Malicious Corruption Resilience in PMU Data and Wide-Area Damping Control

Kaveri Mahapatra, *Student Member, IEEE,* Mahmoud Ashour, *Student Member, IEEE,* Nilanjan Ray Chaudhuri, *Senior Member, IEEE*, and Constantino M. Lagoa, *Member, IEEE*

***Abstract*—This paper presents a framework for malicious corruption resilience in PMU data and a methodology for applying this in wide-area damping control. The problem of detecting corruptions in raw PMU measurements is formulated as a compressed sensing problem and the compromised signals are recovered using an l_p-norm ($0 < p < 1$)-based online robust principal component analysis (RPCA) algorithm. The performance of the proposed method has been compared for different patterns of corruption with an l_1-norm based RPCA algorithm. The effectiveness of using the proposed data preprocessing architecture for correcting raw PMU feedback signals corrupted by missing data attack was demonstrated for closed-loop wide-area power oscillation damping control in 16-machine, 5-area New England-New York system.**

***Index Terms*—PMU, Compressed sensing, Cybersecurity, Sparse optimization, wide-area oscillation damping, Robust PCA**

I. Introduction

With the increase in deployment of advanced sensors such as Phasor Measurement Units (PMUs), many aspects of power system are changing including potential threats from cyber attacks. PMU data is being used extensively for situational awareness in addition to power plant and system modeling. Appropriately placed PMUs facilitate better observability of power system dynamics and thus provide an important opportunity to damp inter-area oscillations.

As pointed out in [1], in spite of a dedicated Intranet-based communication network in NASPInet architecture, it is not immune to cyber-attacks. A cyber attacker could gain access of the communication network of PMUs via GPS spoofing [2] and corrupt the data with carefully crafted anomalous injections. Propagation of these corrupted information [3] can affect wide-area measurement systems (WAMS)-based applications [4] and lead to inappropriate control decisions causing instability to the network.

The effect of cyber intrusion including false data injection (FDI) attack on SCADA measurements used in state estimation has been widely studied and PMU data was assumed to be secure and had been utilized to detect these attacks; e.g., see [5]–[9]. Reference [6] has proposed a robust frequency divider method along with correlation-based projection statistics, which requires different hyper-parameters for handling measurement noise, errors, losses, and false-data injection (FDI)-based cyberattacks. A projection statistics-based outlier detection technique with multiple hypothesis tests has been presented in [7] for handling observation, innovation, and structural bad data outliers in PMU measurements. However, this method is limited in application to the estimation of dynamic states of generators or online bus frequency estimation using PMUs at their terminals. A deep learning based method [10] is presented for FDI attacks in PMU measurements, however the effects of continuous corruption attacks were not studied. A DBSCAN based approach for only step and ramp type of FDI attacks in upto 2 channels is studied in [11]. Literature on bad data detection for wide-area monitoring and control include [12]–[15]. Among available approaches, a Bayesian-based Approximated Filter (BAF) was first proposed in [14] to extract modal damping and frequencies from corrupted data. In [16], the authors have studied the effect of multiple bad data outliers occurring at the same instant in PMU measurements on the lower and higher dimensional principal component scores. Papers [17]–[19] exploit lower dimensionality of PMU data for reconstruction of missing samples.

In case of different types of cyberattacks, the identity of the corrupted samples are not known in advance. This gives rise to a two-stage problem involving detection of the compromised samples followed by correction/reconstruction of those samples. In such cases, matrix-based block processing algorithms [20]–[24] or a vector processing algorithms [25], [26] can be used. References [20], [22] have presented matrix decomposition problem for detecting successive cyberattacks with the assumption of placement of PMUs in a completely observable network. The adversary having access to full system topology information was assumed in reference [22] to design unobservable attacks in a completely observable network. Recently, a method has been proposed in [23], which exploits the low-rank property of the Hankel structure to identify and correct random bad data outliers. However, its reconstruction performance deteriorates in case of continuous injection of correlated corruptions. Moreover, a large set of hyper-parameters are needed to be learned and tuned from historical data. A Principal Component Pursuit (PCP)-based block processing algorithm, which detects and corrects different types of corruptions due to cyberattacks on an unobservable network without any hyperparameter settings was presented in [21]. This is a model-free approach, when used in a moving-window framework. To the best of our knowledge, only [15] proposed a Kalman like particle filter for corruption

Kaveri Mahapatra, Mahmoud Ashour, Nilanjan Ray Chaudhuri, and Constantino Lagoa are with the School of Electrical Engineering and Computer Science, The Pennsylvania State University, State College, PA 16802, USA (e-mail: *kzm221@psu.edu, mma240@psu.edu, nuc88@engr.psu.edu, cml18@psu.edu*).

Financial support from NSF under grant awards CNS 1544621 and CNS 1739206 are gratefully acknowledged.

resilience in wide-area control of bus voltages. However, this only deals with random uncorrelated in time fault injection attacks presented during different intervals.

In this work, our focus is on wide-area control application using PMU data for inter-area oscillation damping. A review of existing literature [5]–[9], [12]–[15], [27]–[29] shows that no work has been performed on the malicious attack resilient wide-area damping control application. In contrast to existing literature, this paper proposes an interface layer based on a robust principal component analysis (RPCA) technique that has been used in the past for solving compressed sensing/sparse recovery [30]–[32] problem. The proposed algorithm pre-processes a vector of data samples from a set of signals at any time instant to detect data corruption stemming from cyberattack or otherwise and reconstructs the data vector at the corrupted positions using an appropriate subspace for inter-area oscillation damping control applications. One way to solve this involves an l_1 norm minimization-based vector processing algorithm, which was proposed in [25], [26]. This provides acceptable accuracy in reconstruction by solving an $l_1$norm-based convex optimization problem when upto 20% of signals are being corrupted at any instant.

The other objective of this work is to address a higher percentage of signals being corrupted simultaneously. An l_p-norm $(0 < p < 1)$-based RPCA algorithm is presented to solve this problem. The effectiveness of the proposed approach is demonstrated when different types of carefully designed cyber-attacks [14] corrupt PMU data during ambient and transient conditions. A comparison between the l_1 norm-based method [25], [26] and the proposed method with l_p norm has been conducted. In addition, the effect of using the proposed pre-processor for wide-area damping control has been demonstrated.

This paper is divided into five sections. Section II presents the proposed architecture for malicious corruption-resilient wide-area damping control using online RPCA algorithm. Section III discusses the problem formulation for detecting malicious injection attack in a data vector of phasor signal samples at any instant and proposes an algorithm to reconstruct the original data from corrupted data samples with the knowledge of operating condition. In Section IV, the reconstructed data samples are then used in closed loop control for damping power oscillations considering missing data attack on feedback signals. Section V concludes the paper.

II. Proposed Architecture

An architecture for malicious corruption-resilient wide-area damping control application is shown in Fig. 1. It is based on a concept of online malicious corruption detection and correction of data received from different PMUs using a data pre-processor. The pre-processor detects corrupted signals by solving a sparse recovery problem with the use of a robust PCA-based convex optimization algorithm and reconstructs the data with minimum mean square error (MSE) by least squares (LS) estimation using a subspace selected from a library of low-rank subspaces derived from uncorrupted offline simulation data. During online operation, the algorithm utilizes the information about changes in network topology obtained from the Topology Processor in the control center to select an appropriate subspace. Any malicious injections through cyberattacks is assumed to take place before the data arrives at the control center by overcoming the communication layer security. The control center is assumed to be secure from such attacks.

In this work, we studied the following types of attacks.

- *Parameter manipulation attack* - Injection of signals with altered modal characteristics.
- *Fault-resembling injection attack* - Injection of signals from fault recordings.
- *Missing data attack* - Stopping data samples from reaching the control center – phasor data Concentrator (PDC) produces the latest available data sample repeatedly unless fresh samples appear.
- *Data repetition attack* - Extracting a block of data from the past and repeat that in the transient condition.

As shown in Fig. 1, we assume that the control center receives signals from n_1 PMUs, which are used for different wide-area monitoring, protection, and control applications. A subset of these signals (k-signals) are used for the wide-area damping controller. The proposed data pre-processor works on all PMU signals.

III. Problem Formulation

The goal of the proposed data preprocessor is to identify the corrupted data samples received from a set of PMU signals and quantify the amount of corruption present in these signals at any sampling instant by using an efficient convex optimization algorithm. Since we are interested in inter-area oscillation modes, a set of PMUs are assumed to be placed on the major inter-tie buses and corresponding number of phasors is n_1. Let the measurements coming from phasor data concentrator (PDC) include time-stamped samples of n_1 different voltage phasor signals. At any instant these samples can be represented by a vector M_t of voltage magnitudes $(n_1 \times 1)$ and another vector of angles $(n_1 \times 1)$. These are highly correlated signals in the sense that all are governed by the system dynamics. Therefore, at any instant, the values of all samples are dependent on each other and interpreted as a dense vector L_t in the proposed problem formulation. The corruption present in each of these samples at any instant can be interpreted as a sparse vector S_t with a few nonzero elements being the additive corrupted values to those signals.

The objective of the proposed formulation is to recover a time-sequence of sparse vectors S_t of dimension $n_1 \times 1$ and a time-sequence of dense vectors L_t of dimension $n_1 \times 1$ from their sum as follows.

$$M_t = L_t + S_t \tag{1}$$

where, L_t originates from a low-dimensional signal subspace $\mathbb{R}^{n_1}$ of uncorrupted past measurements.

In other words, this is a problem of recovering a sparse corruption S_t in signal samples M_t at any instant. In literature [33], this is presented as an online robust principal component analysis (RPCA) problem. Conventional PCA is more

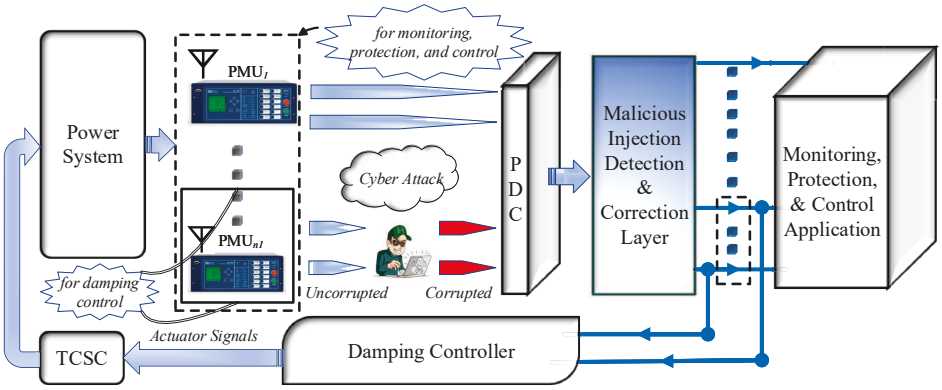

Fig. 1. Proposed architecture for online malicious corruption-resilient wide-area oscillation damping control.

sensitive to outliers whereas RPCA can efficiently compute Principal Components (PCs) in presence of outliers.

IV. Proposed Approach

At every time step t, both L_t and S_t are estimated such that estimate $\hat{L}_t$ lies in the subspace $\hat{U}$ described next and the estimate $\hat{S}_t$ represents the corruptions added to $\hat{L}_t$ to form M_t.

A. Preparation of the Library of Subspaces

A library of subspaces can be extracted from different operating conditions using offline planning simulation data. With the proposed formulation, a batch of subspaces needs to be enacted for current operating condition. Since PMU measures voltage magnitudes, angles, and frequencies, the proposed method considers each of those signal types separately while utilizing corresponding signal subspaces. The simulated data M_{Train}=[M_t;$0 \leq t \leq t_{Train}$], $M_{Train} \in \mathbb{R}^{n_1 \times n_2}$ is generated using ringdown response around each operating point (e.g. following a self-clearing fault) followed by detrending of samples. We propose that a self-clearing fault with a particular network configuration should be created for generating training data M_{Train}, which captures the dynamic behavior of the system around the operating point. M_{Train} for different network topologies can obtained by offline simulation of the network and $\hat{U}$ for each operating condition can be stored in a subspace library.

Given a training data set $M_{Train} \in \mathbb{R}^{n_1 \times n_2}$ containing n_1 signals with n_2 samples, the subspace U is formed by applying the singular value decomposition (SVD).

$$M_{Train} = U\Sigma V^* = \sum_{i=1}^{r} \sigma_i u_i v_i^* \tag{2}$$

where, 'r' represents the true rank of the matrix M_{Train} and σ_1,... σ_r denote 'r' singular values. The left and right singular vectors are given by $U = [u_1, \ldots, u_r]$ and $V = [v_1, \ldots, v_r]$, respectively. The true subspace for M_{Train} is given by matrix U. For a low-rank representation of the subspace, an approximate basis matrix $\hat{U}$ corresponding to the true subspace is calculated from a given training set M_{Train} by performing a low-rank ($r_{approx} < r_{true}$) approximation of the data [34]. This process takes basis vectors corresponding to a certain number r_{approx} of higher singular vectors to form the approximate basis $\hat{U} = [u_1, \ldots, u_{r_{approx}}]$. $\hat{U}$ is then considered as the subspace for a particular operating condition and is stored in the library.

B. Orthogonal Projection and Robust PCA

The key idea is to project any new measurement vector M_t onto a subspace, which is orthogonal to the low-rank signal subspace $\hat{U}$ of the the current operating condition using the projection matrix Φ.

$$y_t := \Phi_t M_t = \Phi_t (L_t + S_t) = \Phi_t S_t + \beta_t \tag{3}$$

$$\Phi_t = I - \hat{U}\hat{U}' \tag{4}$$

where, y_t is the projected measurement vector. The projection ensures that the contribution from corruption S_t is preserved while nullifying the contribution from L_t [32]. This is true when subspace $\hat{U}$ extracted from the training measurements, M_{Train} closely resembles the network behavior. For selecting the appropriate subspace $\hat{U}$ to be used at any time t, the proposed architecture uses network topology information from topology processor. Once $\hat{U}$ is selected, it is changed only if the network topology changes. Here β_t is interpreted as small noise. This leads to an optimization problem, which has a nonconvex objective function in the form of l_0 norm as presented below.

$$\min_{x_t} \|x_t\|_0 \, s.t. \, \|y_t - \Phi_t x_t\|_2 \leq \xi_t \tag{5}$$

where, $\xi_t = \|\beta_t\|_2$ is unknown in advance since $\beta_t = \Phi_t L_t$. Therefore, ξ_t is calculated from $\hat{\beta}_t$, which is taken as $\Phi_t L_{t-1}$. The solution $x_t = \hat{S}_t$ to the above minimization problem is the estimate of the sparse vector S_t.

In literature, this problem is known as "compressed sensing" or "compressed sampling" and overlaps with the basis pursuit problem [35], which is NP-hard. This non-convex problem can be approached with alternatives, which are l_1 norm and l_p norm as a relaxation of l_0 norm in the objective function. With l_1 objective, the resulting problem becomes convex and can be solved using any l_1 solver, see for example [25], [26]. With l_p-norm objective, when $0 < p < 1$, the resulting problem remains nonconvex and can be solved approximately using several methods proposed in literature [36], [37]. In this paper, an algorithm [36] for solving l_p-norm problem is presented for malicious corruption detection and correction of the PMU signals in order to achieve a solution closer to the global solution of the original nonconvex problem.

$$\min_{x_t} \|x_t\|_p \, s.t. \, \|y_t - \Phi_t x_t\|_2 \leq \xi_t \tag{6}$$

The target is to achieve improved accuracy of corruption

detection when as high as 40% of data samples are corrupted simultaneously.

C. Proposed Algorithm

An algorithm is presented to suite the problem of detecting corruptions in PMU measurements. The following describes the procedure to recover the correct signal vector from a set of corrupted measurements when some signals are affected by anomalous injections at any instant. Vectors M_t, $\hat{T}_t$, $\hat{S}_t$, $\hat{L}_t$ are of size $(n_1 \times 1)$ where n_1 denotes the number of signals considered. The iterations for computing $\hat{S}_t$ are started with minimum l_2 norm fit to the data by solving the following problem.

$$\min_{x_t} \|x_t\|_2 \, s.t. \, \|y_t - \Phi_t x_t\|_2 \leq \xi_t \tag{7}$$

Then the search direction d^h for h^{th} iteration is calculated by the steepest descent direction of the l_p norm at current iteration value of x_t obtained.

$$d^h = -\left|x^h\right|^{p-2} x^h \tag{8}$$

This is followed by taking a step in the descent direction and calculation of an intermediate variable z^h as follows with step size factor γ^h.

$$z^h = x^h + \gamma^h d^h \tag{9}$$

This intermediate variable is then projected orthogonally onto the affine constraint space $C = \left\{x : \|\Phi_t x - y_t\|_2^2 \leq \xi_t\right\}$ and the solution $x^h = P_C(z^h)$, which is the projection on C, is updated by solving the following convex optimization problem.

$$\min_{x^h} \left\|x^h - z^h\right\|_2^2 \; s.t. \left\|\Phi_t x^h - y_t\right\|_2^2 \leq \xi_t \tag{10}$$

Equations (8), (9), (10) are calculated at the same time step. The complete algorithm is given as follows.

Input: M_t, $\hat{U}$; **Output**: $\hat{S}_t$, $\hat{L}_t$; **Parameters**: p, h^{max};
Initialization

- Set the initial support $\hat{S} = [.]$.

While $t \geq t_0$

1) Choose subspace $\hat{U}$ from the library such that it closely represents the present condition.
2) Orthogonal projection: Compute $y_t = \phi_t M_t$ where $\phi_t \leftarrow (I\text{-}\hat{U}\hat{U}')$.
3) Compute $\xi_t = \|\beta_t\|_2$ where $\beta_t \leftarrow \Phi_t M_t$ for $t = t_0$ and $\beta_t \leftarrow \Phi_t L_{t-1}$ for $t \geq t_0$.
4) Compute $\hat{S}_t$ as a solution to the nonconvex objective function given in equation (6) as follows.
   a) **While** $h \leq h^{max}$
      i) Find the descent direction using (8).
      ii) Calculate step size γ^h by exact line search for getting minimum l_p norm value with z^h in (9).
      iii) Solve the optimization problem in (10) to get an update of x^h.
   b) Compute $\hat{S}_t \leftarrow x^{h^{max}}$.
5) Estimate $\hat{L}_t \leftarrow M_t - \hat{S}_t$.
6) Increment t by sampling time duration and go to step 1.

Remark: The proposed pre-processor solves an optimization problem and it can introduce delay. We have not focused on writing these codes that can be run in a computationally efficient manner. Moreover, high-end dedicated processors and real-time OS can be deployed to reduce the CPU time. This will be a future direction of research. For a wide-area damping control application, the damping controller needs to be designed to handle such latency – a lot of work has already been done in the area of delay compensation, which is outside the focus of this paper.

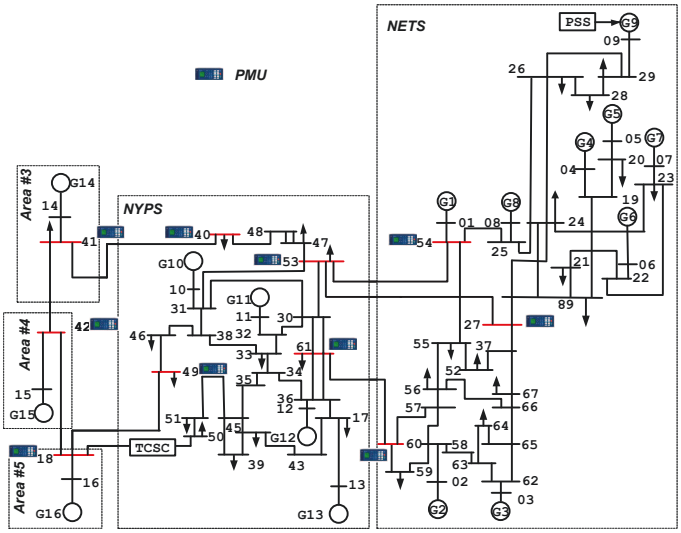

Fig. 2. Single-line diagram of 16-machine, 5-area New England-New York system with PMUs installed at major inter-tie buses highlighted in red.

V. Test System and Case Studies

We have considered a positive-sequence fundamental frequency phasor model of the 16-machine, 5-area New England-New York system [38] as the test system with PMUs installed at major inter-tie buses highlighted in red, see Fig. 2. A PMU data rate of 60Hz is assumed. As per the proposed architecure in Fig. 1, PMU signals received at PDC are passed through the proposed pre-processor. Ten voltage magnitudes (i.e. $n_1 = 10$) are considered for this experiment and detrending was performed on all signals first at the pre-processor. In our case studies, any 4 signals out of 10 are assumed to be corrupted at a particular instant. A comparison study between the proposed l_p norm ($p = 0.5$) based optimization technique ($Approach - l_p$) and previously proposed l_1 norm based optimization technique ($Approach - l_1$) [25], [26] has been conducted. $Approach - l_1$ has been selected for comparison since it represents an existing algorithm for online robust PCA. The reconstruction error with each method has been used as a performance measure for comparison.

The first 3 (r_{approx}= 3) left singular vectors corresponding to higher singular values are retained as basis vectors to form the subspace $\hat{U}$ at different operating points, which build the subspace library. In this work, we have used a window of 40 seconds, which results in $n_2 = 2394$ samples for calculating the orthonormal subspace U for any network configuration.

This section is divided into two parts. The first part presents the reconstruction accuracy of the proposed algorithm with different attacks in ambient and transient conditions in a nominal operating condition along with a comparison study.

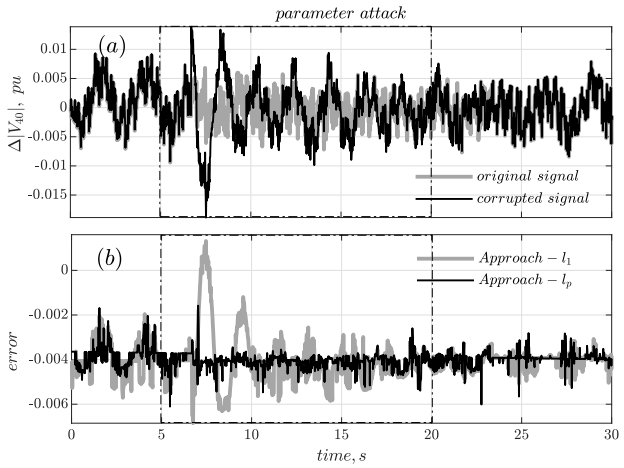

Fig. 3. Case I: Parameter manipulation attack in signal $|V_{40}|$ under ambient condition with original and reconstructed signals are shown in (a). The reconstruction errors by using $Approach - l_1$ [25], [26] and $Approach - l_p$ are shown in (b). Error: difference between original and reconstructed signal.

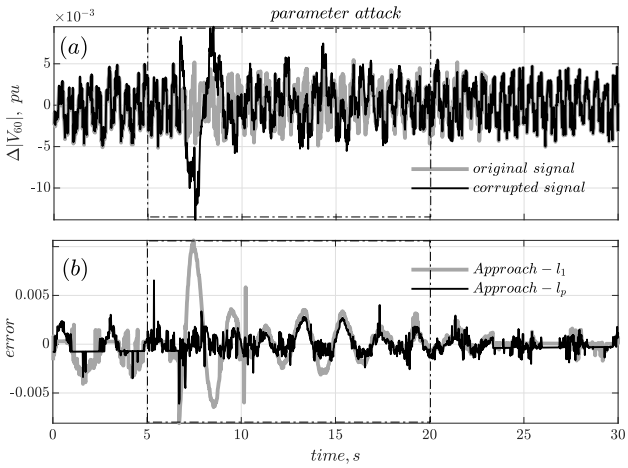

Fig. 4. Case I: Parameter manipulation attack in signal $|V_{60}|$ under ambient condition with original and reconstructed signals are shown in (a). The reconstruction errors by using $Approach - l_1$ [25], [26] and $Approach - l_p$ are shown in (b). Error: difference between original and reconstructed signal.

The second part discusses the effect of using PMU signals under cyberattack for wide-area damping control operation.

A. Nominal Operating Condition without Damping Control

In this case, corruption attacks were performed during ambient state under nominal condition and during transient state following a self-clearing fault. This is an open loop operation, i.e. no PMU signals in Fig. 2 have been fed back as input to a damping controller. This test is conducted for analyzing the performance of the algorithm under different types of attacks.

We assume that the signal subspace $\hat{U}_1$ utilized by the algorithm is formed based on the transient data following a self-clearing fault near bus 53, which is available from offline simulations. All the attacks during nominal operating condition in the network were performed on four signals together at the same time, which are $|V_{27}|$, $|V_{40}|$, $|V_{54}|$, and $|V_{60}|$ representing an attack on 40% of the PMU signals. The data pre-processor in Fig. 1 uses two methods: $Approach - l_1$ and the proposed $Approach - l_p$ norm based optimization.

1) Ambient Condition: To simulate the ambient condition, band-limited zero-mean Gaussian noise was injected in load terminals of the test system. The following two attacks are considered during ambient state, which are parameter manipulation attack and fault resembling injection attack in four signals. Highly correlated data has been injected in those four signals.

■ *Case I: Parameter Manipulation Attack:* This attack has been performed by injecting synthetic signals generated by an attack model using the weighted sum of three damped sinusoids with frequencies equal to 0.382Hz, 0.55Hz, and 0.618Hz with damping ratios 8.0%, 4.4%, and 5.7%, respectively. Figures 3 and 4 show two of the four signals affected due to parameter manipulation attack for 1000 consecutive samples simultaneously. Unless otherwise stated, only deviation in the signals from nominal values are shown. The quality of reconstruction is measured by the difference between original and reconstructed signal denoted by 'error.' A close to zero-error implies a good quality of reconstruction. The error in reconstruction of the samples in signals $|V_{40}|$ and $|V_{60}|$ are also compared and shown in Figs 3(b) and 4(b).

$$error : \bar{\varepsilon}_t = L_t - \hat{L}_t = \begin{bmatrix} \varepsilon_t(1) & \varepsilon_t(2) & \dots & \varepsilon_t(n_1) \end{bmatrix}^T \tag{11}$$

$$\bar{\mu}_{\varepsilon^2} = \sum_{i=1:n_2} \bar{\varepsilon}_{t_i}^2 \Big/ n_2 = \begin{bmatrix} \mu_{\varepsilon(1)^2} & \mu_{\varepsilon(2)^2} & \dots & \mu_{\varepsilon(n_1)^2} \end{bmatrix}^T \tag{12}$$

$$\mu_{\varepsilon_t} = n_1^{-1} \sum_{k=1:n_1} \varepsilon_t(k) = \mu_{error} \tag{13}$$

$$standard\ deviation : \sigma_t = \sqrt{\frac{\sum_{n_1} \left(\bar{\varepsilon}_t - \mu_{\varepsilon_t}\right)^2}{n_1 - 1}} = \sigma_{error} \tag{14}$$

TABLE I
CASE I: COMPARISON OF RECONSTRUCTION ERRORS BETWEEN l_1 [25], [26] AND PROPOSED ALGORITHM

Parameter Attack	Average MSE	Standard deviation	Maximum MSE
l_1	2.1448e-06	8.5755e-04	1.7665e-04
Proposed method	5.5906e-07	5.6759e-04	6.6075e-05

Moreover, different statistical measures such as mean error (μ_{error}) $\pm$ standard deviation of the error (σ_{error}) at each instant are calculated using (13)-(14) during reconstruction of all $|V|$ signals, which are shown in Fig. 5. The plots indicate that $Approach - l_1$ [25], [26] could not detect compromised samples properly when the corruption is present in 40% of signal samples at any instant and thus produces higher reconstruction error compared to $Approach - l_p$.

$$AMSE = \sum_{k=1:n_1} \mu_{\varepsilon(k)^2} \Big/ n_1 \tag{15}$$

Similarly, statistical measures such as average mean square error (AMSE) using (15), standard deviation obtained from (14) averaged over all instants, and maximum mean square error (MMSE) over the entire simulation interval are calculated and presented in Table I. These statistics indicate better performance of the proposed algorithm with l_p as compared

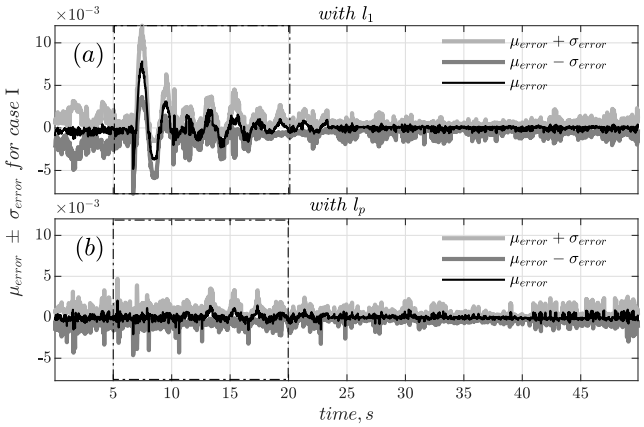

Fig. 5. Case I: Mean error (μ_{error}) $\pm$ Standard deviation of the error (σ_{error}) obtained during reconstruction of $|V|$ signals with (a) $Approach - l_1$ [25], [26] and the (b) $Approach - l_p$ (proposed method). The plots of $\mu_{error} + \sigma_{error}$ and $\mu_{error} - \sigma_{error}$ show statistical dispersion of reconstruction error obtained over 50 seconds.

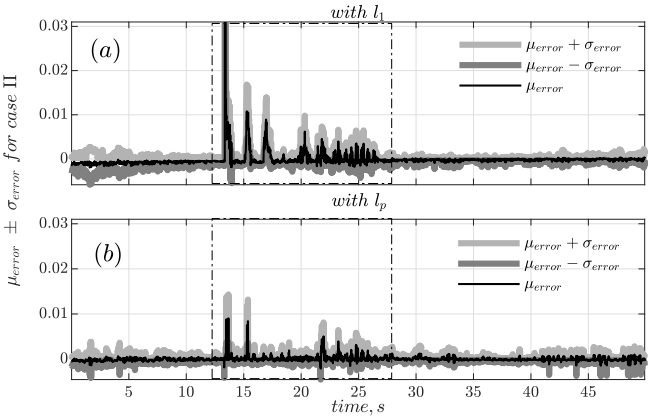

Fig. 6. Case II: Mean error (μ_{error}) $\pm$ Standard deviation of the error (σ_{error}) obtained during reconstruction of $|V|$ signals with (a) $Approach - l_1$ [25], [26] and the (b) $Approach - l_p$ (proposed method). The plots of $\mu_{error} + \sigma_{error}$ and $\mu_{error} - \sigma_{error}$ show statistical dispersion of reconstruction error obtained over 50 seconds.

to l_1.

■ *Case II: Fault-Resembling Injection Attack:* This attack has been performed by injecting a portion of archived transient data following a three-phase self-clearing fault near bus 53 into the considered signals during ambient state. The efficiency of the proposed algorithm $Approach - l_p$ has been compared with $Approach - l_1$ [25], [26] for the reconstruction of the compromised set of PMU signals. Figure 6 shows the central tendency and dispersion of reconstruction error of all PMU signals at each instant over an interval of 50 seconds of ambient data. The plots indicate $Approach - l_1$ produces higher average reconstruction error as compared to the proposed method on $Approach - l_p$. Statistical measures such as AMSE, standard deviation, and MMSE calculated over the reconstruction interval and presented in Table II support the same conclusion.

2) Transient Condition: To simulate the transient condition, a self-clearing three-phase fault near bus 53 is considered. Two types of attacks during transient state were performed on four signals $|V_{27}|$, $|V_{40}|$, $|V_{54}|$, and $|V_{60}|$, which are data repetition attack and missing data attack.

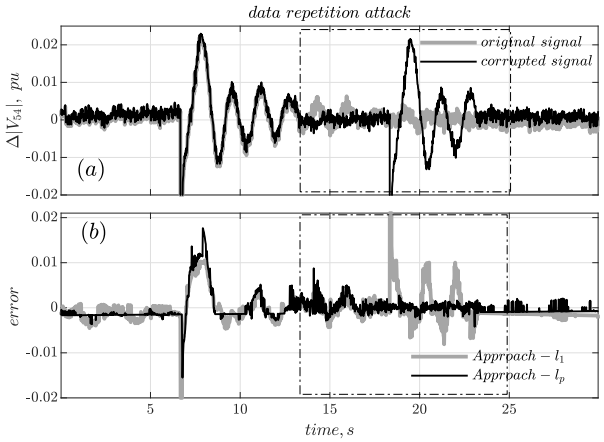

Fig. 7. Case III: Data repetition attack in signal $|V_{54}|$ under transient condition with original and reconstructed signals are shown in (a). The reconstruction errors by using $Approach - l_1$ [25], [26] and $Approach - l_p$ are shown in (b). Error: difference between original and reconstructed signal.

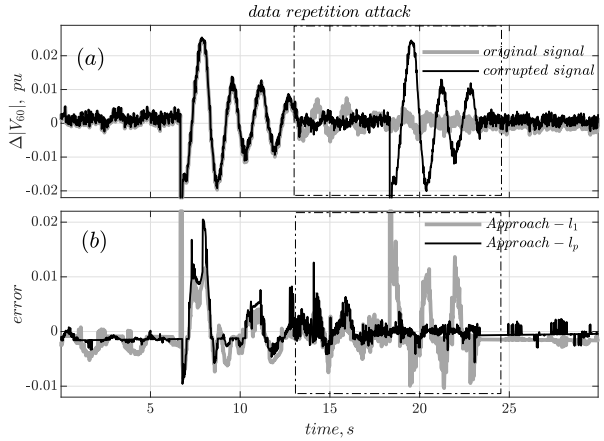

Fig. 8. Case III: Data repetition attack in signal $|V_{60}|$ under transient condition with original and reconstructed signals are shown in (a). The reconstruction errors by using $Approach - l_1$ [25], [26] and $Approach - l_p$ are shown in (b). Error: difference between original and reconstructed signal.

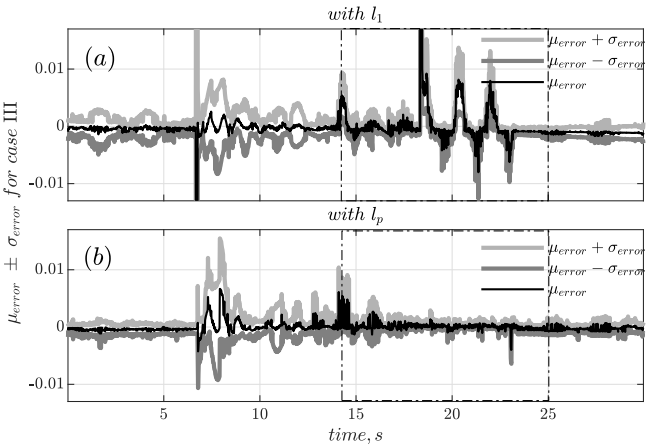

Fig. 9. Case III: Mean error (μ_{error}) $\pm$ Standard deviation of the error (σ_{error}) obtained during reconstruction of $|V|$ signals with (a) $Approach - l_1$ [25], [26] and the (b) $Approach - l_p$ (proposed method). The plots of $\mu_{error} + \sigma_{error}$ and $\mu_{error} - \sigma_{error}$ show statistical dispersion of reconstruction error obtained over 30 seconds.

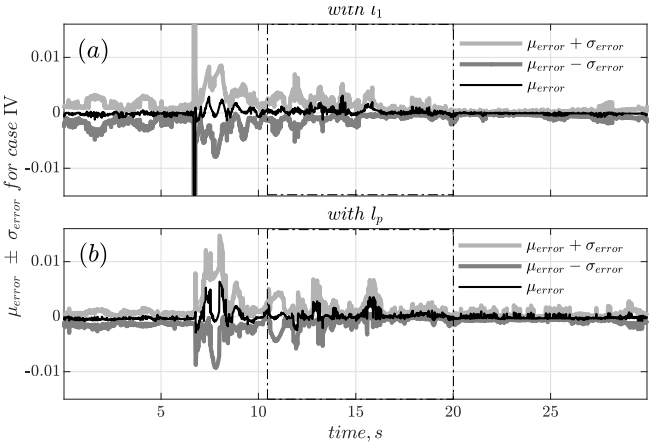

Fig. 10. Case IV: Mean error (μ_{error}) $\pm$ Standard deviation of the error (σ_{error}) obtained during reconstruction of $|V|$ signals with (a) $Approach - l_1$ [25], [26] and the (b) $Approach - l_p$ (proposed method). The plots of $\mu_{error} + \sigma_{error}$ and $\mu_{error} - \sigma_{error}$ show statistical dispersion of reconstruction error obtained over 30 seconds.

■ *Case III: Data Repetition Attack:* A window of ambient and transient data samples archived for the compromised signals are played back in the corresponding signals after the oscillations due to one fault has died down, thereby creating an impression of two consecutive faults. Figures 7 and 8 show two of the compromised signals and their corresponding reconstruction errors. Also, temporal variation of the central tendency and dispersion of this error is shown in Fig. 9. These figures demonstrate superiority of $Approach - l_p$.

■ *Case IV: Missing Data Attack:* The effectiveness of the proposed pre-processor in data reconstruction is shown in Fig. 10. The error in the reconstructed signal is higher at the beginning of the window, but is acceptable for most of the time span.

Similar to the ambient case studies, the proposed approach was compared with $Approach - l_1$ [25], [26] for Case III and IV. A comparison of different statistical measures of reconstruction errors in Tables III and IV clearly show superiority of the proposed method.

TABLE II
CASE II: COMPARISON OF RECONSTRUCTION ERRORS BETWEEN l_1 [25], [26] AND PROPOSED ALGORITHM

Fault Injection Attack	Average MSE	Standard deviation	Maximum MSE
l_1	2.9548e-05	9.8206e-04	0.0431
Proposed method	8.4261e-07	5.8854e-04	2.0878e-04

TABLE III
CASE III: COMPARISON OF RECONSTRUCTION ERRORS BETWEEN l_1 [25], [26] AND PROPOSED ALGORITHM

Data Repetition Attack	Average MSE	Standard deviation	Maximum MSE
l_1	8.0719e-05	0.0021	0.0407
Proposed method	3.8430e-06	0.0012	4.1966e-04

TABLE IV
CASE IV: COMPARISON OF RECONSTRUCTION ERRORS BETWEEN l_1 [25], [26] AND PROPOSED ALGORITHM

Missing Data Attack	Average MSE	Standard deviation	Maximum MSE
l_1	2.5888e-05	0.0016	0.0405
Proposed method	3.8094e-06	0.0012	4.0322e-04

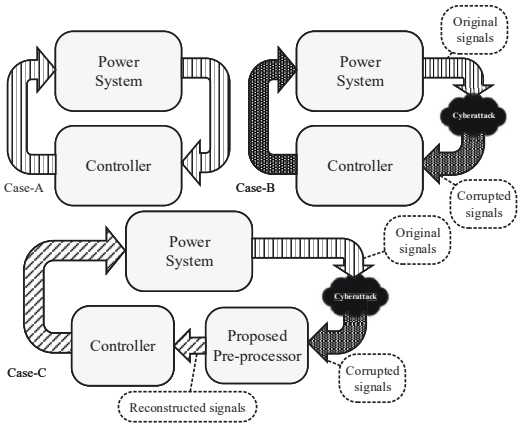

Fig. 11. Case-A: without proposed pre-processor and without any cyberattack on PMU signals; Case-B: without proposed pre-processor and with cyberattack on PMU signals; Case-C: with proposed pre-processor and with cyberattack on PMU signals.

B. Test with Inter-area Oscillation Damping Control

In this section, the effectiveness of using the proposed pre-processor in realizing malicious attack-resilience in wide-area damping control is demonstrated. It is assumed that 10 PMU signals: real power flows in lines 13-17, 14-41, 15-42, 16-18, 17-36, 30-53, 42-18, 51-45, 61-60, 18-69, and 51-45 arrive at the control center for different wide-area monitoring, protection, and control applications, see Fig.1. We have assumed a washout filter with time constant T_W = 10.0s is used before sending each signal, so that we only deal with deviations in them. Out of these, three ($\Delta P_{Line(13-17)}$, $\Delta P_{Line(16-18)}$, $\Delta P_{Line(51-45)}$) were selected as feedback signals for damping control based on observability of inter-area modes. A TCSC is used as an actuator in this system – see Fig. 1. It modulates the impedance of line connected between bus 18 and 50 in the network as shown in Fig. 2. A state feedback controller using linear quadratic regulator (LQR) gains and a reduced-order Luenberger observer were designed for power oscillation damping [39]. The design is performed on a reduced-order (10th order) linear model of the nominal system. The modal frequencies and settling times of the open and closed loop systems are shown in Table V. The parameters of the state-feedback control along with observer gain are mentioned in the Appendix.

Three different scenarios are created as presented in Fig. 11. In the first scenario (Case-A), the PMU signals were not attacked and the controller receives the true measurements from PMUs. In the second scenario (Case-B), PMU signals were attacked and the controller receives the corrupted PMU signals. In the third scenario (Case-C), the PMU signals are attacked and the corrupted signals are passed through the

TABLE V
MODAL FREQUENCIES AND SETTLING TIMES

Without Damping Control		With Damping Control	
$f_s,\ Hz$	$T_s,\ s$	$f_s,\ Hz$	$T_s,\ s$
0.392	31.270	0.399	9.326
0.508	28.962	0.503	12.313
0.623	19.947	0.631	7.277
0.792	16.108	0.792	14.126

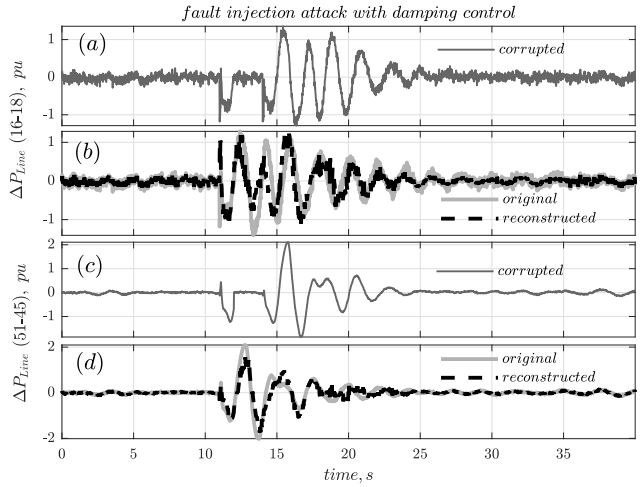

Fig. 12. Fault injection attack in signals $\Delta P_{Line,(16-18)}$, $\Delta P_{Line,(51-45)}$ following a three-phase self-clearing fault near bus 60 at $t = 11.0$s. Corrupted signals sent to the control center are shown in (a) and (c). Reconstructed signals are compared with the signals originally sent by the PMUs in (b) and (d) as per scenario in Case-C of Fig.11.

proposed pre-processor in order to reconstruct those signals and the reconstructed signals are given to the controller.

Remark: Please note that the data pre-processor accepts all 10 PMU signals mentioned earlier and reconstructs each of them for different wide-area monitoring, protection, and control applications. After reconstruction, three of the designated

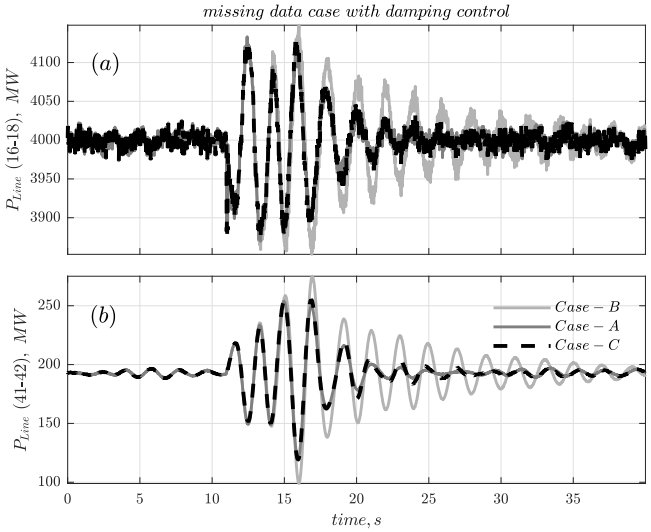

Fig. 13. Dynamic response of the system following a three-phase self-clearing fault near bus 60 at $t = 11.0$s. See Fig.11 for cases-A, B, and C.

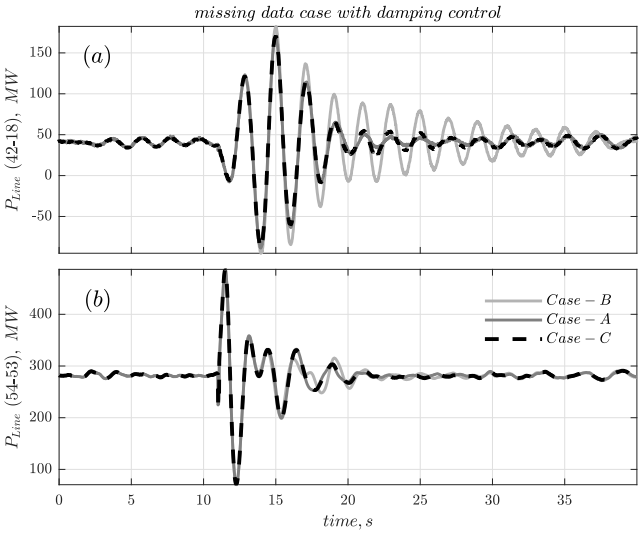

Fig. 14. Dynamic response of the system following a three-phase self-clearing fault near bus 60 at $t = 11.0$s. See Fig.11 for cases-A, B, and C.

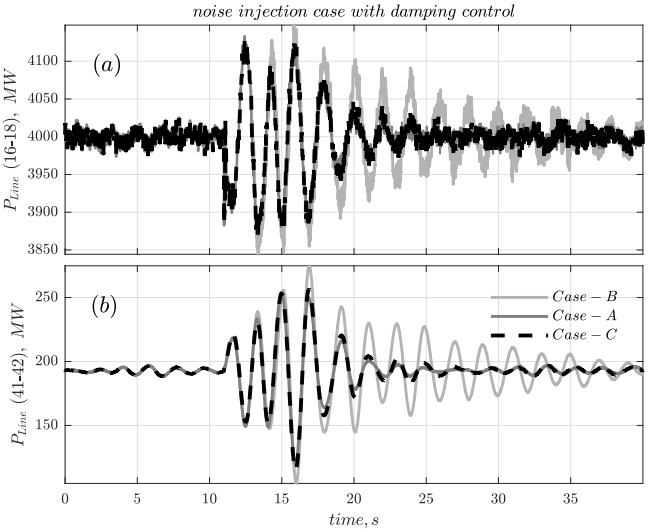

Fig. 15. Dynamic response of the system following a three-phase self-clearing fault near bus 60 at $t = 11.0$s. See Fig.11 for cases-A, B, and C.

signals are used as feedback signals for damping control. It should also be noted that the low-rank subspace $\hat{U}$ used for this case is derived based on offline simulation of Case-A (i.e. the system under closed-loop damping control). ■

Simulations are performed for 40 seconds in the nominal operating condition and a self-clearing fault was created near bus 60 at t =11.0s. The performance of the proposed preprocessor is evaluated with three types of attacks in closed-loop condition, which are (1) fault injection attack, (2) missing data attack, (3) noise injection attack. All these attacks were carried out in two ($\Delta P_{Line,(16-18)}$, $\Delta P_{Line,(51-45)}$) out of three power signals used as feedback signals.

1) Fault injection attack in closed loop: For performing this attack, a past fault-recording of signals $\Delta P_{Line,(16-18)}$, $\Delta P_{Line,(51-45)}$ were played back in the corresponding channels during t= 12.0s-35.0s. As per the scenario in Case-C, the original tie line flows ($\Delta P_{Line,(54-53)}$, $\Delta P_{Line,(16-18)}$) sent

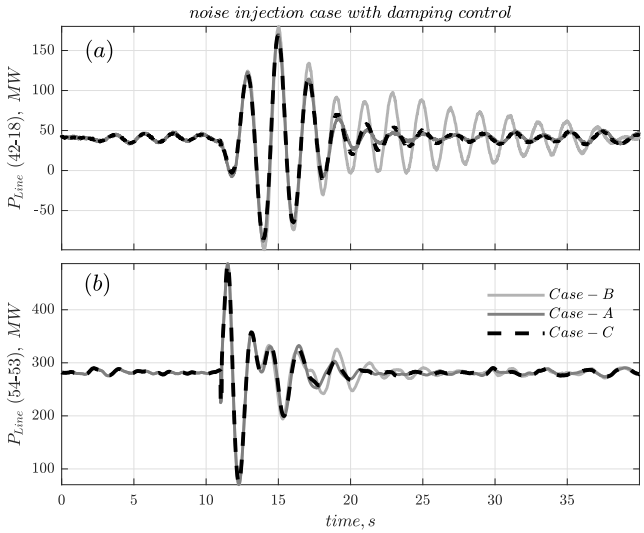

Fig. 16. Dynamic response of the system following a three-phase self-clearing fault near bus 60 at $t = 11.0$s. See Fig.11 for cases-A, B, and C.

by the PMUs, the corresponding corrupted signals after the cyberattack sent out to the control center, and the reconstructed version obtained from the proposed preprocessor are shown in Figure 12. It is evident that the algorithm is able to reconstruct the corrupted signals with reasonable accuracy.

2) Missing data attack in closed loop: A missing data attack was carried out on signals $\Delta P_{Line,(16-18)}$ and $\Delta P_{Line,(51-45)}$ during t =12.0s to 35.0s. Figures 13-14 show the true measurement of different tie-line flows ($P_{Line,(54-53)}$, $P_{Line,(42-18)}$, $P_{Line,(41-42)}$, $P_{Line,(16-18)}$) obtained from the system. Three overlapping traces in each figure represent the true response of the system collected under three different scenarios. It is evident from the dynamical response that corruption in feedback signals deteriorate the damping controller performance in absence of data pre-processor (Case-B). However, with the proposed pre-processor in the loop before controller (Case-C), damping of the power oscillations improves and closely matches that of Case-A. This demonstrates the effectiveness of the proposed pre-processor in wide-area control applications.

3) Noise injection attack in closed loop: Finally, a high bandwidth Gaussian noise was injected in the two feedback signals during t =12.0s to 35.0s. The response of the system is shown in Figs 15-16. This proves the applicability of the proposed preprocessor in wide-area damping control application.

Note that in all of the attack cases, signal $P_{Line,(16-18)}$ has more noise since bus 18 is adjacent to the line with TCSC (line connecting buses 18 and 50). The modulation/fluctuation of TCSC reactance leads to higher noise in $P_{Line,(16-18)}$.

VI. Conclusion

An architecture for preprocessing raw PMU data was presented in this work. PMU data were first processed to detect corruption, which were then reconstructed by two different RPCA methods for numerous patterns of false data injection. It was shown that the reconstruction error is lesser when the proposed l_p norm-based algorithm is used in the preprocesor. In addition, a wide-area damping controller was designed for power oscillation damping. The effectiveness of the proposed preprocessor was evaluated by feeding the attacked signals to the controller with and without the proposed preprocessor. The results showed improved damping of inter-area oscillations in presence of the preprocessor.

Appendix

The state feedback controller gain is given by K.

$K = [-1.7542, -0.8113, -0.0363, 0.5771, 0.8438, 0.1902, 0.3348, -1.9716, -0.2298, 0.0188]$

The observer gain is given by L.

$$L = \begin{bmatrix} 11.2221 & -13.5969 & 50.2235 \\ 27.8438 & -38.2569 & 130.0207 \\ -1.0989 & 2.5065 & -6.9972 \\ 34.0657 & -45.4479 & 156.6030 \\ -14.4815 & 21.0802 & -64.5802 \\ 71.2955 & 95.7564 & -343.3409 \\ 40.4554 & -56.5611 & 192.1323 \\ -15.1038 & 21.0706 & -71.2143 \\ 4.7008 & -2.7593 & 13.9350 \\ -20.1117 & 26.1138 & -93.9429 \end{bmatrix} \quad (16)$$

References

[1] H. Lin, Y. Deng, S. Shukla, J. Thorp, and L. Mili, "Cyber security impacts on all PMU state estimator-a case study on co-simulation platform GECO," in *Smart Grid Commun. (SmartGridComm), 2012 IEEE Third International Conference*. IEEE, 2012, pp. 587–592.

[2] D. P. Shepard, T. E. Humphreys, and A. A. Fansler, "Evaluation of the vulnerability of phasor measurement units to GPS spoofing attacks," *International J. of Critical Infrastructure Protect.*, vol. 5, no. 3, pp. 146–153, 2012.

[3] M. Altunay, S. Leyffer, J. T. Linderoth, and Z. Xie, "Optimal response to attacks on the open science grid," *Computer Netw.*, vol. 55, no. 1, pp. 61–73, 2011.

[4] M. Zima, M. Larsson, P. Korba, C. Rehtanz, and G. Andersson, "Design aspects for wide-area monitoring and control systems," in *Proc. of the IEEE*, vol. 93, no. 5, May 2005, pp. 980–996.

[5] A. Ashok, M. Govindarasu, and V. Ajjarapu, "Online detection of stealthy false data injection attacks in power system state estimation," *IEEE Trans. Smart Grid*, vol. 9, no. 3, pp. 1636–1646, May 2018.

[6] J. Zhao, L. Mili, and F. Milano, "Robust frequency divider for power system online monitoring and control," *IEEE Trans. Power Syst.*, vol. 33, no. 4, pp. 4414–4423, July 2018.

[7] J. Zhao and L. Mili, "Power system robust decentralized dynamic state estimation based on multiple hypothesis testing," *IEEE Trans. Power Syst.*, vol. 33, no. 4, pp. 4553–4562, July 2018.

[8] R. Deng, P. Zhuang, and H. Liang, "CCPA: Coordinated cyber-physical attacks and countermeasures in smart grid," *IEEE Trans. Smart Grid*, vol. 8, no. 5, pp. 2420–2430, Sept. 2017.

[9] G. Hug and J. A. Giampapa, "Vulnerability assessment of AC state estimation with respect to false data injection cyber-attacks," *IEEE Trans. Smart Grid*, vol. 3, no. 3, pp. 1362–1370, Sept 2012.

[10] J. Wei and G. J. Mendis, "A deep learning-based cyber-physical strategy to mitigate false data injection attack in smart grids," in *2016 Joint Workshop on Cyber- Physical Security and Resilience in Smart Grids (CPSR-SG)*, April 2016, pp. 1–6.

[11] X. Wang, D. Shi, J. Wang, Z. Yu, and Z. Wang, "Online identification and data recovery for PMU data manipulation attack," *in Early access of IEEE Trans. Smart Grid*, 2019.

[12] M. Netto and L. Mili, "Robust data filtering for estimating electromechanical modes of oscillation via the multichannel prony method," *IEEE Trans. Power Syst.*, vol. 33, no. 4, pp. 4134–4143, July 2018.

[13] S. Pal, B. Sikdar, and J. Chow, "Classification and detection of PMU data manipulation attacks using transmission line parameters," *IEEE Trans. Smart Grid*, vol. 9, no. 5, pp. 5057–5066, Sept. 2018.

[14] H. M. Khalid and J. C. H. Peng, "A Bayesian algorithm to enhance the resilience of WAMS applications against cyber attacks," *IEEE Trans. Smart Grid*, vol. 7, no. 4, pp. 2026–2037, July 2016.

[15] A. S. Musleh, H. M. Khalid, S. M. Muyeen, and A. Al-Durra, "A prediction algorithm to enhance grid resilience toward cyber attacks in WAMCS applications," *IEEE Syst. J.*, vol. 13, no. 1, pp. 710–719, March 2019.
[16] K. Mahapatra, N. R. Chaudhuri, R. G. Kavasseri, and S. M. Brahma, "Online analytical characterization of outliers in synchrophasor measurements: A singular value perturbation viewpoint," *IEEE Trans. Power Syst.*, vol. 33, no. 4, pp. 3863–3874, July 2018.
[17] P. Gao, M. Wang, J. H. Chow, M. Berger, and L. M. Seversky, "Missing data recovery for high-dimensional signals with nonlinear low-dimensional structures," *IEEE Trans. Signal Process.*, vol. 65, no. 20, pp. 5421–5436, Oct. 2015.
[18] P. Gao, M. Wang, S. G. Ghiocel, J. H. Chow, B. Fardanesh, and G. Stefopoulos, "Missing data recovery by exploiting low-dimensionality in power system synchrophasor measurements," *IEEE Trans. Power Syst.*, vol. 31, no. 2, pp. 1006–1013, March 2016.
[19] S. Zhang, Y. Hao, M. Wang, and J. H. Chow, "Multi-channel missing data recovery by exploiting the low-rank Hankel structures," in *Computational Advances in Multi-Sensor Adaptive Processing (CAMSAP), 2017 IEEE 7th International Workshop*. IEEE, 2017, pp. 1–5.
[20] P. Gao, M. Wang, J. H. Chow, S. G. Ghiocel, B. Fardanesh, G. Stefopoulos, and M. P. Razanousky, "Identification of successive "unobservable" cyber data attacks in power systems through matrix decomposition," *IEEE Trans. Signal Process.*, vol. 64, no. 21, pp. 5557–5570, Nov. 2016.
[21] K. Mahapatra and N. R. Chaudhuri, "Malicious corruption-resilient wide-area oscillation monitoring using Principal Component Pursuit," *IEEE Trans. Smart Grid*, vol. 10, no. 2, pp. 1813–1825, March 2019.
[22] J. Zhang, Z. Chu, L. Sankar, and O. Kosut, "False data injection attacks on phasor measurements that bypass low-rank decomposition," *arXiv preprint arXiv:1705.02038*, 2017.
[23] Y. Hao, M. Wang, J. H. Chow, E. Farantatos, and M. Patel, "Modelless data quality improvement of streaming synchrophasor measurements by exploiting the low-rank hankel structure," *IEEE Trans. Power Syst.*, vol. 33, no. 6, pp. 6966–6977, Nov. 2018.
[24] P. Gao, R. Wang, M. Wang, and J. H. Chow, "Low-rank matrix recovery from noisy, quantized, and erroneous measurements," *IEEE Trans. Signal Process.*, vol. 66, no. 11, pp. 2918–2932, June 2018.
[25] K. Mahapatra and N. R. Chaudhuri, "Malicious corruption-resilient wide-area oscillation monitoring using online robust PCA," in *Proc. IEEE Power & Energy Society General Meeting, 2018.*
[26] K. Mahapatra and N. R. Chaudhuri, "Online robust PCA for malicious attack-resilience in wide-area mode metering application," *in Early access of IEEE Trans. Power Syst.*, 2019.
[27] J. Zhao, L. Mili, and M. Wang, "A generalized false data injection attacks against power system nonlinear state estimator and countermeasures," *IEEE Trans. Power Syst.*, vol. 33, no. 5, pp. 4868–4877, Sept 2018.
[28] J. Zhao and L. Mili, "A framework for robust hybrid state estimation with unknown measurement noise statistics," *IEEE Trans. Ind. Informat.*, vol. 14, no. 5, pp. 1866–1875, May 2018.
[29] J. Zhao, S. Wang, L. Mili, B. Amidan, R. Huang, and Z. Huang, "A robust state estimation framework considering measurement correlations and imperfect synchronization," *IEEE Trans. Power Syst.*, vol. 33, no. 4, pp. 4604–4613, July 2018.
[30] R. Tibshirani, "Regression shrinkage and selection via the LASSO," *Journal of the Royal Statistical Society. Series B (Methodological)*, pp. 267–288, 1996.
[31] E. J. Candès and M. B. Wakin, "An introduction to compressive sampling," *IEEE Signal Process. Mag.*, vol. 25, no. 2, pp. 21–30, 2008.
[32] H. Guo, C. Qiu, and N. Vaswani, "An online algorithm for separating sparse and low-dimensional signal sequences from their sum," *IEEE Trans. Signal Process.*, vol. 62, no. 16, pp. 4284–4297, Aug. 2014.
[33] T. Bouwmans, N. S. Aybat, and E.-h. Zahzah, *Handbook of robust low-rank and sparse matrix decomposition: Applications in image and video processing*. CRC Press, 2016.
[34] G. V. Tim Roughgarden, "CS168: The modern algorithmic toolbox, lecture-9." [Online]. Available: http://theory.stanford.edu/ tim/s15/l/l9.pdf
[35] B. K. Natarajan, "Sparse approximate solutions to linear systems," *SIAM journal on computing*, vol. 24, no. 2, pp. 227–234, 1995.
[36] R. Chartrand, "Exact reconstruction of sparse signals via nonconvex minimization," *IEEE Signal Process. Lett.*, vol. 14, no. 10, pp. 707–710, 2007.
[37] Y. Y. Ge Dongdong, Jiang Xiaoye, "A note on the complexity of Lp minimization," *Mathematical Programming*, vol. 129, no. 2, pp. 285–299, Oct. 2011.
[38] B. Pal and B. Chaudhuri, *Robust control in power systems*, ser. Power Electronics and Power Systems. New York: Springer, 2005.
[39] A. Yogarathinam and N. R. Chaudhuri, "Wide-area damping control using multiple DFIG-based wind farms under stochastic data packet dropouts," *IEEE Trans. Smart Grid*, vol. 9, no. 4, pp. 3383–3393, July 2018.

Kaveri Mahapatra (S'16) received the M. Tech. degree from Siksha 'O' Anusandhan University, India in 2013. She is currently pursuing her Ph.D. degree in the School of Electrical Engineering and Computer Science at the Pennsylvania State University, USA. Her current research interests include wide-area monitoring, protection and control, cybersecurity, soft computing and optimization, and power system dynamics.

Mahmoud Ashour received the B.Sc. and M.Sc. degrees in electrical engineering from Cairo University and Nile University, Egypt, in 2010 and 2013, respectively. He was a research assistant with the Computer Science and Engineering Department, Qatar University, Qatar, for one year in 2014. He is currently pursuing the Ph.D. degree in the Electrical Engineering and Computer Science Department, Penn State University, University Park, PA, USA. His research interests lie in the broad area of communication networks with an emphasis on distributed optimization algorithms.

Nilanjan Ray Chaudhuri (S'08-M'09-SM'16) received his Ph.D. degree from Imperial College London, London, UK in 2011 in Power Systems. From 2005-2007, he worked in General Electric (GE) John F. Welch Technology Center. He came back to GE and worked in GE Global Research Center, NY, USA as a Lead Engineer during 2011-2014. Presently, he is an Assistant Professor with the School of Electrical Engineering and Computer Science at Penn State, University Park, PA. He was an Assistant Professor with North Dakota State University, Fargo, ND, USA during 2014-2016. He is a member of the *IEEE* and *IEEE PES*. Dr. Ray Chaudhuri is the lead author of the book *Multi-terminal Direct Current Grids: Modeling, Analysis, and Control* (Wiley/IEEE Press, 2014), and an Associate Editor of the IEEE TRANSACTIONS ON POWER DELIVERY. Dr. Ray Chaudhuri is the recipient of the National Science Foundation Early Faculty CAREER Award in 2016.

Constantino M. Lagoa received the B.S. and M.S. degrees from the Instituto Superior Tecnico, Techical University of Lisbon, Portugal in 1991 and 1994, respectively, and the Ph.D. degree from the University of Wisconsin at Madison in 1998. He joined the Electrical Engineering Department of Pennsylvania State University, University Park, PA, in August 1998, where he currently holds the position of Professor. He has a wide range of research interests including robust optimization and control, chance constrained optimization, controller design under risk specifications, system identification and control of computer networks. Dr. Lagoa has served as Associate Editor of IEEE Transactions on Automatic Control (2012-2017) and IEEE Transactions on Control systems Technology (2009-2013) and he is currently Associate Editor of Automatica.