Received 8 November 2022; revised 16 December 2022; accepted 22 December 2022. Date of publication 29 December 2022; date of current version 17 January 2023.

*Digital Object Identifier 10.1109/OJCOMS.2022.3232065*

# New LLRT-Based Methods for Active Eavesdropper Detection in Cell-Free Massive MIMO

**SEYYED SALEH HOSSEINI [1] (Student Member, IEEE), XIAO-WEN CHANG [2], AND BENOIT CHAMPAGNE [1] (Senior Member, IEEE)**

[1] Department of Electrical and Computer Engineering, McGill University, Montreal, QC H3A 0E9, Canada

[2] School of Computer Science, McGill University, Montreal, QC H3A 2A7, Canada

CORRESPONDING AUTHOR: S. S. HOSSEINI (e-mail: seyyed.hosseini@mail.mcgill.ca)

This work was supported by the Natural Sciences and Engineering Research Council of Canada (NSERC) under Grant RGPIN2017-05138 and Grant RGPIN-2017-04223.

**ABSTRACT** In this paper, the problem of active eavesdropper detection is considered for a cell-free massive multiple-input multiple-output (m-MIMO) system which is attacked by an active eavesdropper within the uplink training phase, also called *pilot spoofing attack*. Two methods based on log-likelihood-ratio tests (LLRT), one in a centralized and the other in a decentralized fashion, are proposed to detect the signal abnormality. The methods take advantage of a special protocol in which the legitimate users switch to an off-mode irregularly, without significantly affecting the spectral efficiency of the data transmission. The protocol is directly applicable to environments with low to moderate mobility, and can be extended to high mobility through a simple rearrangement of available pilot sequences among users if needed. More importantly, the proposed methods impose low fronthaul overhead which is imperative for a cell-free m-MIMO system with a large number of access points (APs). A closed-form expression for the joint probability density function (PDF) of the processed received signals conditioned on the alternative hypothesis, which is essential for the implementation of LLRT-based detection methods, is also derived. Through an asymptotic analysis, it is shown for the proposed methods that the detection and false-alarm probabilities approach to one and zero, respectively as the number of APs goes to infinity. Numerical results reveal that both methods significantly outperform a recent approach in terms of false-alarm rate with negligible degradation in the per user uplink spectral efficiency.

**INDEX TERMS** Cell-free massive MIMO, physical layer security, pilot spoofing attack, active eavesdropper detection.

## I. INTRODUCTION

CELL-FREE massive multiple-input multiple-output (m-MIMO) systems have been recently introduced as a promising technology for the next generation of wireless communication networks [1], [2], [3], [4], [5], [6], [7], [8], [9], [10], [11], [12], [13], [14]. These systems employ a large number of access points (APs) which are distributed over a wide area without partitioning the network into bounded cells. The APs are connected to a central processing unit (CPU) via a fronthaul network of high-speed links. This type of dense heterogeneous network offers several advantages, e.g.: avoiding the need of frequent requests for handover, providing and taking advantage of shadowing diversity, and alleviating the mutual coupling effect of multiple collocated antennas.

In spite of these advantages, cell-free m-MIMO systems remain vulnerable to possible attacks by eavesdroppers (Eves) who would maliciously attempt to overhear confidential messages sent to legitimate users. Specifically, an Eve can first transmit the pilot signal of a target user, within the uplink training phase, to spoof APs to estimate the channel gains of that user as a linear combination of its true channel gains and those of Eve. Based on estimated channel gains, the APs then collectively form a beamformer associated with the target user which partially covers Eve's channel. Hence, Eve is able to receive data symbols intended for the target

user and overhear its messages. This unauthorized attack by an Eve on a legitimate user is called *pilot spoofing attack* in the literature [3]. In order to shield itself from a pilot spoofing attack, the cell-free m-MIMO system must first be able to detect its occurrence, a procedure referred to as *active eavesdropper detection (AED)*, which is the main focus of this work.

### A. REVIEW OF LITERATURE

Only a few works have addressed AED in the context of cell-free m-MIMO systems. In [3], the authors use a simple method based on total power (TP) for this purpose. In the TP method, each AP measures the received signal power from each user and sends this information to the CPU where an estimation of the total received power by all APs is first computed. Then, a decision about the presence of a counterfeit pilot signal is made by comparing the value of the estimated TP to a threshold, taken as the expected value of TP in the absence of Eve. Although the TP method admits of a simple implementation, it exhibits a high false-alarm rate and relies on the precise estimation of large-scale fading (LSF) gains, which is difficult to realize in a practical wireless network environment.

In [15], an alternative method, based on the minimum description length (MDL) criterion [16], is proposed for AED in a special type of multigroup multicasting cell-free m-MIMO system. However, any sensible attempt to modify and apply this method to a standard cell-free m-MIMO system will need to address the following drawbacks: each user must send its pilot sequence in succession, while the other users keep silent, which significantly reduces the per user spectral efficiency (SE); implementation with $N$ APs requires an eigenvalue decomposition with complexity order of $\mathcal{O}(N^3)$, which poses a significant computational burden for a cell-free m-MIMO system with large $N$; a user must simultaneously transmit a random pilot signal in addition to its assigned pilot signal, which under a transmit power constraint reduces the effective signal-to-noise ratio (SNR) available at the APs for channel estimation. An approach based on random matrix theory has been recently proposed in [17] which follows the same protocol as [15].

Besides, both TP and MDL methods are faced with communication challenges inherent to any centralized AED approach. Firstly, the fronthaul overhead for a network setting with $N$ APs, $K$ users, and pilot length $\tau_{\mathrm{p}}$ is on the order of $\mathcal{O}(NKB_{\mathrm{L}})$ and $\mathcal{O}(\tau_{\mathrm{p}}NKB_{\mathrm{L}})$ per detection cycle for the TP and MDL methods, respectively, where $B_{\mathrm{L}}$ is the number of bits used for the representation of signal values communicated to the CPU. This overhead, which grows linearly with the number of APs, can be quite high for large $N$. Secondly, even choosing an appropriate value of $B_{\mathrm{L}}$ may be challenging since the transmit power by Eve is unknown.

In the literature, there exist several other AED methods that were not specifically designed for application to cell-free m-MIMO systems, and whose extension to such systems would pose major challenges, in terms of adaptability and high overhead on fronthaul links.

For instance, authors in [18] utilize an AED method for a time division multiple access (TDMA) system in which the base station serves users one-by-one. This assumption is not valid for cell-free m-MIMO systems where all users should simultaneously be served by APs. Another method, which has been recently proposed in [19], uses a protocol in which a user performs AED based on estimated channels fed back from the base station. However, the use of channel feedback in a cell-free m-MIMO system incurs a very high overhead due to the large number of APs.

Some AED approaches adopt a training phase with two stages to detect a pilot spoofing attack in multi-antenna wireless systems [20], [21]. The key idea is to divide the pilot sequence into two segments which are then sequentially transmitted with different power levels. Through proper linear combining of the signals received in each stage, this transmission strategy allows to isolate the spoofing pilot transmission for improved AED. However, the orthogonality among pilot sequences will be affected if the system employs a fixed set of orthogonal pilots. Moreover, applying this strategy to cell-free m-MIMO would increase the fronthaul overhead by an order of magnitude, similar to the method in [15].

A different type of AED methods which also performs the training phase in two stages are developed in [22], [23]. In these methods, the second stage is employed to transmit a random sequence that facilitates AED. However, the method in [22] is limited to a single user, while [23] relies on the assumption that the number of legitimate users and Eves are equal.

In [24], an MDL-based AED method is specifically proposed for TDD/SDMA systems in which each legitimate user combines its pilot with a random signal while Eve is unaware of this manipulation. The method requires an iterative algorithm to identify which legitimate user(s) is attacked. In [25], the authors propose an approach for AED of a single legitimate user by identifying directions of arrival in the spatial spectrum domain. However, this method requires the use of long pilot sequences as well as adequate angular separation between the legitimate user and Eve.

For some of the aforementioned works, the decision metric design requires channel state information that might not be easily accessible during the detection process. For example, the LSF gains between the users and the base station should be known for the implementation of the detectors introduced in [21], [23]. In the case of [21], the LSF gains between the Eve and the base station have to be known too. In the context of cell-free m-MIMO systems, this type of approach would be particularly challenging due to the large number of geographically distributed APs.

Below, we elaborate on two challenges related to AED, that are specific for cell-free m-MIMO rather than collocated m-MIMO systems [26], [27], [28], [29], [30], [31], [32]:

First, in a cell-free m-MIMO system, the majority of the signal processing tasks that require to collectively use the information signals received at the APs, must be implemented in the CPU [1], [2], [33]. Hence, a large amount of information should be exchanged between APs and the CPU which might exceed the capacity of fronthaul links [34], [35], [36]. Besides, since there exists a large number of fronthaul links, the total power consumption can reach such a high level as to defeat the spectral efficiency gains [2]. Therefore, it is essential to reduce the fronthaul load induced by signal processing tasks such as AED. In contrast, for a collocated m-MIMO system, the signal processing tasks can easily be performed at the base station since all information signals are locally available. Second, the signals received by antenna elements in a collocated m-MIMO system all experience the same LSF gain [27, p. 31]. However, this is not true for a cell-free m-MIMO system due to the different geographical locations of APs. Hence, the signals received by each AP may experience quite different LSF gains [1], [2], [33], [34], [35], [36]. Therefore, a signal processing technique designed for a collocated m-MIMO system does not usually achieve the optimal performance if it is directly applied to a cell-free m-MIMO system. For the problem of AED, the statistically optimal processing techniques requiring the use of the LSF gains must consider this difference in modelling.

### B. CONTRIBUTIONS

The absence of a more sophisticated method for AED in cell-free m-MIMO systems motivates us to further study this problem and develop two log-likelihood ratio test (LLRT)-based methods. Specifically, the main contributions of the paper are as follows:

- A special protocol in which the legitimate users sporadically switch to an off-mode, without significantly affecting the spectral efficiency of the data transmission, is introduced to facilitate AED in a cell-free m-MIMO system undergoing a pilot spoofing attack. The proposed protocol can simultaneously detect attacks on multiple users operating in the network (Section III). Moreover, it is directly applicable to environments with low to moderate mobility, and can be extended to high mobility through a simple rearrangement of available pilot sequences among users if needed (Section III-C).
- Two novel AED methods are conceived, that take advantage of the above transmission protocol without relying on channel state information. Both methods use the LLRT as the detection metric, but differ from the implementation perspective, i.e.: the first one performs AED in a centralized manner, while the second is decentralized (Sections III-A and III-B). The proposed methods only require statistical information about channel gains, as opposed to instantaneous estimates. Besides, the fronthaul overhead of the proposed centralized and decentralized methods are on the order of $\mathcal{O}(qNKB_{\mathrm{L}})$ and $\mathcal{O}(NKp)$ where $q$ is a positive integer and $0 < p < 1$ is a real number (Sections III-B and IV-C).
- A closed-form expression for the joint probability density function (PDF) of the processed received signals conditioned on the true hypothesis, which is essential for the implementation of LLRT-based detection methods, is derived based on the distributions of the large- and small-scale fading gains (Lemma 1).
- For the proposed methods, an asymptotic analysis[1] is carried out to derive conditions under which the *ideal* operating point[2] of receiver operation characteristic (ROC) curves is attainable. Specifically, it is shown (see Theorem 1) that for the centralized method the ideal point can be achieved as the number of APs increases, which is confirmed numerically. For the decentralized method, it is shown that if each AP operates in a particular region of the ROC plane, the final detection made by the CPU can also attain the ideal operating point (see Theorem 2). Furthermore, the results of Theorem 2 are generic for any decentralized AED method meant to be applied in cell-free m-MIMO systems.
- The results of numerical simulations reveal that the proposed methods significantly outperform the established TP, MDL [15], and energy-ratio-detector (ERD) [37] methods in terms of detection performance metrics (Figs. 11–13). The advantages of the proposed methods, in terms of fronthaul overhead, power efficiency, and SE degradation, are also discussed (Section IV-C).

The rest of the paper is organized as follows: The cell-free m-MIMO system model and AED problem are formulated in Section II. The transmission protocol and proposed AED methods along with their mathematical analysis, are developed in Section III. The simulation methodology and results are presented and discussed in Section IV. A conclusion is drawn in Section V. Finally, the proofs of key results are included in Appendix.

*Notation:* Capital and small boldface letters indicate matrices and vectors, respectively. We use sans serif font for random quantities (e.g., $x$ and $\mathbf{x}$) and normal font for their possible values or realizations. The real and complex Gaussian random variables $x$ and $z$ with means $\mu$ and variances $\sigma^2$ are indicated by $x \sim \mathcal{N}(\mu, \sigma^2)$ and $z \sim \mathcal{CN}(\mu, \sigma^2)$, respectively. The complex Gaussian random vector $\mathbf{x}$ with mean vector $m$ and covariance matrix $R$ is denoted by $\mathbf{x} \sim \mathcal{CN}(m, R)$. $\mathbb{P}(\mathcal{E})$ stands for the probability of event $\mathcal{E}$. The notation $\overline{\mathcal{E}}$ denotes the complement of event $\mathcal{E}$. The symbols $\mathbb{N}$, $\mathbb{R}$ and $\mathbb{C}$ denote the sets of non-negative integers, real numbers, and complex numbers respectively. $||.||_2$ denotes the $\ell_2$-norm of its vector argument. $I_n$ is an identity matrix of size $n$. $\mathbb{E}\{x\}$ and $\mathbb{V}\{x\}$ denote the expectation and variance of random variable $x$, respectively. $[a_1; a_2; \cdots; a_n]$ denotes the vertical concatenation of column vectors $a_1, a_2, \ldots, a_n$. $\mathcal{K} \setminus \{k\}$ denotes the

1. Other types of analytical approach such as secrecy rate analysis or designing a countermeasure approach fall outside of the scope of this paper.
2. That is, the point at which the detection and false alarm probabilities are equal to 1 and 0, respectively.

**TABLE 1.** List of main symbols.

| Symbol | Parameter |
|---|---|
| $N$ | Number of APs |
| $K$ | Number of users |
| $T_{\mathrm{L}}$ | Large-scale fading time interval |
| $T_{\mathrm{C}}$ | Coherence time |
| $B_{\mathrm{C}}$ | Coherence bandwidth |
| $\tau_{\mathrm{c}}$ | Dimension of coherence element |
| $\tau_{\mathrm{p}}$ | Length of pilot sequence |
| $g$ | Channel gain |
| $\beta^{\frac{1}{2}}$ | Large-scale fading gain |
| $h$ | Small-scale fading gain |
| $a$ | Average path loss |
| $z$ | Shadow fading magnitude in dB |
| $\sigma_{\mathrm{sh}}$ | Shadowing variance |
| $\rho_{\mathrm{p}}$ | Transmit power of legitimate users |
| $\rho_{\mathrm{e}}$ | Transmit power of Eve |
| $P_{\mathrm{d}}$ | Probability of detection |
| $P_{\mathrm{f}}$ | Probability of false alarm |
| $q$ | Number of off-mode time slot |

subset that results from excluding element $k$ from $\mathcal{K}$. The function $Q(z)$ is defined as $Q(z) = \frac{1}{\sqrt{2\pi}} \int_z^\infty \exp(-\frac{x^2}{2})dx$.

## II. SYSTEM MODEL AND PROBLEM STATEMENT

In this section, we introduce the cell-free m-MIMO system model and formulate the AED problem under pilot spoofing attack. Unless otherwise mentioned, the model used and main assumptions made here are similar to those in [1], [3].

### A. CELL-FREE M-MIMO SYSTEM MODEL

We consider a cell-free m-MIMO system consisting of $N$ single-antenna APs[3] connected to a common CPU via fronthaul links. The APs simultaneously serve $K < N$ single-antenna users distributed across a relatively large geographical area. It is assumed that the channel gains between the APs and the users remain constant within a time-frequency coherence element with dimension $\tau_{\mathrm{c}} = \lfloor T_{\mathrm{C}} B_{\mathrm{C}} \rfloor$, where $T_{\mathrm{C}}$ and $B_{\mathrm{C}}$ denote the channel coherence time and coherence bandwidth, respectively. Specifically, the composite channel gain between user $k \in \mathcal{K} = \{1, \ldots, K\}$ and AP $n \in \mathcal{N} = \{1, \ldots, N\}$ is modeled as follows:

$$g_{nk} = \beta_{nk}^{\frac{1}{2}} h_{nk}, \tag{1}$$

where $\beta_{nk}^{\frac{1}{2}}$ and $h_{nk}$ are the large-scale and small-scale fading gains, respectively. The former is defined as $\beta_{nk} = a_{nk} 10^{z_{nk}/10}$, where $a_{nk}$ is the average path-loss, $z_{nk} \sim \mathcal{N}(0, \sigma_{\mathrm{sh}})$ is the shadow fading magnitude in dB, and $\sigma_{\mathrm{sh}} > 0$ is the shadowing standard deviation; while the latter follows the Rayleigh model, i.e., $h_{nk} \sim \mathcal{CN}(0, 1)$. We assume that the large-scale fading gains $\beta_{nk}^{\frac{1}{2}}$ can be treated as constants over a time interval of $T_{\mathrm{L}}$, which is much greater than the coherence time $T_{\mathrm{C}}$ of the small-scale fading, i.e., $T_{\mathrm{L}} = \ell T_{\mathrm{C}}$ where $\ell \in \mathbb{N}$, and $\ell \gg 1$. In a typical application, the coherence time $T_{\mathrm{C}}$ could be on the order of milliseconds while $T_{\mathrm{L}}$ is two to three orders of magnitude greater [38], [39]. A list of main symbols used throughout of the paper is provided in Table 1.

Let $\boldsymbol{\varphi}_k \in \mathbb{C}^{\tau_{\mathrm{p}}}$ denote the vector of $\tau_{\mathrm{p}}$ pilot symbols transmitted by the $k$th user, where $||\boldsymbol{\varphi}_k||_2^2 = 1$. We shall first assume (Sections II-A and II-B) that $K \leq \tau_{\mathrm{p}} < \tau_{\mathrm{c}}$, so that orthogonal pilot vectors can be assigned to each user, i.e., $\boldsymbol{\varphi}_k^H \boldsymbol{\varphi}_l = 0$ for all $k \neq l$. It is worthwhile to mention that the condition $K \leq \tau_{\mathrm{p}}$ can be satisfied with large number of users $K$ in low- to moderate-mobility environments. Based on calculations in [27, p. 23], it can be shown that $\tau_{\mathrm{c}}$ reaches values in excess of a thousand in a typical urban environment where $4 \leq T_{\mathrm{C}} \leq 9$ms, $B_{\mathrm{C}} = 300$kHz, and the user speed varies between 30km/h and about 70km/h. For these environments, we can still assign 5 to 10 percent of $\tau_{\mathrm{c}}$ to the pilot symbols to serve over hundred mobile users. Note that number of users typically varies between 40 and 80 in a cell-free m-MIMO system deployed over a square area of 1km$^2$ [1]. Subsequently (Section III-C), we shall extend our proposed methods to a high-mobility environment, i.e., where $K > \tau_{\mathrm{p}}$ and some users must share pilots.

The received signal by the $n$th AP can be expressed as

$$\mathbf{r}_n = \sqrt{\tau_{\mathrm{p}} \rho_{\mathrm{p}}} \sum_{k=1}^{K} g_{nk} \boldsymbol{\varphi}_k + \mathbf{w}_n, \tag{2}$$

where $\rho_{\mathrm{p}}$ is the transmit power of the individual users, which is normalized by the noise power, and $\mathbf{w}_n \sim \mathcal{CN}(\mathbf{0}_{\tau_{\mathrm{p}}}, I_{\tau_{\mathrm{p}}})$ is a complex additive noise vector.

### B. AED UNDER PILOT SPOOFING ATTACK

In this work, we consider a situation in which an active Eve attempts maliciously to overhear user $\bar{k} \in \mathcal{K}$.[4] It is assumed that Eve has access to the vectors $\boldsymbol{\varphi}_k$'s for all $k \in \mathcal{K}$ as the set of pilots is public and standardized. During the pilot training phase, Eve transmits the pilot vector $\boldsymbol{\varphi}_{\bar{k}}$ to spoof APs. In this scenario, the received signal by the $n$th AP can now be expressed as

$$\mathbf{r}_n = \sqrt{\tau_{\mathrm{p}} \rho_{\mathrm{p}}} \sum_{k=1}^{K} g_{nk} \boldsymbol{\varphi}_k + \sqrt{\tau_{\mathrm{p}} \rho_{\mathrm{e}}}\, g_{n\mathrm{e}} \boldsymbol{\varphi}_{\bar{k}} + \mathbf{w}_n, \tag{3}$$

where $\rho_{\mathrm{e}}$ is the unknown normalized transmit power of Eve and $g_{n\mathrm{e}} = \beta_{n\mathrm{e}}^{\frac{1}{2}} h_{n\mathrm{e}}$ is the channel gain between Eve and the $n$th AP, which is modeled as in (1). We assume that the transmit power of Eve $\rho_{\mathrm{e}}$ is unknown at the receiver and therefore modeled by a uniform continuous PDF with mean of $\rho_{\mathrm{p}}$ and variance $\sigma_{\mathrm{e}}^2$.

As observed in (3), the pilot signal vector launched by Eve can spoof APs to estimate the channel gains of user $\bar{k}$ as

3. In the cell-free m-MIMO literature, the adjective *massive* refers to using a large number of distributed APs, as opposed to a large number of collocated antennas.

4. The CPU is assumed to be free of any attacks by an external nuisance.

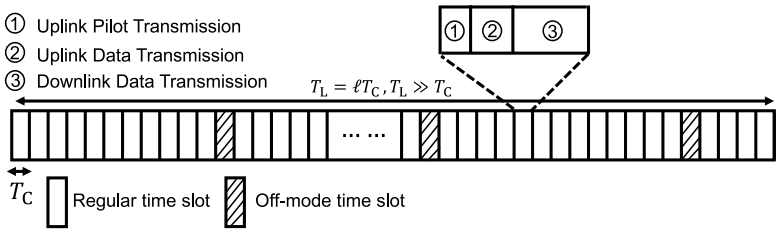



**FIGURE 1.** Division of interval $T_L$ into $\ell$ time slots $T_C$ and allocation of $q \ll \ell$ off-mode time slots to a given user $k$.

a linear combination of its true channel gains, i.e., $\{g_{n\bar{k}}\}_{n=1}^{N}$ and those of Eve $\{g_{ne}\}_{n=1}^{N}$. In turn, these biased estimates will compel the APs to partially beamform the signals intended for user $\bar{k}$ toward Eve. This unwanted process enables Eve to overhear maliciously the message intended for user $\bar{k}$. Detection of this *pilot spoofing* attack, which can be regarded as an abnormality in the received signals by APs, is a key step toward providing secure communication in a cell-free m-MIMO system.

## III. PROPOSED AED METHODS

In this section, we propose two methods for detecting a spoofing attack by an Eve during the uplink training phase in a cell-free m-MIMO system. Both AED methods use the LLRT as the detection metric, which is optimal in the sense of maximizing the detection probability for a given admissible rate of false alarm [40]. In the first method, the detection process is carried out by the CPU in a centralized fashion, while in the second method, a decentralized detection approach via APs is adopted. In both methods, the final decision on whether an abnormality occurs or not is made by the CPU.

The two methods take advantage of the following operational procedures, or protocol, which we propose to employ for the transmission of consecutive pilot symbol vectors of the legitimate users:

- Channel estimation with pilot symbol vectors is performed every $T_C$, simultaneously for all but possibly one user (see below). Note that within a time slot of length $T_C$, channel estimation and data transmission in both uplink and downlink directions are performed.
- During a time interval $T_L = \ell T_C$, each user should switch $q \geq 1$ times to an off-mode of duration $T_C$, by refraining from transmitting pilot symbols and data. That is, $Kq$ out of the $\ell$ non-overlapping time slots of duration $T_C$ available within the interval $T_L$ are selected and assigned to the $K$ users, i.e., $q$ distinct time slots for each user (see Fig. 1).
- The $Kq$ chosen time slots can be assigned through a deterministic or random scheme to different users. The latter scheme can provide a more secure assignment of time slots at the cost of a more complex scheduling.
- We assume that Eve does not have access to the indices of the $Kq$ time slots. One possible approach to achieve this condition is by using a common random number generator at the legitimate users and the CPU, and unpredictably sending a new confidential random seed from the CPU to the users via a secure broadcast channel [41], [42]. Other more sophisticated (and secure) approaches, wherein each user generates non-overlapping random patterns for the off-time slots and communicate them to the CPU, are also feasible (see Remark 1).

*Remark 1:* To avoid Eve to have access to indices of time slots, one can partition the interval $T_L = \ell T_C$ (see Fig. 1) into $S = \min(\tau_p, K)$ subintervals of equal length (but not necessarily contiguous) and assign each user, or group of users sharing the same pilot for the case where $K > \tau_p$, a subinterval $1 \leq s \leq S$. The subinterval indices can be assigned randomly to the users (in $S!$ possible ways), and sent to them at the beginning of training phase. Then, each user chooses randomly a pattern of off-mode time slots out of $\binom{\lceil \ell/S \rceil}{q}$ and send indices (of the selected off-mode time slots) to the CPU via APs during an uplink transmission phase. In the case $K > \tau_p$, the random number generators of users assigned with the same pilots must use a same seed. Therefore, the total number of possible patterns, which is a design parameter, is equal to $S!\binom{\lceil \ell/S \rceil}{q}$. This number can be quite large for practical values of system parameters, which in turn, renders the inference of the correct pattern by Eve almost impossible in advance of pilot transmission. For example, this number varies between $3 \times 10^{19}$ and $6 \times 10^{19}$ by selecting $q = 1$ for an operating system with $K > \tau_p = S = 20$ and $250 \leq \ell \leq 500$.

*Remark 2:* Since the parameter $\ell$ is sufficiently large in practice, i.e., $\ell \gg q$, the per user SE is negligibly affected by allocating a small fraction of the time slots to each user's off-mode. Specifically, for typical values of $\ell$, e.g., $250 \leq \ell \leq 1000$, and $q \leq 5$ the corresponding reduction in SE is $\frac{q}{\ell} \leq 2\%$.

*Remark 3:* We emphasize that off-mode switching by legitimate users allows APs to not only improve AED performance by isolating Eve's signal (see (4) below), but also recognize which user is being attacked by Eve. Moreover, since the occurrence of off-mode time slots is in principle unbeknown to Eve, the latter cannot imitate an off-mode switching that is synchronous with that of the target user.

*Remark 4:* The existence of a secure channel is also considered in the physical security problems addressed in the literature. For example, the ERD as a well-known detector

for pilot spoofing attack, assumes that there exists a secure channel to feedback some data from the base station to a legitimate user during the detection process [37].

*Remark 5:* One might argue that what would happen if Eve only launch the attack for only a fraction of time slot rather than the whole $T_{\mathrm{L}}$ time interval. Let us imagine Eve does not want to send pilots during $\kappa$ time slots out of $\ell$ within a time interval $T_{\mathrm{L}}$. Moreover, let us denote $d_q$ as the distance between the first and the last off-mode time slots and define $d_q = 0$ for $q = 1$. Since Eve is not aware of the pattern of off-mode time slots, we assume that it chooses randomly a subset of time slots. Hence, the probability of choosing an interval that involves all $q$ off-mode time slots is upperbounded as

$$P_c \leq \begin{cases} 0, & \kappa < d_q, \\ \frac{\kappa - d_q}{\binom{\ell}{\kappa}}, & \kappa \geq d_q \end{cases}$$

Note that the proposed method has a high probability of detection (even when $q = 1$) and Eve requires not to send pilots in all $q$ time intervals to avoid being detected. Now, we consider a scenario where $d_q = 0$, $\ell = 100$, and $\kappa = 30$. $P_c$ has a value of close to zero. This also decreases Eve's spectral efficiency by 30%. Note that the achievable EVe's SE is already affected due to the interference between the transmitted pilot by the legitimate user.

The above protocol assumes that $K \leq \tau_{\mathrm{p}}$ which, as explained earlier, may limit its application to low- to moderate-mobility environments. The extension of the protocol to high-mobility environments, where $K > \tau_{\mathrm{p}}$ will be discussed in Section III-C.

### A. CENTRALIZED AED

Let the successive off-mode time slots of a desired (legitimate) user $k \in \mathcal{K}$ be indexed by $t = \{1, 2, \ldots, q\}$. Moreover, let $\mathcal{E}$ denote the condition that Eve is targeting one of the users, say $\bar{k} \in \mathcal{K}$, in the time slot $t$. Following the signal model given in (3), the received signal by the $n$th AP can be written as follows:

$$\mathbf{r}_n[t] = \begin{cases} \sqrt{\tau_{\mathrm{p}}\rho_{\mathrm{p}}} \sum_{\substack{l=1 \\ l \neq k}}^{K} g_{nl}[t]\boldsymbol{\varphi}_l \\ \quad + \sqrt{\tau_{\mathrm{p}}\rho_{\mathrm{e}}} g_{n\mathrm{e}}[t]\boldsymbol{\varphi}_{\bar{k}} + \mathbf{w}_n[t], \ \text{if } \mathcal{E} \\ \sqrt{\tau_{\mathrm{p}}\rho_{\mathrm{p}}} \sum_{\substack{l=1 \\ l \neq k}}^{K} g_{nl}[t]\boldsymbol{\varphi}_l + \mathbf{w}_n[t], \ \text{if not } \mathcal{E} \end{cases} \tag{4}$$

The goal is to determine whether Eve, if present, is targeting desired user $k$ or not at time slot $t$. To this end, we define binary hypotheses $H_1$ and $H_0$ as follows:

- $H_1$: Eve is present and targets user $k$, i.e., $\bar{k} = k$.
- $H_0$: Eve is either absent or, if present, does not target $k$, i.e., $\bar{k} \neq k$.

During each off-mode time slot $t$, the $n$th AP finds the projection of $\mathbf{r}_n[t]$ on $\boldsymbol{\varphi}_k$ and sends the resulting scalar projection $y_{nt} = \boldsymbol{\varphi}_k^H \mathbf{r}_n[t]$ to the CPU where detection will be carried out based on all received $y_{nt}$'s. From a detection perspective, the scalar projections $y_{nt}$'s include sufficient information for the AED; besides, sending $y_{nt}$'s from APs to the CPU, imposes a low overhead on the fronthaul links which is a critical issue for cell-free m-MIMO systems. Depending on whether $H_1$ occurs or $H_0$, two possibilities are considered for the scalar projection $y_{nt}$:

$$y_{nt} = \begin{cases} \sqrt{\tau_{\mathrm{p}}\rho_{\mathrm{e}}} g_{n\mathrm{e}}[t] + v_{nt}, & H_1 \\ v_{nt}, & H_0 \end{cases} \tag{5}$$

where $v_{nt} = \boldsymbol{\varphi}_k^H \mathbf{w}_n[t] \sim \mathcal{CN}(0, 1)$ is a complex additive noise term uncorrelated over the AP and time slot indices, i.e., $n$ and $t$.

*Remark 6:* Clearly, the signals $\mathbf{r}_n[t]$'s in (4) could be used instead of their scalar projections $y_{nt}$'s in (5), to detect the abnormality through the LLRT metric by using more information. By doing so, however, the fronthaul overhead would be unacceptably increased by a factor of $\tau_{\mathrm{p}}$ per detection cycle where typically $\tau_{\mathrm{p}} \geq K \gg 1$ [3]. Moreover, finding some closed-form expressions for conditional PDFs of $\mathbf{r}_n[t]$ given $H_1$ and $H_0$ is not generally an easy task since it requires $K$-fold integration of a $\tau_{\mathrm{p}}$-variate normal distribution with correlated components. Besides, the proposed methods derived under the projection model in (5) achieves notable performance in terms of detection and false-alarm probabilities (see Section IV).

*Remark 7:* The detection process for a desired user $k \in \mathcal{K}$ is performed *independently* of other legitimate users $k' \in \mathcal{K} \setminus \{k\}$, via processing the received signals collected during the $q$ off-mode time slots of user $k$. Hence, the AED methods, working under the proposed protocol, can identify simultaneous attacks launched by multiple Eves on multiple legitimate users for a maximum duration of $T_{\mathrm{L}}$. This property allows us to simplify our analysis to the case where the system is comprised of one legitimate user (herein identified as user $k$) and one Eve.

After receiving all $y_{nt}$'s, the CPU first assembles them into a long vector:

$$\mathbf{y} = [\mathbf{y}_1; \mathbf{y}_2; \ldots; \mathbf{y}_N], \quad \mathbf{y}_n = [y_{n1}, y_{n2}, \ldots, y_{nq}]^T. \tag{6}$$

Then, the following LLRT metric will be calculated by the CPU [40]:

$$\Lambda(y) = \ln f_{\mathbf{y}}(y|H_1) - \ln f_{\mathbf{y}}(y|H_0) \underset{\mathcal{H}_0}{\overset{\mathcal{H}_1}{\gtrless}} \ln \eta, \tag{7}$$

where $y$ is a realization of $\mathbf{y}$, and $\eta \in \mathbb{R}$ is the threshold value. As seen from (5), the conditional PDF $f_{\mathbf{y}}(y|H_0)$ can be readily derived since $\mathbf{y}$ is a circularly symmetric complex Gaussian vector under hypothesis $H_0$. Specifically, we have

$$f_{\mathbf{y}}(y|H_0) = \frac{1}{\pi^{qN}} \exp\left\{-\|y\|^2\right\}. \tag{8}$$

Under hypothesis $H_1$, $\mathbf{y}$ is a mixed complex normal-lognormal vector with $N$ independent random subvectors $\mathbf{y}_n$ each one consisting of $q$ dependent random elements due to their sharing of a common large-scale fading gain $\beta_{n\mathrm{e}}^{\frac{1}{2}}$, as seen from (5). By using this fact, we shall first derive the conditional PDF $f_{\mathbf{y}_n}(y_n|H_1, \rho_{\mathrm{e}})$ and then, invoke

the independence of the $\mathbf{y}_n$'s to obtain $f_{\mathbf{y}}(y|H_1, \rho_e)$ via the multiplicative rule, i.e.,

$$f_{\mathbf{y}}(y|H_1, \rho_e) = \prod_{n=1}^{N} f_{\mathbf{y}_n}(y_n|H_1, \rho_e). \tag{9}$$

Finally, we can obtain the conditional PDF $f_{\mathbf{y}}(y|H_1)$ via integration as [43]

$$f_{\mathbf{y}}(y|H_1) = \int_{\rho_e} f_{\mathbf{y}}(y|H_1, \rho_e) f_{\boldsymbol{\rho}_e}(\rho_e) d\rho_e. \tag{10}$$

For simplicity in our mathematical analyses, we assume that the average path loss $a_{ne}$ associated with Eve's channel is deterministic and normalized to unity from now on. In our study, the parameter $a_{ne}$ only represents the *average* path loss due to spatial propagation. Hence, for the sake of simplifying derivations, it makes sense to assume that this parameter is deterministic. It should be noted that in this section, while we set $a_{ne}$ to 1, we still use the general channel gain model (1) wherein shadow fading is considered through the lognormal random variable $z_{nk}$. The generalization to the random case can be obtained by using the PDF $f_{\boldsymbol{a}_{ne}}(a_{ne})$ and refining (10) as

$$f_{\mathbf{y}}(y|H_1) = \int_{a_{ne}} \int_{\rho_e} f_{\mathbf{y}}(y|H_1, a_{ne}, \rho_e) \times f_{\boldsymbol{a}_{ne}}(a_{ne}) f_{\boldsymbol{\rho}_e}(\rho_e) da_{ne} d\rho_e. \tag{11}$$

Specifically, analytical and simulation results for the random case based on the refined model in (11) show a very similar trend to the normalized case (Section IV-C), as reported in Section IV-D.

Lemma 1 provides a closed-form expression for $f_{\mathbf{y}_n}(y_n|H_1, \rho_e)$ in terms of a finite summation including weighted functions of zeros of a Hermite polynomial [44, p. 890].

*Lemma 1:* The conditional PDF of the mixed complex normal-lognormal vector $\mathbf{y}_n = [y_{n1}, y_{n2}, \ldots, y_{nq}]^T$ can be expressed as

$$f_{\mathbf{y}_n}(y_n|H_1, \rho_e) = \frac{1}{\pi^{q+\frac{1}{2}}} \times \sum_{i=1}^{I} \frac{\omega_i}{\Psi^q(x_i)} \exp\left\{\frac{-\|y_n\|^2}{\Psi(x_i)}\right\} + R_{I,n}(\xi), \tag{12}$$

for some real number $\xi$, where

$$\Psi(x) = 1 + \tau_p \rho_e \exp\{b\,\sigma_{sh} x\}, \quad b = \left(\sqrt{2}\ln 10\right)/10,$$
$$R_{I,n}(\xi) = \frac{\pi^{-q} I!}{2^I (2I)!} \frac{\partial^{2I}\left[\Psi^{-q}(\xi)\exp\left\{-\|y_n\|^2/\Psi(\xi)\right\}\right]}{\partial \xi^{2I}},$$
$$\omega_i = \frac{\sqrt{\pi} 2^{I-1} I!}{(I H_{I-1}(x_i))^2},$$

$x_i$ is the $i$th zero of the Hermite polynomial $H_I(x)$ with degree $I$, greater than one.[5]

*Proof:* See Appendix A. ∎

5. The Hermite polynomial $H_I(x)$ is constant for $I = 0$ and does not have any zeros. Hence, $\omega_i$ is not well defined for $I = 1$.

*Remark 8:* Note that $R_{I,n}(\xi)$ in (12) is a residual term that can be neglected under appropriate conditions (see Remark 9 below). Therefore, the PDF $f_{\mathbf{y}_n}(y_n|H_1, \rho_e)$ can be approximated by a closed-form expression consisting of a finite sum of weighted exponential functions. That is, $f_{\mathbf{y}_n}(y_n|H_1, \rho_e) \approx \hat{f}_{\mathbf{y}_n}(y_n|H_1, \rho_e)$ where

$$\hat{f}_{\mathbf{y}_n}(y_n|H_1, \rho_e) = \frac{1}{\pi^{q+\frac{1}{2}}} \sum_{i=1}^{I} \frac{\omega_i}{\Psi^q(x_i)} \exp\left\{\frac{-\|y_n\|^2}{\Psi(x_i)}\right\}. \tag{13}$$

The main reason behind using the above approximation lies in the fact that a closed-form expression of the conditional PDF $f_{\mathbf{y}_n}(y_n|H_1, \rho_e)$ will be required for our analyses in Theorem 1 (below). Using the integral form of the PDF $f_{\mathbf{y}_n}(y_n|H_1, \rho_e)$ renders these analyses intractable.

*Remark 9:* Since random vectors $\mathbf{y}_n$'s are independent with respect to index $n$, the multiplication rule of independent PDFs can be applied to obtain the conditional PDF of $\mathbf{y}$ by using $\hat{f}_{\mathbf{y}_n}(y_n|H_1, \rho_e)$. However, it is possible that the multiplication of approximated PDFs might bring about a large difference between the approximated and true PDF of $\mathbf{y}$. To investigate this concern, we conduct a Monte Carlo simulation for the average relative error between the exact and approximate conditional PDFs of $\mathbf{y}$ in Section IV-B and observe that the relative error is quite negligible for a practical range of parameters $\sigma_{sh}$, $\rho_e$, and $q$ when $I \geq 70$. Based on this observation, we can use the expression in (13) and approximate the conditional PDF of $\mathbf{y}$ as

$$\hat{f}_{\mathbf{y}}(y|H_1, \rho_e) = \prod_{n=1}^{N} \hat{f}_{\mathbf{y}_n}(y_n|H_1, \rho_e). \tag{14}$$

So far, the left-hand side (LHS) of the LLRT in (7) is specified, while it is still necessary to determine the threshold value $\eta$. Let $P_d$ and $P_f$ respectively denote the probabilities of detection and false alarm, defined as

$$P_d = \mathbb{P}(\Lambda(\mathbf{y}) > \ln\eta \,|\, H_1), \tag{15}$$
$$P_f = \mathbb{P}(\Lambda(\mathbf{y}) > \ln\eta \,|\, H_0). \tag{16}$$

In practice, $\eta$ should be chosen such that a high $P_d$ is achieved while keeping $P_f$ close to zero. This can be done, prior to system deployment, by calculating or measuring both probabilities for different values of $\eta$ and sketching the receiver operation characteristic (ROC) in the $P_f P_d$-plane [40], [45]. In the next section, several ROC curves corresponding to different values of $N$ are provided where it can be observed that $P_d$ and $P_f$ go to one and zero, respectively as the number of APs, i.e., $N$ increases without bound. This result can also be shown by an asymptotic analysis summarized as Theorem 1 where $\rho_e$ is assumed to be deterministic.

*Theorem 1:* Let $P_{d|\rho_e}$ and $P_{f|\rho_e}$ be the detection and false-alarm probabilities, respectively, conditioned on $\rho_e = \rho_e$. Write the threshold value in (7) as $\eta = \eta_0^{-N}$ for some $\eta_0 > 0$. If

$$L_{H_1} < \ln\eta_0 < U_{H_0}, \tag{17}$$

where

$$L_{H_1} = \ln\left(\frac{\sqrt{\pi}}{\Upsilon_q}\right) - q\left(1 + \tau_p \rho_e \exp\left\{b^2\sigma_{sh}^2/4\right\}\right)\left(1 - \frac{\Upsilon_{q+1}}{\Upsilon_q}\right),$$

$$U_{H_0} = \ln\left(\frac{\sqrt{\pi}}{\Omega_q I}\right) - q(1-\psi),$$

$$\Upsilon_q = \sum_{i=1}^{I\geq 2} \frac{\omega_i}{\Psi^q(x_i)},\ \Omega_q = \max_i \frac{\omega_i}{\Psi^q(x_i)},\ \psi = \min_i \frac{1}{\Psi(x_i)},$$

then

$$\lim_{N\longrightarrow\infty} P_{d|\rho_e} = 1, \quad \lim_{N\longrightarrow\infty} P_{f|\rho_e} = 0.$$

*Proof:* See Appendix B ∎

*Remark 10:* It should be noted that assumption (17) requires $U_{H_0} - L_{H_1} > 0$ to be fulfilled for different values of $\rho_e$, $q$, and $\sigma_{sh}$. In Section IV-B it is shown that this condition is readily satisfied for different values of $q$ and $\sigma_{sh}$, except when $\rho_e$ is too small.

*Remark 11:* The analytical expression for $\Lambda(\mathbf{y})$ in (7) is intractable when $\boldsymbol{\rho}_e$ is random, which renders difficult a similar proof for the general case. Although the results of Theorem 1 hold true under the assumption that $\rho_e$ is deterministic, simulations conducted in Section IV-C indicate that they still hold when $\boldsymbol{\rho}_e$ is random. Moreover, it can be understood from Theorem 1 that in order to approach an ideal performance for AED, i.e., having a high $P_{d|\boldsymbol{\rho}_e}$ and a low $P_{f|\boldsymbol{\rho}_e}$, the absolute value of $\ln\eta$ should increase with the number of APs, i.e., $N$. This result is also confirmed in Section IV-C.

### B. DECENTRALIZED AED

Although the centralized method can approach the ideal point (0, 1) in the $P_fP_d$-plane by increasing the number of APs, it may suffer from two issues in practice. Firstly, the fronthaul overhead is high as the number of APs is large in a cell-free m-MIMO system. Specifically, the fronthaul overhead of the centralized method during the time interval $T_L$, which is on the order of $\mathcal{O}(qNKB_L)$ where $B_L$ is the number of bits used for the representation of signal values communicated to the CPU, grows linearly with $N$ as each AP must send several bits to the CPU. Secondly, due to the unknown power of Eve, choosing an appropriate value of $B_L$ to minimize the fronthaul overhead without degrading AED performance remains challenging. To alleviate these difficulties, we propose a decentralized method which can be performed in three steps:

- The $n$th AP uses the signal vector $y_n$ to detect the abnormality via the LLRT. To this end, each AP uses the given PDF in (13).
- If the AP detects an abnormality, it informs the CPU about the presence of a possible pilot spoofing attack. This can be simply done by sending a *one-bit* message through the fronthaul links.[6]
- The CPU first collects all one-bit signals sent by the APs which have detected a possible abnormality. Then, the CPU decides whether a pilot spoofing attack occurred or not based on a majority-decision principle.
- Different strategies can be adopted by the CPU to make the final decision on the presence of a spoofing attack. Generally, the one-bit messages received from the different APs can be weighted (by a factor reflecting to the quality of this information), summed and compared to a global threshold. While this practice may improve the final detection performance, it would require the APs to send additional information to the CPU (e.g., strength of signals $y_{nt}$, noise power level) which, in turn increases the fronthaul overhead. In this work, we use a special case of this general approach, i.e., majority voting, to make the final decision at the CPU.

Let $p_d$ and $p_f$ be the detection and false-alarm probabilities of an AP, respectively, for a given threshold. The fronthaul overhead complexity imposed by the decentralized method is on the order of $\mathcal{O}(NKp_d)$ when an attack is launched by an Eve while it is on the order of $\mathcal{O}(NKp_f)$ when there is no attack. Comparing with the centralized method, the fronthaul overhead decreases by a factor of $qB_L/p_f$ when no attack occurred and $qB_L/p_d$ when an attack is launched.

Next, we conduct an asymptotic analysis, similar to the centralized AED, to see the impact of $N$ over the detection and false-alarm probabilities. To this end, we need to redefine $P_d$ and $P_f$ for the decentralized AED since the final decision is made by the CPU based on the received bits (not the signals $\mathbf{y}_n$) from the APs. Specifically, we define $P_d$ and $P_f$ as the probabilities of observing at least $\frac{N}{2}$ one-bit messages at the CPU[7] when $H_1$ and $H_0$ are true, respectively. The following theorem reveals that the ideal point (0, 1) in the $P_fP_d$-plane is achievable as the number of APs goes to infinity.

*Theorem 2:* If $p_d > \frac{1}{2}$ and $p_f < \frac{1}{2}$, then, we have

$$\lim_{N\longrightarrow\infty} P_d = 1, \quad \lim_{N\longrightarrow\infty} P_f = 0.$$

*Proof:* See Appendix C ∎

*Remark 12:* The conditions $p_d > \frac{1}{2}$ and $p_f < \frac{1}{2}$ in the theorem should be fulfilled to approach the ideal point (0, 1) in the $P_fP_d$-plane as $N$ increases. The feasibility of these conditions is examined in Section IV-B where it is shown that there exist points of the ROC curves which lie in the square region defined by $p_d > \frac{1}{2}$ and $p_f < \frac{1}{2}$ in the $p_fp_d$-plane.

6. In this work, the overhead is evaluated in terms of required *information bits*. In practice, such bits must be embedded as payload in larger messages along with header and framing bits, so that in fact, each information bit requires the transmission of $\gamma > 1$ bits. The exact value of $\gamma$ depends on higher layer protocols, which falls outside the scope of this work. Without loss of generality in our comparison, we herein set $\gamma = 1$.

7. In order to avoid confusion in decision when the number of APs is even, an AP can be turned off during the detection cycle or the CPU discards a received bit by an AP.

### C. EXTENSION TO HIGH-MOBILITY ENVIRONMENTS ($K > \tau_p$)

In this subsection, we discuss how the proposed protocol can be extended to a high-mobility environment through a rearrangement of available pilots *if needed*.

Let us assume that the number of users exceeds the number of available orthogonal pilots, i.e., $K > \tau_p$, so that pilot reuse is necessary. Let $K_{\max}$ denote the maximum number of users sharing a common pilot sequence, referred to as a *group* in the following discussion. Under these conditions, our detection protocol is still applicable since users belonging to the same group can switch simultaneously to an off-mode during the same time slot. Note that the system model used under the constraint $K \leq \tau_p$ will not be invalidated. The only task that might be required is the identification of the specific user within a group being targeted by the attack. If this is necessary, the following identification strategy can be incorporated into the proposed protocol.

Once the system recognizes that a group of user associated to a common pilot is being attacked by a malicious Eve, the system first removes the pilot of the attacked group from its pilot set and then, renews its pilot assignment such that users of the group do not share the same pilot. After the rearrangement, the system will be able to identify which user is under attack once Eve has changed its pilot to the new one. The rearrangement process can be performed in two ways: the system reshuffles all pilot signals to find a subset of orthogonal pilots for the group; or a subset of orthogonal pilots with cardinality $K_{\max}$ is set aside in advance and used for the pilot rearrangement. The value of $K_{\max}$ is dependent upon the number of users $K$ and pilot length $\tau_p$. For example, if the system operates under high mobility (e.g., $v = 108$km/h and $\tau_c = 750$) and needs to support 100 users with $K_{\max} = 4$, we require a total of $25 + 4 = 29$ pilots to accommodate the rearrangement, which represents 3.87% of $\tau_c$.

In the problem of active eavesdropping, the ultimate goal is to maximize the achievable rate of the attacked user while limiting that of Eve to a low predefined threshold (without affecting other legitimate users). This goal can be achieved at the CPU where the power allocation task is performed by solving a constraint optimization problem [3]. Note that the optimization problem should be formulated to maximize the sum rate or the minimum achievable rate of users in the group under attack. Therefore, if knowledge of the specific user under attack is not needed, the identification stage can be excluded from the protocol to reduce the countermeasure delay.

Based on the above discussion, our analysis of the probability of detection $P_d$ and false alarm $P_f$ for an Eve remains valid even if $K > \tau_p$. Under the latter condition, while some users will be forced to share a common pilot sequence, they will simultaneously switch to the off-mode, so that only Eve is active during the detection phase. Hence, $P_d$ and $P_f$ will not be affected.

Next, we examine the performance of the identification strategy when it is applied to the proposed methods. To this end, we consider a situation in which a particular user, belonging to a group of users sharing the same pilot sequence, is being targeted by Eve. Let $\mathcal{A}$ denote the event that the group is correctly detected during a first off-mode time slot, and let $\mathbb{P}(\mathcal{A})$ denote the corresponding probability. Following the detection, the pilots will be reassigned so that in the next off-mode time slot for that particular user, there is no longer ambiguity as to which user is being attacked. Let $P_{\text{id}}$ denote the probability of correctly identifying the user during this second off-mode time slot, which can be expressed as

$$P_{\text{id}} = P_{\text{id}|\mathcal{A}}\mathbb{P}(\mathcal{A}) + P_{\text{id}|\bar{\mathcal{A}}}\mathbb{P}(\bar{\mathcal{A}}), \tag{18}$$

for the decentralized method. Clearly, the probability $\mathbb{P}(\mathcal{A})$ is equal to $P_d$ (see (15)) and so is $P_{\text{id}|\mathcal{A}}$. The reason for the latter is that the identification process becomes the same as the detection process after the pilot rearrangement. Hence, from Theorem 2 we have

$$\lim_{N\to\infty} P_{\text{id}} = \lim_{N\to\infty} P_d^2 = 1, \tag{19}$$

For the centralized method, it can similarly be argued that $\lim_{N\longrightarrow\infty} P_{\text{id}|\rho_e} = 1$ by using the result of Theorem 1.

## IV. SIMULATION RESULTS AND DISCUSSION

In this Section, we first describe the methodology employed in our simulations. Then, we examine the validity of conditions and approximations made in Section III. Finally, we present our simulation results which are obtained under the scenarios of normalized and random path loss.

### A. METHODOLOGY

For our simulations with normalized path loss, we consider the system model given in (3) with composite channel gains as in (1), where the average path loss $a_{ne}$ is set to a deterministic value such that $\mathbb{E}\{\beta_{ne}\} = 1$. Since the variances of the small-scale fading gains and additive noise terms are set to 1, the parameter $\rho_e$ in effect represents the average signal-to-noise ratio (SNR) when the effect of $\tau_p$ is absorbed into $\rho_e$ (see (3)-(5)). We consider this case in Figs. 7–11 to accentuate the effects of the number of APs $N$ and off-mode time slots $q$ on the system performance. In our experiments for this case, the unknown $\rho_e$ is uniformly distributed in the interval $[1.4, 4.9]$ which yields a mean of 3.15 (or 5dB) and unit variance. This assumption is only applied to a subset of the figures, where the aim is to investigate the effect of some key parameters such as number of APs. The performance of system is also investigated over the much wider SNR interval $\rho_e \in [-15, 5]$dB in Figs. 9–10 and 12–13.

In Theorem 1 and Remark 11, the threshold $\eta$ for the centralized method is set as $\eta_0^{-N}$ with $\eta_0 \in [0.01, 500]$ (or approximately equivalently $\ln(\eta_0) \in [-4.61, 6.21]$). For

the decentralized AED method, the threshold is chosen as $\eta = \eta_0^{-1}$. The chosen range for $\eta_0$ is sufficiently large to represent the performance of the proposed methods via ROC curves, which constitute a complete description for the performance of an LLRT-based detection approach. To obtain the ROC curves, we use the following standard procedure (see, e.g., [40], [46], [47]): For each point on the curve, which corresponds to a particular value of the detection threshold, we run several independent simulation runs for the given parameter setting (SNR, number of APs, etc.), implement the LRT detectors, and average the detection results to estimate the probability of detection $P_{\rm d}$ and probability of false alarm $P_{\rm f}$ for that point. The integrals in (10) is numerically computed by MATLAB's built-in function `trapz`, since their derivation in closed-form is an intractable task.

It should be noted that in our simulation runs we do not directly fix geometrical or transmission parameters of Eve, but only assume some general knowledge about the statistics of these parameters, e.g., SNR and shadowing variance. In practice, these statistics can be obtained using standard, well-understood estimation methods whose description falls outside the scope of this work. In fact, our simulation methodology is to some extent more general than that employed in other works (e.g., [20] and [37]), where the large-scale fading is normalized to 1. Besides, the proposed detector does not need to know the location of Eve since the detector is designed based on the statistical knowledge of channel parameters. Moreover, we evaluate the performance of the proposed detector for both hypotheses, i.e., the presence and absence of Eve. In each simulation run of Section IV-D, we change the positions of Eve and APs randomly and generate the channel gains between Eve and each one of the APs. Which APs are the closest and farthest to Eve is in fact irrelevant from the perspective of our simulations, wherein the collection of data received by all APs is used to perform the detection, using either centralized or decentralized AED. It should be noted that in practice, large-scale fading parameters (e.g., path loss exponent or shadowing variance) are intrinsic properties of the radio environment which do not change with distance (in a given geographical area) [39]. That is, the distances affect the gains computed from these parameters, but not the parameters themselves.

### B. VALIDITY OF KEY ASSUMPTIONS AND APPROXIMATIONS

In this subsection, we investigate the validity of the approximations in (14), as well as the conditions invoked in Theorems 1 and 2.

First, we start by conducting Monte Carlo simulations to corroborate the accuracy of the approximated conditional probabilities in (14) for different parameter values. To this end, the following average relative error is used as accuracy metric:

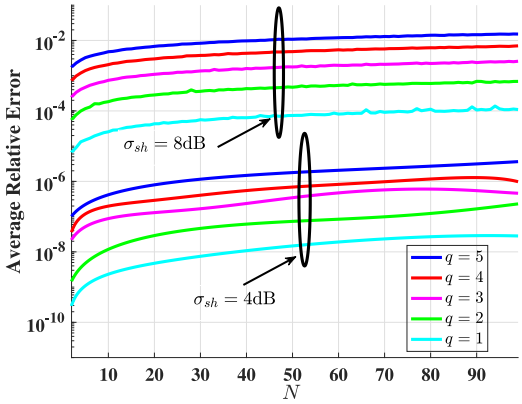



**FIGURE 2.** Average relative error between the approximated and true conditional PDFs of y versus $N$ for different values of $q$ ($\rho_{\rm p} = 5$dB, $\tau_{\rm p} = 16$).

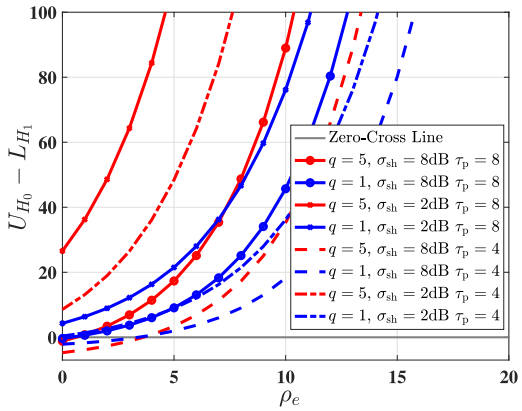



**FIGURE 3.** $U_{H_0} - L_{H_1}$ versus $\rho_{\rm e}$ (in dB) ($I = 70$).

$$\frac{1}{J}\sum_{j=1}^{J}\left|\frac{f_{\mathbf{y}}\left(y^{(j)}|H_1,\rho_{\rm e}\right)-\hat{f}_{\mathbf{y}}\left(y^{(j)}|H_1,\rho_{\rm e}\right)}{f_{\mathbf{y}}\left(y^{(j)}|H_1,\rho_{\rm e}\right)}\right|. \tag{20}$$

For the computation of $f_{\mathbf{y}}(y|H_1,\rho_{\rm e})$, we employ the integration form of the PDF of $\mathbf{y}_n$, i.e.,

$$f_{\mathbf{y}_n}\left(y_n|H_1,\boldsymbol{\rho}_{\rm e}\right) = \frac{1}{\pi^{q+\frac{1}{2}}} \times \int_{-\infty}^{\infty}\frac{1}{\Psi^q(\xi)}\exp\left\{\frac{-\|y_n\|^2}{\Psi(\xi)}-\xi^2\right\}d\xi, \tag{21}$$

and $\hat{f}_{\mathbf{y}}(y|H_1,\rho_{\rm e})$ is obtained by means of (13)-(14), and superscript $j$ refers to a realization. Fig. 2 displays the average relative error versus $N$ for different values of $q$, the number of off-mode time slots, and $\sigma_{\rm sh}$, the shadowing standard deviation. As seen from Fig. 2, the average relative error is negligible for a wide range of parameter values and increases with the shadowing standard deviation. Note that the curves, plotted for $\sigma_{\rm sh} = 4$dB, are fitted by polynomial functions to smooth fluctuations for a finer representation.

Second, we examine the validity of the condition $U_{H_0} - L_{H_1} > 0$ in Theorem 1 for different values of $q$ and $\sigma_{\rm sh}$. Fig. 3 depicts the value of $U_{H_0} - L_{H_1}$ versus $\rho_{\rm e}$ for different choices of these parameters. As seen from the figure, the condition

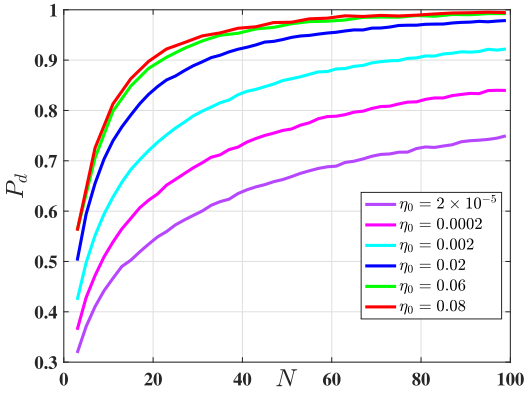



**FIGURE 4.** $P_{\mathrm{d}}$ versus $N$ for different values of $\eta_0$ (Centralized AED, $P_{\mathrm{f}} \approx 0$, $q = 1$, $\rho_{\mathrm{p}} = 5$dB, $\sigma_{\mathrm{sh}} = 8$dB, $\tau_{\mathrm{p}} = 8$).

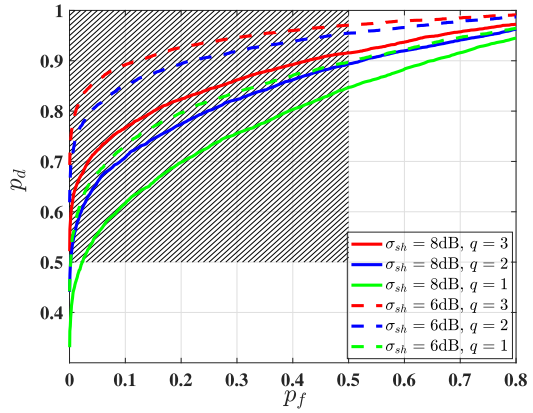



**FIGURE 5.** ROC curves of an AP for different values of $q$ and $\sigma_{\mathrm{sh}}$. The region associated with Theorem 2 is shown as the shaded area. ($\tau_{\mathrm{p}} = 8$).

can be readily satisfied except for values of $\rho_{\mathrm{e}} < 4$dB when $\tau_{\mathrm{p}} = 4$. Next, we validate the selection of $\eta = \eta_0^{-N}$ as a threshold value for the centralized method, which according to Theorem 1 allows to approach the ideal point $(0, 1)$ in the $P_{\mathrm{f}}P_{\mathrm{d}}$-plane. To this end, we present a plot of $P_{\mathrm{d}}$ versus $N$ in Fig. 4 by choosing different values for $\eta_0$, which satisfy the bound given in Theorem 1 (we note that $P_{\mathrm{f}} \approx 0$ for the plotted curve). It is evident from the figure that for a larger value of $\eta_0$, $P_{\mathrm{d}}$ approaches faster to the ideal point 1 as $N$ increases. Specifically for $\eta_0 > 0.02$, the proposed centralized method achieves the ideal point for $N$ on the order of $10^2$.

Third, we examine the condition $p_{\mathrm{d}} > 1/2$ and $p_{\mathrm{f}} < 1/2$ given in Theorem 2. To this end, Fig. 5 depicts this region in $p_{\mathrm{f}}p_{\mathrm{d}}$-plane (the shaded area) as well as ROC curves associated with an AP for different values of $q$ and $\sigma_{\mathrm{sh}}$. As seen from this figure, there exist points of the ROC curves which lie in the cross-hatched square. These observations along with results of Theorem 2 indicate for the decentralized method that the ideal point $(0, 1)$ in the $P_{\mathrm{f}}P_{\mathrm{d}}$-plane can be achieved as $N$ goes to infinity. In Fig. 6, we show a 3D plot of $P_{\mathrm{f}}$ and $P_{\mathrm{d}}$ versus $N$ for different values of $\eta_0$, selected such that $p_{\mathrm{d}} > 0.5$ and $p_{\mathrm{f}} < 0.5$. It can be seen that the projections of all curves onto the $P_{\mathrm{f}}P_{\mathrm{d}}$-plane converge to the ideal point $(1, 0)$ as $N$ increases, which is consistent with the result of Theorem 2. We note however that the convergence rate of the curves depends on the value of $\eta_0$. In particular, for $\eta_0 < 1.4$ or $\eta_0 > 2.2$, the value of either $p_{\mathrm{d}}$ or $p_{\mathrm{f}}$ is about 0.5 which explains the slower convergence.

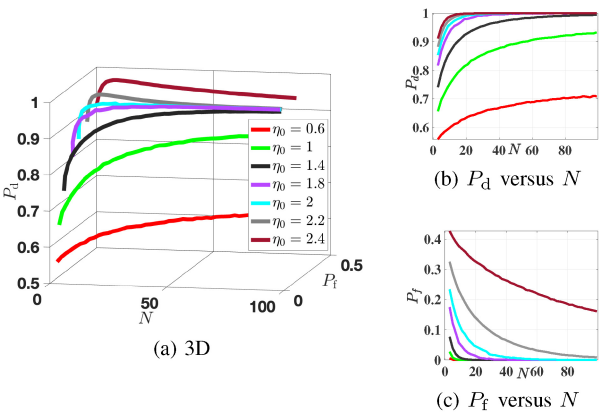



**FIGURE 6.** $P_{\mathrm{d}}$ versus $N$ and $P_{\mathrm{f}}$ for different values of $\eta_0$ (Decentralized AED, $q = 1$, $\rho_{\mathrm{p}} = 5$dB, $\sigma_{\mathrm{sh}} = 8$dB, $\tau_{\mathrm{p}} = 8$).

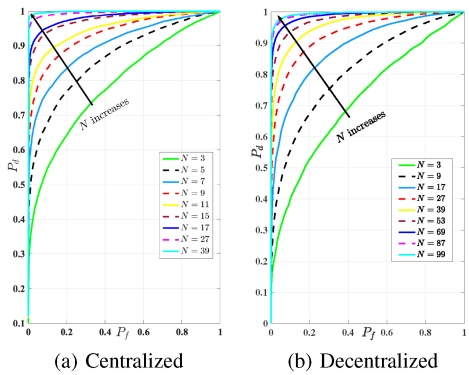



**FIGURE 7.** ROC curves of AED methods for different number of APs ($q = 1$, $\rho_{\mathrm{p}} = 5$dB, $\sigma_{\mathrm{sh}} = 8$dB, and the effect of $\tau_{\mathrm{p}}$ is absorbed).

### C. SIMULATION RESULTS FOR NORMALIZED PATH LOSS

In this subsection, we compare the performance of the centralized and decentralized AED methods for a cell-free m-MIMO system. To this end, we consider the system model in (5) with normalized path loss for Eve, i.e., $a_{ne} = 1$. Fig. 7 displays the ROC curves of the centralized and decentralized methods for different number of APs $N$[8] when the number of off-mode time slot per user is minimum, i.e., $q = 1$. As seen from Fig. 7, the probability of detection $P_{\mathrm{d}}$, for a given $P_{\mathrm{f}}$, approaches to 1 as the number of APs increases, for both methods. This result is consistent with the theoretical analysis in Section III. Moreover, the centralized method outperforms the decentralized one for given $P_{\mathrm{f}}$ and $N$. For instance, when $P_{\mathrm{f}} = 0.02$ and $N = 39$, the corresponding values of $P_{\mathrm{d}}$ are 0.99 and 0.75, respectively. This is explained

8. The number of APs varies typically between 60 to 100 in cell-free m-MIMO systems [1].

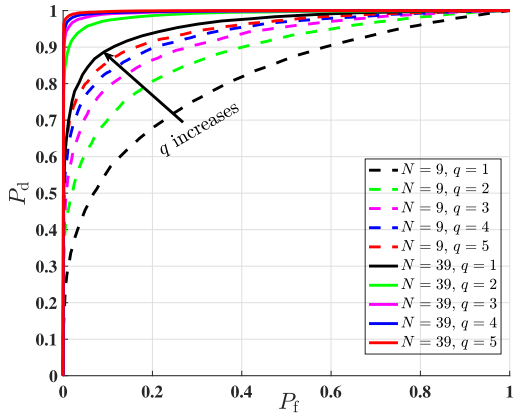



**FIGURE 8.** ROC curves of the decentralized method for different number of off-mode time slot $q$ ($\rho_p = 5$dB, $\sigma_{sh} = 8$dB, and the effect of $\tau_p$ is absorbed).

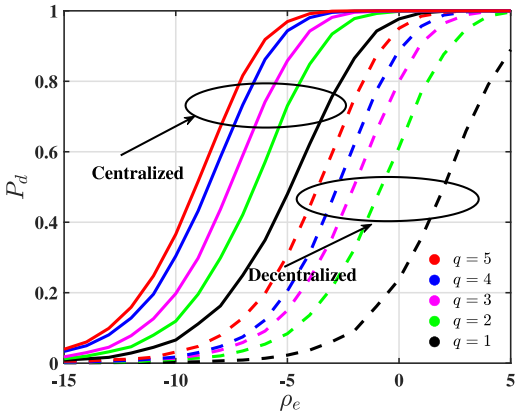



**FIGURE 9.** $P_d$ versus $\rho_e$ for different values of $q$. ($N = 99$, $\rho_p = 5$dB, $P_f \leq 0.001$, and the effect of $\tau_p$ is absorbed).

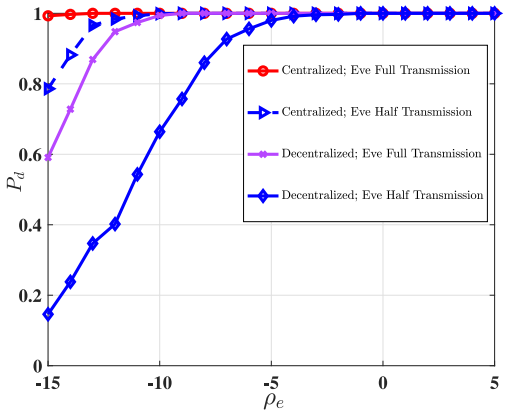



**FIGURE 10.** $P_d$ versus $\rho_e$ when Eve transmits over half of time slots within $T_L$. ($N = 69$, $q = 2$, $\rho_p = 5$dB, $P_f \leq 0.001$, $\tau_p = 32$).

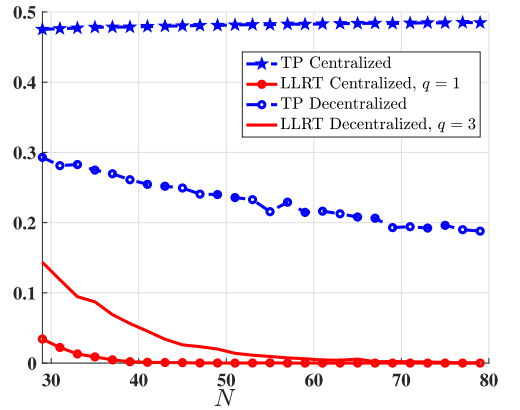



**FIGURE 11.** False alarm probability $P_f$ versus the number of APs $N$ for the TP approach and the proposed centralized method (the effect of $\tau_p$ is absorbed).

by the fact that in the centralized method, the CPU uses $N$ signal samples to detect the abnormality while each AP in the decentralized method uses only $q = 1$ sample.

In order to improve the performance of the decentralized method, one can use more samples, i.e., select $q > 1$ to enhance the detection performance at each AP. Fig. 8 depicts the ROC curves of the decentralized method for different values of $q$. As observed, the performance improves significantly by increasing the value of $q$ from 1 to 5. For example, $P_d$ varies from 0.73 to 0.99 for given $P_f = 0.02$, $N = 39$, as $q$ is increased from 1 to 5.

Next, we compare the performance of the proposed AED methods when Eve changes its transmission power $\rho_e$ while APs use the previous uniform distribution, with mean 5dB and unit variance, to model the unknown $\rho_e$. Fig. 9 depicts $P_d$ versus $\rho_e$ for different values of off-mode time slots $q$ when the number of APs $N$ is fixed to 99. The parameter $\eta_0$ is selected by solving

$$\max_{\eta_0} \; P_d(\eta_0), \quad \text{s.t.} \; P_f(\eta_0) \leq 10^{-3}, \tag{22}$$

where $\eta_0 \in [0.01, 500]$ and $\rho_e = -15$. For the decentralized method, the threshold $\eta$ is the same at all APs. As seen from Fig. 9, the performance of both methods improves as $q$ increases and that a value of $P_d$ exceeding 0.9 can be achieved at $\rho_e = -6$dB for the centralized method and $\rho_e = 0$dB for the decentralized one.

Here, we conduct a simulation in which Eve is assumed not to send a pilot during a fraction of time interval $T_L$. Specifically, Eve does not send the pilot within half of off-mode time slots. The results are displayed here in Fig. 10. As seen from the figure, the detection performance is affected over low values of SNR since the system sees noise during half of the time slots. However, the performance does not change and is still excellent over high SNR values.

Now, we compare the performance of the proposed methods with the TP scheme [3]. Fig. 11 illustrates the false alarm probability $P_f$ versus $N$ when the detection probability is $P_d \geq 0.98$ for both methods. It is seen that for the proposed centralized method, $P_f$ decays rapidly towards 0 as $N$ increases while it remains constant for the TP approach. In its decentralized form, the proposed method also significantly outperforms the TP approach. Interestingly, the TP approach has a better performance when it is implemented

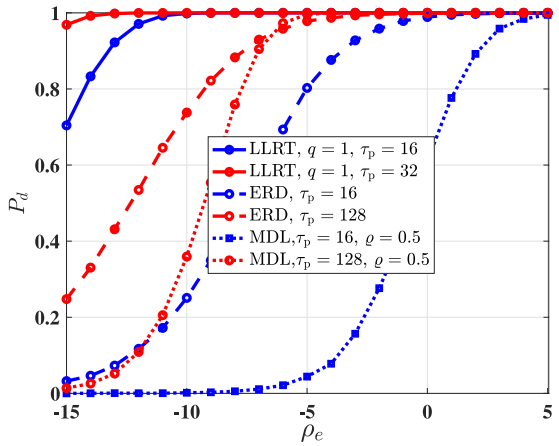



**FIGURE 12.** $P_d$ versus $\rho_e$ for different methods implemented in the centralized fashion ($N = 99$, $\rho_p = 5$dB).

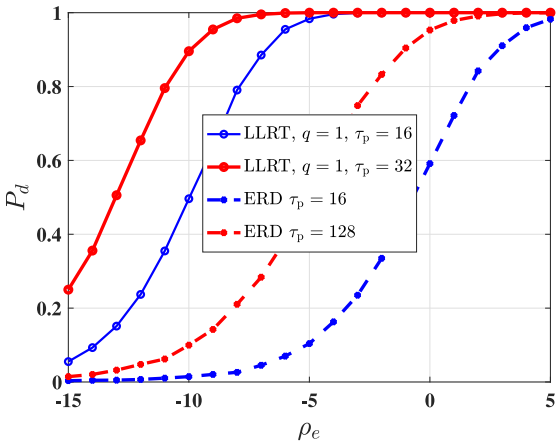



**FIGURE 13.** $P_d$ versus $\rho_e$ for different methods implemented in the decentralized fashion ($N = 99$, $\rho_p = 5$dB).

in a decentralized way. This result is not surprising since the false alarm probability of the TP approach for a single-antenna AP is less than 0.5 (i.e., $p_f \approx 0.45$). Therefore, $P_f$ for the decentralized implementation of TP decreases as the number of APs increases (see Theorem 2).[9]

Now, we compare the detection performance of the proposed centralized method and that of a slightly modified version of the MDL-based approach used in [15] and the ERD approach [37]. Specifically, while the original MDL-based approach is developed for a multigroup multicasting cell-free m-MIMO system, here it is modified such that there exists only one user in each group; from now on, this modified version is referred to as MDL. As mentioned in Section I, the MDL approach requires all users in the set $\mathcal{K} \setminus \{k\}$ to remain silent during the detection process of user $k$. Moreover, a fraction of the available power, denoted here by $\varrho$, is allocated for the transmission of a random sequence linearly combined with the user pilot sequence. For the ERD approach, we consider the same protocol as the MDL, i.e., all users keep silent except for the active one. Furthermore, the CPU calculates an average energy based on the received signals by all APs and send it to the APs via fronthaul links. The APs modulate the received quantity as a signal of length $\tau_p$ and transmits the resultant signal to the active user, who decides whether there exists an attack or not.

Fig. 12 displays $P_d$ versus $\rho_e$ for the proposed centralized method and the ERD and MDL approaches. The detector's threshold of the proposed method and the ERD approach is chosen to achieve $P_f = 0.001$ (see (22) and [37] for the proposed method and ERD, respectively), while $P_f$ is nearly zero for the MDL approach.[10] As seen from Fig. 12, the performance of all methods is enhanced by increasing the pilot length $\tau_p$. It can be seen that the centralized method significantly outperforms the MDL and ERD approaches even when $q$ is equal to the minimum value of one.

The total number of bits communicated per detection cycle via fronthaul links for the LLRT method is on the order of $\mathcal{O}(qNKB_L)$, while for both the MDL and ERD approaches this number is $\mathcal{O}(\tau_p NKB_L)$. Hence, the MDL and ERD approaches impose a higher overhead on the fronthaul links than the proposed centralized method since $\tau_p$ is usually greater than $q$ by an order of magnitude. Regarding the SE degradation, the proposed protocol of the LLRT method and that of the MDL approach impose reduction factors $q/\ell$ and $(K-1)/\ell$, respectively. Since the number of users in a cell-free m-MIMO system is typically much larger than $q$, the proposed centralized method degrades the SE to a lesser extent than the MDL approach.

Now, we compare the performance of the proposed decentralized method with that of ERD in Fig. 13. Note that the MDL cannot be implemented in a decentralized manner for a *single-antenna* system, which is the case in this paper. Also, the detector's threshold for both methods is set to achieve $P_f \leq 0.001$. As seen from Fig. 13, the performance of the proposed decentralized method is distinctly superior to that of ERD.

Finally, we investigate the effect of time-varying channel on $P_d$ and $P_f$ for the centralized method. To this end, we first consider this effect as loss of orthogonality among users' pilots and model it as an additive Gaussian noise whose variance is proportional to Doppler frequency and coherence time, i.e.,

$$\gamma f_c (\nu/\nu_0) T_C, \tag{23}$$

where $\gamma$ is a constant, $f_c$ is the carrier frequency, $\nu$ is the velocity, $\nu_0$ is the velocity of light. Then, we plot $P_d$ and $P_f$ versus velocity in Fig. 14, where the detector threshold is optimized when $\nu = 100$km/h. As seen from the figure, both $P_d$ and $P_f$ are not affected up to $\nu = 150$km/h. However, $P_f$ starts increasing as the velocity goes beyond 150km/h.

9. The result of Theorem 2 is generic for detectors implemented in a decentralized manner.

10. The MDL approach does not require a detector's threshold and both $P_d$ and $P_f$ almost simultaneously improve or worsen as parameters $N$, $\tau_p$, and $\varrho$ change. Hence, $P_f$ can hardly be adjusted to a specific value.

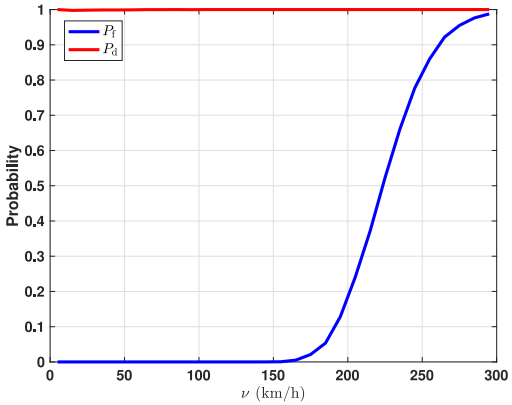
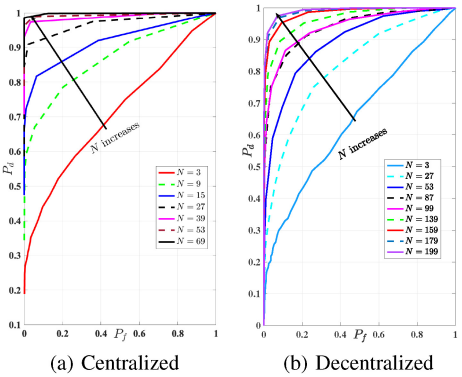



**FIGURE 14.** $P_d$ and $P_f$ versus $\nu$ for the centralized method ($\tau_p = K = 24$, $f_c = 1.9$GHz, $T_C = 1$ms, $N = 99$, $q = 1$, $\gamma = 1$, $\rho_e = -5$dB, $\rho_p = 5$dB).




(a) Centralized (b) Decentralized

**FIGURE 15.** ROC curves of AED methods for different number of APs and random path loss: (a) centralized, (b) decentralized ($q = 1$, $\sigma_{sh} = 8$dB, and $\tau_p = 16$).

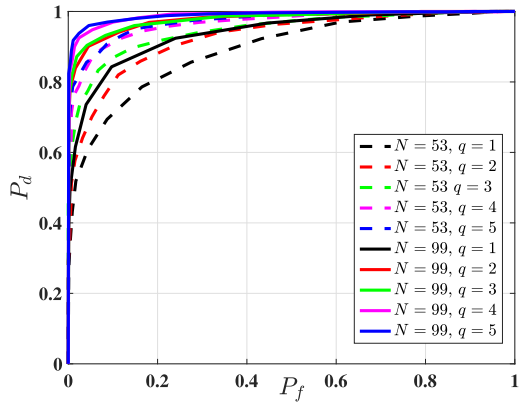



**FIGURE 16.** ROC curves of the decentralized method for different number of off-mode time slot $q$ ($\sigma_{sh} = 8$dB, and $\tau_p = 16$).

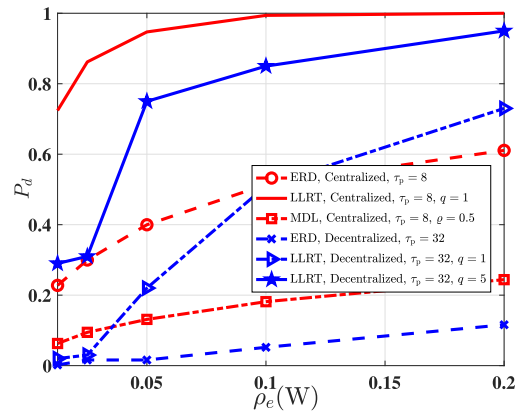



**FIGURE 17.** $P_d$ versus $\rho_e$ for different methods implemented in the centralized and decentralized fashions ($N = 99$).

### D. SIMULATION RESULTS FOR RANDOM PATH LOSS

Now, we consider the case where path loss is random where we use the path loss model in [48, p. 511] with locations of Eve and APs uniformly distributed over the square area $[-0.5, 0.5] \times [-0.5, 0.5]\,\text{km}^2$, which is a typical range for operation in cell-free m-MIMO systems. For this particular configuration, the PDF of $d_{ne}^2$ can be modeled as follows:

$$f_{d_{ne}^2}(z) = g(z, \min(1, z)) - g(z, \max(0, z-1)), \quad (24)$$

where

$$g(z, u) = 2\sin^{-1}\left(\sqrt{\frac{u}{z}}\right) - 2\sqrt{u} + 2\sqrt{z-u} + u, \quad (25)$$

for $0 < z \leq 2$. Besides, the transmission power of Eve (in mW) is uniformly distributed in the interval $[100, 200]$. In order to calculate the noise power, the system bandwidth, noise temperature, and noise figure are set to 20MHz, 290Kelvin, and 9dB, respectively.

In this subsection, we investigate the effect of random path loss on the performance of the proposed approaches. To this end, Fig. 15 depicts ROC curves of centralized and decentralized AED methods for different values of $N$. Generally, a similar trend as in the case of the normalized path loss is observed for both approaches, i.e.: the probability of achieving the desired point $(0, 1)$ in the $P_f P_d$-plane increases as $N$ grows, and the performance of the centralized method is superior to that of the decentralized one.

For the decentralized method, the desired point $(0, 1)$ in the $P_f P_d$-plane can also be approachable by increasing the number of off-mode time slots $q$. Fig. 16 displays the ROC curves of the decentralized method for different values of $q$ and, when $N$ is equal to 53 and 99. As seen from this figure, for a small and fixed value of $P_f$, $P_d$ increases monotonically with $q$. For instance, for $P_f = 0.02$ and $N = 99$, $P_d$ increases from 0.62 to 0.94 when $q$ increases from 1 to 5.

Finally, we compare the performance of the proposed methods with that of the MDL and ERD in Fig. 17. Here, a methodology similar to the normalized case (see previous subsection) is considered. As seen from Fig. 17, the proposed methods outperform significantly the MDL and ERD approaches.

### E. COMMENTS ON THRESHOLD SELECTION IN PRACTICE

A practical matter is with the choice of the proper threshold $\eta$ in (7) under practical operating conditions. In this regard, our presented simulation studies are quite useful as they provide guidelines about the behavior of the detector for different

parameter settings (i.e., SNR, number of APs, pilot length, and number of off-mode time slots) and radio propagation conditions (i.e., small-scale and small-scale fading). From the simulations, we obtain ROC curves which provide a useful range for the operating points of the detector in practice.

Also, it should be mentioned that any such simulation study relies on nominal parameter values and channel models that are likely to differ (to some extent) from the true conditions of operation. This is why in practice, following implementation, any properly engineered detector system needs to be calibrated under real operating conditions. This does not affect in any way the signal processing operations of the detector, but simply how to adjust the threshold under practical conditions of operation. This type of calibration is employed in nearly all applications of statistical detection, from ship or whale detection in sonar systems [46], to aircraft detection in modern radars [47].

## V. CONCLUSION

In this work, the problem of AED in a cell-free massive m-MIMO system was considered. Two methods based on LLRT, one in a centralized and the other in a decentralized fashion, were proposed to detect the abnormality. A closed-form approximate expression for the joint PDF of the processed received signals conditioned on the true hypothesis, which is essential for the implementation of LLRT-based detection methods, was also obtained. Through an asymptotic analysis, it was shown for the proposed methods that the detection and false-alarm probabilities approach to one and zero, respectively as the number of APs goes to infinity. Numerical results revealed that both methods significantly outperform a recent approach in terms of false-alarm rate with negligible degradation in the per user spectral efficiency.

## APPENDIX A
## PROOF OF LEMMA 1

We first define $\mathbf{y}_n = [y_{n1}, y_{n2}, \ldots, y_{nq}]^T$ as a mixed complex normal-lognormal vector with $q$ statistically dependent random variables. However, when conditioned on a given value of the large scale fading, i.e., $\beta_{ne}^{\frac{1}{2}} = \alpha$, these random variables become independent. By using this fact, the conditional PDF $f_{\mathbf{y}_n}(y_n|H_1, \rho_e)$ can be obtained as follows [43, p. 103]:

$$\begin{aligned} f_{\mathbf{y}_n}\left(y_n|H_1,\rho_e\right) &= \int_0^\infty f_{\beta_{ne}^{\frac{1}{2}}}(\alpha|H_1) f_{\mathbf{y}_n}\left(y_n|\beta_{ne}^{\frac{1}{2}}=\alpha,H_1,\rho_e\right)d\alpha \\ &= \int_0^\infty f_{\beta_{ne}^{\frac{1}{2}}}(\alpha|H_1) \prod_{j=1}^{q} f_{y_{nj}}\left(y_{nj}|\beta_{ne}^{\frac{1}{2}}=\alpha,H_1,\rho_e\right)d\alpha, \end{aligned} \tag{26}$$

where

$$f_{\beta_{ne}^{\frac{1}{2}}}(\alpha|H_1) = \frac{2}{\sqrt{\pi}b\sigma_{sh}}\frac{1}{\alpha}\exp\left\{\frac{-4\ln^2(\alpha)}{b^2\sigma_{sh}^2}\right\}, \alpha \geq 0$$

and

$$f_{y_{nj}}\left(y_{nj}|\beta_{ne}^{\frac{1}{2}}=\alpha,H_1,\rho_e\right) = \frac{1}{\pi\left(1+\tau_p\rho_e\alpha^2\right)} \times \exp\left\{-\frac{|y_{nj}|^2}{1+\tau_p\rho_e\alpha^2}\right\}.$$

Replacing the PDFs in (26) with their explicit expressions and making the change of variable $\xi = \frac{2}{b\sigma_{sh}}\ln(\alpha)$, we arrive at

$$\begin{aligned} f_{\mathbf{y}_n}\left(y_n|H_1,\rho_e\right) = \frac{1}{\pi^{q+\frac{1}{2}}} &\times \int_{-\infty}^{\infty} \frac{1}{\left(1+\tau_p\rho_e\exp\{b\sigma_{sh}\xi\}\right)^q} \\ &\times \exp\left\{\frac{-\|y_n\|^2}{1+\tau_p\rho_e\exp\{b\sigma_{sh}\xi\}} - \xi^2\right\}d\xi. \end{aligned} \tag{27}$$

The above integral can be expressed in terms of a finite summation by applying the Gauss-Hermite quadrature method [43, p. 890]:

$$\begin{aligned} f_{\mathbf{y}_n}\left(y_n|H_1,\rho_e\right) = \frac{1}{\pi^{q+\frac{1}{2}}} &\times \sum_{i=1}^{I} \frac{w_i}{\Psi^q(x_i)}\exp\left\{\frac{-\|y_n\|^2}{\Psi(x_i)}\right\} + R_{I,n}(\xi), \end{aligned} \tag{28}$$

where $w_i$'s are weight factors expressible as in the lemma statement. This completes the proof of lemma.

## APPENDIX B
## PROOF OF THEOREM 1

For a fixed value of $\rho_e$, we first define the LLR

$$\Lambda(y|\rho_e) = \ln f_{\mathbf{y}}(y|H_1,\rho_e) - \ln f_{\mathbf{y}}(y|H_0). \tag{29}$$

Then, we define the events

$$\begin{aligned} \mathcal{E}_{H_1,\rho_e} &= \{\Lambda(\mathbf{y}|\rho_e) > \ln\eta \,|\, H_1\}, \\ \mathcal{E}_{H_0,\rho_e} &= \{\Lambda(\mathbf{y}|\rho_e) > \ln\eta \,|\, H_0\}. \end{aligned} \tag{30}$$

Then, for a fixed value of $\rho_e$, the detection and false-alarm probabilities can be written as

$$P_{d|\rho_e} = \mathbb{P}\left(\mathcal{E}_{H_1,\rho_e}\right), \quad P_{f|\rho_e} = \mathbb{P}\left(\mathcal{E}_{H_0,\rho_e}\right).$$

To prove the theorem, we shall first derive a lower bound and an upper bound on the conditional probabilities $P_{d|\rho_e}$ and $P_{f|\rho_e}$, respectively; we will then take limit on the derived bounds as $N \to \infty$ under the assumption $L_{H_1} < \ln\eta_0 < U_{H_0}$.

Upon substitution of the explicit expressions of $f_{\mathbf{y}}(y|H_1,\rho_e)$ (see (13)-(14)) and $f_{\mathbf{y}}(y|H_0) = \pi^{-qN}\exp\{-\sum_{n=1}^{N}\|y_n\|^2\}$ into the LHS of (29), we can express the random LLR

$$\Lambda(\mathbf{y}|\rho_{\mathrm{e}}) = \sum_{n=1}^{N} \ln\left( \sum_{i=1}^{I} \frac{w_i}{\Psi^q(x_i)} \exp\left\{ \frac{-1}{\Psi(x_i)} \|\mathbf{y}_n\|^2 \right\} \right) + \sum_{n=1}^{N} \|\mathbf{y}_n\|^2 + N \ln\left( \frac{1}{\sqrt{\pi}} \right). \tag{31}$$

To derive lower and upper bounds on $\Lambda(\mathbf{y}|\rho_{\mathrm{e}})$, we use the following inequalities, where $a_i$,$b_i$, and $c$ are arbitrary positive real numbers:

$$\ln\left( \sum_{i=1}^{I} a_i \right) - c \frac{\sum_{i=1}^{I} a_i b_i}{\sum_{i=1}^{I} a_i} \le \ln\left( \sum_{i=1}^{I} a_i \exp(-c b_i) \right) \tag{32}$$

$$\le \ln\left( I \max_i \left[ a_i \exp(-c b_i) \right] \right) \le \ln\left( \left[ I \max_i a_i \right] \left[ \exp\left( -c \min_i b_i \right) \right] \right) = \ln\left( I \max_i a_i \right) - c \min_i b_i, \quad a_i, b_i, c > 0 \tag{33}$$

where (32) is due to Jensen's inequality[11] [49, p. 197]. Applying the inequalities in (32) and (33) to the right-hand side (RHS) of (31), we obtain the bounds on the LLR as follows:

$$\Lambda^{\mathrm{L}}(\mathbf{y}|\rho_{\mathrm{e}}) \le \Lambda(\mathbf{y}|\rho_{\mathrm{e}}) \le \Lambda^{\mathrm{U}}(\mathbf{y}|\rho_{\mathrm{e}}), \tag{34}$$

where

$$\Lambda^{\mathrm{L}}(\mathbf{y}|\rho_{\mathrm{e}}) = \left( 1 - \frac{\Upsilon_{q+1}}{\Upsilon_q} \right) Y_N + N \ln\left( \frac{\Upsilon_q}{\sqrt{\pi}} \right), \tag{35}$$

$$\Lambda^{\mathrm{U}}(\mathbf{y}|\rho_{\mathrm{e}}) = (1-\psi) Y_N + N \ln\left( \frac{\Omega_q I}{\sqrt{\pi}} \right), \tag{36}$$

$$\Upsilon_q = \sum_{i=1}^{I} \frac{\omega_i}{\Psi^q(x_i)}, \ \Omega_q = \max_i \frac{\omega_i}{\Psi^q(x_i)}, \ \psi = \min_i \frac{1}{\Psi(x_i)}, \quad Y_N = \sum_{n=1}^{N} \|\mathbf{y}_n\|^2 = \|\mathbf{y}\|^2. \tag{37}$$

Now, we define the following events:

$$\mathcal{E}^{\mathrm{L}}_{H_1,\rho_{\mathrm{e}}} = \{ \Lambda^{\mathrm{L}}(\mathbf{y}|\rho_{\mathrm{e}}) > \ln \eta \,|\, H_1 \}, \quad \mathcal{E}^{\mathrm{U}}_{H_0,\rho_{\mathrm{e}}} = \{ \Lambda^{\mathrm{U}}(\mathbf{y}|\rho_{\mathrm{e}}) > \ln \eta \,|\, H_0 \}. \tag{38}$$

From (34), (30) and (38), we conclude that

$$\mathcal{E}_{H_1,\rho_{\mathrm{e}}} \supseteq \mathcal{E}^{\mathrm{L}}_{H_1,\rho_{\mathrm{e}}}, \quad \mathcal{E}_{H_0,\rho_{\mathrm{e}}} \subseteq \mathcal{E}^{\mathrm{U}}_{H_0,\rho_{\mathrm{e}}}.$$

Then we have

$$P_{\mathrm{d}|\rho_{\mathrm{e}}} \equiv \mathbb{P}\left( \mathcal{E}_{H_1,\rho_{\mathrm{e}}} \right) \ge \mathbb{P}\left( \mathcal{E}^{\mathrm{L}}_{H_1,\rho_{\mathrm{e}}} \right), \quad P_{\mathrm{f}|\rho_{\mathrm{e}}} \equiv \mathbb{P}\left( \mathcal{E}_{H_0,\rho_{\mathrm{e}}} \right) \le \mathbb{P}\left( \mathcal{E}^{\mathrm{U}}_{H_0,\rho_{\mathrm{e}}} \right). \tag{39}$$

11. Let $\Phi$ be a real concave function with domain $\mathcal{D}$. For given $x_i \in \mathcal{D} \subseteq \mathbb{R}$ and $a_i > 0$ where $i = 1, 2, \ldots n$, we have: $\Phi\left( \frac{\sum_i a_i x_i}{\sum_i a_i} \right) \ge \frac{\sum_i a_i \Phi(x_i)}{\sum_i a_i}$.

Using the expressions for $\Lambda^{\mathrm{L}}(\mathbf{y}|\rho_{\mathrm{e}})$ in (35), $\Lambda^{\mathrm{U}}(\mathbf{y}|\rho_{\mathrm{e}})$ in (36), and $\eta = \eta_0^{-N}$, we rewrite the two inequalities in (39) as follows:

$$P_{\mathrm{d}|\rho_{\mathrm{e}}} \ge \mathbb{P}\left( Y_N > \frac{N\Upsilon_q}{\Upsilon_q - \Upsilon_{q+1}} \ln\left( \frac{\sqrt{\pi}}{\Upsilon_q \eta_0} \right) \Big| H_1 \right) = 1 - \mathbb{P}\left( Y_N \le \frac{N\Upsilon_q}{\Upsilon_q - \Upsilon_{q+1}} \ln\left( \frac{\sqrt{\pi}}{\Upsilon_q \eta_0} \right) \Big| H_1 \right), \tag{40}$$

$$P_{\mathrm{f}|\rho_{\mathrm{e}}} \le \mathbb{P}\left( Y_N > \frac{N}{1-\psi} \ln\left( \frac{\sqrt{\pi}}{\Omega_q I \eta_0} \right) \Big| H_0 \right), \tag{41}$$

where in deriving (40), we used the fact that $\Upsilon_{q+1} < \Upsilon_q$ which follows from $\Psi(x_i) > 1$ and $\omega_i > 0$, and in deriving (41), we used the fact that $\psi < 1$. For later use, we denote

$$\mu_{H_1} = \mathbb{E}\left( \|\mathbf{y}_n\|^2 \,|\, H_1 \right), \quad \mu_{H_0} = \mathbb{E}\left( \|\mathbf{y}_n\|^2 \,|\, H_0 \right), \quad \sigma^2_{H_1} = \mathbb{V}\left( \|\mathbf{y}_n\|^2 \,|\, H_1 \right), \quad \sigma^2_{H_0} = \mathbb{V}\left( \|\mathbf{y}_n\|^2 \,|\, H_0 \right).$$

It can be verified by using (6) and (5) that

$$\mu_{H_1} = q\left( 1 + \tau_{\mathrm{p}} \rho_{\mathrm{e}} \exp\{ b^2 \sigma^2_{\mathrm{sh}}/4 \} \right), \quad \mu_{H_0} = q. \tag{42}$$

From (37) and the fact that $\mathbf{y}_n$'s are independent, we obtain

$$\mathbb{E}(Y_N \,|\, H_1) = N\mu_{H_1}, \quad \mathbb{E}(Y_N \,|\, H_0) = N\mu_{H_0}, \quad \mathbb{V}(Y_N \,|\, H_1) = N\sigma^2_{H_1}, \quad \mathbb{V}(Y_N \,|\, H_0) = N\sigma^2_{H_0}.$$

Then, after shifting $Y_N$ by its corresponding means, we can recast (40) and (41) as

$$P_{\mathrm{d}|\rho_{\mathrm{e}}} \ge 1 - \mathbb{P}\left( Y_N - N\mu_{H_1} \le N\left[ \frac{\Upsilon_q}{\Upsilon_q - \Upsilon_{q+1}} \ln\left( \frac{\sqrt{\pi}}{\Upsilon_q \eta_0} \right) - \mu_{H_1} \right] \Big| H_1 \right), \tag{43}$$

$$P_{\mathrm{f}|\rho_{\mathrm{e}}} \le \mathbb{P}\left( Y_N - N\mu_{H_0} > N\left[ \frac{1}{1-\psi} \ln\left( \frac{\sqrt{\pi}}{\Omega_q I \eta_0} \right) - \mu_{H_0} \right] \Big| H_0 \right). \tag{44}$$

For any $\eta_0$ satisfying $L_{H_1} < \ln \eta_0 < U_{H_0}$ (see Theorem 1 for the two bounds here), it can be verified that the RHS of the inequality inside the probability in (43) is negative and the RHS of the inequality inside the probability in (44) is positive. By applying the Chebyshev's inequality to (43) and (44), we obtain the proper lower and upper bounds as follows:

$$P_{\mathrm{d}|\rho_{\mathrm{e}}} \ge 1 - \frac{\sigma^2_{H_1}}{N\left[ \frac{\Upsilon_q}{\Upsilon_q - \Upsilon_{q+1}} \ln\left( \frac{\sqrt{\pi}}{\Upsilon_q \eta_0} \right) - \mu_{H_1} \right]^2}, \tag{45}$$

$$P_{\mathrm{f}|\rho_{\mathrm{e}}} \le \frac{\sigma^2_{H_0}}{N\left[ \frac{1}{1-\psi} \ln\left( \frac{\sqrt{\pi}}{\Omega_q I \eta_0} \right) - \mu_{H_0} \right]^2}. \tag{46}$$

Obviously, the RHSs of (45) and (46) go to one and zero, respectively, as $N$ approaches to infinity. Hence, it follows that

$$\lim_{N \longrightarrow \infty} P_{\mathrm{d}|\rho_{\mathrm{e}}} = 1, \quad \lim_{N \longrightarrow \infty} P_{\mathrm{f}|\rho_{\mathrm{e}}} = 0.$$

## APPENDIX C
## PROOF OF THEOREM 2

Let $S$ be the sum of the bits received by the CPU. From the definitions of detection and false-alarm probabilities for the decentralized AED method, we have

$$P_{\mathrm{d}} = 1 - \mathbb{P}\left\{ S < \frac{N}{2} \middle| H_1 \right\}, \tag{47}$$

$$P_{\mathrm{f}} = \mathbb{P}\left\{ S \geq \frac{N}{2} \middle| H_0 \right\}. \tag{48}$$

Note that $\mathbb{E}\{S|H_1\} = Np_{\mathrm{d}}$ and $\mathbb{E}\{S|H_0\} = Np_{\mathrm{f}}$.

In order to find a lower and an upper bound for (47) and (48), respectively, we apply Hoeffding's inequalities[12] [50, p. 122] to the RHSs of (47) and (48) and arrive at

$$\begin{aligned} P_{\mathrm{d}} &= 1 - \mathbb{P}\left\{ S - Np_{\mathrm{d}} < -N\left(p_{\mathrm{d}} - \frac{1}{2}\right) \middle| H_1 \right\} \\ &\geq 1 - \mathbb{P}\left\{ S - Np_{\mathrm{d}} \leq -N\left(p_{\mathrm{d}} - \frac{1}{2}\right) \middle| H_1 \right\} \\ &\geq 1 - \exp\left\{ -\frac{2\left(N\left(p_{\mathrm{d}} - \frac{1}{2}\right)\right)^2}{N} \right\}, \end{aligned} \tag{49}$$

$$\begin{aligned} P_{\mathrm{f}} &= \mathbb{P}\left\{ S - Np_{\mathrm{f}} \geq N\left(\frac{1}{2} - p_{\mathrm{f}}\right) \middle| H_0 \right\} \\ &\leq \exp\left\{ -\frac{2\left(N\left(\frac{1}{2} - p_{\mathrm{f}}\right)\right)^2}{N} \right\}. \end{aligned} \tag{50}$$

Taking the limit as $N$ goes to infinity in (49)-(50), we can arrive at the conclusion of the theorem.

## 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] 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.

[4] T. H. Nguyen, T. K. Nguyen, H. D. Han, and V. D. Nguyen, "Optimal power control and load balancing for uplink cell-free multi-user massive MIMO," *IEEE Access*, vol. 6, pp. 14462–14473, 2018.

[5] Y. Jin, J. Zhang, S. Jin, and B. Ai, "Channel estimation for cell-free mmwave massive MIMO through deep learning," *IEEE Trans. Veh. Technol.*, vol. 68, no. 10, pp. 10325–10329, Oct. 2019.

[6] T. C. Mai, H. Q. Ngo, M. Egan, and T. Q. Duong, "Pilot power control for cell-free massive MIMO," *IEEE Trans. Veh. Technol.*, vol. 67, no. 11, pp. 11264–11268, Nov. 2018.

[7] S. S. Hosseini, B. Champagne, and X.-W. Chang, "A green downlink power allocation scheme for cell-free massive MIMO systems," *IEEE Access*, vol. 9, pp. 6498–6512, 2020.


12. Let $z_1, z_2, \ldots z_n$ be independent bounded random variables such that $z_i \in [a_i, b_i]$ with probability one and $S_n = \sum_{i=1}^{n} z_i$. Then for any $t > 0$, tail probabilities $\mathbb{P}\{S_n - \mathbb{E}\{S_n\} \leq -t\}$ and $\mathbb{P}\{S_n - \mathbb{E}\{S_n\} \geq t\}$ are both upper bounded by $\exp\{-\frac{2t^2}{\sum_{i=1}^{n}(b_i - a_i)^2}\}$.


[8] S. S. Hosseini, B. Champagne, and X.-W. Chang, "A low-complexity DNN-based DoA estimation method for EHF and THF cell-free massive MIMO," in *Proc. IEEE Veh. Technol. Conf. (VTC-Fall)*, London, U.K., Sep. 2002, pp. 1–7.

[9] J. Zhang, S. Chen, Y. Lin, J. Zheng, B. Ai, and L. Hanzo, "Cell-free massive MIMO: A new next-generation paradigm," *IEEE Access*, vol. 7, pp. 99878–99888, 2019.

[10] Y. Zhang, M. Zhou, X. Qiao, H. Cao, and L. Yang, "On the performance of cell-free massive MIMO with low-resolution ADCs," *IEEE Access*, vol. 7, pp. 117968–117977, 2019.

[11] H. Liu, J. Zhang, S. Jin, and B. Ai, "Graph coloring based pilot assignment for cell-free massive MIMO systems," *IEEE Trans. Veh. Technol.*, vol. 69, no. 8, pp. 9180–9184, Aug. 2020.

[12] A. Abdallah and M. M. Mansour, "Efficient angle-domain processing for FDD-based cell-free massive MIMO systems," *IEEE Trans. Commun.*, vol. 68, no. 4, pp. 2188–2203, Apr. 2020.

[13] G. Femenias, J. García-Morales, and F. Riera-Palou, "SWIPT-enhanced cell-free massive MIMO networks," *IEEE Trans. Commun.*, vol. 69, no. 8, pp. 5593–5607, Aug. 2021.

[14] S. Chen, J. Zhang, J. Zhang, E. Björnson, and B. Ai, "A survey on user-centric cell-free massive MIMO systems," *Digit. Commun. Netw.*, vol. 2, no. 1, pp. 25–39, Mar. 2022.

[15] X. Zhang, D. Guo, K. An, Z. Ding, and B. Zhang, "Secrecy analysis and active pilot spoofing attack detection for multigroup multicasting cell-free massive MIMO systems," *IEEE Access*, vol. 7, pp. 57332–57340, 2019.

[16] 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.

[17] X. Zhang, X. Qiao, T. Liang, and K. An, "Secure performance analysis and pilot spoofing attack detection in cell-free massive MIMO systems with finite-resolution ADCs," *Int. J. Distrib. Sens. Netw.*, vol. 18, no. 1, pp. 1–11, Jan. 2022.

[18] K.-W. Huang, H.-M. Wang, Y. Wu, and R. Schober, "Pilot spoofing attack by multiple eavesdroppers," *IEEE Trans. Wireless Commun.*, vol. 17, no. 10, pp. 6433–6447, Oct. 2018.

[19] J. Zeng, D. Wang, W. Xu, and B. Li, "An efficient detection algorithm of pilot spoofing attack in massive MIMO systems," *Signal Process.*, vol. 182, pp. 1–9, May 2021.

[20] J. Xie, Y.-C. Liang, J. Fang, and X. Kang, "Two-stage uplink training for pilot spoofing attack detection and secure transmission," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Paris, France, May 2017, pp. 1–6.

[21] W. Xu, C. Yuan, S. Xu, H. Q. Ngo, and W. Xiang, "On pilot spoofing attack in massive MIMO systems: Detection and countermeasure," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 1396–1409, 2021.

[22] X. Tian, M. Li, and Q. Liu, "Random-training-assisted pilot spoofing detection and security enhancement," *IEEE Access*, vol. 5, pp. 27384–27399, 2017.

[23] W. Wang, N. Cheng, K. C. Teh, X. Lin, W. Zhuang, and X. Shen, "On countermeasures of pilot spoofing attack in massive MIMO systems: A double channel training based approach," *IEEE Trans. Veh. Technol.*, vol. 68, no. 7, pp. 6697–6708, Jul. 2019.

[24] J. K. Tugnait, "Detection and identification of spoofed pilots in TDD/SDMA systems," *IEEE Wireless Commun. Lett.*, vol. 6, no. 4, pp. 550–553, Aug. 2017.

[25] L. Ning, B. Li, C. Zhao, Y. Tao, and X. Wang, "Detection and localization of the eavesdropper in MIMO systems," *IEEE Access*, vol. 8, pp. 94984–94993, 2020.

[26] 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.

[27] T. L. Marzetta, E. G. Larsson, H. Yang, and H. Q. Ngo, *Fundamentals of Massive MIMO*. New York, NY, USA: Cambridge Univ. Press, 2004.

[28] A. Morsali, S. S. Hosseini, B. Champagne, and X.-W. Chang, "Design criteria for omnidirectional STBC in massive MIMO systems," *IEEE Wireless Commun. Lett.*, vol. 8, no. 5, pp. 1435–1439, Oct. 2019.

[29] S. S. Hosseini, J. Abouei, and M. Uysal, "Fast-decodable MIMO HARQ systems," *IEEE Trans. Wireless Commun.*, vol. 14, no. 5, pp. 2827–2840, May 2015.

[30] N. Kaur, S. S. Hosseini, and B. Champagne, "Enhanced channel tracking in THz beamspace massive MIMO: A deep CNN approach," in *Proc. Asia–Pacific Sig. Inf. Process. Assoc. Annu. Summit Conf. (APSIPA ASC)*, Auckland, New Zealand, Dec. 2020, pp. 76–81.

[31] S. S. H. Bidaki, S. Talebi, and M. Shahabinejad, "A full-rate full-diversity 2×2 space-time block code with linear complexity for the maximum likelihood receiver," *IEEE Commun. Lett.*, vol. 15, no. 8, pp. 842–844, Aug. 2011.

[32] S. S. Hosseini, S. Talebi, and J. Abouei, "Comprehensive study on a 2×2 full-rate and linear decoding complexity space–time block code," *IET Commun.*, vol. 9, no. 1, pp. 122–132, 2015.

[33] M. Bashar, K. Cumanan, A. G. Burr, M. Debbah, and H. Q. Ngo, "On the uplink max–min SINR of cell-free massive MIMO systems," *IEEE Trans. Wireless Commun.*, vol. 18, no. 4, pp. 2021–2036, Apr. 2019.

[34] Q. Huang and A. G. Burr, "Compute-and-forward in cell-free massive MIMO: Great performance with low backhaul load," in *Proc. IEEE Int. Conf. Commun. Workshops (ICC Workshops)*, Paris, France, May 2017, pp. 601–606.

[35] M. Bashar, K. Cumanan, A. G. Burr, H. Q. Ngo, and M. Debbah, "Cell-free massive MIMO with limited backhaul," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Kansas City, MO, USA, May 2018, pp. 1–7.

[36] M. Bashar, K. Cumanan, A. G. Burr, H. Q. Ngo, M. Debbah, and P. Xiao, "Max–min rate of cell-free massive MIMO uplink with optimal uniform quantization," *IEEE Trans. Commun.*, vol. 67, no. 10, pp. 6796–6815, Oct. 2019.

[37] 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, pp. 932–940, 2015.

[38] D. Tse and P. Viswanath, *Fundamentals of Wireless Communication*. Cambridge, U.K.: Cambridge Univ. Press, 2005.

[39] A. Goldsmith, *Wireless Communication*. Cambridge, U.K.: Cambridge Univ. Press, 2005.

[40] H. L. V. Trees, *Detection, Estimation, and Modulation Theory, Part I*. Hoboken, NJ, USA: Wiley, 2004.

[41] A. Khisti, A. Tchamkerten, and G. W. Wornell, "Secure broadcasting over fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2453–2469, Jun. 2008.

[42] H. Sun, "Secure broadcasting over fading channels," *IEEE Trans. Inf. Theory*, submitted for publication.

[43] A. Papoulis and S. U. Pillai, *Probability, Random Variables, and Stochastic Processes*. New York, NY, USA: McGraw-Hill, 2002.

[44] M. Abramowitz and I. A. Stegun, *Handbook of Mathematical Functions with Formulas, Graphs, and Mathematical Tables* (Applied Mathematics Series 55). Washington, DC, USA: U.S. Dept. Commerce Nat. Bureau Stand., 1965.

[45] R. M. Bolle, J. H. Connell, S. Pankanti, N. K. Ratha, and A. W. Senior, "The relation between the ROC curve and the CMC," in *Proc. 4th IEEE Workshop Autom. Ident. Adv. Technol. (AutoID)*, Buffalo, NY, USA, Oct. 2005, pp. 15–20.

[46] R. O. Nielsen, *Sonar Signal Processing*. Norwood, MA, USA: Artech House, Inc., 1991.

[47] M. A. Richards, *Fundamentals of Radar Signal Processing*, 2nd ed. New York, NY, USA: McGraw-Hill Educ., 2014.

[48] E. E. Bjornson, J. Hoydis, and L. Sanguinetti, "Massive MIMO networks: Spectral, energy, and hardware efficiency," *Found. Trends Signal Process.*, vol. 11, nos. 3–4, pp. 154–655, Nov. 2017.

[49] M. Kuczma, *An Introduction to the Theory of Functional Equations and Inequalities: Cauchy's Equation and Jensen's Inequality*. New York, NY, USA: Springer, 2009.

[50] L. Devroye, L. Gyorfi, and G. Lugosi, *A Probabilistic Theory of Pattern Recognition*, vol. 31. New York, NY, USA: Springer, 1996.