Secure Multicast Transmission for Massive MIMO with Statistical Channel State Information

Li You, *Member, IEEE*, Jiaheng Wang, *Senior Member, IEEE*,
Wenjin Wang, *Member, IEEE*, and Xiqi Gao, *Fellow, IEEE*

Abstract

We investigate physical layer security in massive multiple-input multiple-output multicast transmission where the base station only knows the statistical channel state information of the legitimate user terminals and the eavesdropper. We first introduce a tight lower bound of the achievable secrecy multicast rate as the design objective. Then, we find the closed-form transmit directions, i.e., the eigenvectors of the optimal multicast transmit covariance matrix, which simplifies the matrix-valued multicast transmit strategy design into a beam domain power allocation problem. We further propose an efficient iterative power allocation algorithm with guaranteed convergence to a local optimal solution by invoking the concave-convex procedure. We also derive the deterministic equivalent of the optimization objective to reduce the computation complexity. Numerical results demonstrate the performance gains of the proposed approach over the conventional approach.

Index Terms

Physical layer security, multicast transmission, massive MIMO, beam domain, statistical channel state information (CSI).

The authors are with the National Mobile Communications Research Laboratory, Southeast University, Nanjing 210096, China (e-mail: liyou@seu.edu.cn; jhwang@seu.edu.cn; wangwj@seu.edu.cn; xqgao@seu.edu.cn).

I. INTRODUCTION

Massive multiple-input multiple-output (MIMO) is promising for future wireless communication systems due to its great potential to boost the system spectral efficiency and energy efficiency [1]. Wireless multicast transmission where the base station (BS) delivers common messages to multiple user terminals (UTs) simultaneously is incorporated in the Long-Term Evolution (LTE) standards as evolved Multimedia Broadcast Multicast Service (eMBMS) for efficient transmission of group-oriented signals [2]. Wireless multicasting combined with massive MIMO is appealing due to the capability of massive MIMO to efficiently shape the multicast transmission signals and further improve the quality of service [3].

Security is a critical issue in wireless transmission due to the open nature of the wireless medium. Compared with the cryptographic based approaches, physical layer security solely exploits the wireless channel properties to safeguard the wireless data confidentiality and has received extensive research interest [4], [5]. Physical layer security for massive MIMO unicast transmission was investigated in previous works, see, e.g., [6]–[8]. Meanwhile, physical layer security for multicast transmission has also been investigated in some existing works. For example, secure multicast transmission using pure precoding was investigated in e.g., [9], [10]. In addition, secure multicast transmission exploiting the artificial noise was investigated in e.g., [11].

Most of the existing works, e.g., [6], [7], [9]–[11], assume that instantaneous channel state information (CSI) of the legitimate UTs is known. However, perfect instantaneous CSI is usually difficult to obtain in massive MIMO due to the CSI acquisition/feedback overhead. Compared with instantaneous CSI, statistical CSI varies much more slowly and thus can be more accurately acquired by the BS. Therefore, in scenarios with, e.g., high mobility, statistical CSI is more practical to be exploited for wireless transmission designs. Moreover, massive MIMO channels usually exhibit new statistical properties due to the high spatial resolution with a large antenna array [12], [13]. These properties can be further exploited to optimize the wireless transmission designs.

Motivated by the above considerations, we investigate secure multicast transmission for massive MIMO where only statistical CSI of the legitimate UTs and the eavesdropper is available at the BS. We first present a tight lower bound of the achievable secrecy multicast rate as the optimization objective. We then show the closed-form eigenvectors of the optimal multicast

transmit covariance matrix, which simplifies the matrix-valued multicast transmit covariance design into a beam domain power allocation problem. Via invoking the concave-convex procedure (CCCP), we further propose an efficient iterative power allocation algorithm which is guaranteed to converge to a local optimal solution. In addition, the deterministic equivalent (DE) of the design objective is derived to reduce the optimization complexity. Simulation results demonstrate the superior performance of the proposed approach for secure multicast massive MIMO transmission.

II. Massive MIMO Channel Model

Consider massive MIMO secure single-group multicast transmission with one M-antenna BS, K legitimate UTs, each with N_{r} antennas, and one N_{e}-antenna eavesdropper. The BS transmits a common confidential message to legitimate UTs, while the eavesdropper attempts to decode the message.

Denote by $\mathbf{x} \in \mathbb{C}^{M\times 1}$ the multicast signal intended for the legitimate UTs, which satisfies $\mathsf{E}\{\mathbf{x}\} = \mathbf{0}$ and $\mathsf{E}\left\{\mathbf{x}\mathbf{x}^H\right\} = \mathbf{Q} \in \mathbb{C}^{M\times M}$, where $\mathbf{Q}$ is the transmit covariance matrix. The signals received at legitimate UT k and the eavesdropper can be respectively written as

$$\mathbf{y}_k = \mathbf{H}_k\mathbf{x} + \mathbf{n}_k \in \mathbb{C}^{N_{\mathrm{r}}\times 1}, \tag{1}$$

$$\mathbf{y}_{\mathrm{ev}} = \mathbf{H}_{\mathrm{ev}}\mathbf{x} + \mathbf{n}_{\mathrm{ev}} \in \mathbb{C}^{N_{\mathrm{e}}\times 1}, \tag{2}$$

where $\mathbf{H}_k$ and $\mathbf{H}_{\mathrm{ev}}$ denote the downlink channel matrices from the BS to legitimate UT k and the eavesdropper, respectively, and $\mathbf{n}_k \sim \mathcal{CN}\left(\mathbf{0}, \mathbf{I}_{N_{\mathrm{r}}}\right)$ and $\mathbf{n}_{\mathrm{ev}} \sim \mathcal{CN}\left(\mathbf{0}, \mathbf{I}_{N_{\mathrm{e}}}\right)$ represent the additive Gaussian noise at legitimate UT k and the eavesdropper, respectively.

In this work, we consider the jointly spatially correlated Rayleigh fading MIMO channel model [14], 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 respectively modeled as

$$\mathbf{H}_k = \mathbf{U}_k\mathbf{G}_k\mathbf{V}_k^H \in \mathbb{C}^{N_{\mathrm{r}}\times M}, \tag{3}$$

$$\mathbf{H}_{\mathrm{ev}} = \mathbf{U}_{\mathrm{ev}}\mathbf{G}_{\mathrm{ev}}\mathbf{V}_{\mathrm{ev}}^H \in \mathbb{C}^{N_{\mathrm{e}}\times M}, \tag{4}$$

where $\mathbf{U}_k \in \mathbb{C}^{N_{\mathrm{r}}\times N_{\mathrm{r}}}$, $\mathbf{V}_k \in \mathbb{C}^{M\times M}$, $\mathbf{U}_{\mathrm{ev}} \in \mathbb{C}^{N_{\mathrm{e}}\times N_{\mathrm{e}}}$, and $\mathbf{V}_{\mathrm{ev}} \in \mathbb{C}^{M\times M}$ are deterministic unitary matrices, and $\mathbf{G}_k \in \mathbb{C}^{N_{\mathrm{r}}\times M}$ and $\mathbf{G}_{\mathrm{ev}} \in \mathbb{C}^{N_{\mathrm{e}}\times M}$ are random matrices with zero-mean independent elements. Note that $\mathbf{G}_k$ and $\mathbf{G}_{\mathrm{ev}}$ are referred to as the downlink beam domain channel matrices

between the BS and legitimate UT k and the eavesdropper, respectively [15], [16]. The statistics of the beam domain channels $\mathbf{G}_k$ and $\mathbf{G}_{\rm ev}$ can be described as

$$\mathbf{\Omega}_k = \mathsf{E}\left\{\mathbf{G}_k \odot \mathbf{G}_k^*\right\} \in \mathbb{R}^{N_{\rm r}\times M}, \tag{5}$$

$$\mathbf{\Omega}_{\rm ev} = \mathsf{E}\left\{\mathbf{G}_{\rm ev} \odot \mathbf{G}_{\rm ev}^*\right\} \in \mathbb{R}^{N_{\rm e}\times M}, \tag{6}$$

respectively.

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 [12], [13], [16], i.e., the channel matrices can be well approximated by

$$\mathbf{H}_k \overset{M\to\infty}{=} \mathbf{U}_k\mathbf{G}_k\mathbf{V}^H, \tag{7}$$

$$\mathbf{H}_{\rm ev} \overset{M\to\infty}{=} \mathbf{U}_{\rm ev}\mathbf{G}_{\rm ev}\mathbf{V}^H, \tag{8}$$

respectively. Note that the above approximations have been widely adopted in previous works and shown to be quite accurate for a practical number of antennas [12], [13]. Thus, we will adopt the massive MIMO channel model in (7) and (8) in this work.

III. Secure Multicast Transmission Design

Assume that the BS only has statistical CSI of all legitimate UTs as well as the eavesdropper, and the legitimate UTs and the eavesdropper know their own instantaneous CSI. Then the achievable secrecy multicast rate with transmit covariance $\mathbf{Q}$ can be represented as [8]

$$R_{\rm se} \triangleq \left[R_{\rm mc} - R_{\rm ev}\right]^+, \tag{9}$$

where $R_{\rm mc}$ is the ergodic multicast rate given by

$$\begin{aligned} R_{\rm mc} &= \min_k \quad \mathsf{E}\left\{\log\det\left\{\mathbf{I}_{N_{\rm r}} + \mathbf{H}_k\mathbf{Q}\mathbf{H}_k^H\right\}\right\} \\ &= \min_k \quad \mathsf{E}\left\{\log\det\left\{\mathbf{I}_{N_{\rm r}} + \mathbf{G}_k\mathbf{V}^H\mathbf{Q}\mathbf{V}\mathbf{G}_k^H\right\}\right\}, \end{aligned} \tag{10}$$

and $R_{\rm ev}$ is the ergodic rate between the BS and the eavesdropper given by

$$\begin{aligned} R_{\rm ev} &= \mathsf{E}\left\{\log\det\left\{\mathbf{I}_{N_{\rm e}} + \mathbf{H}_{\rm ev}\mathbf{Q}\mathbf{H}_{\rm ev}^H\right\}\right\} \\ &= \mathsf{E}\left\{\log\det\left\{\mathbf{I}_{N_{\rm e}} + \mathbf{G}_{\rm ev}\mathbf{V}^H\mathbf{Q}\mathbf{V}\mathbf{G}_{\rm ev}^H\right\}\right\}, \end{aligned} \tag{11}$$

where the identity $\det\{\mathbf{I}+\mathbf{AB}\}=\det\{\mathbf{I}+\mathbf{BA}\}$ is exploited in (10) and (11). From Jensen's inequality, $R_{\rm ev}$ in (11) can be upper bounded by

$$R_{\rm ev}\le R_{\rm ev,ub}\triangleq\log\det\left\{\mathbf{I}_{N_{\rm e}}+\underbrace{\mathsf{E}\left\{\mathbf{G}_{\rm ev}\mathbf{V}^H\mathbf{Q}\mathbf{V}\mathbf{G}_{\rm ev}^H\right\}}_{\triangleq\mathbf{A}_{\rm ev}(\mathbf{V}^H\mathbf{Q}\mathbf{V})}\right\}, \tag{12}$$

where $\mathbf{A}_{\rm ev}(\mathbf{X})\triangleq\mathsf{E}\left\{\mathbf{G}_{\rm ev}\mathbf{X}\mathbf{G}_{\rm ev}^H\right\}\in\mathbb{C}^{N_{\rm e}\times N_{\rm e}}$ is a matrix-valued function which outputs a diagonal matrix with the ith diagonal element given by

$$[\mathbf{A}_{\rm ev}(\mathbf{X})]_{i,i}=\mathsf{tr}\left\{\mathsf{diag}\left\{\left([\mathbf{\Omega}_{\rm ev}]_{i,:}\right)^T\right\}\mathbf{X}\right\}. \tag{13}$$

Then, a lower bound of the secrecy multicast rate in (9) can be obtained as follows

$$R_{\rm se}\ge R_{\rm se,lb}\triangleq[R_{\rm mc}-R_{\rm ev,ub}]^+. \tag{14}$$

It will be seen in Section **??** that the secrecy multicast rate lower bound in (14) is tight over a wide signal-to-noise-ratio (SNR) region. In the following, we investigate secure multicast transmission design and our objective is to design the optimal transmit covariance matrix $\mathbf{Q}$ that can maximize the lower bound of the secrecy multicast rate in (14), which can be formulated as the following problem

$$\begin{aligned}\max_{\mathbf{Q}}\quad & R_{\rm se,lb}=[R_{\rm mc}-R_{\rm ev,ub}]^+,\\ \text{s.t.}\quad & \mathsf{tr}\{\mathbf{Q}\}\le P,\ \mathbf{Q}\succeq\mathbf{0},\end{aligned} \tag{15}$$

where P denotes the multicast power budget at the BS. Since the feasible solution $\mathbf{Q}=\mathbf{0}$ results in a zero value of $R_{\rm se,lb}$, and all feasible points that lead to a negative secrecy rate can not be optimum to the problem in (15). Thus, the operator $[\cdot]^+$ can be omitted without loss of any optimality, which leads to the following equivalent problem

$$\begin{aligned}\max_{\mathbf{Q}}\quad & R_{\rm mc}-R_{\rm ev,ub},\\ \text{s.t.}\quad & \mathsf{tr}\{\mathbf{Q}\}\le P,\ \mathbf{Q}\succeq\mathbf{0}.\end{aligned} \tag{16}$$

Denote the eigenvalue decomposition of the transmit covariance matrix as $\mathbf{Q}=\mathbf{\Phi}\mathbf{\Lambda}\mathbf{\Phi}^H$ where the columns of $\mathbf{\Phi}$ are the eigenvectors of $\mathbf{Q}$ and the diagonal elements of $\mathbf{\Lambda}$ are the eigenvalues of

$\mathbf{Q}$. Note that the 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 to each direction.

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

Proposition 1: The eigenvectors of the optimal transmit covariance matrix $\mathbf{Q}^{\mathrm{opt}}$ to problem (16) are given by the columns of $\mathbf{V}$, i.e.,

$$\mathbf{Q}^{\mathrm{opt}} = \mathbf{V}\mathbf{\Lambda}\mathbf{V}^{H}. \tag{17}$$

Proof: Please refer to the Appendix. ■

Proposition 1 shows that the optimal multicast signaling directions should align with the eigenvectors of the transmit correlation matrices at the BS, which indicates that the optimal secure multicast transmission should be performed in the beam domain.

With Proposition 1 which reveals the optimal transmit directions, we then focus on the optimization of the eigenvalues of the transmit covariance matrix. In particular, the optimization problem in (16) can be simplified to

$$\begin{aligned} \arg\max_{\mathbf{\Lambda}} \quad & R_{\mathrm{mc}}\left(\mathbf{\Lambda}\right) - R_{\mathrm{ev,ub}}\left(\mathbf{\Lambda}\right), \\ \text{s.t.} \quad & \mathsf{tr}\left\{\mathbf{\Lambda}\right\} \leq P,\ \mathbf{\Lambda} \succeq \mathbf{0},\ \mathbf{\Lambda} \text{ diagonal}, \end{aligned} \tag{18}$$

where

$$R_{\mathrm{mc}}\left(\mathbf{\Lambda}\right) \triangleq \min_{k} \quad R_{k}\left(\mathbf{\Lambda}\right), \tag{19}$$

$$R_{k}\left(\mathbf{\Lambda}\right) \triangleq \mathsf{E}\left\{\log\det\left\{\mathbf{I}_{N_{\mathrm{r}}} + \mathbf{G}_{k}\mathbf{\Lambda}\mathbf{G}_{k}^{H}\right\}\right\}, \tag{20}$$

$$R_{\mathrm{ev,ub}}\left(\mathbf{\Lambda}\right) \triangleq \log\det\left\{\mathbf{I}_{N_{\mathrm{e}}} + \mathbf{A}_{\mathrm{ev}}\left(\mathbf{\Lambda}\right)\right\}. \tag{21}$$

Note that $R_{\mathrm{mc}}\left(\mathbf{\Lambda}\right)$ and $R_{\mathrm{ev,ub}}\left(\mathbf{\Lambda}\right)$ in the objective function of (18) are both concave functions with respect to $\mathbf{\Lambda}$ and therefore the problem in (18) is a difference of convex functions (d.c.) program. We adopt the CCCP [17] to solve this d.c. program. The CCCP is an iterative approach, where the basic idea is to first form a convex optimization problem via linearizing the second

term of the objective function $R_{\mathrm{ev,ub}}(\mathbf{\Lambda})$ at the current iteration and then solves it, which further yields the next iteration. In particular, the problem in (18) is tackled via iteratively solving the following sequence of convex optimization problems

$$\begin{aligned}\mathbf{\Lambda}^{(\ell+1)} = \arg\max_{\mathbf{\Lambda}} \quad & R_{\mathrm{mc}}(\mathbf{\Lambda}) - \mathsf{tr}\left\{\left(\frac{\partial}{\partial \mathbf{\Lambda}} R_{\mathrm{ev,ub}}\left(\mathbf{\Lambda}^{(\ell)}\right)\right)^{T}\mathbf{\Lambda}\right\}, \\ \text{s.t.} \quad & \mathsf{tr}\{\mathbf{\Lambda}\} \le P,\ \mathbf{\Lambda} \succeq \mathbf{0},\ \mathbf{\Lambda} \text{ diagonal},\end{aligned} \tag{22}$$

where ℓ is the iteration index, and the gradient of $R_{\mathrm{ev,ub}}(\mathbf{\Lambda})$ with respect to $\mathbf{\Lambda}$ is a diagonal matrix, whose kth diagonal element is given by

$$\left[\frac{\partial}{\partial \mathbf{\Lambda}} R_{\mathrm{ev,ub}}\left(\mathbf{\Lambda}^{(\ell)}\right)\right]_{k,k} = \sum_{i=1}^{N_{\mathrm{e}}} \frac{[\mathbf{\Omega}_{\mathrm{ev}}]_{i,k}}{1 + \sum_{j=1}^{M} [\mathbf{\Omega}_{\mathrm{ev}}]_{i,j} [\mathbf{\Lambda}^{(\ell)}]_{j,j}}. \tag{23}$$

According to [18], the solution sequence $\left\{\mathbf{\Lambda}^{(\ell)}\right\}_{\ell=0}^{\infty}$ generated by the CCCP in (22) is provable to converge to a local optimal point of the original problem in (16).

The computational complexity of the convex optimization problem in (22) in each iteration can still be prohibitive in practice if the expectation operation involved in the ergodic multicast rate is calculated via Monte-Carlo averaging over channel realizations. To overcome this difficulty, we further employ the large dimensional random matrix theory [19], [20] and use the DE of the ergodic rate in each iteration. By replacing the multicast rate with its DE, the sequence of convex optimization problems in (22) can be rewritten as

$$\begin{aligned}\mathbf{\Lambda}^{(\ell+1)} = \arg\max_{\mathbf{\Lambda}} \quad & \min_{k}\ \overline{R}_{k}^{(\ell)}(\mathbf{\Lambda}) - \mathsf{tr}\left\{\left(\frac{\partial}{\partial \mathbf{\Lambda}} R_{\mathrm{ev,ub}}\left(\mathbf{\Lambda}^{(\ell)}\right)\right)^{T}\mathbf{\Lambda}\right\}, \\ \text{s.t.} \quad & \mathsf{tr}\{\mathbf{\Lambda}\} \le P,\ \mathbf{\Lambda} \succeq \mathbf{0},\ \mathbf{\Lambda} \text{ diagonal}.\end{aligned} \tag{24}$$

In (24), $\overline{R}_{k}^{(\ell)}(\mathbf{\Lambda})$ is the DE expression of $R_k(\mathbf{\Lambda})$ in the ℓth iteration given by

$$\overline{R}_{k}^{(\ell)}(\mathbf{\Lambda}) = \log\det\left\{\mathbf{I}_M + \mathbf{\Gamma}_{k}^{(\ell)}\mathbf{\Lambda}\right\} + \log\det\left\{\widetilde{\mathbf{\Phi}}_{k}^{(\ell)}\right\} - \mathsf{tr}\left\{\widetilde{\mathbf{\Gamma}}_{k}^{(\ell)}\left(\widetilde{\mathbf{\Phi}}_{k}^{(\ell)}\right)^{-1}\right\}, \tag{25}$$

where $\mathbf{\Gamma}_{k}^{(\ell)} \in \mathbb{C}^{M\times M}$, $\widetilde{\mathbf{\Gamma}}_{k}^{(\ell)} \in \mathbb{C}^{N_{\mathrm{r}}\times N_{\mathrm{r}}}$, and $\widetilde{\mathbf{\Phi}}_{k}^{(\ell)} \in \mathbb{C}^{N_{\mathrm{r}}\times N_{\mathrm{r}}}$ can be obtained by solving the following fixed-point equations

$$\mathbf{\Gamma}_{k}^{(\ell)} = \mathbf{B}_k\left(\left(\widetilde{\mathbf{\Phi}}_{k}^{(\ell)}\right)^{-1}\right), \tag{26a}$$

Algorithm 1 Beam Domain Secure Multicast Power Allocation Algorithm

Input: An initial power allocation $\mathbf{\Lambda}^{(0)}$, the beam domain channel statistics $\mathbf{\Omega}_k$ and $\mathbf{\Omega}_{\mathrm{ev}}$, the preset threshold ϵ

Output: Beam domain power allocation matrix $\mathbf{\Lambda}$

1: Initialization: $\overline{R}^{(-1)} = 0$, $\ell = 0$
2: Calculate $\overline{R}^{(\ell)} = \min\limits_{k} \ \overline{R}_k^{(\ell)}\left(\mathbf{\Lambda}^{(\ell)}\right) - R_{\mathrm{ev,ub}}\left(\mathbf{\Lambda}^{(\ell)}\right)$ using (21) and (25)
3: **while** $\left|\overline{R}^{(\ell)} - \overline{R}^{(\ell-1)}\right| \geq \epsilon$ **do**
4: Update $\ell \leftarrow \ell + 1$
5: Calculate $\mathbf{\Lambda}^{(\ell)}$ via solving (24) with $\mathbf{\Lambda}^{(\ell-1)}$
6: Calculate $\overline{R}^{(\ell)} = \min\limits_{k} \ \overline{R}_k^{(\ell)}\left(\mathbf{\Lambda}^{(\ell)}\right) - R_{\mathrm{ev,ub}}\left(\mathbf{\Lambda}^{(\ell)}\right)$ using (21) and (25)
7: **end while**
8: Return $\mathbf{\Lambda} = \mathbf{\Lambda}^{(\ell)}$

$$\widetilde{\mathbf{\Gamma}}_k^{(\ell)} = \mathbf{C}_k\left(\mathbf{\Lambda}^{(\ell)}\left(\mathbf{I}_M + \mathbf{\Lambda}^{(\ell)}\mathbf{\Gamma}_k^{(\ell)}\right)^{-1}\right), \tag{26b}$$

$$\widetilde{\mathbf{\Phi}}_k^{(\ell)} = \mathbf{I}_{N_{\mathrm{r}}} + \widetilde{\mathbf{\Gamma}}_k^{(\ell)}, \tag{26c}$$

where $\mathbf{B}_k(\mathbf{X}) \triangleq \mathsf{E}\left\{\mathbf{G}_k^H\mathbf{X}\mathbf{G}_k\right\} \in \mathbb{C}^{M\times M}$ and $\mathbf{C}_k(\mathbf{X}) \triangleq \mathsf{E}\left\{\mathbf{G}_k\mathbf{X}\mathbf{G}_k^H\right\} \in \mathbb{C}^{N_{\mathrm{r}}\times N_{\mathrm{r}}}$ are both matrix-valued functions which both output diagonal matrices with the corresponding ith diagonal elements given by

$$\left[\mathbf{B}_k(\mathbf{X})\right]_{i,i} = \mathsf{tr}\left\{\mathsf{diag}\left\{\left[\mathbf{\Omega}_k\right]_{:,i}\right\}\mathbf{X}\right\}, \tag{27}$$

$$\left[\mathbf{C}_k(\mathbf{X})\right]_{i,i} = \mathsf{tr}\left\{\mathsf{diag}\left\{\left(\left[\mathbf{\Omega}_k\right]_{i,:}\right)^T\right\}\mathbf{X}\right\}, \tag{28}$$

respectively. The DE expression $\overline{R}_k^{(\ell)}(\mathbf{\Lambda})$ can be efficiently calculated using the channel statistics $\mathbf{\Omega}_k$ in a few fixed-point iterations without exhaustive averaging via the Monte-Carlo approach, and thus the computational complexity of the optimization problem in (22) can be significantly reduced.

It is worth noting that the DE expression $\overline{R}_k^{(\ell)}(\mathbf{\Lambda})$ is a quite tight approximation of $R_k(\mathbf{\Lambda})$ even in the case of small numbers of antennas [19], [20]. In addition, we can observe from (25) that $\overline{R}_k(\mathbf{\Lambda})$ is still concave with respect to $\mathbf{\Lambda}$. Thus, each sub-problem in (24) is still convex and can be efficiently solved using standard convex optimization methods, and the solution sequence is still guaranteed to converge. The proposed beam domain power allocation algorithm for secure massive MIMO multicast transmission using CCCP and DE is formally described in Algorithm 1.

$$R_k\left(\mathbf{\Lambda}_1, \mathbf{\Lambda}_2, \ldots, \mathbf{\Lambda}_K\right) = R_{k,1}\left(\mathbf{\Lambda}_1, \mathbf{\Lambda}_2, \ldots, \mathbf{\Lambda}_K\right) - R_{k,2}\left(\mathbf{\Lambda}_1, \mathbf{\Lambda}_2, \ldots, \mathbf{\Lambda}_K\right) \tag{29}$$

$$R_{k,1}\left(\mathbf{\Lambda}_1, \mathbf{\Lambda}_2, \ldots, \mathbf{\Lambda}_K\right) = \mathsf{E}\left\{\log\det\left\{\overline{\mathbf{K}}_k + \mathbf{G}_k \mathbf{\Lambda}_k \mathbf{G}_k^H\right\}\right\} \tag{30}$$

$$R_{k,2}\left(\mathbf{\Lambda}_1, \mathbf{\Lambda}_2, \ldots, \mathbf{\Lambda}_K\right) = \log\det\left\{\overline{\mathbf{K}}_k\right\} + \log\det\left\{\overline{\mathbf{K}}_k^{\mathrm{eve}}\right\} \tag{31}$$

$$\overline{\mathbf{K}}_k = \mathbf{I} + \sum_{j \neq k} \mathsf{E}\left\{\mathbf{G}_k \mathbf{\Lambda}_j \mathbf{G}_k^H\right\} \tag{32}$$

$\mathbf{A}_k\left(\mathbf{X}\right) \triangleq \mathsf{E}\left\{\mathbf{G}_k \mathbf{X} \mathbf{G}_k^H\right\} \in \mathbb{C}^{N_{\mathrm{e}} \times N_{\mathrm{e}}}$ is a matrix-valued function which outputs a diagonal matrix with the ith diagonal element given by

$$\left[\mathbf{A}_k\left(\mathbf{X}\right)\right]_{n,n} = \mathsf{tr}\left\{\mathsf{diag}\left\{\left(\left[\mathbf{\Omega}_k\right]_{n,:}\right)^T\right\}\mathbf{X}\right\} = \sum_{q=1}^{M}\left[\mathbf{\Omega}_k\right]_{n,q}\left[\mathbf{X}\right]_{q,q} \tag{33}$$

$$\overline{\mathbf{K}}_k^{\mathrm{eve}} = \mathbf{I} + \mathsf{E}\left\{\mathbf{G}^{\mathrm{eve}} \mathbf{\Lambda}_k \left(\mathbf{G}^{\mathrm{eve}}\right)^H\right\} \tag{34}$$

first-order Taylor series expansion

$$\begin{aligned} R_{k,2}\left(\mathbf{\Lambda}_1, \mathbf{\Lambda}_2, \ldots, \mathbf{\Lambda}_K\right) = {} & R_{k,2}\left(\mathbf{\Lambda}_1^{(\ell)}, \mathbf{\Lambda}_2^{(\ell)}, \ldots, \mathbf{\Lambda}_K^{(\ell)}\right) \\ & + \sum_{i=1}^{K} \mathsf{tr}\left\{\left(\frac{\partial}{\partial \mathbf{\Lambda}_i} R_{k,2}\left(\mathbf{\Lambda}_1^{(\ell)}, \mathbf{\Lambda}_2^{(\ell)}, \ldots, \mathbf{\Lambda}_K^{(\ell)}\right)\right)^T \left(\mathbf{\Lambda}_i - \mathbf{\Lambda}_i^{(\ell)}\right)\right\} \end{aligned} \tag{35}$$

$$\frac{\partial}{\partial \mathbf{\Lambda}_i} R_{k,2}\left(\mathbf{\Lambda}_1^{(\ell)}, \mathbf{\Lambda}_2^{(\ell)}, \ldots, \mathbf{\Lambda}_K^{(\ell)}\right) = \frac{\partial}{\partial \mathbf{\Lambda}_i}\log\det\left\{\overline{\mathbf{K}}_k\right\} + \frac{\partial}{\partial \mathbf{\Lambda}_i}\log\det\left\{\overline{\mathbf{K}}_k^{\mathrm{eve}}\right\} \tag{36}$$

when $i \neq k$,

$$\left[\frac{\partial}{\partial \mathbf{\Lambda}_i}\log\det\left\{\overline{\mathbf{K}}_k\right\}\right]_{m,m} = \frac{\partial}{\partial\left[\mathbf{\Lambda}_i\right]_{m,m}}\log\det\left\{\overline{\mathbf{K}}_k\right\}$$

$$
\begin{aligned}
&= \frac{\partial}{\partial \left[\mathbf{\Lambda}_i\right]_{m,m}} \log\det\left\{\mathbf{I} + \sum_{j\neq k} \mathsf{E}\left\{\mathbf{G}_k \mathbf{\Lambda}_j \mathbf{G}_k^H\right\}\right\} \\
&= \frac{\partial}{\partial \left[\mathbf{\Lambda}_i\right]_{m,m}} \sum_{n=1}^{N_k} \log\left(1 + \sum_{j\neq k}\sum_{q=1}^{M} \left[\mathbf{\Omega}_k\right]_{n,q} \left[\mathbf{\Lambda}_j\right]_{q,q}\right) \\
&= \sum_{n=1}^{N_k} \frac{\partial}{\partial \left[\mathbf{\Lambda}_i\right]_{m,m}} \log\left(1 + \sum_{j\neq k}\sum_{q=1}^{M} \left[\mathbf{\Omega}_k\right]_{n,q} \left[\mathbf{\Lambda}_j\right]_{q,q}\right) \\
&= \sum_{n=1}^{N_k} \frac{\left[\mathbf{\Omega}_k\right]_{n,m}}{1 + \sum_{j\neq k}\sum_{q=1}^{M} \left[\mathbf{\Omega}_k\right]_{n,q} \left[\mathbf{\Lambda}_j\right]_{q,q}}
\end{aligned} \tag{37}
$$

$$
\log\det\left\{\mathbf{I} + \sum_{j\neq k} \mathsf{E}\left\{\mathbf{G}_k \mathbf{\Lambda}_j \mathbf{G}_k^H\right\}\right\} = \sum_{n=1}^{N_k} \log\left(1 + \sum_{j\neq k}\sum_{q=1}^{M} \left[\mathbf{\Omega}_k\right]_{n,q} \left[\mathbf{\Lambda}_j\right]_{q,q}\right) \tag{38}
$$

IV. Conclusion

In this letter, we have studied physical layer secure multicast transmission for massive MIMO with only statistical CSI of the legitimate UTs and the eavesdropper available at the BS. We first introduced a tight lower bound of the achievable secrecy multicast rate. We then showed the optimal multicast signaling directions, which simplifies the optimal multicast transmit covariance matrix design into a beam domain power allocation problem. An efficient iterative beam domain power allocation algorithm, which is guaranteed to converge to a local optimal solution, was proposed based on the CCCP and the large dimensional random matrix theory. The performance gains of the proposed approach over the conventional approach were demonstrated via numerical results.

Appendix
Proof of Proposition 1

From (12) and (13), we can observe that the off-diagonal elements of $\mathbf{V}^H\mathbf{Q}\mathbf{V}$ do not affect the value of $R_{\text{ev,ub}}$. In addition, as R_{mc} is a concave function with respect to $\mathbf{V}^H\mathbf{Q}\mathbf{V}$, we can show that $\mathbf{V}^H\mathbf{Q}\mathbf{V}$ should be diagonal to maximize R_{mc} using a proof technique similar to that presented in [21]. Moreover, the multicast power $\mathsf{tr}\left\{\mathbf{Q}\right\}$ is only related to the diagonal elements of $\mathbf{V}^H\mathbf{Q}\mathbf{V}$. Therefore, we can obtain that the objective of problem (16) can be maximized provided that $\mathbf{V}^H\mathbf{Q}\mathbf{V}$ is diagonal. This concludes the proof.

REFERENCES

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

[2] D. Lecompte and F. Gabin, "Evolved multimedia broadcast/multicast service (eMBMS) in LTE-advanced: Overview and Rel-11 enhancements," *IEEE Commun. Mag.*, vol. 50, no. 11, pp. 68–74, Nov. 2012.

[3] Z. Xiang, M. Tao, and X. Wang, "Massive MIMO multicasting in noncooperative cellular networks," *IEEE J. Sel. Areas Commun.*, vol. 32, no. 6, pp. 1180–1193, Jun. 2014.

[4] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 3, pp. 1550–1573, 3rd Quart. 2014.

[5] 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.

[6] J. Wang, J. Lee, F. Wang, and T. Q. S. Quek, "Jamming-aided secure communication in massive MIMO Rician channels," *IEEE Trans. Wireless Commun.*, vol. 14, no. 12, pp. 6854–6868, Dec. 2015.

[7] 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.

[8] 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.

[9] X. Liu, F. Gao, G. Wang, and X. Wang, "Joint beamforming and user selection in multicast downlink channel under secrecy-outage constraint," *IEEE Commun. Lett.*, vol. 18, no. 1, pp. 82–85, Jan. 2014.

[10] M. F. Hanif, L.-N. Tran, M. Juntti, and S. Glisic, "On linear precoding strategies for secrecy rate maximization in multiuser multiantenna wireless networks," *IEEE Trans. Signal Process.*, vol. 62, no. 14, pp. 3536–3551, Jul. 2014.

[11] B. Wang and P. Mu, "Artificial noise-aided secure multicasting design under secrecy outage constraint," *IEEE Trans. Commun.*, vol. 65, no. 12, pp. 5401–5414, Dec. 2017.

[12] 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.

[13] 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.

[14] X. Q. Gao, B. Jiang, X. Li, A. B. Gershman, and M. R. McKay, "Statistical eigenmode transmission over jointly correlated MIMO channels," *IEEE Trans. Inf. Theory*, vol. 55, no. 8, pp. 3735–3750, Aug. 2009.

[15] 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.

[16] 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.

[17] A. L. Yuille and A. Rangarajan, "The concave-convex procedure," *Neural Comput.*, vol. 15, no. 4, pp. 915–936, Apr. 2003.

[18] 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.

[19] R. Couillet and M. Debbah, *Random Matrix Methods for Wireless Communications*. New York, NY, USA: Cambridge Univ. Press, 2011.

[20] 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.

[21] 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.