Active Pilot Contamination Attack Detection in Sub-6 GHz Massive MIMO NOMA Systems

Diluka Loku Galappaththige and Gayan Amarasuriya
Department of Electrical and Computer Engineering, Southern Illinois University, Carbondale, IL, USA 62901
Email: {diluka.lg,gayan.baduge}@siu.edu

***Abstract*—Active pilot attack detection in time division duplexing based sub-6 GHz massive multiple-input multiple-output (MIMO) non-orthogonal multiple-access (NOMA) systems is investigated. A practically realizable generalized likelihood ratio test (GLRT) is formulated when the eavesdropper's signal parameters are unknown to the massive MIMO base-station. The performance of this detector is analyzed by deriving the probability of false alarm, probability of detection and receiver operating characteristics. The underlying performance is compared with respect to an optimal Neyman-Pearson (NP) based Clairvoyant detector, which is designed by assuming the perfect knowledge of eavesdropper's signal parameters. Thereby, we conclude that the limited knowledge of the eavesdropper's signal parameters must be taken into account in designing practically viable active pilot detectors because the Clairvoyant detector overestimates the detection performance. Nevertheless, we show that the proposed GLRT based detector asymptotically becomes optimal in NP sense when the number of antennas at the base-station grows without bound. Moreover, we reveal that there is a fundamental trade-off between the number of NOMA users that can be served simultaneously in the same time-frequency resource element and the detection performance of active pilot attacks.**

I. Introduction

Massive multiple-input multiple-output (MIMO) non-orthogonal multiple access (NOMA) has been identified as a key enabler for massive connectivity in the next-generation wireless systems [1]. In particular, NOMA is leveraged to support overloaded-case in massive MIMO systems in which the number of users that needs to be served simultaneously in the same time-frequency resource element exceeds the number of antennas at the base-station (BS). In time division duplexing (TDD) based massive MIMO NOMA systems operating at sub-6 GHz, the uplink channels are typically estimated at the BS by using pilots sent by the clusters of users [2]. Thus, the uplink training phase is vulnerable to pilot contamination attacks by active eavesdroppers. Active pilot contamination attack detection in TDD-based sub-6 GHz massive MIMO NOMA is the primary focus of this work.

In active pilot attacks, an adversary sends a spoofing pilot sequence, which is identical to one being used by a legitimate user [3]–[12]. This spoofing pilot sequence contaminates the uplink channel estimate at the massive MIMO BS. Since the BS constructs downlink precoder based on its uplink channel estimate, the confidential data belonging to a legitimate user will be implicitly beamformed toward the active eavesdropper. The high beamforming gain rendered by the massive MIMO antenna array facilitates boosted information leakage rate for the active eavesdropper. Thus, active pilot attacks can significantly hinder the achievable secrecy rates.

Since the uplink channel estimation of TDD-based wireless systems is vulnerable to pilot contamination attacks, the detection of active eavesdroppers has recently gained much research interest [7]–[12]. In [9], an energy ratio based pilot attack detector is proposed by leveraging the asymmetry of received signal powers when there exists such an attack. In [7], by exploiting source enumeration techniques and minimum description length criterion, a detector for pilot contamination attacks is proposed based on superimposing random sequences on the pilot sequence at the legitimate receiver. By extending the key idea of [7], the legitimate/eavesdropper channel estimation and secure precoding techniques are investigated in [8] to mitigate pilot contamination attacks. In particular, the pilot contamination attack detectors of [7]–[9] are primarily applicable only to small-scale MIMO systems.

With the recent proliferation of massive MIMO techniques, active pilot attack detection has been extended to large-scale MIMO systems [10]–[12]. In [12], an active pilot attack detector is designed by using random training sequences, and thereby, the detection performance is investigated when the number of BS antennas grows without bound. In [11], the probability of false alarm and probability of error in detecting active pilot attacks are derived. The detectors and the corresponding performance metrics in [12] and [11] are valid for single-user massive MIMO systems. In [10], the active pilot attack detection is investigated for massive MIMO NOMA systems operating in millimeter-wave (mm-wave) band by leveraging the virtual channel sparsity exhibited in very large frequencies. In particular, implementation of the detectors in [11] and [10] requires the perfect/partial knowledge of eavesdropper's channel/signal parameters at the massive MIMO BS. However, acquiring eavesdropper's channel/signal parameters typically cumbersome/infeasible in practice [4]. Moreover, since the detector in [10] exploits channel sparsity of mm-wave channels, the underlying detector and performance metrics are not applicable to massive MIMO NOMA operating in sub-6 GHz band in which the channels undergo rich-scattering.

Having been motivated by the aforementioned gaps in related prior literature, in this work, we investigate active pilot contamination attack detection and its performance metrics for TDD-based sub-6 GHz massive MIMO NOMA systems. In particular, the performance metrics of a practically realizable detector, which does not require the prior knowledge of eavesdropper's channel/signal parameters, are compared against the Clairvoyant Neyman-Pearson (NP) detector having perfect channel state information. The proposed detector is designed based on the generalized likelihood ratio test (GLRT) and the unknown channel/signal parameters are replaced by the corresponding maximum likelihood estimates (MLEs). The probability of false alarm, probability of detection and receiver operating characteristics (ROC) are derived

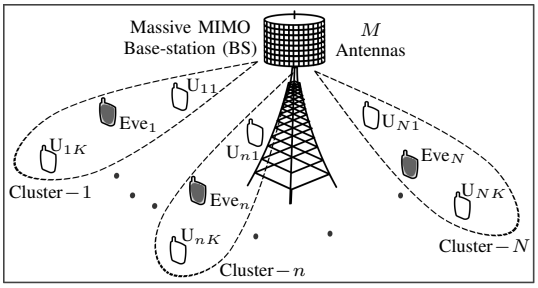

Fig. 1. System model consisting of N clusters each having K users

for both Clairvoyant and GLRT detectors. Consequently, we reveal that the Clairvoyant detector, which assumes the perfect knowledge of eavesdropper's channel/signal parameters, considerably overestimates the performance of pilot contamination attack detection in sub-6 GHz massive MIMO NOMA systems when compared against a practically realizable GLRT-based detector. By extending our analysis to asymptotic BS antenna regime, we show that the proposed GLRT-based detector and its performance metrics asymptotically approach those of Clairvoyant detector. We show that the performance of active pilot contamination detectors significantly degrades as the number of intra-cluster users that is served in the same time-frequency resource element increases. Consequently, we reveal the existence of this fundamental trade-off, which must be optimized to fully leverage the benefits of massive MIMO NOMA in the presence of active pilot contamination attacks.

II. System, channel and signal models

A. System and channel model

We consider a massive MIMO NOMA system having M antennas at the BS, which simultaneously serves NK single-antenna users in the same time-frequency resource element (see Fig. 1). The users are grouped into N clusters according to their spatial directions [1]. Each cluster consists of K users, which share the same spatial direction but may have different long-term fading coefficients [1]. An active eavesdropper is assumed to be located within each cluster aiming to intercept the downlink legitimate transmissions.

The uplink channel between the kth user in the nth cluster and the BS is denoted by $\mathbf{h}_{nk}$, where $n \in \{1, \cdots, N\}$ and $k \in \{1, \cdots, K\}$. The uplink channel between the eavesdropper in the nth cluster and the BS is denoted by $\mathbf{g}_n$. These two channels can be modeled as [2]

$$\mathbf{h}_{nk} = \zeta_{h_{nk}}^{1/2} \tilde{\mathbf{h}}_{nk} \qquad \text{and} \qquad \mathbf{g}_n = \zeta_{g_n}^{1/2} \tilde{\mathbf{g}}_n, \tag{1}$$

where $\tilde{\mathbf{h}}_{nk} \sim \mathcal{CN}(\mathbf{0}_{M\times 1}, \mathbf{I}_M)$ and $\tilde{\mathbf{g}}_n \sim \mathcal{CN}(\mathbf{0}_{M\times 1}, \mathbf{I}_M)$ capture the small-scale quasi-static Rayleigh fading, while $\zeta_{h_{nk}}$ and ζ_{g_n} capture the path-losses, respectively.

B. Uplink channel estimation with active pilot attacks

In TDD-based sub-6 GHz massive MIMO, the uplink channels are estimated at the BS by leveraging pilots sent by the users. Since the maximum allowable orthogonal pilot sequence length is constrained by the finite channel coherence interval, intra-cluster users share the same pilot sequence. A set of N orthogonal pilot sequences is allocated for N clusters such that the pilots of inter-cluster users are orthogonal [1]. This pilot assignment minimizes the channel estimation overhead in the overloaded NOMA case in which the total number of users exceeds the number of BS antennas ($NK > M$). In active attacks, the user pilot sequences are typically assumed to be known at the eavesdroppers [5]. Thus, an active eavesdropper imitates a legitimate user by sending the same user pilot sequence. In such cases, the BS inadvertently estimates the eavesdropper's channel, and a precoder, which is constructed by using this contaminated estimate, will eventually implicitly beamform legitimate data toward the active eavesdropper [5].

When no pilot attack is present, the pilot signal received at the BS can be written as

$$\mathbf{Y}_p = \sum_{n=1}^{N}\sum_{k=1}^{K} \sqrt{\tau_p P_{nk}^p}\mathbf{h}_{nk}\boldsymbol{\phi}_n + \mathbf{W}_p, \tag{2}$$

where τ_p is the pilot duration in symbols, and P_{nk}^p is the pilot transmit power at the kth user in the nth cluster. In (2), $\boldsymbol{\phi}_n \in \mathbb{C}^{1\times\tau_p}$ denotes the pilot sequence sent by the users in the nth cluster, satisfying $\boldsymbol{\phi}_n\boldsymbol{\phi}_n^H = 1$ and $\boldsymbol{\phi}_n\boldsymbol{\phi}_{n'}^H = 0$ for $n \neq n'$ and $n, n' \in \{1, \cdots, N\}$. Moreover, $\mathbf{W}_p \sim \mathcal{CN}(\mathbf{0}_{M\times\tau_p}, \mathbf{I}_{M\times\tau_p})$ is an additive white Gaussian noise (AWGN) at the BS.

In the presence of a pilot attack, the pilot signal received at the BS is given by

$$\mathbf{Y}_p = \sum_{n=1}^{N}\sum_{k=1}^{K} \sqrt{\tau_p P_{nk}^p}\mathbf{h}_{nk}\boldsymbol{\phi}_n + \sum_{n=1}^{N} \sqrt{P_{E,n}^p}\mathbf{g}_n\boldsymbol{\phi}_n + \mathbf{W}_p, \tag{3}$$

where $P_{E,n}^p$ is the pilot transmit energy of the eavesdropper in the nth cluster. A sufficient statistic can be obtained by projecting the received pilot signal onto the pilot sequence $\boldsymbol{\phi}_n$. The sufficient statistic under no pilot attack is given by

$$\mathbf{y}_{p,n} = \mathbf{Y}_p\boldsymbol{\phi}_n^H = \sum_{k=1}^{K} \sqrt{\tau_p P_{nk}^p}\mathbf{h}_{nk} + \mathbf{w}_{p,n}, \tag{4}$$

where $\mathbf{w}_{p,n} = \mathbf{W}_p\boldsymbol{\phi}_n^H$. The sufficient statistic in the presence of a pilot attack can be written as

$$\mathbf{y}_{p,n} = \mathbf{Y}_p\boldsymbol{\phi}_n^H = \sum_{k=1}^{K} \sqrt{\tau_p P_{nk}^p}\mathbf{h}_{nk} + \sqrt{P_{E,n}^p}\mathbf{g}_n + \mathbf{w}_{p,n}. \tag{5}$$

Then, a hypothesis test can be formulated by treating the case with no pilot attack as the null hypothesis ($\mathcal{H}_0$), and the case with a pilot attack as the alternative hypothesis ($\mathcal{H}_1$) as

$$\mathcal{H}_0 : y_{p,n}[m] = \sum_{k=1}^{K} \sqrt{\tau_p P_{nk}^p} h_{nk}[m] + w_{p,n}[m], \tag{6a}$$

$$\mathcal{H}_1 : y_{p,n}[m] = \sum_{k=1}^{K} \sqrt{\tau_p P_{nk}^p} h_{nk}[m] + \sqrt{P_{E,n}^p} g_n[m] + w_{p,n}[m], \tag{6b}$$

where $m \in \{1, \cdots, M\}$. In (6a) and (6b), since channels are assumed to be static during the coherence interval, the received signals at each BS antenna are considered as data inputs to the hypothesis test based on spatial sampling [13].

III. Detection of active pilot attacks

A. Eavesdroppers with known signal parameters

When the eavesdropper's signal/channel parameters are known to the BS, a hypothesis test can be reformulated as

$$\mathcal{H}_0 : y_{p,n}[m] = s_0[m] + w_{p,n}[m], \tag{7a}$$

$$\mathcal{H}_1 : y_{p,n}[m] = s_1[m] + w_{p,n}[m], \tag{7b}$$

$$f(\mathbf{y}_{p,n},\sigma_E^2;\mathcal{H}_1)=\frac{1}{(2\pi)^{\frac{M}{2}}\det^{\frac{1}{2}}(\mathbf{C}_1+\mathbf{I}_M)}\exp\left[-\frac{1}{2}\mathbf{y}_{p,n}^H(\mathbf{C}_1+\mathbf{I}_M)^{-1}\mathbf{y}_{p,n}\right] \tag{22}$$

$$\ln\left(f(\mathbf{y}_{p,n},\sigma_E^2;\mathcal{H}_1)\right)=-\frac{M}{2}\ln(2\pi)-\frac{M}{2}\ln\left(\sigma_0^2+\sigma_E^2+1\right)-\frac{1}{2\left(\sigma_0^2+\sigma_E^2+1\right)}\sum_{m=1}^{M}y_{p,n}^2[m] \tag{24}$$

where the signal components under $\mathcal{H}_0$ and $\mathcal{H}_1$ are given by

$$s_0[m]=\sum_{k=1}^{K}\sqrt{\tau_p P_{nk}^p}h_{nk}[m]\sim\mathcal{CN}(0,\sigma_0^2), \tag{8}$$

$$s_1[m]=\sum_{k=1}^{K}\sqrt{\tau_p P_{nk}^p}h_{nk}[m]+\sqrt{P_{E,n}^p}g_n[m]\sim\mathcal{CN}(0,\sigma_1^2), \tag{9}$$

where σ_0^2 and σ_1^2 are given by (see Appendix A)

$$\sigma_0^2=\mathbb{V}\text{ar}[s_0[m]]=\tau_p\sum_{k=1}^{K}P_{nk}^p\zeta_{h_{nk}}, \tag{10a}$$

$$\sigma_1^2=\mathbb{V}\text{ar}[s_1[m]]=\tau_p\sum_{k=1}^{K}P_{nk}^p\zeta_{h_{nk}}+P_{E,n}^p\zeta_{g_n}. \tag{10b}$$

Then, the hypothesis test can be rewritten as

$$\mathcal{H}_0:\mathbf{y}_{p,n}\sim\mathcal{CN}(\mathbf{0},(\sigma_0^2+1)\mathbf{I}_M), \tag{11a}$$

$$\mathcal{H}_1:\mathbf{y}_{p,n}\sim\mathcal{CN}(\mathbf{0},(\sigma_1^2+1)\mathbf{I}_M). \tag{11b}$$

This is equivalent to detection of Gaussian signals with known/different variances embedded in AWGN, and thus, the NP-based detector is optimal [13]. This NP detector decides $\mathcal{H}_1$ to maximize the probability of detection of pilot attack $P_D=P_r(\mathcal{H}_1;\mathcal{H}_1)$ for a given/fixed false alarm probability $P_{FA}=P_r(\mathcal{H}_1;\mathcal{H}_0)=\alpha$ if

$$L(\mathbf{y}_{p,n})=\frac{f(\mathbf{y}_{p,n};\mathcal{H}_1)}{f(\mathbf{y}_{p,n};\mathcal{H}_0)}>\gamma, \tag{12}$$

where $L(\mathbf{y}_{p,n})$ is a likelihood ratio, the notation $f(.)$ denotes the probability density function (PDF) and γ is given by

$$P_{FA}=\int_{\{\mathbf{y}_{p,n}:L(\mathbf{y}_{p,n})>\gamma\}}f(\mathbf{y}_{p,n};\mathcal{H}_0)d\mathbf{y}_{p,n}=\alpha. \tag{13}$$

By substituting the corresponding PDFs, the likelihood ratio in (12) can be rewritten as

$$L(\mathbf{y}_{p,n})=\frac{\frac{1}{[2\pi(\sigma_1^2+1)]^{\frac{M}{2}}}\exp\left[\frac{-1}{2(\sigma_1^2+1)}\sum_{m=1}^{M}y_{p,n}^2[m]\right]}{\frac{1}{[2\pi(\sigma_0^2+1)]^{\frac{M}{2}}}\exp\left[\frac{-1}{2(\sigma_0^2+1)}\sum_{m=1}^{M}y_{p,n}^2[m]\right]}>\gamma. \tag{14}$$

By using (14), the log-likelihood ratio can be computed as

$$\ln\left(L(\mathbf{y}_{p,n})\right)=l(\mathbf{y}_{p,n})>\ln(\gamma), \tag{15}$$

where $l(\mathbf{y}_{p,n})$ is given by

$$l(\mathbf{y}_{p,n})=\frac{M}{2}\ln\left(\frac{\sigma_0^2+1}{\sigma_1^2+1}\right)-\frac{1}{2}\left(\frac{\sigma_0^2-\sigma_1^2}{(\sigma_1^2+1)(\sigma_0^2+1)}\right)\sum_{m=1}^{M}y_{p,n}^2[m]. \tag{16}$$

Thus, the NP detector decides $\mathcal{H}_1$ if

$$T(\mathbf{y}_{p,n})=\sum_{m=1}^{M}y_{p,n}^2[m]>\gamma', \tag{17}$$

where $T(\mathbf{y}_{p,n})$ is the sufficient test statistics of the NP detector, and γ' is given by

$$\gamma'=\frac{(\sigma_1^2+1)(\sigma_0^2+1)}{\sigma_1^2-\sigma_0^2}\left[2\ln(\gamma)-M\ln\left(\frac{\sigma_0^2+1}{\sigma_1^2+1}\right)\right]. \tag{18}$$

The NP detector compares the received signal energy with a threshold, and hence, the energy detector becomes optimal. In order to analyze the detector performance, the distributions of $T(\mathbf{y}_{p,n})$ under two hypotheses can be written as

$$T(\mathbf{y}_{p,n})\Big/\left[(\sigma_0^2+1)/2\right]\sim\chi_{2M}^2,\quad\text{under }\mathcal{H}_0, \tag{19a}$$

$$T(\mathbf{y}_{p,n})\Big/\left[(\sigma_1^2+1)/2\right]\sim\chi_{2M}^2,\quad\text{under }\mathcal{H}_1. \tag{19b}$$

Since the received signal $\mathbf{y}_{p,n}$ has a complex Gaussian distribution, the test statistic $T(\mathbf{y}_{p,n})$ becomes Chi-Squared distributed with $2M$ degrees-of-freedom [13].

B. Eavesdroppers with unknown signal parameters

When the eavesdropper's signal parameters are unknown to the BS, the hypothesis test can be reformulated as

$$\mathcal{H}_0:y_{p,n}[m]=s_0[m]+w_{p,n}[m], \tag{20a}$$

$$\mathcal{H}_1:y_{p,n}[m]=s_1[m]+w_{p,n}[m], \tag{20b}$$

where $s_0[m]$ and $s_1[m]$ are Gaussian random processes with zero mean and covariance matrices $\mathbf{C}_0=\sigma_0^2\mathbf{I}_M$ and $\mathbf{C}_1=(\sigma_0^2+\sigma_E^2)\mathbf{I}_M$, respectively. Furthermore, σ_0^2 is given in (10a), and $\sigma_E^2=\mathbb{E}[|\sqrt{P_{E,n}^p}g_n[m]|^2]$ is the variance of the eavesdropper's signal. In particular, σ_E^2 is assumed to be incompletely known to the BS, and it is the same for all $m\in\{1,\cdots,M\}$ co-located BS antennas. Thus, the hypothesis test in (20), can be reformulated as

$$\mathcal{H}_0:\mathbf{y}_{p,n}\sim\mathcal{CN}(\mathbf{0},(\sigma_0^2+1)\mathbf{I}_M), \tag{21a}$$

$$\mathcal{H}_1:\mathbf{y}_{p,n}\sim\mathcal{CN}(\mathbf{0},(\sigma_0^2+\sigma_E^2+1)\mathbf{I}_M). \tag{21b}$$

Since a signal parameter under $\mathcal{H}_1$ is unknown, the underlying test becomes a composite hypothesis test. Thus, the optimal NP test is not practically realizable as the threshold will depend on the unknown signal parameter. If we assume the perfect knowledge of the unknown parameter in designing the NP test, the underlying detector becomes a Clairvoyant detector [13], which can only be used for performance comparison purposes. Since the eavesdropper's signal parameters are typically unknown to the BS, the optimal NP detector in (17) is indeed a Clairvoyant detector.

Nonetheless, a GLRT can be formulated for the composite hypothesis test in (21). To this end, the unknown σ_E^2 can be replaced by its MLE under $\mathcal{H}_1$. The probability density function (PDF) of $\mathbf{y}_{p,n}$ under $\mathcal{H}_1$ is given in (22) at the top of this page. Since $\mathbf{C}_1$ is a diagonal matrix, $\det(\mathbf{C}_1+\mathbf{I}_M)$ and $(\mathbf{C}_1+\mathbf{I}_M)^{-1}$ are computed as

$$\det(\mathbf{C}_1+\mathbf{I}_M)=\left(\sigma_0^2+\sigma_E^2+1\right)^M, \tag{23a}$$

$$(\mathbf{C}_1+\mathbf{I}_M)^{-1}=\frac{1}{(\sigma_0^2+\sigma_E^2+1)}\mathbf{I}_M. \tag{23b}$$

By substituting (23) into (22) and then by taking the logarithm, the PDF under $\mathcal{H}_1$ can be written as (24). By using (24), the MLE of σ_E^2 can be derived as (see Appendix B)

$$\hat{\sigma}_E^2=\max\left(0,\frac{1}{M}\sum_{m=1}^{M}y_{p,n}^2[m]-\left(\sigma_0^2+1\right)\right). \tag{25}$$

The GLRT decides $\mathcal{H}_1$ if

$$L_G(\mathbf{y}_{p,n})=\frac{f(\mathbf{y}_{p,n},\hat{\sigma}_E^2;\mathcal{H}_1)}{f(\mathbf{y}_{p,n};\mathcal{H}_0)}>\gamma, \tag{26}$$

where γ is the threshold and is given in (13). Then, by taking the logarithm in both sides of (26), we have

$$\ln\left(L_G(\mathbf{y}_{p,n})\right)=\ln\left(\frac{f(\mathbf{y}_{p,n},\hat{\sigma}_E^2;\mathcal{H}_1)}{f(\mathbf{y}_{p,n};\mathcal{H}_0)}\right)>\ln(\gamma), \tag{27}$$

where $\ln\left(L_G(\mathbf{y}_{p,n})\right)$ is given by

$$\begin{aligned}\ln\left(L_G(\mathbf{y}_{p,n})\right) &= \ln\left(f(\mathbf{y}_{p,n},\hat{\sigma}_E^2;\mathcal{H}_1)\right) - \ln\left(f(\mathbf{y}_{p,n};\mathcal{H}_0)\right)\\ &= -\frac{1}{M}\ln\left(1+\frac{\hat{\sigma}_E^2}{\sigma_0^2+1}\right)\\ &\quad+\frac{1}{2}\sum_{m=1}^{M} y_{p,n}^2[m]\left(\frac{1}{\sigma_0^2+1}-\frac{1}{\sigma_0^2+\hat{\sigma}_E^2+1}\right). \quad (28)\end{aligned}$$

Under $\mathcal{H}_1$, $\hat{\sigma}_E^2 \geq 0$, and hence, (28) can be rearranged as

$$\ln\left(L_G(\mathbf{y}_{p,n})\right) = \frac{1}{M}\left[\left(\frac{\hat{\sigma}_E^2}{\sigma_0^2+1}+1\right)-\ln\left(\frac{\hat{\sigma}_E^2}{\sigma_0^2+1}+1\right)-1\right]. \quad (29)$$

Next we define $g(x) = x - \ln(x) - 1$, which is a monotonically increasing one-to-one function of its argument x for $x > 1$. Thus, the inverse function $g^{-1}(x)$ exists. By defining $x = \left(\hat{\sigma}_E^2/(\sigma_0^2+1)\right)+1$, (27) can be rewritten as

$$\begin{aligned}&\frac{M}{2}g\left(\frac{\hat{\sigma}_E^2}{\sigma_0^2+1}+1\right) > \ln(\gamma)\\ &\hat{\sigma}_E^2 > \left(\sigma_0^2+1\right)\left[g^{-1}\left(\frac{2}{M}\ln(\gamma)\right)-1\right]. \quad (30)\end{aligned}$$

By using (25) and (30), a sufficient test statistic is derived as

$$T(\mathbf{y}_{p,n}) = \sum_{m=1}^{M} y_{p,n}^2[m] > \gamma'', \quad (31)$$

where γ'' is given by

$$\gamma'' = M\left(\sigma_0^2+1\right)g^{-1}\left(\frac{2}{M}\ln(\gamma)\right). \quad (32)$$

Next, the probability distributions of $T(\mathbf{y}_{p,n})$ under two hypotheses are given by

$$T(\mathbf{y}_{p,n})\Big/\left[(\sigma_0^2+1)/2\right] \sim \chi^2_{2M}, \quad \text{under } \mathcal{H}_0, \quad (33a)$$

$$T(\mathbf{y}_{p,n})\Big/\left[(\sigma_0^2+\hat{\sigma}_E^2+1)/2\right] \sim \chi^2_{2M}, \quad \text{under } \mathcal{H}_1. \quad (33b)$$

IV. Performance analysis

A. Performance of Clairvoyant detector with known eavesdropper signal parameters

By using the sufficient test statistic (17), the false alarm probability can be defined as

$$P_{FA} = P_r\left(T(\mathbf{y}_{p,n}) > \gamma'; \mathcal{H}_0\right), \quad (34)$$

where γ' is given in (18). Then, by using the PDF of $T(\mathbf{y}_{p,n})$ given in (19a) under $\mathcal{H}_0$, P_{FA} can be derived as

$$P_{FA} = P_r\left(\frac{T(\mathbf{y}_{p,n})}{(\sigma_0^2+1)/2} > \frac{\gamma'}{(\sigma_0^2+1)/2}\right) = \mathcal{Q}_{\chi^2_{2M}}\left(\frac{2\gamma'}{\sigma_0^2+1}\right), \quad (35)$$

where $\mathcal{Q}_{\chi^2_{2M}}(\cdot)$ is the right-tail probability of the central Chi-squared PDF with $2M$ degrees-of-freedom defined by [13]

$$\mathcal{Q}_{\chi^2_{2M}}(x) = \exp(-x/2)\sum_{k=0}^{M-1}\frac{(x/2)^k}{k!}, \quad \text{for } M > 1. \quad (36)$$

For a given/fixed P_{FA}, the threshold γ' can be computed as

$$\gamma' = \left(\frac{\sigma_0^2+1}{2}\right)\mathcal{Q}^{-1}_{\chi^2_{2M}}(P_{FA}). \quad (37)$$

The probability of detection of an active pilot attack can be defined by using the sufficient test statistic in (17) as follows:

$$\begin{aligned}P_D &= P_r\left(T(\mathbf{y}_{p,n}) > \gamma'; \mathcal{H}_1\right)\\ &= P_r\left(\frac{T(\mathbf{y}_{p,n})}{(\sigma_1^2+1)/2} > \frac{\gamma'}{(\sigma_1^2+1)/2}\right) = \mathcal{Q}_{\chi^2_{2M}}\left(\frac{2\gamma'}{\sigma_1^2+1}\right). \quad (38)\end{aligned}$$

By substituting (37) into (38), P_D can be derived as

$$P_D = \mathcal{Q}_{\chi^2_{2M}}\left(\left(\frac{\sigma_0^2+1}{\sigma_1^2+1}\right)\mathcal{Q}^{-1}_{\chi^2_{2M}}(P_{FA})\right). \quad (39)$$

The above closed-form expression of P_D serves as the ROC of the Clairvoyant detector when the signal parameters of the eavesdropper are assumed to be known to the BS.

B. Performance of GLRT detector with unknown eavesdroppers signal parameters

By using the sufficient test statistic in (33), P_{FA} can be computed as

$$\begin{aligned}P_{FA} &= P_r\left(T(\mathbf{y}_{p,n}) > \gamma''; \mathcal{H}_0\right)\\ &= P_r\left(\frac{T(\mathbf{y}_{p,n})}{(\sigma_0^2+1)/2} > \frac{\gamma''}{(\sigma_0^2+1)/2}\right) = \mathcal{Q}_{\chi^2_{2M}}\left(\frac{2\gamma''}{\sigma_0^2+1}\right), \quad (40)\end{aligned}$$

where the threshold γ'' is defined in (32). For a given P_{FA}, this threshold can be derived as

$$\gamma'' = \left(\frac{\sigma_0^2+1}{2}\right)\mathcal{Q}^{-1}_{\chi^2_{2M}}(P_{FA}). \quad (41)$$

Then, the detection probability P_D can be derived as

$$\begin{aligned}P_D &= P_r\left(T(\mathbf{y}_{p,n}) > \gamma''; \mathcal{H}_1\right)\\ &= P_r\left(\frac{T(\mathbf{y}_{p,n})}{(\sigma_0^2+\hat{\sigma}_E^2+1)/2} > \frac{\gamma''}{(\sigma_0^2+\hat{\sigma}_E^2+1)/2}\right)\\ &= \mathcal{Q}_{\chi^2_{2M}}\left(\frac{2\gamma''}{\sigma_0^2+\hat{\sigma}_E^2+1}\right). \quad (42)\end{aligned}$$

By substituting γ'' in (41) into (42), the ROC of the GLRT detector can be derived as follows:

$$P_D = \mathcal{Q}_{\chi^2_{2M}}\left(\left(\frac{\sigma_0^2+1}{\sigma_0^2+\hat{\sigma}_E^2+1}\right)\mathcal{Q}^{-1}_{\chi^2_{2M}}(P_{FA})\right). \quad (43)$$

V. Asymptotic Analysis

In this section, the asymptotic performance of GLRT detector is investigated when the number of BS antennas grows without bound ($M \to \infty$). To begin with, when M grows large, the MLE of σ_E^2 in (25) can be derived as

$$\lim_{M\to\infty}\hat{\sigma}_E^2 = \max\left(0, \lim_{M\to\infty}\frac{1}{M}\sum_{m=1}^{M} y_{p,n}^2[m] - \left(\sigma_0^2+1\right)\right). \quad (44)$$

By using Tchebyshev's theorem [14], the limit term in (44) can be derived as

$$\lim_{M\to\infty}\frac{1}{M}\sum_{m=1}^{M}|y_{p,n}[m]|^2 - \frac{1}{M}\sum_{m=1}^{M}\mathbb{E}\left[|y_{p,n}[m]|^2\right] \xrightarrow{a} 0, \quad (45)$$

where $\mathbb{E}\left[|y_{p,n}[m]|^2\right]$ is given by

$$\begin{aligned}&\mathbb{E}\left[|y_{p,n}[m]|^2\right]\\ &= \mathbb{E}\left[\left|\sum_{k=1}^{K}\sqrt{\tau_p P_{nk}^p}h_{nk}[m] + \sqrt{P_{E,n}^p}g_n[m] + w_{p,n}[m]\right|^2\right]\\ &= \sum_{k=1}^{K}\tau_p P_{nk}^p\mathbb{E}\left[|h_{nk}[m]|^2\right] + P_{E,n}^p\mathbb{E}\left[|g_n[m]|^2\right] + 1\\ &= \sum_{k=1}^{K}\tau_p P_{nk}^p\zeta_{h_{nk}} + P_{E,n}^p\zeta_{g_n} + 1 = \sigma_0^2 + \sigma_E^2 + 1, \quad (46)\end{aligned}$$

where σ_0^2 is defined in (10a) and $\sigma_E^2 = \mathbb{E}[|\sqrt{P_{E,n}^p}g_n[m]|^2] = P_{E,n}^p\zeta_{g_n}$. By substituting (46) into (44), the asymptotic MLE of σ_E^2 can be derived as

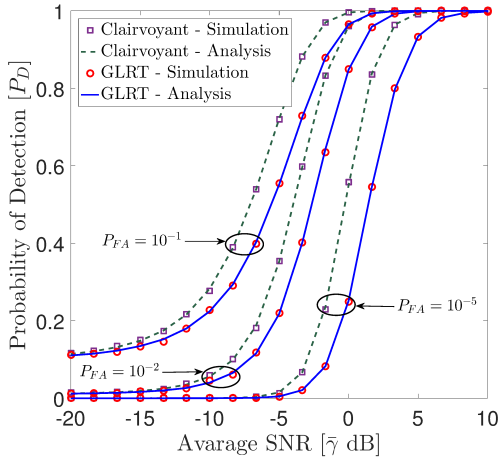

Fig. 2. Impact of P_{FA} on P_D for $M = 64$ and $K = N = 2$.

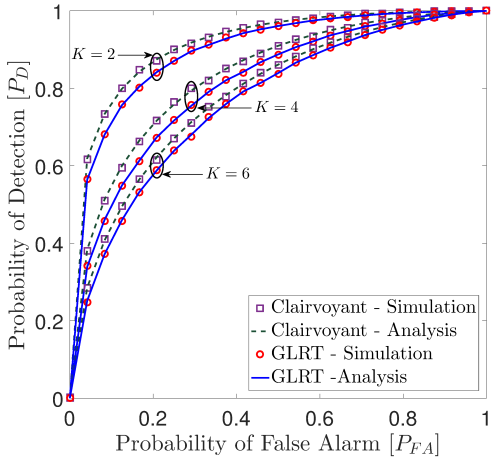

Fig. 3. Impact of user count on ROC for $M = 64$, $N = 3$ and $\bar{\gamma} = 10$ dB.

$$\lim_{M\to\infty} \hat{\sigma}_E^2 = \hat{\sigma}_{E,\infty}^2 = \max\left(0, \left(\sigma_0^2 + \sigma_E^2 + 1\right) - \left(\sigma_0^2 + 1\right)\right)$$
$$= \max\left(0, \sigma_E^2\right). \quad (47)$$

Thus, when $M \to \infty$, the MLE of the unknown eavesdropper's signal parameter ($\hat{\sigma}_E^2$) asymptotically approaches its true value σ_E^2. Consequently, the proposed GLRT detector asymptotically approaches the Clairvoyant detector, and the corresponding performance metrics become asymptotically optimal in NP sense.

VI. Numerical Results

Simulation parameters are as follows: $\tau_c = 196$, $\tau_p = N$ and $\zeta_{h_{nk}} = (d_0/d_{nk})^{\nu} \times 10^{\varphi_{nk}/10}$, where d_{nk} is the transmission distance between the kth user in the nth cluster and the BS, $d_0 = 1$ m is the reference distance, $\nu = 3.4$ is the path-loss exponent and $10^{\varphi_{nk}/10}$ captures the shadow fading with $\varphi_{nk} \sim \mathcal{N}(0, 8)$. The BS is placed at the center of a circular cell, which has a radius of 150 m.

In Fig. 2, the impact of different false alarm probabilities on the performance of active pilot attack detectors is investigated. To this end, our analyses in (39) and (43) are used, and Monte-Carlo simulations are used to validate our analysis. Three sets of curves are plotted by varying the false alarm probability as $P_{FA} = \{10^{-5}, 10^{-2}, 10^{-1}\}$. Fig. 2 clearly reveals that if the false alarm probability can be significantly traded-off, then, the probability of detection for a given average transmit SNR can be boosted. For instance, at an average transmit signal-to-noise-ratio (SNR) of -3 dB, the probability of detection can be boosted by 80.6% when the false alarm probability is allowed to increase to 10^{-1} from 10^{-2}. Both Clairvoyant and GLRT detectors behave similarly with respect to variations in false alarm probability. Performance of the Clairvoyant detector is investigated by assuming all eavesdropper's signal parameters are known to the BS, while GLRT detector is implemented by assuming an unknown eavesdropper's signal covariance matrix. Fig. 2 clearly reveals that the Clairvoyant detector outperforms the practically realizable GLRT detector. For instance, at the average transmit SNR of -5 dB, the Clairvoyant detector provides an 62.0% gain in terms of probability of detection over the GLRT detector at $P_{FA} = 10^{-2}$. Thus, the unknown eavesdropper's signal parameters must be taken into account in designing active pilot attack detectors. Unless otherwise, the probability of detection will be overestimated by the Clairvoyant detector, which is designed based on the NP test.

In Fig. 3, the impact of number of NOMA users per cluster on the ROC of active pilot attack detection is investigated by plotting the probability of detection as a function on false alarm probability. Three sets of ROC curves are plotted by varying the number of intra-cluster users as $K = \{2, 4, 6\}$. Fig. 3 clearly reveals that the detection performance decreases as the number of NOMA users increases. For example, the probability of detection is decreased by 16.0% for the same false alarm probability of 0.4 when the number of intra-cluster NOMA users is increased from $K = 2$ to $K = 6$. This behavior is a direct consequence of increased residual interference owing to sharing of the same pilot sequence among more intra-cluster NOMA users. On one hand, the density of wireless connections in the same time-frequency resource block can be boosted by grouping more users into the same NOMA cluster. On the other hand, the detection performance of active pilot attacks is significantly degraded as a result of more intra-cluster NOMA users. Thus, there exists a fundamental trade-off between the number of NOMA users that can be served simultaneously and the detection of active pilot contamination attacks.

In Fig. 4, the impact of the number of BS antennas on the ROC of active pilot attack detection is investigated. To this end, three sets of ROC curves are plotted by letting $M = \{32, 64, 128\}$. We conclude from Fig. 4 that the ROC curve moves in the desired direction when the number of BS antennas gradually grows large. For instance, at a false alarm probability of 0.4, the probability of detection can be boosted by 35.4% when the number of BS antennas increases from 32 to 128. Moreover, the performance gap between the practically viable GLRT-based detector and the Clairvoyant detector significantly narrows in the large BS antenna regime. This observation also validates our asymptotic analysis in Section V. Thus, we conclude that even with no prior

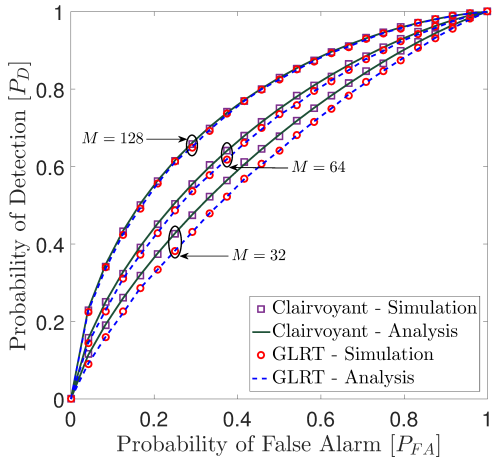

Fig. 4. Impact of M on ROC for $K = N = 2$ and $\bar{\gamma} = 10$ dB.

knowledge of eavesdropper's signal/channel parameters, the proposed GLRT-based detector can be accurately used to detect active pilot attacks in massive MIMO NOMA systems.

VII. Conclusion

Detection of active pilot attacks has been investigated for massive MIMO NOMA systems. When the active eavesdropper's signal parameters are unknown to the BS, a GLRT has been formulated, and thereby, a practically realizable active pilot attack detector has been proposed. The performance of this detector has been compared against a Clairvoyant NP detector, which assumes the perfect knowledge of eavesdropper's channel parameters. To this end, the probability of false alarm, probability of detection, and ROC have been quantified for both detectors. Our analysis reveals that the unknown parameters of eavesdropper's signal cannot be taken for granted in designing the pilot attack detectors because the Clairvoyant detectors may not be practically implementable and always overestimate the detector performance. Nonetheless, when the number of BS antennas grows unbounded, we show that the proposed GLRT detector asymptotically approaches Clairvoyant detector and the underlying performance metrics become asymptotically optimal in NP sense. A fundamental trade-off between the number of simultaneously served NOMA users and the detection performance of active pilot contamination attacks has been investigated.

Appendix A
The Derivation of Variances in (10)

By substituting $s_0[m]$ into (10a), σ_0^2 can be computed as

$$\sigma_0^2 = \mathbb{V}\mathrm{ar}[s_0[m]] = \mathbb{E}\left[\left|\sum_{k=1}^{K}\sqrt{\tau_p P_{nk}^p}h_{nk}[m]\right|^2\right]$$
$$= \sum_{k=1}^{K}\tau_p P_{nk}^p \mathbb{E}\left[|h_{nk}[m]|^2\right] = \sum_{k=1}^{K}\tau_p P_{nk}^p \zeta_{h_{nk}}. \quad (48)$$

Similarly, σ_1^2 can be computed as

$$\sigma_1^2 = \mathbb{V}\mathrm{ar}[s_1[m]]$$
$$= \mathbb{E}\left[\left|\sum_{k=1}^{K}\sqrt{\tau_p P_{nk}^p}h_{nk}[m] + \sqrt{P_{E,n}^p}g_n[m]\right|^2\right]$$
$$= \sum_{k=1}^{K}\tau_p P_{nk}^p \mathbb{E}\left[|h_{nk}[m]|^2\right] + P_{E,n}^p \mathbb{E}\left[|g_n[m]|^2\right]$$
$$= \sum_{k=1}^{K}\tau_p P_{nk}^p \zeta_{h_{nk}} + P_{E,n}^p \zeta_{g_n}. \quad (49)$$

Appendix B
The Derivation of MLE of σ_E^2 in (25)

The MLE of σ_E^2 can be derived by maximizing the logarithm of PDF given in (24). By differentiating (24) with respect to σ_E^2, we have

$$\frac{\partial \ln f(\mathbf{y}_{p,n}, \sigma_E^2; \mathcal{H}_1)}{\partial \sigma_E^2} = -\frac{M}{2}\left(\frac{1}{\sigma_0^2 + \sigma_E^2 + 1}\right)$$
$$+ \frac{1}{2\left(\sigma_0^2 + \sigma_E^2 + 1\right)^2}\sum_{m=1}^{M} y_{p,n}^2[m]. \quad (50)$$

Then, the MLE of σ_E^2 is derived by equating (50) to zero as

$$\hat{\sigma}_E^2 = \frac{1}{M}\sum_{m=1}^{M} y_{p,n}^2[m] - \left(\sigma_0^2 + 1\right). \quad (51)$$

When there exists a pilot attack, $\hat{\sigma}_E^2 > 0$, and hence, the final form of the MLE of σ_E^2 can be given as (25).

References

[1] H. V. Cheng, E. Björnson, and E. G. Larsson, "Performance Analysis of NOMA in Training-Based Multiuser MIMO Systems," *IEEE Trans. Wireless Commun.*, vol. 17, no. 1, pp. 372–385, Jan 2018.

[2] T. L. Marzetta, E. G. Larsson, H. Yang, and H. Q. Ngo, *Fundamentals of Massive MIMO*. Cambridge University Press, Cambridge, UK, 2016.

[3] X. Zhou, B. Maham, and A. Hjorungnes, "Pilot Contamination for Active Eavesdropping," *IEEE Trans. Wireless Commun.*, vol. 11, no. 3, pp. 903–907, March 2012.

[4] D. Kapetanovic, G. Zheng, and F. Russek, "Physical Layer Security for Massive MIMO: An Overview on Passive Eavesdropping and Active Attacks," *IEEE Commun. Mag.*, vol. 53, pp. 21–27, Jun. 2015.

[5] Y. Wu, R. Schober, D. W. K. Ng, C. Xiao, and G. Caire, "Secure Massive MIMO Transmission With an Active Eavesdropper," *IEEE Trans. Inf. Theory*, vol. 62, no. 7, pp. 3880–3900, Jul. 2016.

[6] B. Akgun, M. Krunz, and O. Ozan Koyluoglu, "Vulnerabilities of Massive MIMO Systems to Pilot Contamination Attacks," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 5, pp. 1251–1263, May 2019.

[7] J. K. Tugnait, "Self-Contamination for Detection of Pilot Contamination Attack in Multiple Antenna Systems," *IEEE Trans. Wireless Commun.*, vol. 4, no. 5, pp. 525–528, Oct 2015.

[8] ——, "Pilot Spoofing Attack Detection and Countermeasure," *IEEE Trans. Commun.*, vol. 66, no. 5, pp. 2093–2106, May 2018.

[9] Q. Xiong, Y. Liang, K. H. Li, and Y. Gong, "An Energy-Ratio-Based Approach for Detecting Pilot Spoofing Attack in Multiple-Antenna Systems," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 5, pp. 932–940, May 2015.

[10] N. Wang, L. Jiao, and K. Zeng, "Pilot Contamination Attack Detection for NOMA in mm-Wave and Massive MIMO 5G Communication," in *Proc. IEEE Conf. on Commun. and Network Security (CNS)*, May 2018, pp. 1–9.

[11] M. Hassan, A. Ahmed, and M. Zia, "Detection of Pilot Contamination Attack in Massive MIMO System," in *Proc. 52nd Asilomar Conference on Signals, Systems, and Computers*, Oct 2018, pp. 1674–1678.

[12] D. Kapetanovic, G. Zheng, K. Wong, and B. Ottersten, "Detection of Pilot Contamination Attack Using Random Training and Massive MIMO," in *Proc. IEEE 24th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, Sep. 2013, pp. 13–18.

[13] S. Kay, *Fundamentals of Statistical Signal Processing: Detection Theory*. PTR Prentice-Hall, 1993.

[14] H. Cramer, *Random Variables and Probability Distributions*. Cambridge University Press, 1970.