IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received April 2, 2019, accepted April 27, 2019, date of publication April 30, 2019, date of current version May 13, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2914028

Secrecy Analysis and Active Pilot Spoofing Attack Detection for Multigroup Multicasting Cell-Free Massive MIMO Systems

XIANYU ZHANG[1], DAOXING GUO[1], (Member, IEEE), KANG AN[2], ZHIGUO DING[3], (Senior Member, IEEE), AND BANGNING ZHANG[1], (Member, IEEE)

[1]College of Communication Engineering, Army Engineering University of PLA, Nanjing 210007, China
[2]Sixth-Third Research Institute, National University of Defense Technology, Nanjing 210007, China
[3]School of Electrical and Electronic Engineering, University of Manchester, Manchester M13 9PL, U.K.

Corresponding author: Xianyu Zhang (zhangxy_sat@126.com)

This work was supported by the Natural Science Foundation of China under Grant 61471392 and Grant 61771486.

ABSTRACT In this paper, we investigate the secure transmission in multigroup multicasting cell-free massive MIMO system in the presence of pilot spoofing attack. With the imperfect uplink and downlink channel estimation, a distributed conjugate beamforming processing with normalized power constraint policy is exploited at access points (APs) for downlink multicasting data transmission. Closed-form expressions for the per-user achievable rate are derived with and without downlink training, respectively. Also, the analytical results of the upper bound on the information leakage to eavesdropper are carried out. Moreover, a mechanism based on the minimum description length (MDL) is presented to detect pilot spoofing attack. Consequently, the achievable ergodic secrecy rate is obtained to evaluate the system's secrecy performance. The numerical results are presented to quantitatively analyze the impacts of eavesdropper's spoofing pilot power and the number of groups on the secrecy performance of the considered systems.

INDEX TERMS Physical layer security, cell-free massive MIMO, multigroup multicasting, pilot spoofing attack.

I. INTRODUCTION

Cell-Free massive multiple-input multiple-output (MIMO) is a promising network architecture where many geographically distributed access points (APs) jointly serve some users in the same frequency-time resource [1]. Compared to both small cell and co-located massive MIMO, Cell-Free massive MIMO can offer very high coverage, spectral and energy efficiency by exploiting the advantages of both network MIMO and colocated massive MIMO systems [2], [3]. Moreover, multigroup multicasting is an appealing scenario for massive MIMO due to the increasing demand for the multicasting applications [4], such as group communications, software updates, news headlines and mobile TV. In general, multicasting involves multiple groups where the users in each group are interested in different multicasting data streams, which has been incorporated in 3GPP Rel-9 known as evolved multimedia broadcast/multicasting service (eMBMS) [5].

In recent years, many aspects including of performance analysis, power control and beamforming in Cell-Free massive MIMO networks have been further studied [1], [2],5,6. Additionally, as a supplement, a user-centric (UC) virtual-cell massive MIMO approach has been proposed to improve the system performance [6]. Via time-division duplex (TDD) operation, channel state information (CSI) can be acquired by uplink training exploiting the channel reciprocity property in Cell-Free massive MIMO systems. Due to the channel hardening, downlink data can be reliably decoded using only statistical CSI [1], [2]. However, the channel hardening is less pronounced in Cell-Free massive MIMO owing to the wide geographic distribution. In this case, downlink pilots have the potential to improve the achievable information rate [8]. In addition, some researchers recently have investigated the performance of the multigroup multicasting massive MIMO systems. Authors in [4] investigated the optimal multicasting beamformer design and analyzed the asymptotic performance of the proposed scheme. Authors in [9] presented the asymptotic performance of multi-cell multi-group massive multicasting MIMO systems under

The associate editor coordinating the review of this manuscript and approving it for publication was Luyu Zhao.

pilot contamination. Different from [4] and [9], the closed-form net throughput of the multigroup multicasting Cell-Free massive MIMO system has been presented in [10] which has taken into account the imperfect estimated channel state information (CSI).

Different from the traditional higher-layer cryptographic techniques, physical layer security has been proposed based on the principles of information theoretic security which exploits the inherent randomness of the wireless medium to achieve perfect secrecy with remarkably low computational complexity [11]. In MIMO scenario, confidential messages can be spatially multiplexed onto multiple independent subchannels which may change drastically over frequency, time and space [12]. Therefore, signal processing techniques in the physical layer (e.g., secrecy beamforming and precoding, artificial noise etc.) can be exploited to enhance secrecy by enlarging substantial signal quality differences at the destination and the eavesdropper [13]. As one of the emerging and most promising techniques, large-scale antenna systems (massive MIMO) can provide extremely high spectral efficiency which can help to meet the anticipated demands in the fifth generation (5G) era [14]. The integration of physical layer security in massive MIMO communication systems is a very promising domain. The passive eavesdropping and active attacks have been well considered in [15], [16] and [17], which verifies that massive MIMO is robust against passive attacks while it is seriously threatened by active attacks. Due to the serious damages, active eavesdropping has attracted much attention. An active eavesdropper can attack the channel training phase by transmitting the same pilot sequence, which is the so-called pilot spoofing attacks [18]. In particular, Wu *et al.* studied the secure transmission schemes in multi-user multi-cell massive MIMO systems with a multi-antenna active eavesdropper by exploiting matched filter precoding and artificial noise (AN) generation [19]. However, they only focused on co-located massive MIMO network. The authors in [20] investigated the secure transmission of the Cell-Free massive MIMO system under a pilot spoofing attack, which also provided optimal power allocation schemes to maximize the achievable data rate or achievable secrecy rate. Moreover, authors in [21] firstly studied the security aspect of multigroup multicasting Cell-Free massive MIMO systems and provided the closed-form expressions for the achievable secrecy rate. However, only uplink training was considered in this paper. To mitigate the significant information leakage, it is of crucial importance to be aware of the pilot contamination attack. Authors in [22] presented three different schemes (at base station, intended user, or jointly) for detecting active eavesdropping. In addition, some slowly changing parameters including signal power, large-scale fading, or certain statistics can be exploited in detection schemes [18], [23]. Specially, Minimum description length (MDL) is one simple but favorable information theoretic criteria for determining the number of present signals which has been successfully utilized for active attack detection in multi-antenna systems [24], [25].

Inspired by these works, this paper studies the secure communication and active attack detection of multigroup multicasting Cell-Free massive MIMO network with both uplink and downlink training. And the closed-form secrecy rate expression is provided. Most importantly, this is the first work on the integration of security with the multigroup multicasting Cell-Free massive MIMO network with both uplink and downlink training in the presence of active spoofing attack. Main contributions of this paper are summarized as follows:

- For the classical multigroup multicasting Cell-Free massive MIMO network, the secure transmission under active spoofing attack has been considered. We consider a new scheme with both uplink and downlink training. Besides, the conjugate beamforming is used for downlink data transmission and downlink training, which takes imperfect channel estimation into account.
- We consider two different schemes, namely, one only with the conventional uplink training and the other with both uplink and downlink training. Under the assumption that the eavesdropper can acquire perfect CSI, we derive the closed-form expressions of the achievable information rate of legitimate user and information leakage to the eavesdropper, which show that the active spoofing attack is dangerous for secure communication of the considered systems.
- Motivated by minimizing the damages caused by the pilot spoofing attack, we propose a novel effective approach based on MDL criterion to detect the active attackers. In this scheme, new pilot signals are designed for active attack detection. Then, the detection is operated by computing the subspace dimension of the received signal correlation matrix.

The rest of the paper is outlined as follows. In Section II, we describe the system model, also introduce the uplink training, downlink multicasting data transmission and downlink training. Section III derives the secrecy performance analysis on the considered system. Section IV presents an active spoofing attack detection algorithm. Simulation results are presented in Section V. Finally, Section VI concludes the paper.

Notations: Boldface letters represent the vector, e.g. $\mathbf{h}$. $(\cdot)^T$, $(\cdot)^*$ and $(\cdot)^H$ stand for transpose, conjugate and conjugate-transpose. $\mathbb{E}\{\cdot\}$ and $\mathrm{Var}\{\cdot\}$ denote operations of expectation and variance, respectively. A circularly symmetric complex Gaussian random vector $\mathbf{x}$ with mean $\mathbf{m}$ and covariance matrix $\mathbf{A}$ can be denoted by $\mathbf{x} \sim \mathcal{CN}(\mathbf{m}, \mathbf{A})$. $\mathbb{C}^{M\times N}$ stands for $M \times N$ dimensional complex space. In addition, i.i.d indicates the abbreviation of independent and identically distributed.

II. SYSTEM MODEL

We consider a multigroup multicasting Cell-Free massive MIMO system with M single-antenna APs in the presence of an active eavesdropper (Eve) as shown in Fig. 1. It is assumed that the cell has N groups where each group has K

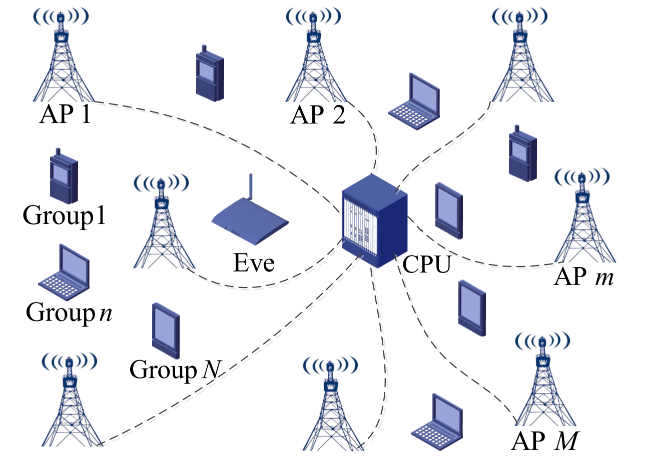

FIGURE 1. Illustration of secure multigroup multicasting Cell-Free massive MIMO system with M APs and N groups in the presence of an active Eve.

single-antenna users. All users in the same group request the same message. Moreover, all APs are connected to a central processing unit (CPU) via perfect backhaul links to share and exchange information. Let $g_{mn_k} = \beta_{mn_k}^{1/2} h_{mn_k}$ ($g_{mE} = \beta_{mE}^{1/2} h_{mE}$) be the channel coefficient between the kth user in the nth group (Eve) and the mth AP, where β_{mn_k} (β_{mE}) denotes the large scale fading known in advance and h_{mn_k} (h_{mE}) $\sim \mathcal{CN}(0,1)$ implies the small scale fading. To utilize the channel reciprocity property, TDD protocol is considered in this letter. This transmission protocol allows utilizing uplink training to obtain the CSI. An intelligent active Eve can pretend to be one legitimate user node in the target group and sends the same pilot sequence as legitimate users to attack the uplink training. In most previous studies, users always decode the downlink data using only statistical CSI without downlink training. To obtain performance improvements in Cell-Free massive MIMO systems, users can exploit the instantaneous CSI by downlink training to operate signal detection. In this paper, we consider both uplink and downlink training.

A. UPLINK TRAINING

It is important to obtain the CSI to perform the precoding at APs and data detection at user terminals. All APs can obtain the CSI by uplink training. As the same scheme in [8], [10], different groups are allocated different pair wisely orthogonal pilot sequences of length τ_p (all users in the same group use the same pilot sequence). Let $\sqrt{\tau_p}\boldsymbol{\varphi}_n \in \mathbb{C}^{\tau_p \times 1}$, where $\left\|\boldsymbol{\varphi}_n\right\|^2 = 1$, $\tau_p \geq N$, be the pilot sequence sent by the users in nth group. In general, as the pilot sequences are public and standardized, Eve can easily spoof to send the same pilot as legitimate users to change the beam direction. Without loss of generality, we assume that Eve aims to intercept the confidential messages intended for the nth group, that is, $\sqrt{\tau_p}\boldsymbol{\varphi}_E = \sqrt{\tau_p}\boldsymbol{\varphi}_n$, where $\sqrt{\tau_p}\boldsymbol{\varphi}_E$ denotes the pilot sequence of Eve. Hence, the received pilot vector at the mth AP is given by

$$\mathbf{y}_m^{(p)} = \sqrt{\tau_p \rho_u} \sum_{n'=1}^{N} \sum_{k=1}^{K} g_{mn'_k} \boldsymbol{\varphi}_{n'} + \sqrt{\tau_p \rho_E} g_{mE} \boldsymbol{\varphi}_n + \boldsymbol{\omega}_m, \quad (1)$$

where ρ_u (ρ_E) represents the normalized average signal-to-noise ratio (SNR) of user (Eve) uplink pilot symbol, and $\boldsymbol{\omega}_m$ is the additive white Gaussian noise (AWGN) vector with $\boldsymbol{\omega}_m \sim \mathcal{CN}(\mathbf{0}, \mathbf{I})$. By projecting $\mathbf{y}_m^{(p)}$ onto $\boldsymbol{\varphi}_{n'}$, we can rewrite the processed signal as

$$\tilde{y}_{mn'}^{(p)} = \sqrt{\tau_p \rho_u} \sum_{k=1}^{K} g_{mn'_k} + \sqrt{\tau_p \rho_E} g_{mE} \delta\left(n' - n\right) + \varphi_{n'}^{H} \omega_m, \quad (2)$$

where $\delta(0) = 1$ and $\delta(n) = 0, n \neq 0$. Then minimum mean squared error (MMSE) approach is adopted to estimate the channels as

$$\hat{g}_{mn'_{k'}} = \frac{\sqrt{\tau_p \rho_u} \beta_{mn'_{k'}} \tilde{y}_{mn'}^{(p)}}{1 + \tau_p \rho_u \sum_{k=1}^{K} \beta_{mn'_k} + \tau_p \rho_E \beta_{mE} \delta(n' - n)}. \quad (3)$$

Since $\tilde{y}_{mn'}^{(p)}$ follows Gaussian distribution, we can denote that $\hat{g}_{mn'_{k'}} = \sqrt{\gamma_{mn'_{k'}}} z_{mn'}$, where $z_{mn'} \sim \mathcal{CN}(0, 1)$ and

$$\gamma_{mn'_{k'}} = \frac{\tau_p \rho_u \beta_{mn'_{k'}}^2}{1 + \tau_p \rho_u \sum_{k=1}^{K} \beta_{mn'_k} + \tau_p \rho_E \beta_{mE} \delta(n' - n)}.$$

Similarly, the estimate of Eve's channel can be given by $\hat{g}_{mE} = \sqrt{\gamma_{mE}} z_{mn}$ with $\gamma_{mE} = \frac{\tau_p \rho_E \beta_{mE}^2}{1 + \tau_p \rho_u \sum_{k=1}^{K} \beta_{mn_k} + \tau_p \rho_E \beta_{mE}}$.

B. DOWNLINK MULTICASTING TRANSMISSION

In order to avoid sharing of CSI and exchanging data among the APs or the CPU, the conjugate beamforming is exploited to precode the messages to all groups [4], [8], [10]. The set of messages to all multicasting groups is represented by $\mathbf{s} = \{s_1, s_2, \cdots, s_N\}$, $\mathbb{E}\left\{|s_i|^2\right\} = 1$, $i = 1, 2, \cdots, N$. Then, with the acquired CSI from the uplink training, the transmit multicasting signal at the mth AP is given by

$$x_m = \sqrt{\frac{\rho_d}{N}} \sum_{n=1}^{N} \frac{z_{mn}^*}{|z_{mn}|} s_n, \quad (4)$$

where ρ_d is the normalized SNR at downlink transmission. Note that, all APs simultaneously transmit signals to all users. We denote the received signal at the kth user in the nth group and Eve as

$$\begin{cases} y_{n_k} = \sqrt{\rho_d} a_{n_k} s_n + \sqrt{\rho_d} \sum\limits_{n' \neq n}^{N} a_{n'_k} s_{n'} + \omega_{n_k} \\ y_E = \sqrt{\rho_d} a_{nE} s_n + \sqrt{\rho_d} \sum\limits_{n' \neq n}^{N} a_{n'E} s_{n'} + \omega_E \end{cases}, \quad (5)$$

where $a_{n_k} \triangleq \sum_{m=1}^{M} \sqrt{\frac{1}{N}} \frac{g_{mn_k} z_{mn}^*}{|z_{mn}|}$, $a_{n'_k} \triangleq \sum_{m=1}^{M} \sqrt{\frac{1}{N}} \frac{g_{mn_k} z_{mn'}^*}{|z_{mn'}|}$, $a_{nE} \triangleq \sum_{m=1}^{M} \sqrt{\frac{1}{N}} \frac{g_{mE} z_{mn}^*}{|z_{mn}|}$, $a_{n'E} \triangleq \sum_{m=1}^{M} \sqrt{\frac{1}{N}} \frac{g_{mE} z_{mn'}^*}{|z_{mn'}|}$, $\omega_{n_k} \sim \mathcal{CN}(0,1)$ and $\omega_E \sim \mathcal{CN}(0, 1)$ are additive noise components.

C. DOWNLINK TRAINING

Thanks to channel hardening in massive MIMO, the users can use only the channel statistics, i.e., $\mathbb{E}\left\{a_{n_k}\right\}$, to decode the downlink data. Hence, most existing works assume there is no downlink training. However, in a Cell-Free system, due to the large distribution area of the APs, each user is effectively served by finite APs [8]. Especially for a moderately large M, channel hardening does not hold, and hence, downlink training can be operated to achieve more accurate CSI.

To avoid information exchange among the APs, the Beamforming Training scheme is adopted for downlink training. In this letter, the downlink pilots are beamformed to the groups. The overhead of this pilot scheme is independent of M which depends on the number of the groups as well as uplink training.

Let $\sqrt{\tau_{d,p}}\boldsymbol{\psi}_n \in \mathbb{C}^{\tau_{d,p}\times 1}$ be the downlink pilot sequence for nth group, where $\left\|\boldsymbol{\psi}_n\right\|^2 = 1$, $\tau_{d,p} \geq N$. Moreover, the APs exploit the same beamforming scheme as multicasting data transmission to precode the downlink pilot sequences. The precoded pilot sequence at mth AP can be denoted by

$$\mathbf{x}_{m,p} = \sqrt{\frac{\tau_{d,p}\rho_{d,p}}{N}} \sum_{n=1}^{N} \frac{z_{mn}^{*}}{|z_{mn}|} \boldsymbol{\psi}_n, \tag{6}$$

where $\rho_{d,p}$ is the total normalized average SNR of downlink pilot sequence at mth AP, and $\boldsymbol{\psi}_n$ $(n = 1, 2, \cdots, N)$ are assumed pairwise orthogonal, i.e. $\boldsymbol{\psi}_{n'}^{H}\boldsymbol{\psi}_n = 0$, $n' \neq n$. Then the received signal at the kth user in the nth group can be denoted by

$$\mathbf{y}_{dp,n_k} = \sqrt{\tau_{d,p}\rho_{d,p}} \sum_{n'=1}^{N} a_{n'_k}\boldsymbol{\psi}_{n'} + \mathbf{w}_{dp,n_k}, \tag{7}$$

where $\mathbf{w}_{dp,n_k}$ represents the additive noise vector at the kth user in the nth group with i.i.d $\mathcal{CN}(0, 1)$ random variable elements.

In order to estimate the effective channel gain a_{n_k}, the received downlink pilot signal $\mathbf{y}_{dp,n_k}$ can be firstly projected onto $\boldsymbol{\psi}_n$ as

$$\begin{aligned} \bar{y}_{dp,n_k} &= \boldsymbol{\psi}_n^{H}\mathbf{y}_{dp,n_k} = \sqrt{\tau_{d,p}\rho_{d,p}}a_{n_k} + \boldsymbol{\psi}_n^{H}\mathbf{w}_{dp,n_k} \\ &= \sqrt{\tau_{d,p}\rho_{d,p}}a_{n_k} + w_{dp,n_k}, \end{aligned} \tag{8}$$

where $w_{dp,n_k} = \boldsymbol{\psi}_n^{H}\mathbf{w}_{dp,n_k} \sim \mathcal{CN}(0, 1)$. Then the linear MMSE estimation is performed to estimate a_{n_k} as

$$\begin{aligned} \hat{a}_{n_k} = \mathbb{E}\left\{a_{n_k}\right\} &+ \frac{\sqrt{\tau_{d,p}\rho_{d,p}}\mathrm{Var}\left\{a_{n_k}\right\}}{\tau_{d,p}\rho_{d,p}\mathrm{Var}\left\{a_{n_k}\right\} + 1} \\ &\times \left(\bar{y}_{dp,n_k} - \sqrt{\tau_{d,p}\rho_{d,p}}\mathbb{E}\left\{a_{n_k}\right\}\right). \end{aligned} \tag{9}$$

III. SECRECY PERFORMANCE ANALYSIS

To obtain the achievable secrecy rate, the achievable information rates of legitimate users and Eve should be investigated respectively. Firstly, we consider the scheme only with uplink training. Due to the property of channel hardening, legitimate users can utilize the statistics, i.e. $\mathbb{E}\left\{a_{n_k}\right\}$, as the real a_{n_k} to detect s_n. And the other terms can be treated as effective noise. Provided that the worst-case Gaussian noise argument, we obtain a lower bound for the achievable rate* given in (10), as shown at the top of the next page. Note that downlink training has not been used in the above scheme.

Then, we focus on the situation with both uplink and downlink training. As a_{n_k} is the sum of many terms, it is asymptotically Gaussian distributed. With MMSE estimate scheme, the effective channel gain can be denoted by $a_{n_k} = \hat{a}_{n_k} + \tilde{a}_{n_k}$, where estimation error $\tilde{a}_{n_k}$ is independent with $\hat{a}_{n_k}$. Hence, the achievable downlink rate of the aim user can be written as (11), as shown at the top of the next page.

On the other hand, to consider the worst case in terms of security, we assume that Eve perfectly knows channel gains. Hence, Eve can get the upper bound on the eavesdropping information rate, which can be represented as

$$R_{nE} = \log_2\left(1 + \frac{\rho_d \mathbb{E}\left\{|a_{nE}|^2\right\}}{\rho_d \sum\limits_{n'\neq n}^{N} \mathbb{E}\left\{|a_{n'E}|^2\right\} + 1}\right). \tag{12}$$

Besides, this paper only considers one eavesdropper equipped with only a single antenna. If there are multiple eavesdroppers or eavesdropper equipped with multiple antennas existing in the networks which can be called as the multiple-input, multiple-output, multiantenna eavesdropper (MIMOME). According to some existing literatures [12], [26], the model in this paper can be extended to MIMOME scenario by utilizing secrecy precoding (or beamforming) and random matrix theory. As this issue is outside the scope of this paper, it can be left for future works.

Based on (10), (11) and (12), we can obtain the lower bound of the achievable secrecy rate as follows:

$$R_n^{\mathrm{sec}} = \left[\min_{k=1,2,\cdots,K}\left\{R_{n_k}\right\} - R_{nE}\right]^{+}, \tag{13}$$

where $[x]^{+} = \max\{0, x\}$.

Theorem 1: With the active pilot spoofing attack, imperfect channel estimation and conjugate beamforming, the closed-form expression of the achievable rate of kth user in nth group is given by (14), as shown at the top of the next page, where ς_{n_k} is defined as $\varsigma_{n_k} \overset{\Delta}{=} \frac{\sum_{m=1}^{M}\beta_{mn_k} - \sum_{m=1}^{M}\frac{\pi}{4}\gamma_{mn_k}}{\tau_{d,p}\rho_{d,p}\left(\sum_{m=1}^{M}\beta_{mn_k} - \sum_{m=1}^{M}\frac{\pi}{4}\gamma_{mn_k}\right)+N}$.

And the information intended to nth group leaked to Eve can be given by (15), as shown at the top of the next page.

Proof: Please see Appendix A.

IV. ACTIVE ATTACK DETECTION

According to the above analysis, pilot spoofing attack injures channel estimation to achieve a significant information leakage to Eve. To migrate this effect, we can operate pilot

*Strictly speaking, the derived results are spectral efficiency (bits/s/Hz) as bandwidth hasn't been considered at the expressions of R_{n_k} and R_{nE}.

$$R_{n_k}=\log_2\left(1+\frac{\rho_d\left|\mathbb{E}\left\{a_{n_k}\right\}\right|^2}{\rho_d\mathrm{Var}\left\{a_{n_k}\right\}+\rho_d\sum\limits_{n'\neq n}^{N}\mathbb{E}\left\{\left|a_{n'_k}\right|^2\right\}+1}\right). \tag{10}$$

$$R_{n_k}=\log_2\left(1+\frac{\rho_d\left|\hat{a}_{n_k}\right|^2}{\rho_d\mathbb{E}\left\{\left|\tilde{a}_{n_k}\right|^2\right\}+\rho_d\sum\limits_{n'\neq n}^{N}\mathbb{E}\left\{\left|a_{n'_k}\right|^2\right\}+1}\right). \tag{11}$$

$$R_{n_k}=\begin{cases}\log_2\left(1+\dfrac{\dfrac{\pi\rho_d}{4N}\left(\sum\limits_{m=1}^{M}\sqrt{\gamma_{mn_k}}\right)^2}{\rho_d\sum\limits_{m=1}^{M}\beta_{mn_k}-\dfrac{\pi\rho_d}{4N}\sum\limits_{m=1}^{M}\gamma_{mn_k}+1}\right), & \text{Only with uplink training,}\\ \log_2\left(1+\dfrac{\rho_d\left|\hat{a}_{n_k}\right|^2}{\rho_d\varsigma_{n_k}+\dfrac{(N-1)\rho_d}{N}\sum\limits_{m=1}^{M}\beta_{mn_k}+1}\right), & \text{With both uplink and downlink training.}\end{cases} \tag{14}$$

$$R_{nE}=\log_2\left(1+\frac{\frac{\rho_d}{N}\sum\limits_{m=1}^{M}\beta_{mE}+\frac{\pi\rho_d}{4N}\sum\limits_{m=1}^{M}\sum\limits_{i\neq m}^{M}\sqrt{\gamma_{mE}\gamma_{iE}}}{\frac{N-1}{N}\rho_d\sum\limits_{m=1}^{M}\beta_{mE}+1}\right). \tag{15}$$

$$\mathbf{y}_m=\left(\sqrt{\tau_p(1-\phi)\rho_u}\sum_{k=1}^{K}g_{mn_k}+\sqrt{\tau_p\rho_E}g_{mE}\right)\boldsymbol{\varphi}_n+\sqrt{\tau_p\phi\rho_u}\sum_{k=1}^{K}g_{mn_k}\cdot\boldsymbol{\varphi}_r+\boldsymbol{\omega}_m. \tag{16}$$

spoofing attack detection at APs, which can be considered as a hypothesis testing problem. Note that the dimension of signal subspace at APs is two while it is one with spoofing attack absent. Thus, the minimum description length (MDL) criterion can be used to operate the detection. Assuming broadcast content to nth group is the confidential information, only TUs in nth group transmit pilot sequence in the detection phase. In addition, a fraction ϕ of the pilot power ρ_u has been allocated to add another random detection pilot sequence $\boldsymbol{\varphi}_r$ (zero-mean, i.i.d., normalized norm, $\left\|\boldsymbol{\varphi}_r\right\|^2=1$), that is, $\widehat{\boldsymbol{\varphi}}_n=\sqrt{\tau_p(1-\phi)\rho_u}\boldsymbol{\varphi}_n+\sqrt{\tau_p\phi\rho_u}\boldsymbol{\varphi}_r\in\mathbb{C}^{\tau_p\times 1}$. Other groups keep silent in this phase. Hence, the received signal at mth AP can be given by (16), as shown at the top of this page. In addition, the pilot spoofing power is zero with a passive Eve, i.e. $\rho_E=0$.

Firstly, we present two hypotheses with $\mathcal{H}_0$ denoting no active attack and $\mathcal{H}_1$ representing presence of active attack [27]. For easy description, we define a receiving signal matrix at APs as $\mathbf{Y}_{R,\mathrm{d}}=[\mathbf{y}_1,\mathbf{y}_2,\cdots,\mathbf{y}_M]\in\mathbb{C}^{\tau_p\times M}$. Then the correlation matrix of the received pilot signals can be obtained by

$$\mathbf{R}_{Y,i}=\frac{1}{\tau_p}\mathbb{E}\left\{\mathbf{Y}_{R,d}^H\mathbf{Y}_{R,\mathrm{d}}\middle|\mathcal{H}_i\right\},\quad i=0,1. \tag{17}$$

Then we can further obtain that

$$\mathbf{R}_{Y,i}=\mathbf{R}_{S,i}+\mathbf{I}_M, \tag{18}$$

$$\mathbf{R}_{S,0}=\tau_p^{-1}\left\|\widehat{\boldsymbol{\varphi}}_k\right\|^2\mathbf{g}_n\mathbf{g}_n^H, \tag{19}$$

$$\mathbf{R}_{S,1}=\mathbf{H}\left(\tau_p^{-1}\mathbf{s}_{\varphi}\mathbf{s}_{\varphi}^H\right)\mathbf{H}^H. \tag{20}$$

where $\mathbf{g}_n = \left[\sum_{k=1}^{K} g_{1n_k}, \sum_{k=1}^{K} g_{2n_k}, \cdots, \sum_{k=1}^{K} g_{Mn_k}\right]^T \in \mathbb{C}^{M\times 1}$, $\mathbf{g}_E = [g_{1E}, g_{2E}, \cdots, g_{ME}]^T \in \mathbb{C}^{M\times 1}$, $\mathbf{H} = \left[\sqrt{(1-\phi)\,\rho_p}\mathbf{g}_n + \sqrt{\rho_E}\mathbf{g}_E, \sqrt{\phi\rho_p}\mathbf{g}_n\right] \in \mathbb{C}^{M\times 2}$, $\mathbf{s}_\varphi = \left[\sqrt{\tau_p}\varphi_n, \sqrt{\tau_p}\varphi_r\right]^T \in \mathbb{C}^{2\times\tau_p}$.

Evidently, we note that $\operatorname{rank}\left(\mathbf{R}_{S,0}\right) = 1$. Since UTs and Eve always have different fading channels, i.e. $\mathbf{g}_n \neq \mathbf{g}_E$, we can always obtain that $\operatorname{rank}\left(\mathbf{R}_{S,1}\right) = 2$ if $\phi > 0$. Thus, the binary hypothesis testing is essentially equivalent to estimate the signal correlation matrix rank d (signal subspace dimension $d = \operatorname{rank}\left(\mathbf{R}_{S,i}\right)$). Then we discuss the typical MDL estimation algorithm.

In the first place, we need the eigenvalue decomposition of matrix $\mathbf{R}_{Y,i}$ and order the eigenvalues by $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_{N_d}$, $N_d = \min\left\{M, \tau_p\right\}$. Then, the MDL estimator of d is presented as [27], [28]

$$\hat{d} = \arg \min_{1\leq d\leq N_d-1} \mathrm{MDL}\,(d)\,. \tag{21}$$

where the object function is given by

$$\begin{aligned}\mathrm{MDL}\,(d) = &-\sum_{i=d+1}^{N_d} \ln\lambda_i \\ &+ (N_d - d)\ln\left(\frac{1}{N_d-d}\sum_{i=d+1}^{N_d}\lambda_i\right) \\ &+ \frac{d\,(2N_d-d)\ln\tau}{2\tau}.\end{aligned} \tag{22}$$

Now the hypotheses can be formulated as

$$\begin{aligned}\mathcal{H}_0 &: \operatorname{rank}\left(\mathbf{R}_{S,0}\right) = d = 1,\\ \mathcal{H}_1 &: \operatorname{rank}\left(\mathbf{R}_{S,1}\right) = d > 1.\end{aligned} \tag{23}$$

Note that the MDL estimation method needs no threshold calculation. In addition, we acknowledge that the detection probability P_d can be represented as $P_d = P\left(\hat{d} \geq 2 \middle| d = 2\right) = 1 - P\left(\hat{d} = 1 \middle| d = 2\right)$. Meanwhile, the miss probability is given by $P\left(\hat{d} = 1 \middle| d = 2\right)$ which has been precisely calculated with the parameters N_d, ρ and β [24], [29]. Due to the space restrictions, we neglect the details in this paper.

V. SIMULATION RESULTS

Simulations are provided to evaluate the secrecy performance of our considered system. 10^5 independent Monte-Carlo experiments are operated for this following scenario: all APs and served users are randomly located within a circle cell of 600m. The active eavesdropper also locates randomly in this region. The large-scale path-loss is modeled as $\beta = \left(\frac{d_r}{d}\right)^v$ where d, $d_r = 50m$ and $v = 3$ respectively represent geographical distance, reference distance and path-loss exponent [30]. Moreover, we choose that $M = 100$, $K = 5$, $\tau_p = \tau_{d,p} = N$ and $\rho_u = \rho_d = \rho_{d,p} = 10$dB. The simulation area is wrapped around to avoid the cell-edge effects.

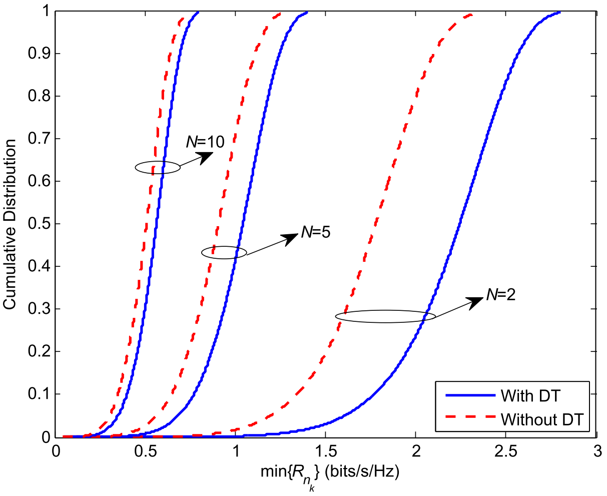

FIGURE 2. Cumulative distribution of the minimum achievable rates by legitimate users in the same group with ρ_E = 0dB and N = 2, 5, 10.

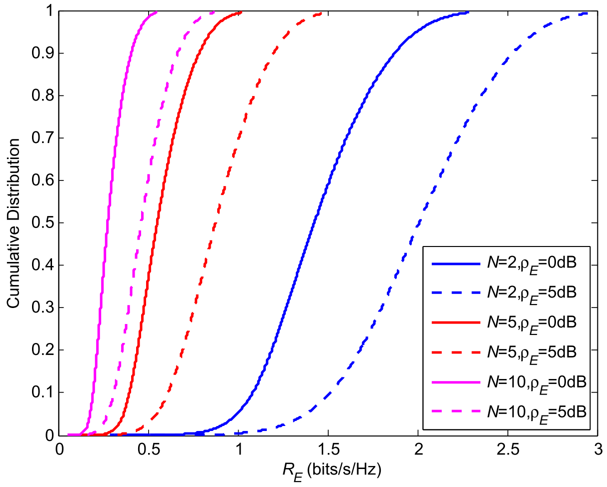

FIGURE 3. Cumulative distribution of information leakage to Eve with ρ_E = 0dB, 5dB and N = 2, 5, 10.

First, we focus on the performance gain, where two scenarios (with downlink training (DT) and without DT) have been considered. Fig. 2 and Fig. 3 illustrate the cumulative distributions of the achievable rates by users and Eve, which show that the achievable information rates of the legitimate users with DT is significantly higher than the case without DT. Moreover, both information rates are monotonically decreasing in group number. It can be explained by the fact that the inter-group interference increases with increasing N, then the rates decrease. Also, Fig. 2 shows that the performance gap decreases with group number N. It is because of the fact that channel hardening is more pronounced in a higher network density scenario and the downlink beamforming training scheme yields a lower performance gain. Moreover, it can be observed that R_{nE} is impaired with increasing N and is improved with increasing ρ_E. Fig. 3 indicates that Eve's rates strongly depend on ρ_E. Obviously, Eve is able

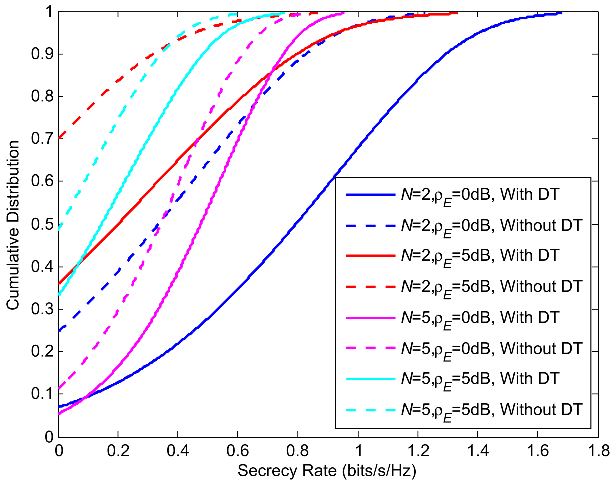

FIGURE 4. **The cumulative distribution of the achievable secrecy rates with and without downlink training (with or without DT).**

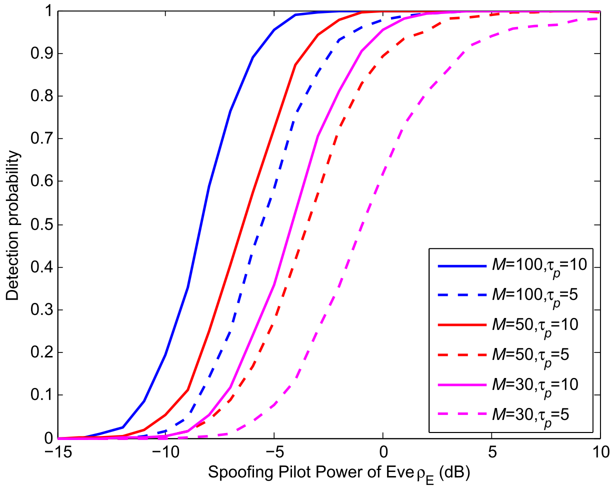

FIGURE 5. **Probability of active attack detection P_d versus Eve's spoofing pilot power budget ρ_E with τ_p= 5, 10 and M = 30, 50, 100.**

to improve its eavesdropping ability by increasing spoofing signals power.

Next, Fig. 4 shows the cumulative distributions of the secrecy rates under different schemes with and without downlink training, respectively. As we can see, downlink training scheme outperforms the statistical CSI case with any N or ρ_E. Moreover, it is observed that the secrecy performance degrades with increasing ρ_E. Obviously, increasing ρ_E enlarges the information leakage and decreases the secrecy rate. Hence, the secrecy rate decreases. Besides, we can observe that the curves has crossed with each other when system utilizes the same training scheme with the same Eve's spoofing pilot power ρ_E. It's easy to explain that both R_{n_k} and R_{nE} monotonically decrease with increasing N. While the decrease speeds of the two achievable information rates may be different which depend on the layout locations of legitimate users and Eve. Hence, the impacts of N on the secrecy performance should be investigated in fixed network layout. Moreover, since the coherence interval generally is sufficiently-large [20], we ignore the training overhead in the simulations.

Here, we further investigate the active attack detection algorithm presented in Fig. 5, where the probability values were averaged over 5000 runs. Some simulation parameters are chosen as $\rho_p = 10$dB, $\phi= 0.5$, $\tau_p= 5, 10$ and $M= 30, 50, 100$. It is evident that the detection performance improves with increasing the number of APs and pilot sequence length. Besides, the probabilities are all over 0.96 at $\rho_E = 7$dB. Thus, the presented detection method is able to detect active attacks at low power levels. Note that we have only investigated the impact on detection performance over few parameters (ρ_E, M and τ_p). Actually, we can make an extension that all users have the autonomy to adjust their own transmit power and pilot sequence design. These issues can be left for future works.

VI. CONCLUSIONS

In this paper, we have considered the secure transmission in a multigroup multicasting Cell-Free massive MIMO network in the presence of active spoofing attack. Based on the imperfect CSI obtained by uplink and downlink channel estimation, distributed conjugate beamforming with normalized power constraint is utilized for downlink multicasting data transmission. We derive a closed-form lower bound on the ergodic secrecy rate which is adopted to evaluate the security performance. In addition, we presented a novel mechanism using the MDL algorithm to detect spoofing relay attack. Simulation results confirm that higher Eve's spoofing pilot power or larger group number cause a significant secrecy performance degradation. In addition, non-orthogonal pilots scheme and active eavesdropping attack detection may be included in future work. In addition, the AN scheme is an effective enabling technology for secure transmission over MIMO systems. To avoid cooperation and data interchanging among the APs, AN has not been considered in this paper. To further improve systems' secrecy performance, physical layer jamming techniques, including secrecy beamforming and AN aiding, should also been considered in future works.

ACKNOWLEDGMENT

The authors would like to thank the anonymous reviewers and the editors for helping to improve this paper.

APPENDIX

A. PROOF OF THEOREM 1

Based on the deduction of Theorem 1 in [10], we have that $\mathbb{E}\left\{a_{n_k}\right\} = \sqrt{\frac{1}{N}}\sum_{m=1}^{M}\frac{\sqrt{\pi\gamma_{mn_k}}}{2}$, $\mathrm{Var}\left\{a_{n_k}\right\} = \frac{1}{N}\sum_{m=1}^{M}\beta_{mn_k} - \frac{1}{N}\sum_{m=1}^{M}\frac{\pi}{4}\gamma_{mn_k}$ and $\mathbb{E}\left\{\left|a_{n'_k}\right|^2\right\} = \frac{1}{N}\sum_{m=1}^{M}\beta_{mn_k}$. By using the similar derivation in [10], we can easily derive the expression of R_{n_k} as (14) in the case of no downlink training. Now let us focus on the case with both uplink and downlink training.

Specifically, we consider the term $\mathbb{E}\left\{\left|\tilde{a}_{n_k}\right|^2\right\}$ as

$$\begin{aligned}
\mathbb{E}\left\{\left|\tilde{a}_{n_k}\right|^2\right\} &= \mathbb{E}\left\{\left|a_{n_k} - \hat{a}_{n_k}\right|^2\right\} \\
&= \mathbb{E}\left\{\left|a_{n_k} - \frac{\sqrt{\tau_{d,p}\rho_{d,p}}\mathrm{Var}\left\{a_{n_k}\right\}\bar{y}_{dp,n_k} - \mathbb{E}\left\{a_{n_k}\right\}}{\tau_{d,p}\rho_{d,p}\mathrm{Var}\left\{a_{n_k}\right\}+1}\right|^2\right\} \\
&= \mathbb{E}\left\{\left|\frac{a_{n_k} - \mathbb{E}\left\{a_{n_k}\right\} - \sqrt{\tau_{d,p}\rho_{d,p}}\mathrm{Var}\left\{a_{n_k}\right\}w_{dp,n_k}}{\tau_{d,p}\rho_{d,p}\mathrm{Var}\left\{a_{n_k}\right\}+1}\right|^2\right\} \\
&= \frac{\mathrm{Var}\left\{a_{n_k}\right\} + \tau_{d,p}\rho_{d,p}\left(\mathrm{Var}\left\{a_{n_k}\right\}\right)^2}{\left(\tau_{d,p}\rho_{d,p}\mathrm{Var}\left\{a_{n_k}\right\}+1\right)^2} \\
&= \frac{\mathrm{Var}\left\{a_{n_k}\right\}}{\tau_{d,p}\rho_{d,p}\mathrm{Var}\left\{a_{n_k}\right\}+1} \\
&= \frac{\sum\limits_{m=1}^{M}\beta_{mn_k} - \sum\limits_{m=1}^{M}\frac{\pi}{4}\gamma_{mn_k}}{\tau_{d,p}\rho_{d,p}\left(\sum\limits_{m=1}^{M}\beta_{mn_k} - \sum\limits_{m=1}^{M}\frac{\pi}{4}\gamma_{mn_k}\right)+N}.
\end{aligned}$$

By substituting the expressions of the terms into (11), we can obtain the closed form expression of R_{n_k} with both uplink and downlink training in (14).

Then, we compute the component $\mathbb{E}\left\{|a_{nE}|^2\right\}$ in (12). Due to the fact that $z_{mn'} \sim \mathcal{CN}(0,1)$, we can get the result that $\mathbb{E}\{|z_{mn'}|\} = \int_0^{+\infty}\sqrt{x}\exp(-x)\,dx = \sqrt{\pi}/2$. Hence, the term can be rewritten as

$$\begin{aligned}
\mathbb{E}\left\{|a_{nE}|^2\right\} &= \frac{1}{N}\mathbb{E}\left\{\left|\sum_{m=1}^{M}\frac{g_{mE}z_{mn}^*}{|z_{mn}|}\right|^2\right\} \\
&= \frac{1}{N}\mathbb{E}\left\{\sum_{m=1}^{M}\left|\frac{g_{mE}z_{mn}^*}{|z_{mn}|}\right|^2\right\} \\
&\quad + \frac{1}{N}\mathbb{E}\left\{\sum_{m=1}^{M}\sum_{i\neq m}^{M}\frac{g_{mE}z_{mn}^*g_{iE}^*z_{in}}{|z_{mn}|\cdot|z_{in}|}\right\} \\
&= \frac{1}{N}\sum_{m=1}^{M}\beta_{mE} + \frac{\pi}{4N}\sum_{m=1}^{M}\sum_{i\neq m}^{M}\sqrt{\gamma_{mE}\gamma_{iE}}.
\end{aligned}$$

Utilizing the similar analytic procedures, we can easily derive the other terms expressions in Theorem 1. Due to the space limit, we don't state the deduction process in details here. This concludes the proof.

REFERENCES

[1] H. Q. Ngo, A. Ashikhmin, H. Yang, E. G. Larsson, and T. L. Marzetta, "Cell-free massive MIMO versus small cells," *IEEE Trans. Wireless Commun.*, vol. 16, no. 3, pp. 1834–1850, Mar. 2017.

[2] H. Q. Ngo, L.-N. Tran, T. Q. Duong, M. Matthaiou, and E. G. Larsson, "On the total energy efficiency of cell-free massive MIMO," *IEEE Trans. Green Commun. Netw.*, vol. 2, no. 1, pp. 25–39, Mar. 2018.

[3] H. Q. Ngo, A. Ashikhmin, H. Yang, E. G. Larsson, and T. L. Marzetta, "Cell-free massive MIMO: Uniformly great service for everyone," in *Proc. IEEE 16th Int. Workshop Signal Process. Adv. Wireless Commun. (SPAWC)*, Stockholm, Sweden, Jun./Jul. 2015, pp. 201–205.

[4] 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.

[5] 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.

[6] S. Buzzi and C. D'Andrea, "Cell-free massive MIMO: User-centric approach," *IEEE Wireless Commun. Lett.*, vol. 6, no. 6, pp. 706–709, Dec. 2017.

[7] L. D. Nguyen, T. Q. Duong, H. Q. Ngo, and K. Tourki, "Energy efficiency in cell-free massive MIMO with zero-forcing precoding design," *IEEE Commun. Lett.*, vol. 21, no. 8, pp. 1871–1874, Aug. 2017.

[8] G. Interdonato, H. Q. Ngo, E. G. Larsson, and P. Frenger, "How much do downlink pilots improve cell-free massive MIMO?" in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Washington, DC, USA, Dec. 2016, pp. 1–7.

[9] M. Sadeghi and C. Yuen, "Multi-cell multi-group massive MIMO multicasting: An asymptotic analysis," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, San Diego, CA, USA, Dec. 2015, pp. 1–6.

[10] T. X. Doan, H. Q. Ngo, T. Q. Duong, and K. Tourki, "On the performance of multigroup multicast cell-free massive MIMO," *IEEE Commun. Lett.*, vol. 21, no. 12, pp. 2642–2645, Dec. 2017.

[11] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, Jun. 2008.

[12] Y.-W. P. Hong, P.-C. Lan, and C.-C. J. Kuo, "Enhancing physical-layer secrecy in multiantenna wireless systems: An overview of signal processing approaches," *IEEE Signal Process. Mag.*, vol. 30, no. 5, pp. 29–40, Sep. 2013.

[13] X. Chen, D. W. K. Ng, W. H. Gerstacker, and H.-H. Chen, "A survey on multiple-antenna techniques for physical layer security," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 2, pp. 1027–1053, 2nd Quart., 2017.

[14] V. W. S. Wong, R. Schober, D. W. K. Ng, and L.-C. Wang, *Key Technologies for 5G Wireless Systems*. Cambridge, U.K.: Cambridge Univ. Press, 2017.

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

[16] X. Zhang, D. Guo, K. Guo, and H. Niu, "Secure performance analysis and detection of pilot attack in massive multipleinput multiple-output system," *Int. J. Distrib. Sens. Netw.*, vol. 14, no. 5, pp. 1–12, May 2018.

[17] A. Al-nahari, "Physical layer security using massive multiple-input and multiple-output: Passive and active eavesdroppers," *IET Commun.*, vol. 10, no. 1, pp. 50–56, 2016.

[18] Q. Xiong, Y.-C. Liang, K. H. Li, and Y. Gong, "An energy-ratio-based approach for detecting pilot spoofing attack in multiple-antenna systems," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 5, pp. 932–940, May 2015.

[19] 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.

[20] T. M. Hoang, H. Q. Ngo, T. Q. Duong, H. D. Tuan, and A. Marshall, "Cell-free massive MIMO networks: Optimal power control against active eavesdropping," *IEEE Trans. Commun.*, vol. 66, no. 10, pp. 4724–4737, Oct. 2018.

[21] X. Zhang, D. Guo, and K. An, "Secure communication in multigroup multicasting cell-free massive MIMO networks with active spoofing attack," *Electron. Lett.*, vol. 55, no. 2, pp. 96–98, Jan. 2019.

[22] D. Kapetanovic, A. Al-Nahari, A. Stojanovic, and F. Rusek, "Detection of active eavesdroppers in massive MIMO," in *Proc. IEEE Int. Symp. Pers., Indoor, Mobile Radio Commun. (PIMRC)*, Washington, DC, USA, Sep. 2014, pp. 585–589.

[23] D. Kapetanović, G. Zheng, K.-K. Wong, and B. Ottersten, "Detection of pilot contamination attack using random training and massive MIMO," in *Proc. IEEE Int. Symp. Pers., Indoor, Mobile Radio Commun. (PIMRC)*, London, U.K., Sep. 2013, pp. 13–18.

[24] F. Haddadi, M. Malek-Mohammadi, M. M. Nayebi, and M. R. Aref, "Statistical performance analysis of MDL source enumeration in array processing," *IEEE Trans. Signal Process.*, vol. 58, no. 1, pp. 452–457, Jan. 2010.

[25] K. Yuan, L. Guo, C. Dong, and T. Kang, "Detection of active eavesdropper using source enumeration method in massive MIMO," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Paris, France, May 2017, pp. 1–5.

[26] X. Zhang, D. Guo, K. Yang, and S. Xie, "Secure downlink transmission with finite resolution analog beamforming in massive multiple-input multiple-output system," *Int. J. Distrib. Sensor Netw.*, vol. 14, no. 9, pp. 1–13, Sep. 2018.

[27] J. K. Tugnait, "Self-contamination for detection of pilot contamination attack in multiple antenna systems," *IEEE Wireless Commun. Lett.*, vol. 4, no. 5, pp. 525–528, Oct. 2015.

[28] J. K. Tugnait, "Detection of active eavesdropping attack by spoofing relay in multiple antenna systems," *IEEE Wireless Commun. Lett.*, vol. 5, no. 5, pp. 460–463, Oct. 2016.

[29] B. Nadler, "Nonparametric detection of signals by information theoretic criteria: Performance analysis and an improved estimator," *IEEE Trans. Signal Process.*, vol. 58, no. 5, pp. 2746–2756, May 2010.

[30] Q. Zhang, S. Jin, K.-K. Wong, H. Zhu, and M. Matthaiou, "Power scaling of uplink massive MIMO systems with arbitrary-rank channel means," *IEEE J. Sel. Topics Signal Process.*, vol. 8, no. 5, pp. 966–981, Oct. 2014.

XIANYU ZHANG received the B.S. and M.S. degrees with the Chongqing Communication Institute, Chongqing, China, in 2007 and 2010, respectively. He is currently pursuing the Ph.D. degree with the Army Engineering University of PLA. His research interests focus on massive MIMO communication, physical layer security, cooperative relay networks, channel estimation, multiuser communication systems, and green communication.

DAOXING GUO received the B.S., M.S., and Ph.D. degrees from the Institute of Communications Engineering (ICE), Nanjing, China, in 1995, 1999, and 2002, respectively. He is currently a Full Professor and also a Ph.D. Supervisor with the Army Engineering University of PLA. He has authored and coauthored more than 40 conference and journal papers and has been granted over 20 patents in his research areas. He has served as a Reviewer for several journals in communication field. His current research interests include satellite communications systems and transmission technologies, communication anti-jamming technologies, communication anti-interception technologies including physical layer security, and so on.

KANG AN received the B.E. degree in electronic engineering from the Nanjing University of Aeronautics and Astronautics, Nanjing, China, in 2011, the M.E. degree in communication engineering from the PLA University of Science and Technology, Nanjing, in 2014, and the Ph.D. degree in communication engineering from Army Engineering University, Nanjing, in 2017. Since 2018, he has been with the National University of Defense Technology, Nanjing, where he is currently an Engineer. His current research interests are satellite communication, 5G mobile communication networks, and cognitive radio.

ZHIGUO DING received the B.Eng. degree in electrical engineering from the Beijing University of Posts and Telecommunications, in 2000, and the Ph.D. degree in electrical engineering from Imperial College London, in 2005. From 2005 to 2018, he was with Queen's University Belfast, Imperial College London, Newcastle University, and Lancaster University. From 2012 to 2018, he was an Academic Visitor with Princeton University. Since 2018, he has been with the University of Manchester as a Professor in communications. His research interests are 5G networks, game theory, cooperative and energy harvesting networks, and statistical signal processing. He received the Best Paper Award in the IET ICWMC-2009 and the IEEE WCSP-2014, the EU Marie Curie Fellowship, in 2012–2014, the Top IEEE TVT Editor Award, in 2017, the IEEE Heinrich Hertz Award, in 2018, and the IEEE Jack Neubauer Memorial Award, in 2018. He was an Editor of the IEEE Wireless Communication Letters and the IEEE Communication Letters, from 2013 to 2016. He is serving as an Editor for the IEEE Transactions on Communications, the IEEE Transactions on Vehicular Technology, and the *Journal of Wireless Communications* and *Mobile Computing*.

BANGNING ZHANG received the B.S. and M.S. degrees from the Institute of Communications Engineering (ICE), Nanjing, China, in 1984 and 1987, respectively. He is currently a Full Professor and also the Head of the College of Communications Engineering. He has authored and coauthored more than 80 conference and journal papers and has been granted over 20 patents in his research areas. He has served as a Reviewer for several journals in communication field. His current research interests include communication anti-jamming technologies, microwave technologies, satellite communications systems, cooperative communications, and physical layer security.