{(\ell)}\right)\right\}\right\} \\ &\text{subject to} \quad \text{tr}\left(\sum_{k=1}^{K}\mathbf{\Lambda}_k\right) \le P \\ &\qquad\qquad\quad \mathbf{\Lambda}_k \succeq \mathbf{0}, \quad k = 1,...,K, \end{aligned} \tag{32}$$

Moreover, $\frac{\partial}{\partial \mathbf{\Lambda}_i}\text{logdet}\left(\overline{\mathbf{K}}_k\right)$ and $\frac{\partial}{\partial \mathbf{\Lambda}_k}\text{logdet}\left(\overline{\mathbf{K}}_{\text{eve},k}\right)$ are diagonal matrices, whose mth element is given by

$$\left[\frac{\partial}{\partial \boldsymbol{\Lambda}_i}\mathrm{logdet}\left(\overline{\mathbf{K}}_k\right)\right]_{m,m} = \sum_{n=1}^{N_r} \frac{[\boldsymbol{\Omega}_k]_{n,m}}{1+\sum_{j\neq k}\sum_{q=1}^{M}[\boldsymbol{\Omega}_k]_{n,q}\left[\boldsymbol{\Lambda}_j^{(\ell)}\right]_{q,q}} \tag{33}$$

and

$$\left[\frac{\partial}{\partial \boldsymbol{\Lambda}_k}\mathrm{logdet}\left(\overline{\mathbf{K}}_{\mathrm{eve},k}\right)\right]_{m,m} = \sum_{n=1}^{N_{\mathrm{eve}}} \frac{[\boldsymbol{\Omega}_{\mathrm{eve}}]_{n,m}}{1+\sum_{q=1}^{M}[\boldsymbol{\Omega}_{\mathrm{eve}}]_{n,q}\left[\boldsymbol{\Lambda}_k^{(\ell)}\right]_{q,q}} \tag{34}$$

respectively.

According to [27,29], the solution sequence $\left\{\boldsymbol{\Lambda}^{(\ell)}\right\}_{\ell=0}^{\infty}$ generated by the proposed approach in (31) is proven to be convergent and approximately optimal of the original problem in (23).

To reduce the computational complexity of the expectation operation, we further employ the large dimensional random matrix theory [30–32] to calculate the deterministic equivalent (DE) of $f_k(\boldsymbol{\Lambda})$ in each iteration, rather than utilize Monte-Carlo method averaging over the channels. In particular, the DE of $f_k(\boldsymbol{\Lambda})$ in the ℓth iteration is given by

$$\overline{f}_k(\boldsymbol{\Lambda}) = \mathrm{logdet}\left(\mathbf{I}_M + \boldsymbol{\Gamma}_k\boldsymbol{\Lambda}_k\right) + \mathrm{logdet}\left(\widetilde{\boldsymbol{\Gamma}}_k + \overline{\mathbf{K}}_k(\boldsymbol{\Lambda})\right) - \mathrm{tr}\left(\mathbf{I}_{N_r} - \left(\widetilde{\boldsymbol{\Phi}}_k\right)^{-1}\right), \tag{35}$$

where $\boldsymbol{\Gamma}_k \in \mathbb{C}^{M\times M}$, $\widetilde{\boldsymbol{\Gamma}}_k \in \mathbb{C}^{N_k\times N_k}$ and $\widetilde{\boldsymbol{\Phi}}_k \in \mathbb{C}^{N_k\times N_k}$ are given by the iterative equations

$$\boldsymbol{\Gamma}_k = \boldsymbol{\Pi}_k\left(\left(\overline{\mathbf{K}}_k(\boldsymbol{\Lambda})\,\widetilde{\boldsymbol{\Phi}}_k\right)^{-1}\right), \tag{36}$$

$$\widetilde{\boldsymbol{\Gamma}}_k = \boldsymbol{\Xi}_k\left(\left(\mathbf{I}_M + \boldsymbol{\Gamma}_k\boldsymbol{\Lambda}_k\right)^{-1}\boldsymbol{\Lambda}_k\right), \tag{37}$$

$$\widetilde{\boldsymbol{\Phi}}_k = \mathbf{I}_{N_k} + \widetilde{\boldsymbol{\Gamma}}_k\left(\mathbf{K}_k(\boldsymbol{\Lambda})\right)^{-1}, \tag{38}$$

where the matrix-valued function $\boldsymbol{\Xi}_k(\mathbf{X})$ is given by (16) and $\boldsymbol{\Pi}_k(\mathbf{X}) \triangleq \mathbb{E}\left\{\mathbf{G}_k^H\mathbf{X}\mathbf{G}_k\right\} \in \mathbb{C}^{M\times M}$ is also a matrix operation with the elements given by

$$[\boldsymbol{\Pi}_k(\mathbf{X})]_{i,j} = \begin{cases} \mathrm{tr}\left\{\mathrm{diag}\left\{\left([\boldsymbol{\Omega}_k]_{:,i}\right)^T\right\}\mathbf{X}\right\}, & i=j, \\ 0, & i\neq j. \end{cases} \tag{39}$$

Compared with utilizing Monte-Carlo method to average over the channels for expectation operation, the DE can be calculated in a few iterations with a quite tight accuracy. In addition $\overline{f}_k^{(\ell)}(\boldsymbol{\Lambda})$ is strictly concave on $(\boldsymbol{\Lambda}_1,\ldots,\boldsymbol{\Lambda}_K)$ [33,34]. Via replacing $R_{k,1}(\boldsymbol{\Lambda}_1,\ldots,\boldsymbol{\Lambda}_K)$ with its DE in (35) in each iteration, we turn to consider the following series of convex programs instead of (32)

Algorithm 1 Beam Domain Secure Transmission Power Allocation Algorithm

1: Initialize $\mathbf{\Lambda}^{(0)}$, $\overline{\mathcal{R}}\left(\mathbf{\Lambda}^{(-1)}\right)=0$, threshold ϵ, and iteration index $\ell=-1$.
2: **repeat**
3: $\quad\ell=\ell+1$.
4: $\quad$Calculate DE $\overline{f}_k\left(\mathbf{\Lambda}^{(\ell)}\right)$ by (35).
5: $\quad$Calculate $\overline{\mathcal{R}}\left(\mathbf{\Lambda}_1^{(\ell)},\ldots,\mathbf{\Lambda}_U^{(\ell)}\right)=\min\limits_k\left(\overline{f}_k\left(\mathbf{\Lambda}\right)-g_k\left(\mathbf{\Lambda}\right)\right)$.
6: $\quad$Calculate the gradient of $g_k\left(\mathbf{\Lambda}^{(\ell)}\right)$ by (33) and (34).
7: $\quad$Calculate $\left(\mathbf{\Lambda}^{(\ell+1)}\right)$ via solving (40).
8: **until** $\left|\overline{\mathcal{R}}^{(\ell)}-\overline{\mathcal{R}}^{(\ell-1)}\right|\leq\epsilon$.
9: Return $\mathbf{\Lambda}=\mathbf{\Lambda}^{(\ell)}$.

Table 1. Simulation Setup Parameters

Parameter	Value
Channel model	3GPP spatial channel model (SCM)
Scenario	Suburban macro scenario
Array topology	ULA with half wavelength antenna spacing
Number of BS antennas	$M=32,64,128$
Number of legitimate UTs in the cell	$K=8$
Number of legitimate UT antennas	$N_r=4\ (\forall k)$
Number of eavesdropper antennas	$N_{\mathrm{eve}}=4$

$$\begin{aligned}\left\{\mathbf{\Lambda}^{(\ell+1)}\right\}=\arg\max_{\mathbf{\Lambda}}\quad&\min_k\Bigg\{\overline{f}_k\left(\mathbf{\Lambda}\right)-g_k\left(\mathbf{\Lambda}^{(\ell)}\right)-\sum_{i\neq k}\mathrm{tr}\left\{\left(\frac{\partial}{\partial\mathbf{\Lambda}_i}\mathrm{logdet}\left(\overline{\mathbf{K}}_k\right)\right)^T\left(\mathbf{\Lambda}_i-\mathbf{\Lambda}_i^{(\ell)}\right)\right\}\\&-\mathrm{tr}\left\{\left(\frac{\partial}{\partial\mathbf{\Lambda}_k}\mathrm{logdet}\left(\overline{\mathbf{K}}_{\mathrm{eve},k}\right)\right)^T\left(\mathbf{\Lambda}_k-\mathbf{\Lambda}_k^{(\ell)}\right)\right\}\Bigg\}\\\text{subject to}\quad&\mathrm{tr}\left(\sum_{k=1}^K\mathbf{\Lambda}_k\right)\leq P\\&\mathbf{\Lambda}_k\succeq\mathbf{0},\quad k=1,...,K,\end{aligned}\tag{40}$$

The proposed QoS guaranteed beam domain secure transmission power allocation algorithm is described in Algorithm 1.

4. Numerical Results

Numerical results are provided to evaluate the performance of our proposed Qos guaranteed beam domain secure transmission power allocation algorithm. We adopt 3GPP spatial channel model (SCM) channel model suburban macro-cell massive propagation environment in the simulation [35]. The signal-to-noise ratio (SNR) is defined as P, and the major simulation setup are listed in Table 1.

We first evaluate the convergence performance of the proposed algorithm 1 in Figure 1. The proposed algorithm exhibits very fast convergence performance under different values of SNRs.

We then compare the system minimum secrecy rate (17) with its lower bound (20) and DE for different numbers of BS antennas in Figure 2. The minimum secrecy rate and its lower bound are

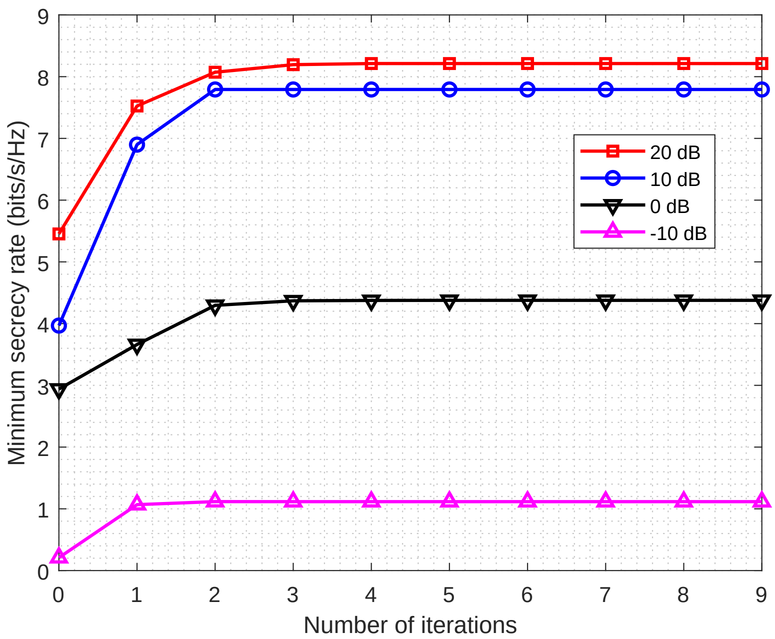

Figure 1. Convergence performance of Algorithm 1. Results are shown versus the iteration times for different SNRs with $M = 128$.

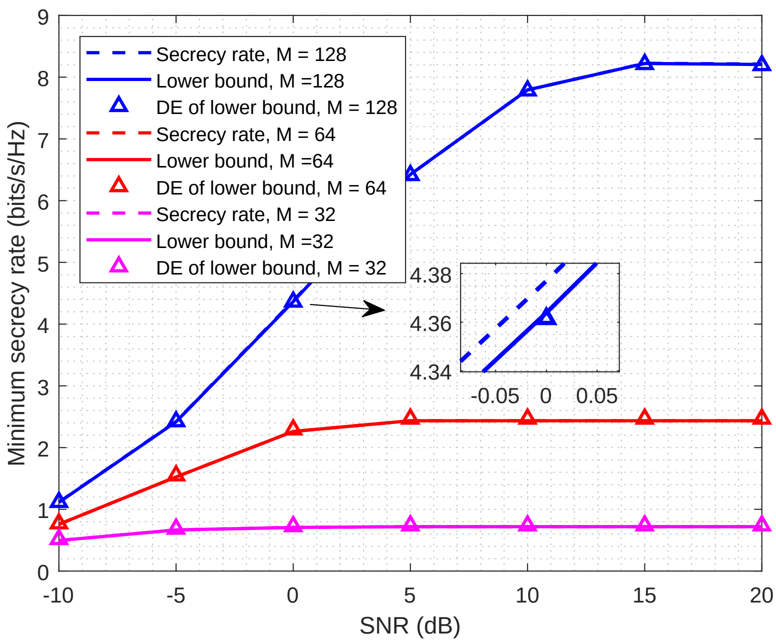

Figure 2. Comparison of the system minimum secrecy rate and the lower bound. Results are shown versus the SNRs of the SCM channel with $M = 32, 64, 128$. The deterministic equivalent of the lower bound is also depicted.

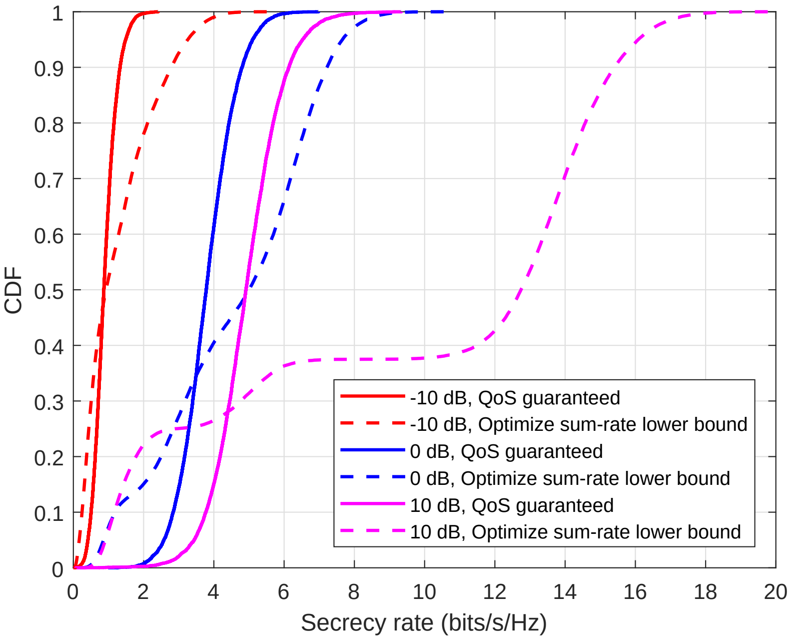

Figure 3. System UT ergodic secrecy rate distribution of Algorithm 1 and secure transmission method in [15] for different SNRs with $M = 128$, respectively.

evaluated by Monte-Carlo simulations. The lower bound is quite tight in the considered SNR ranges. The accuracy of the DE results compared with the Monte-Carlo result in a wide range of SNRs is also verified in Figure 2. In addition, the system minimum secrecy rate performance increases as the number of BS antennas increases.

Finally, we compare the performance of our proposed QoS guaranteed secure transmission with secure transmission method in [15], which optimized for secure transmission sum-rate lower bound. Here, we set the SNR as -10dB, 0dB and 10dB. As can be seen from the system UT ergodic secrecy rate distribution in Figure 3, in our proposed transmission method the system minimum secrecy rate has been greatly improved.

5. Conclusion

In this paper, we have investigated massive MIMO secure transmission with QoS guarantee where only statistical CSI of all legitimate UTs and eavesdropper are known at the BS. Our optimization goal was to maximize the lower bound of the system minimum secrecy rate. Based on a massive MIMO channel model, we first showed the closed-form optimal secure transmit directions, which simplified the large-dimensional matrix valued secure transmission design into a beam domain power allocation problem. We then proposed an iterative power allocation algorithm with guaranteed convergence to a stationary point based on the MM framework and the DE. Numerical results show the proposed method can guarantee all legitimate UTs have a suitable ergodic secrecy rate.

Author Contributions: W.W. perceived the idea and wrote the manuscript. X.C. performed the simulations. L.Y. and X.G. gave valuable suggestions on the structuring of the paper and assisted in the revising and proofreading.

Funding: This work was supported in part by the National Natural Science Foundation of China under Grants 61320106003, 61761136016, 61801114, 61471113, 61631018, and 61521061, the Natural Science Foundation of Jiangsu Province under Grant BK20170688, and the National Science and Technology Major Project of China under Grant 2017ZX03001002-004.

Acknowledgments:

Conflicts of Interest: The authors declare no conflict of interest.

Appendix Proof of Theorem 1

From (26) (27) and (16), we can observe that for all k, the off-diagonal entries of $\mathbf{V}^H\mathbf{Q}_k\mathbf{V}$ do not affect the value of $\overline{\mathbf{K}}_k$ and $\overline{\mathbf{K}}_{\mathrm{eve},k}$. Use the similar technique in [36], we can prove $\mathbf{V}^H\mathbf{Q}_k\mathbf{V}_{\forall k}$ should be diagonal to maximize $R^{\mathrm{sec}}_{k,\mathrm{lb}}$ in (19) for all UT k. Moreover, the transmit power $\mathrm{tr}\left(\sum_{k=1}^{K}\mathbf{\Lambda}_k\right)$ is only related to the diagonal entries of $\mathbf{V}^H\mathbf{Q}_k\mathbf{V}$ for all k. Therefore we can obtain the conclusion that the objective (17) can be maximized when $\mathbf{V}^H\mathbf{Q}_k\mathbf{V}_{\forall k}$ is diagonal. This concludes the proof.

References

1. Mukherjee, A.; Fakoorian, S.A.A.; Huang, J.; Swindlehurst, A.L. Principles of physical layer security in multiuser wireless networks: A survey. *IEEE Commun. Surveys Tuts.* **2014**, *16*, 1550–1573.
2. Wyner, A.D. The wire-tap channel. *Bell Syst.tech.j* **1975**, *54*, 1355–1387.
3. Goel, S.; Negi, R. Guaranteeing Secrecy using Artificial Noise. *IEEE Trans. Wireless Commun.* **2008**, *7*, 2180–2189.
4. Cumanan, K.; Ding, Z.; Sharif, B.; Gui, Y.T.; Leung, K.K. Secrecy Rate Optimizations for a MIMO Secrecy Channel With a Multiple-Antenna Eavesdropper. *IEEE Trans. Veh. Technol.* **2014**, *63*, 1678–1690.
5. Zhang, J.; Yuen, C.; Wen, C.K.; Jin, S.; Wong, K.K.; Zhu, H. Large System Secrecy Rate Analysis for SWIPT MIMO Wiretap Channels. *IEEE Trans. Inf. Forensics Security* **2017**, *11*, 74–85.
6. Li, J.; Petropulu, A.P. On Ergodic Secrecy Rate for Gaussian MISO Wiretap Channels. *IEEE Trans. Wireless Commun.* **2010**, *10*, 1176–1187.
7. Marzetta, T.L. Noncooperative cellular wireless with unlimited numbers of base station antennas. *IEEE Trans. Wireless Commun.* **2010**, *9*, 3590–3600.
8. Zhu, J.; Schober, R.; Bhargava, V.K. Secure Transmission in Multicell Massive MIMO Systems. *IEEE Trans. Wireless Commun.* **2014**, *13*, 4766–4781.
9. Hoydis, J.; ten Brink, S.; Debbah, M. Massive MIMO in the UL/DL of cellular networks: How many antennas do we need? *IEEE J. Sel. Areas Commun.* **2013**, *31*, 160–171.
10. Larsson, E.G.; Edfors, O.; Tufvesson, F.; Marzetta, T.L. Massive MIMO for next generation wireless systems. *IEEE Commun. Mag.* **2014**, *52*, 186–195.
11. Guo, K.; Guo, Y.; Ascheid, G. Security-Constrained Power Allocation in MU-Massive-MIMO With Distributed Antennas. *IEEE Trans. Wireless Commun.* **2016**, *15*, 8139–8153.
12. Wu, Y.; Schober, R.; Ng, D.W.K.; Xiao, C.; Caire, G. Secure massive MIMO transmission with an active eavesdropper. *IEEE Trans. Inf. Theory* **2016**, *62*, 3880–3900.
13. Zhu, J.; Schober, R.; Bhargava, V.K. Linear Precoding of Data and Artificial Noise in Secure Massive MIMO Systems. *IEEE Trans. Wireless Commun.* **2016**, *15*, 2245–2261.
14. Sun, C.; Gao, X.Q.; Jin, S.; Matthaiou, M.; Ding, Z.; Xiao, C. Beam division multiple access transmission for massive MIMO communications. *IEEE Trans. Commun.* **2015**, *63*, 2170–2184.
15. Wu, W.; Gao, X.Q.; Wu, Y.; Xiao, C. Beam domain secure transmission for massive MIMO communications. *IEEE Trans. Veh. Technol.* **2018**, *67*, 7113–7127.
16. Gao, X.Q.; Jiang, B.; Li, X.; Gershman, A.B.; McKay, M.R. Statistical eigenmode transmission over jointly correlated MIMO channels. *IEEE Trans. Inf. Theory* **2009**, *55*, 3735–3750.
17. Weichselberger, W.; Herdin, M.; Özcelik, H.; Bonek, E. A stochastic MIMO channel model with joint correlation of both link ends. *IEEE Trans. Wireless Commun.* **2006**, *5*, 90–100.
18. You, L.; Gao, X.Q.; Li, G.Y.; Xia, X.G.; Ma, N. BDMA for millimeter-wave/Terahertz massive MIMO transmission with per-beam synchronization. *IEEE J. Sel. Areas Commun.* **2017**, *35*, 1550–1563.
19. You, L.; Gao, X.Q.; Li, G.Y.; Xia, X.G.; Ma, N. Millimeter-wave/Terahertz massive MIMO BDMA transmission with per-beam synchronization. Proc. IEEE ICC; , 2017.
20. Barriac, G.; Madhow, U. Space-time communication for OFDM with implicit channel feedback. *IEEE Trans. Inf. Theory* **2004**, *50*, 3111–3129.
21. You, L.; Gao, X.Q.; Xia, X.G.; Ma, N.; Peng, Y. Pilot reuse for massive MIMO transmission over spatially correlated Rayleigh fading channels. *IEEE Trans. Wireless Commun.* **2015**, *14*, 3352–3366.
22. You, L.; Gao, X.Q.; Swindlehurst, A.L.; Zhong, W. Channel acquisition for massive MIMO-OFDM with adjustable phase shift pilots. *IEEE Trans. Signal Process.* **2016**, *64*, 1461–1476.

23. You, L.; Chen, X.; Wang, W.; Gao, X.Q. Coordinated Multicast Precoding for Multi-Cell Massive MIMO Transmission Exploiting Statistical Channel State Information. *Electronics* **2018**, *7*, 338.
24. You, L.; Xiong, J.; Li, K.X.; Wang, W.; Gao, X.Q. Non-orthogonal unicast and multicast transmission for massive MIMO with statistical channel state information. *IEEE Access* **2018**. to be published, doi: 10.1109/ACCESS.2018.2879366.
25. You, L.; Wang, W.; Gao, X.Q. Energy-efficient multicast precoding for massive MIMO transmission with statistical CSI. *Energies* **2018**, *11*, 3175.
26. Wang, W.; Liu, A.; Zhang, Q.; You, L.; Gao, X.Q.; Zheng, G. Robust multigroup multicast transmission for frame-based multi-beam satellite systems. *IEEE Access* **2018**, *6*, 46074–46083.
27. Sun, Y.; Babu, P.; Palomar, D.P. Majorization-Minimization Algorithms in Signal Processing, Communications, and Machine Learning. *IEEE Trans. Signal Process.* **2016**, *65*, 794–816.
28. Yuille, A.L.; Rangarajan, A. The concave-convex procedure. *Neural Comput.* **2003**, *15*, 915–936.
29. Sriperumbudur, B.K.; Lanckriet, G.R.G. A proof of convergence of the concave-convex procedure using Zangwill's theory. *Neural Comput.* **2012**, *24*, 1391–1407.
30. Couillet, R.; Debbah, M. *Random Matrix Methods for Wireless Communications*; Cambridge Univ. Press: New York, NY, USA, 2011.
31. Lu, A.A.; Gao, X.Q.; Xiao, C. Free deterministic equivalents for the analysis of MIMO multiple access channel. *IEEE Trans. Inf. Theory* **2016**, *62*, 4604–4629.
32. Lu, A.A.; Gao, X.Q.; Zheng, Y.R.; Xiao, C. Low complexity polynomial expansion detector with deterministic equivalents of the moments of channel Gram matrix for massive MIMO uplink. *IEEE Trans. Commun.* **2016**, *64*, 586–600.
33. Dumont, J.; Lasaulce, S.; Lasaulce, S.; Loubaton, P.; Najim, J. On the capacity achieving covariance matrix for Rician MIMO channels: an asymptotic approach. *IEEE Trans. Inf. Theory* **2010**, *56*, 1048–1069.
34. Dupuy, F.; Loubaton, P. On the capacity achieving covariance matrix for frequency selective MIMO channels using the asymptotic approach. *IEEE Trans. Inf. Theory* **2011**, *57*, 5737–5753.
35. Salo, J.; Del Galdo, G.; Salmi, J.; Kyösti, P.; Milojevic, M.; Laselva, D.; Schneider, C. MATLAB implementation of the 3GPP spatial channel model (3GPP TR 25.996). Technical report, 2005.
36. Tulino, A.M.; Lozano, A.; Verdú, S. Capacity-achieving input covariance for single-user multi-antenna channels. *IEEE Trans. Wireless Commun.* **2006**, *5*, 662–671.