Int. J. Electron. Commun. (AEÜ) 113 (2020) 152945

Contents lists available at ScienceDirect

International Journal of Electronics and Communications (AEÜ)

journal homepage: www.elsevier.com/locate/aeue

Regular paper

Pilot contamination attack detection for multi-cell MU-massive MIMO system

Muhammad Hassan, Muhammad Zia *, Awais Ahmed, Naeem Bhatti

COMSIP LAB, Department of Electronics, Quaid-i-Azam University, Islamabad, Pakistan

ARTICLE INFO

Article history:
Received 23 January 2019
Accepted 4 October 2019

Keywords:
PCA
PHY
Active eavesdropping
Multi-cell MU-MaMIMO
Detection
Low-complexity

ABSTRACT

This work presents a low-complexity pilot contamination attack (PCA) detector for a multi-cell multi-user massive multiple-input, multiple-output (MU-MaMIMO) system. An active eavesdropper (Eve) in the reference cell transmits synchronized training sequence of the legitimate user (LU) under attack in order to alter precoder to steel information in the downlink data phase. The detection of an active Eve is vital for the information security and enhances secrecy capacity of the LU. We formulate binary hypotheses for active Eve detection from the contaminated channel estimation. We provide performance analysis of the proposed detector. The comparison of analysis and Monte Carlo runs verifies the accuracy of the analysis. The simulation results demonstrate that the performance of the proposed PCA detector is better than the well-known minimum descriptive length (MDL) method in low SNR regime.

1. Introduction

Wireless communication systems are vulnerable to both active and passive eavesdropping due to broadcast nature of the wireless channels [1–4]. The secret key generation from channel randomness [5] and secrecy capacity [6–10] are two fundamental approaches to secure information of the wireless networks at the physical layer (PHY). The secret key generation from the reciprocal and non-reciprocal channel by exploiting channel randomness has been interest of the research community [11–14]. The secrecy capacity of the MaMIMO system is much higher as compared to MIMO system due to the availability of large number of base station (BS) antennas to design beam (precoder) towards the LU [15–17]. Thus, passive eavesdropping is not effective when transmitter has large number of transmit antennas [18]. In MaMIMO system, Eve launches PCA on the LU in training phase by transmitting pilot sequence of the user under attack [19] in order to steer partial beam towards Eve in the downlink direction. The PCA has detrimental impact on the secrecy capacity of MaMIMO system [19]. The secrecy capacity of MaMIMO system under PCA can be enhanced by adding artificial noise (AN) in the null sub-space of the signal space [20,21] at the expense of signal power. In the event of absence of PCA, the knowledge of PCA can further improve the secrecy capacity of the LU by allocating all power to the signal. The impact of pilot contamination on the performance of multi-cell MaMIMO systems can also be reduced by optimizing the pilot assignment [8,9].

The detection of an active attack (PCA) is important to prevent leakage of private information towards Eve. The detection of Eve foretells the BS whether to add AN or not with the precoded data during the downlink phase. AN shares downlink power with the precoded data. Hence, Eve detection is vital to enhance secrecy capacity due to the fact that in the absence of Eve, total downlink power will be allocated to signal part.

1.1. Related work

The seminal work in [19] investigated PCA for BS with multiple antennas. Work in [22] used the random pilot sequence for PCA detection. Multiple PCA detection approaches for MaMIMO systems were discussed in [23]. Secure transmission under PCA and jamming for MaMIMO system was presented in [24]. Pilot spoofing attack (PSA) detection and channel estimation for single cell MaMIMO system using sub-space based MDL method was proposed in [25]. The two-way pilot method for discriminatory channel estimation was presented in [26] using whitening-rotation based semi-blind technique. A number of PCA detection techniques for MIMO systems were presented in [26,27], which are based on the NeymanPearson test assuming the knowledge of channel and noise covariance matrices.

The energy ratio based PCA detector presented in [28] exploited the asymmetry power levels of the received signal at the legitimate receiver and transmitter. The two-way pilot assisted PCA detector in

* Corresponding author.
E-mail address: mzia@ucdavis.edu (M. Zia).

https://doi.org/10.1016/j.aeue.2019.152945
1434-8411/

[29] achieves better performance than [28] and also estimates channels from user and Eve. However, the techniques in [28,29] need uplink and downlink pilots. A recent work in [30] added a random signal to the pilot sequence for reverse channel estimation at LU. The BS used the source enumeration method to detect Eve. The MDL scheme in [30,31] depends on uplink pilots and is extended for multi-user time-division duplex/space-division multiple access (TDD/SDMA) uplink model [2]. The PCA detector based on MDL technique has poor performance at low SNR regime and higher complexity. The proposed PCA detector for single user in [32] using random symbols has better performance in low SNR regime.

The improved energy detector (IED) in [33,34] achieves better performance in comparison with the conventional energy detector (ED). Gahane et al. [33] extended the IED for the mobile cognitive users of cooperative cognitive networks for fading channels, which have generalized Nakagami-q, Nakagami-m, $\nu-\mu$ and $\kappa-\mu$ distributions. Authors in [33] investigated the receiver operating characteristic (ROC) curves and its area under the curves. Moreover, the performance of the cooperative spectrum sensing for the multi-hop cognitive radio network using multiple antennas is investigated in [34] with the help of IED. Gahane and Sharma [35] explored the performance of improved energy detector in cooperative cognitive radio, which have selection combining diversity. Furthermore, imperfect channel state information and cognitive user mobility are considered to assess probability of false alarm, probability of miss detection, and probability of error over a Rayleigh fading wireless channel. However, detection statistics in [35] were obtained based on single sample of the signal. In [33–35], authors constructed hypotheses $\mathcal{H}_0$ (noise only) and $\mathcal{H}_1$ (primary user active) from the observation for the detection of primary user in cognitive network. In the proposed PCA detector, least square (LS) channel estimate is used to construct $\mathcal{H}_0$ (LU only in training phase) and $\mathcal{H}_1$ (LU and Eve both active). Furthermore, the proposed method also considers interference from the neighboring cells due to pilot reuse.

The existing methods have higher complexity due to sub-space based approaches and PCA detection for multi-cell MU-MaMIMO systems is not addressed.

1.2. Contributions

The existing works focused on the PCA detection for single cell communication systems. The sub-space based PCA detection methods have poor performance in low SNR regime and higher complexity [31] and references therein. Most of the existing methods transmit customized waveform with pilot sequence, which impairs channel estimate of the LU [31,28]. We propose a low-complexity PCA detector for multi-cell MU-MaMIMO systems, which has better performance in low SNR regime. The proposed method works for short pilot length and does not require modifications in the pilot sequence. The proposed method evaluates the energy of LU's estimated channel and compares it with the threshold value which is obtained from likelihood ratio test [36] to detect PCA in a multi-cell MU-MaMIMO system. We also explore the impact of location of Eve and change in the number of BS antennas in our proposed PCA detector. This work has the following key contributions:

- We formulate binary hypotheses from the channel estimate of LU to detect PCA for a multi-cell MU-MaMIMO system. The proposed method uses norm of the reverse channel estimate in pilot phase at BS for Eve's detection. The performance of the proposed method is better than the existing methods.
- We also provide performance analysis of the proposed PCA detector for single and multiple cells. The comparison of analysis and Monte Carlo results reveal that our analysis agrees with simulation results.
- The complexity of the proposed method increases linearly with the number of BS antennas, whereas the complexity of sub-space based methods increases exponentially with the number of BS antennas [2,30,31].
- The proposed method does not impose constraints on the length of pilot sequence. The existing sub-space based methods require training length larger or equal to the BS antennas [2,30,31].
- The proposed method achieves better performance in low SNR regime as compared to MDL based PCA detectors and is applicable for the multi-cell MU-MaMIMO network.

The rest of our work is organized as follows. In Section 2, we present the system model for PCA. In Section 3, we propose PCA detector for multi-cell MU-MaMIMO system. Section 4 provides analysis of the proposed PCA detector. Section 5 discusses the performance of the proposed PCA detector and its comparison with MDL based method. We conclude our work in Section 6.

1.2.1. Notations

We represent vectors and matrices by bold-face lowercase and bold-face uppercase letters, respectively. We use $(.)^H$ for Hermitian, $(.)^T$ for transpose and $\mathbf{E}\{.\}$ for expectation operator. $\mathbf{I}_N$ represents $N \times N$ identity matrix. Note that $\mathcal{C}$ is set of complex numbers.

2. System model

We consider a multi-cell MU-MaMIMO system in Fig. 1 consisting of $L+1$ cells, each cell has a BS equipped with M antennas and K single antenna users ($M \gg K$). A single antenna active Eve contaminates pilot of a user under attack in the reference (0-th) cell. We assume time-division duplex (TDD) mode and channel reciprocity. All the users in a cell transmit orthogonal pilot sequences of length τ to the respective BS for the estimation of reverse channel state information (CSI). The BS designs precoders using estimate of the reverse CSI of each user in the cell for data transmission in the downlink direction. An active Eve in the reference cell launches PCA by transmitting synchronized pilot sequence of the LU (the 1st user of 0-th cell) under attack towards the BS in order to contaminate channel estimation of the LU [19,21]. In this work, we assume that LUs and Eve transmit signals with unit power, whereas interference from the neighboring cells in pilot and data phases are scaled by power normalization factor

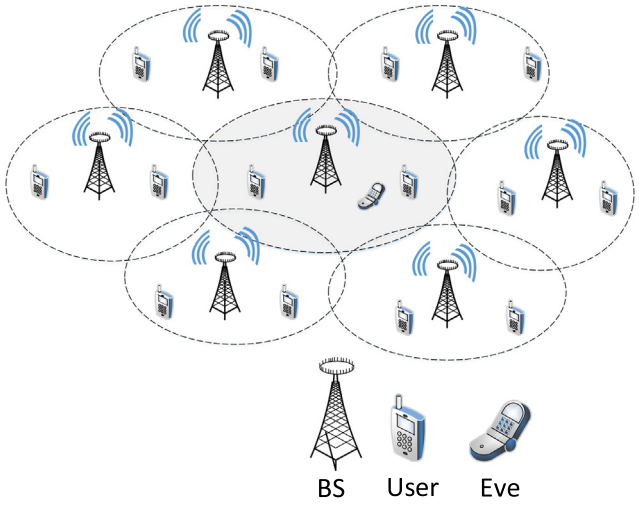

Fig. 1. System model of a multi-cell MU-MaMIMO wireless communication system with an active Eve present in the reference cell.