Online Robust PCA for Malicious Attack-Resilience in Wide-Area Mode Metering Application

Kaveri Mahapatra, *Student Member, IEEE*, and Nilanjan Ray Chaudhuri, *Senior Member, IEEE*

***Abstract*—This paper presents a method for detecting and correcting malicious data corruptions in PMU measurements. Detection of malicious injections is formulated as a compressed sensing problem and the actual signals are recovered using an online robust principal component analysis (PCA)-based algorithm. Different patterns of malicious injection attacks on PMU data are considered and the effect of corruption and reconstruction using the algorithm is analyzed on wide-area mode metering application. The performance of the proposed algorithm has been evaluated with different subspace selection. A suitable threshold for the algorithm is selected by a graphical analysis of the receiver operating characteristics curve. Data from a 16-machine, 5-area New England-New York system is used along with a recursive modal estimation algorithm to validate the effectiveness of the proposed approach under ambient and transient conditions.**

***Index Terms*—PMU, Compressed sensing, Cybersecurity, Sparse optimization, Oscillation monitoring, Robust PCA**

I. Introduction

The power grid is becoming increasingly vulnerable to cyber-attacks due to its ever growing dependence on the wide area measurement systems (WAMS) integrated with advanced sensors such as Phasor Measurement Units (PMUs). As pointed out in [1], in spite of a dedicated Intranet-based communication network in NASPInet architecture, it is not immune to cyber-attacks. Also PMUs use civilian GPS signals, which are prone 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 in some signals. Propagation of these corrupted information [3] can affect WAMS-based applications [4] and lead to inappropriate control decisions causing instability to the network.

WAMS applications can be divided into two categories. 1. applications requiring full observability of the network — e.g. voltage stability assessment of meshed networks. 2. applications not requiring full network observability — e.g. oscillation monitoring and stability assessment. The first type of application requires the so called 'dynamic' state estimation, which estimates system voltages and angles using PMU measurements. In contrast 'dynamic state' estimation, which estimates generators' dynamic states like speed, power angle, etc. from PMU measurements at generator terminals, falls under the second type of application.

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

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

In this work, our focus is on mode metering application using PMU data, which also falls under the second category. Mode meters are already operational in control centers of many utilities including California ISO, PG&E, BPA [5], and TVA [6], and a corresponding web-based version has been deployed in 7 operations centers and 11 reliability coordinators in the Eastern Interconnection [5] for quite some time.

Literature on false data injection (FDI) originated by cyber-attacks in PMU dynamic data samples includes a common path algorithm [7], a hybrid intrusion detection system [8], and a Bayesian-based approximation filter proposed in [9]. Effect of bad data or cyber intrusion detection in state estimation has been rigorously studied in most of the past works [9]–[21].

Reference [12] proposed a solution for FDI, which can detect corruptions in SCADA measurements used for 'dynamic state' estimation utilizing a secure set of PMU measurements. A similar work on detection of FDI attacks on state estimation with the use of a secure set of PMUs has been reported in [13]. Marcos-et-al [14] have presented an iteratively reweighted phase-phase correlator to detect randomly occuring outliers at different instances in different PMU signals by exploiting robust Mahalanobis distance. Leveraging the same metric, reference [15] utilizes network model and correlation between PMU and SCADA signals to detect multiple isolated bad data outliers. Reference [22] proposes a classification method for distinguishing between disturbance outliers and multiple bad data outliers with Principal Component Analysis (PCA) features. A robust generalized maximum-likelihood estimator based on projection statistics is proposed in [16] for handling multiple interacting and conforming (but isolated in time) bad data outliers in SCADA and PMU measurements. However, the effect of 'continuous' injection of correlated corruption attacks on multiple signals, which can increase the bias error during the estimation over time has not been studied.

Reference [17] 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 FDI-based cyberattacks. A projection statistics-based outlier detection technique with multiple hypothesis tests in [18] has been presented 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.

As mentioned earlier, in this paper our focus is on the mode-metering application, which requires PMUs to be placed on major tie-line buses for monitoring critical modes of the system. However, this type of PMU placement does not ensure

complete network observability, which is critical for PMU-enabled state estimation. To the best of our knowledge, due to this reason PMU-enabled state estimators are yet to be integrated with the WAMS-based mode metering application. Therefore, most of the detection techniques specific to state estimation are not applicable here.

In literature, a Baysian-based Approximated Filter (BAF) was first proposed in [9] to extract modal damping and frequencies from corrupted data. Reference [19] proposed a Kalman-like particle filter for random uncorrelated FDI attacks such as fault injection and data repetition attacks. Reference [20], [21] proposed a heuristics, which depends on continuous monitoring or tracking of the transmission line parameters along with setting of different hyper-parameters for detection of only step or ramp manipulation attacks. However, the heuristics need to be updated every time network configuration changes.

In [22], 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 [23]–[25] also exploit lower dimensionality of PMU data for reconstruction of missing samples. In such cases, reconstruction of samples are very accurate since the identity of the corrupted samples are known a-priori. A simple least squares (LS) solution can provide accurate estimates for the missing samples in this case. However, in 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 reconstruction of those samples. In such cases, matrix-based block processing algorithms [26]–[30] or vector processing algorithms [31] can be used. References [26], [28] have presented matrix decomposition problem for detecting successive cyberattacks with the assumption of placement of PMUs for a completely observable network. The adversary having access to full system topology information was assumed in reference [28] to design unobservable attacks in a completely observable network. Recently, a method has been proposed in [29], which exploits the low-rank property of the Hankel structure to identify and correct random bad data outliers. The algorithm can estimate samples in all the channels at any instant during simultaneous data losses due to communication congestion. Although this method works very well in presence of large magnitude bad data outliers and simultaneous missing data, 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. With increasing number of PMUs, the number of hyper-parameters increases and this process can become challenging.

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 [27]. Although this is a model-free approach, when used in a moving-window framework, it produces redundant estimates for past samples in the current window. The block processing algorithms give reasonably fast solution, but the algorithm or application has to wait until the data window gets filled in.

Our main objective here is online detection of malicious injections in measurements and their accurate reconstruction for the purpose of real-time modal estimation. 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 [32]–[34] problem. Unlike PCP, 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 cyber-attack or otherwise and reconstructs the data vector at the corrupted positions using an appropriate subspace for wide-area mode metering applications. Building on our latest work in [31], the proposed algorithm selects an appropriate subspace from a library of subspaces generated from offline simulations of different operating conditions. The effectiveness of the proposed approach is demonstrated when different types of carefully designed cyber-attacks [9] corrupt PMU data during ambient and transient conditions. In addition, the effect of the proximity of different subspaces to the subspace representing current operating condition on the reconstruction of data and corresponding modal estimation are presented. We show that a measure of this proximity is the angle between these subspaces, which gets reflected in the reconstruction error. A comparison with the PCP-based method [27] and the method from [29] reveals the effectiveness of the proposed approach.

This paper is divided into five sections. Section II presents the proposed architecture for malicious corruption-resilient wide-area mode metering 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. The reconstructed data samples are then used by a simple Recursive Least Squares (RLS)-based algorithm [35] to estimate the modal damping ratios and frequencies. The test results considering different types of corruption attacks on signals during nominal and off-nominal operating conditions are demonstrated in Section IV. The performance of the algorithm with different subspaces is evaluated by their ability to reconstruct and to estimate the modal frequency and damping ratios. Section V concludes the paper.

II. Proposed Architecture

An architecture for malicious corruption-resilient wide-area mode metering 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. There are two inputs to the proposed data pre-processor. The first input is the vector of PMU measurements coming from PDC and second input is coming from the library of subspaces. The pre-processor detects corruption in PMU measurements by solving a sparse recovery problem with the use of a robust PCA-based convex optimization algorithm. The data vector is then reconstructed with minimum mean square error (MSE) by least squares (LS) estimation using a subspace selected from a library of low-rank subspaces derived from

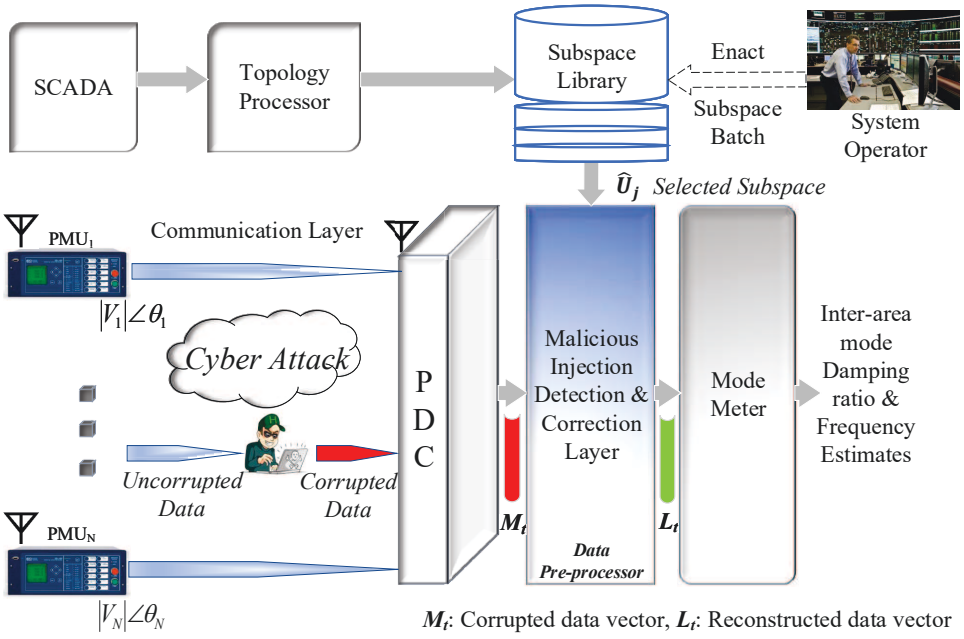

Figure 1. Proposed architecture for online malicious corruption-resilient wide-area mode metering application.

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 based on the current operating condition. 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 – 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.

The effect of these attacks on the estimations of the frequency and damping ratio of inter-area modes is presented. For example, the damping ratio estimates can appear to be higher or lower than the actual values, which can potentially misinform the operators' decision making.

We would like to emphasize that these are intelligent cyberattacks. Someone who has access to PMU signals used for interarea oscillation monitoring can launch false data injection (FDI) attacks. An intelligent attacker would device ways to inject bad data whose magnitude does not exceed 3-sigma rule and thus gets undetected by most of the algorithms. Moreover, we have injected correlated corruption into the compromised signals instead of choosing random corruption at any instant on any signal. Attackers without any domain-knowledge might attempt step or ramp attacks which are much easier to detect with the proposed method as compared to these intelligent attacks.

We consider the performance of the data pre-processing algorithm with change in operating condition. This is demonstrated by testing different subspaces for reconstruction of data. We have shown that the angle between subspaces representing the current operating point and another operating point can be qualitatively related to the MSE of data reconstruction.

III. Problem Formulation

The goal of the data pre-processor block is to identify the corrupted signals among a set of signals and quantify the amount of corruption present at any sampling instant by using an efficient convex optimization algorithm.

Let the measurements coming from PMUs include time-stamped samples of n_1 different voltage phasors which includes two types of signals: voltage magnitudes, angles. At any instant these samples can be represented by a vector M_t of voltage magnitudes $(n_1 \times 1)$ or angles $(n_1 \times 1)$. Since we are interested in observing interarea oscillation modes, the PMUs are assumed to be placed on the major inter-tie buses and corresponding number of signals of either voltage magnitudes or angles is n_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 our proposed model. 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 model 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 subspace $\mathbb{R}^{n_1}$ of uncorrupted past measurements (Fig. 1). When the vector of signal samples obtained M_t is uncorrupted, S_t is 100% sparse

($||S_t||_0 = 0$), which means no corruption is present in the samples, i.e. $M_t = L_t$. When 20% of the signals are corrupted at any instant, S_t is 80% sparse ($\|S_t\|_0$= multiple of 2), which implies 20% of samples in the vector are corrupted. Therefore, the degree of sparsity in S_t will depend on how much corruption is present.

In other words, this is a problem of recovering a sparse corruption S_t in signal samples M_t at any instant. In literature [36], this is presented as an online robust principal component analysis (RPCA) problem. Conventional PCA is more sensitive to outliers whereas RPCA can efficiently compute Principal Components (PCs) in presence of outliers.

In this work, a modified version of the recursive projected compressed sensing (ReProCS) [34] method-based algorithm is proposed to solve the above problem. As shown in the Fig. 1, the algorithm takes the incoming new data vector M_t of one sample from each signal at an instant t as an input vector. In this work, we process voltage magnitude vector of dimension $n_1 \times 1$ separately from the voltage angle vector. The knowledge of current operating condition of the network is utilized by the algorithm to select an appropriate set of basis vectors $\hat{U}$ representing current subspace from a library, see Fig. 1. At every time step t, both L_t and S_t estimated by the algorithm are such that $\hat{L}_t$ lies in the subspace spanned by $\hat{U}$ and $\hat{S}_t$ represents the corruptions added to $\hat{L}_t$ to form M_t.

■ *Preparation of the Library of Subspaces:* The algorithm, for detection of corruption in current operating condition, takes input $\hat{U}$ from a library of subspaces formed using offline planning simulation data. Since PMU measures voltage magnitude, angles, and frequencies, which are three type of signals, three different subspaces are extracted for each type of signals for any operating condition. Therefore, the proposed algorithm will be running in parallel on each type of signals separately utilizing corresponding subspaces. We propose that a self-clearing fault with a particular network configuration should be created for generating training data at each operating point through offline simulation, which captures the dynamic behavior of the system around that operating point. This transient data is rich in information about the electromechanical modes, which are supposed to be estimated through wide-area monitoring. Therefore, 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 de-trending of samples.

The following considerations determine the choice of window size n_2 of the data-(a) The starting point is chosen from an instant following the first half cycle after the fault clearing in order to avoid the nonlinearities associated with the fault. (b) The end-point of the window is selected based on the settling time of the low frequency electromechanical oscillations. ■

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 spanned by U is formed by applying the singular value decomposition (SVD).

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

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 spanned by the basis vectors in 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 [37]. This process takes basis vectors corresponding to a certain number r_{approx} of higher singular vectors to form the approximate basis $\hat{U} = \left[u_1, \ldots, u_{r_{approx}}\right]$. $\hat{U}$ is then considered as the basis matrix representing the subspace for a particular operating condition and is stored in the library.

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

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

where, $\Phi_t = I - \hat{U}\hat{U}'$ and 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 [34]. 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.

$$\min_{x_t} \|x_t\|_0 \, s.t. \, \|y_t - \Phi_t x_t\|_2 \leq \xi_t \tag{4}$$

where, $\xi_t = \|\beta_t\|_2$ is unknown in advance since true $\beta_t = \Phi_t L_t$. Therefore, ξ_t is calculated from $\hat{\beta}_t$, which is taken as $\Phi_t L_{t-1}$. The solution vector $x_t = \hat{S}_t^x$ of size $(n_1 \times 1)$ to the above minimization problem is the correct estimate of the sparse vector S_t.

To overcome the nonconvexity of the objective, a convex relaxation of the above is utilized, which leads to a compressed sensing/sparse recovery problem [32]–[34] called the "least absolute shrinkage and selection operator (LASSO)." This tries to recover the sparse S_t from y_t. The problem can now be formulated as follows.

$$\min_{x_t} \|x_t\|_1 \, s.t. \, \|y_t - \Phi_t x_t\|_2 \leq \xi_t \tag{5}$$

The solution to the above problem is achieved with any efficient l_1 solver as long as the corruption support size is less than 20% of the total number of signals. We used 'CVX', a package for specifying and solving convex programs [38], [39], for solving this optimization problem.

The estimated corrupted positions or the estimated support of $\hat{S}_t$ can be determined by thresholding $\hat{S}_t^x$ by a small positive number ω. Thresholding is performed to delete the extra elements in the solution vector $\hat{S}_t^x$, which in turn eliminates the false positives. General practice is to use ω proportional to the energy of the signal where $\omega = \sqrt{\|L_t\|_2^2 / n_1}$ and in case of $\|S_t\|_2 \ll \|L_t\|_2$, ω is a fraction of $\sqrt{\|L_t\|_2^2 / n_1}$, $\omega = q\sqrt{\|L_t\|_2^2 / n_1}$ [34].

The estimate $\hat{S}_t$ can be obtained on this determined support using least squares (LS) method. This estimate $\hat{S}_t$ is used to find the estimate $\hat{L}_t$ = M_t - $\hat{S}_t$. By recovering S_t correctly, an

accurate estimate of L_t can be recovered from M_t. We will refer to $\hat{L}_t$ as '***reconstructed data***'.

A. Proposed Algorithm

We present a modified version of the algorithm proposed in [34] to suite the problem of detecting corruptions in PMU measurements. The following describes the procedure derived from [34] 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.

Input: M_t, $\hat{U}_t$; **Output**: $\hat{T}_t$, $\hat{S}_t$, $\hat{L}_t$; **Parameters**: q;
Initialization

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

While $t \geq t_0$

1) Choose basis matrix $\hat{U}_t$ from the library such that it closely represents the present condition. (See the remark below on control room implementation)
2) Orthogonal projection: Compute $y_t = \Phi_t M_t$ where $\Phi_t \leftarrow (I\text{-}\hat{U}_t\hat{U}_t')$.
3) Compute $\xi_t = \|\beta_t\|_2$ where $\beta_t \leftarrow \Phi_t M_t$ for $t = 0$ and $\beta_t \leftarrow \Phi_t L_{t-1}$ for $t \geq 0$.
4) Compute $\hat{S}_t^x$ as a solution to equation (5) using l_1 solver from 'CVX'.
5) Calculate $\omega = q\sqrt{\|M_t\|_2^2 / n_1}$ for $t = 0$ for the first sample and $\omega = q\sqrt{\|L_{t-1}\|_2^2 / n_1}$ for $t \geq 0$.
6) Compute the support set $\hat{T}_t$ by thresholding $\hat{S}_t^x$ where $\hat{T}_t = \left\{i : \left|\hat{S}_t^x(i)\right| \geq \omega\right\}$ and $\hat{T}_t^c = \left\{i : \left|\hat{S}_t^x(i)\right| < \omega\right\}$.
7) Compute $\hat{S}_t \leftarrow LS(y_t, \Phi_t, \hat{T}_t)$ where $H \leftarrow LS(y, A, \Psi)$ means that $H_\Psi = (A_\Psi' A_\Psi)^{-1} A_\Psi' y$ and $H_{\Psi^c} = \bar{0}$. Here A_Ψ denotes a submatrix of matrix A containing the columns with indices in the set Ψ.
8) Estimate $\hat{L}_t \leftarrow M_t - \hat{S}_t$.
9) Increment t by sampling time duration and go to step 1.

■ *Remark on Assumptions:* Since higher sparsity in S_t leads to more efficient correction, our assumption is that the attackers do not have access to all the PMUs. As will be shown from empirical results in Section IV C, our algorithm can detect corruption with reasonable accuracy when upto 30% of signals are attacked simultaneously. However, it is more efficient when 20% of the signals are corrupted simultaneously. Therefore, we assume that the attacker has access to no more than 20% of PMU signals.

■ *Remark on Implementation in Control Center:* Figure 1 shows the practical implementation of the proposed approach in Control Center. As described before, the library of subspaces is generated from the offline (planning) simulation. The simulations are conducted under typical loading conditions taking into account the daily and seasonal variations. Under each condition the (N-1) contingency scenarios are simulated for which individual subspaces represented by $\hat{U}$ will be calculated and stored. As the day progresses, the operators will enact appropriate batches of subspaces. From such a batch of subspaces, an appropriate $\hat{U}$ is chosen using the input from the Topology Processor - see Fig. 1. Experience of system planners is invaluable in generating an exhaustive library of subspaces. As a new time-aligned vector of PMU data samples from PDC appear, this vector is passed through a data preprocessor containing the RPCA algorithm. Here, the new measurement vector M_t is projected into a subspace, which is orthogonal to the low-rank signal subspace represented by $\hat{U}$ and subsequent steps described in the algorithm above are executed. At the output, the reconstructed measurement vector is obtained, which is used by the mode meter - see Fig. 1.

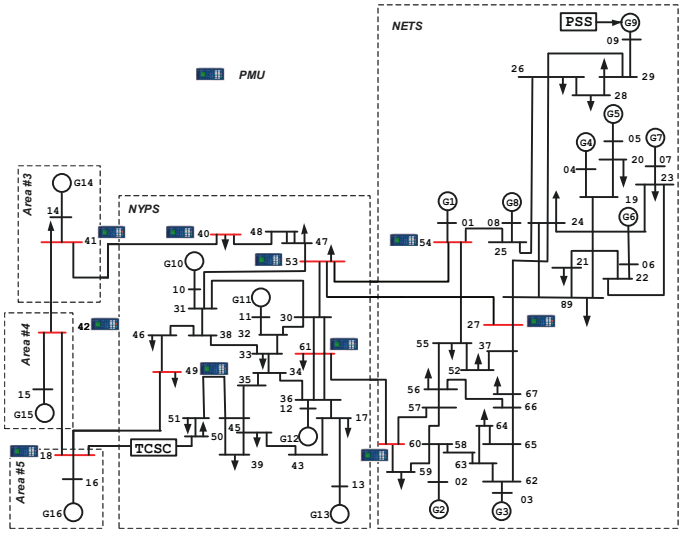

Figure 2. Single-line diagram of 16-machine, 5-area New England-New York system with PMUs installed at major inter-tie buses highlighted in red.

B. Modal Estimation

As shown in Fig. 1, the reconstructed data $\hat{L}_t$ is used by the mode meter. Different algorithms can be used for modal estimation [5], [6]. In this work, we have applied a variable forgetting factor-based Recursive Least Squares (RLS) algorithm [35], which is well-known and is not repeated here.

IV. 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 [40] 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. Ten voltage magnitudes and angle measurements (i.e. 20 signals) are considered as two separate data sets and de-trending was performed on all signals. In our case studies, any two signals out of 10 (either 10 voltage magnitudes and/or 10 voltage angles) is assumed to be corrupted at a particular instant. The threshold parameter q used by the algorithm can be chosen as a small positive number. Unless otherwise stated, all simulation results use $q = 0.1$. Only the corrupted sample is recovered at each instant through LS estimation, see step (7) in the proposed algorithm. The reconstructed samples $\hat{L}_t$ at any instant are utilized by an RLS-based mode metering algorithm.

The first 4 (r_{approx}= 4) left singular vectors corresponding to higher singular values are retained as basis vectors to form the basis matrix $\hat{U}$ which span the subspace at different operating points, which build the subspace library. In this work, we have used a window of 40 seconds, which results in

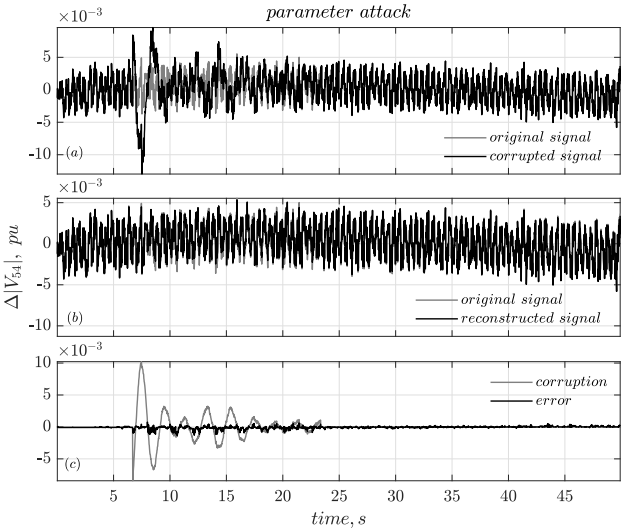

Figure 3. Case I: Parameter manipulation attack in signal $|V_{54}|$ under ambient condition. Corruption: difference between original and corrupted signal, Error: difference between original and reconstructed signal.

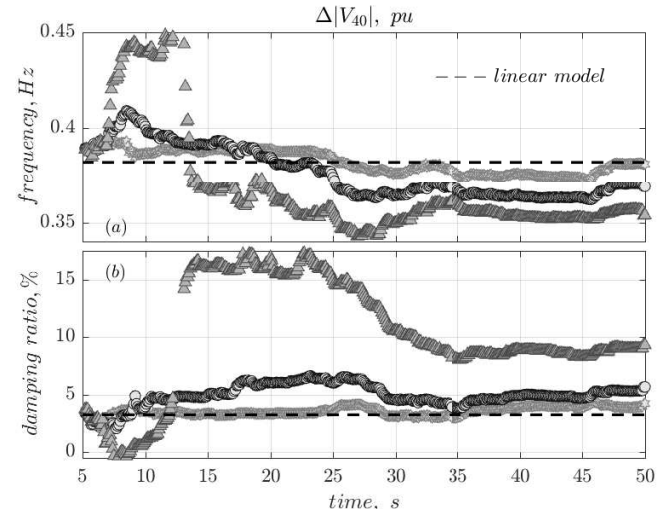

Figure 4. Case I: Estimated frequency and damping ratio from corrupted **(dark grey 'Δ')** signal is misleading. Reconstruction **(black 'o')** produces reasonable accuracy as compared to original **(light grey '$*$')**.

$n_2 = 2394$ samples for calculating the basis vectors U of the orthonormal subspace for any network configuration.

A. Test Under Nominal Operating Condition

In this case, corruption attacks are performed during ambient state under nominal condition $(Op-1)$ and transient state following a self-clearing fault. We assume that a basis matrix $\hat{U}_1$ based on the transient data following a self-clearing fault near bus 53 is available based on offline simulations.

1) Ambient Condition: To simulate the ambient condition, band-limited zero-mean Gaussian noise was injected in load terminals of the test system. All the attacks during ambient state of the network were performed on four signals, which are $\angle V_{40}$, $\angle V_{54}$, $|V_{40}|$, and $|V_{54}|$.

■ *Case I: Parameter Manipulation Attack:* Figure 3 shows the parameter manipulation attack in signal $|V_{54}|$ for 1000 samples. Unless otherwise stated, only deviation in the signals from nominal values are shown. The attack model uses the

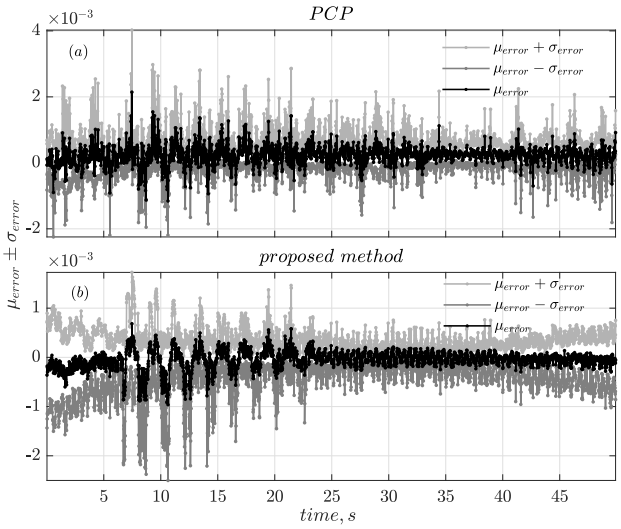

Figure 5. Case I: Mean error (μ_{error}) $\pm$ Standard deviation of the error (σ_{error}) obtained during reconstruction of $|V|$ signals with (a) PCP [27] and the (b) proposed method. The plots of $\mu_{error}+\sigma_{error}$ and $\mu_{error}-\sigma_{error}$ show statistical dispersion of reconstruction error obtained over 50 seconds.

weighted sum of three damped sinusoids with frequencies equal to 0.382Hz, 0.55Hz, and 0.618Hz. The damping ratios are chosen to be 8.0%, 4.4%, and 5.7%, respectively. Figure 3 also compares the degree of malicious injection in the signal and the quality of reconstruction. These are measured by the difference between the original and the corrupted signal denoted by 'corruption,' and the difference between original and reconstructed signal denoted by 'error.' The error is close to zero, which shows a good quality of reconstruction.

Figure 4 shows the estimated frequencies and damping ratios of an inter-area mode obtained from (i) linear model of the network at the current operating point **(dash)**, (ii) original signal **(light grey '$*$')**, (iii) corrupted signal **(dark grey 'Δ')**, and (iv) reconstructed signal **(black 'o')**. These also show that a small window of corrupted data (Fig. 3(a)) can jeopardize the estimates **('Δ')** of frequency and damping ratio as compared to the linear model, original and reconstructed signals, and give out misleading information. The estimates obtained from reconstructed signal closely follows that of original.

The efficiency of the proposed algorithm with Principal Component Pursuit (PCP) [27] has been compared for the reconstruction of the compromised set of PMU signals. PCP has been selected for comparison since it represents an existing low-rank matrix decomposition method based on principal component analysis. Different statistical measures such as mean error (μ_{error}), standard deviation of the error (σ_{error}), $\mu_{error} \pm \sigma_{error}$ at each instant are calculated during reconstruction of all $|V|$ signals. Figure 5 shows the statistical dispersion of reconstruction error with (a) PCP and (b) proposed method. The plots indicate higher dispersion of error with PCP as compared to the proposed method.

Similarly, statistical measures such as average mean square error (AMSE), average standard deviation, and maximum mean square error (MMSE) over the reconstruction interval are calculated and presented in Table I. These statistics indicate better performance of the proposed algorithm as compared to

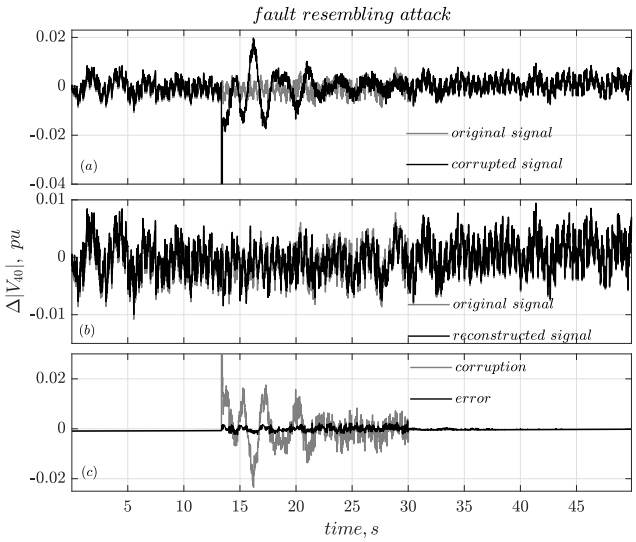

Figure 6. Case II: Fault-resembling injection attack in signal $|V_{40}|$ under ambient condition. Corruption: difference between original and corrupted signal, Error: difference between original and reconstructed signal.

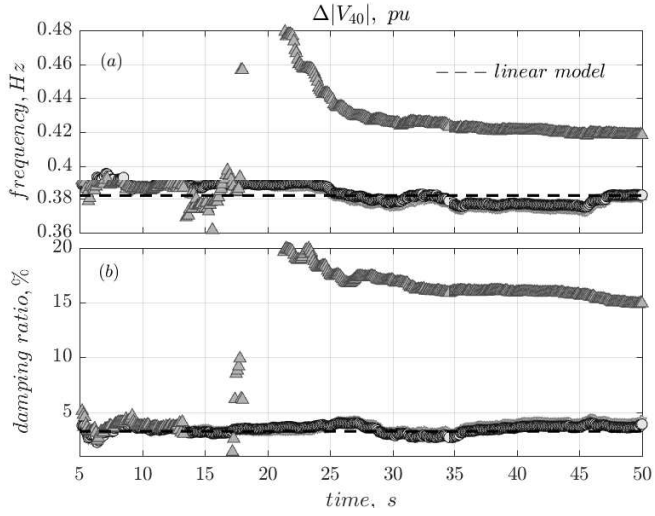

Figure 7. Case II: Estimated frequency and damping ratio from corrupted **(dark grey 'Δ')** signal is misleading. Reconstruction **(black 'o')** produces reasonable accuracy as compared to original **(light grey '$*$')**.

PCP. The reason behind this is the following. Any low-rank matrix decomposition algorithm corrects the compromised signals as well as the uncompromised signals over an interval. However, the proposed algorithm first detects the compromised signals at any instant and then corrects only those signals through LS estimation.

Table I
CASE I: COMPARISON OF RECONSTRUCTION ERRORS BETWEEN PCP [27] AND PROPOSED ALGORITHM

Parameter Attack	Average MSE	Standard deviation	Maximum MSE
PCP	3.5557e-07	4.6526e-04	2.6383e-05
Proposed method	2.4833e-07	4.2343e-04	1.3918e-05

■ *Case II: Fault-Resembling Injection Attack:* In this case, the attacker is assumed to inject a portion of archived transient data following a three-phase self-clearing fault near bus 53 into the considered signals during ambient state. Due to space restrictions, only signal $\Delta|V_{40}|$ is shown in Fig. 6. The quality of reconstruction is very good and is reflected in the estimated

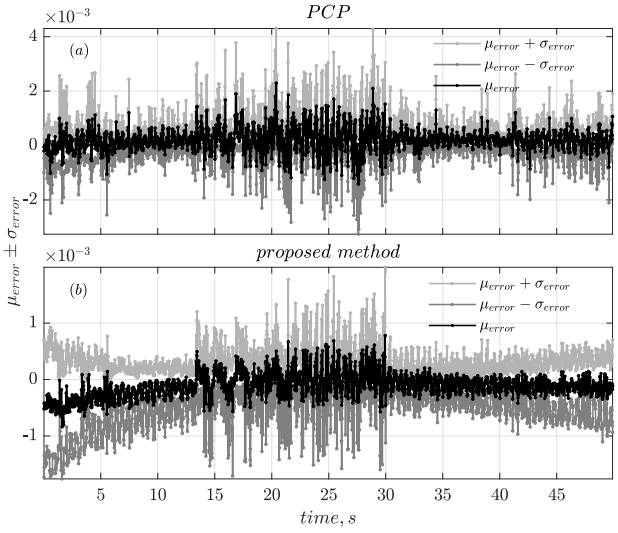

Figure 8. Case II: Mean error (μ_{error}) $\pm$ Standard deviation of the error (σ_{error}) obtained during reconstruction of $|V|$ signals with (a) PCP [27] and the (b) proposed method. The plots of $\mu_{error}+\sigma_{error}$ and $\mu_{error}-\sigma_{error}$ show statistical dispersion of reconstruction error obtained over 50 seconds.

frequency and damping ratio in Fig. 7. Due to transient signal injection, a large deviation is witnessed in all estimates obtained from the corrupted signal.

Statistical dispersion of reconstruction error obtained from the proposed method has been compared with PCP in Fig. 8, which leads to similar conclusion as before. Statistical measures over the whole interval are calculated in Table II, which show better performance of the proposed algorithm.

Table II
CASE II: COMPARISON OF RECONSTRUCTION ERRORS BETWEEN PCP [27] AND PROPOSED ALGORITHM

Fault Injection Attack	Average MSE	Standard deviation	Maximum MSE
PCP	5.2163e-07	5.5586e-04	4.6135e-05
Proposed method	2.5602e-07	4.3006e-04	1.4898e-05

2) Transient Condition: A self-clearing three-phase fault near bus 53 is considered. The first half-cycle of oscillatory data immediately after fault is disregarded in our analysis to avoid the effect of higher nonlinearity on the modal estimates. This is acceptable since the accuracy of most of the mode-metering algorithms is poor in this region. All the attacks during transient state of the network were performed on four signals, which are $\angle V_{54}$, $\angle V_{60}$, $|V_{54}|$, and $|V_{60}|$.

■ *Case III: Missing Data Attack:* The effectiveness of the proposed pre-processor in data reconstruction is shown in Fig. 9. The error in the reconstructed signal is higher at the beginning of the window, but is acceptable for most of the time span.

■ *Case IV: Data Repetition Attack:* In this case, a window of ambient and transient data samples archived for those 4 signals is repeated in 4 signals. One of those is shown in Fig. 11, which resembles a consecutive fault in the system. The original and the reconstructed signals are very similar. Modal estimation of Case III and IV are not shown due to space restrictions.

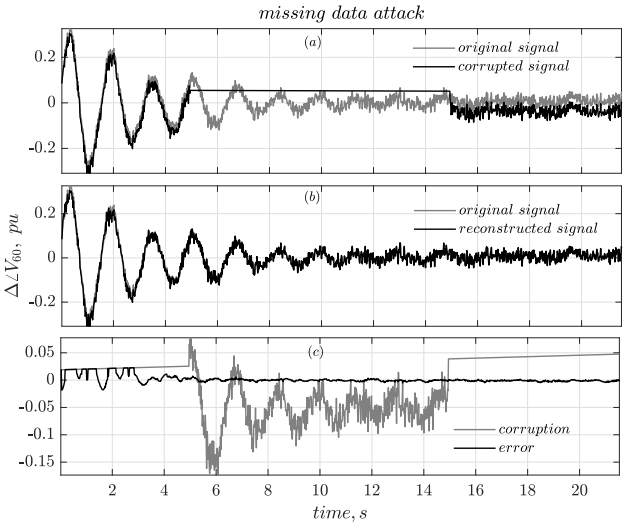

Figure 9. Case III: Missing data attack in signal $\angle V_{60}$ under transient condition. Corruption: difference between original and corrupted signal, Error: difference between original and reconstructed signal.

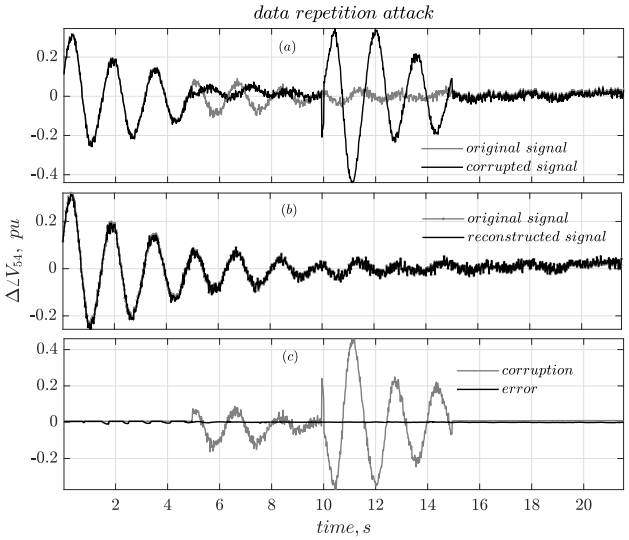

Figure 11. Case IV: Data repetition attack in signal $\angle V_{54}$ under transient condition. Corruption: difference between original and corrupted signal, Error: difference between original and reconstructed signal.

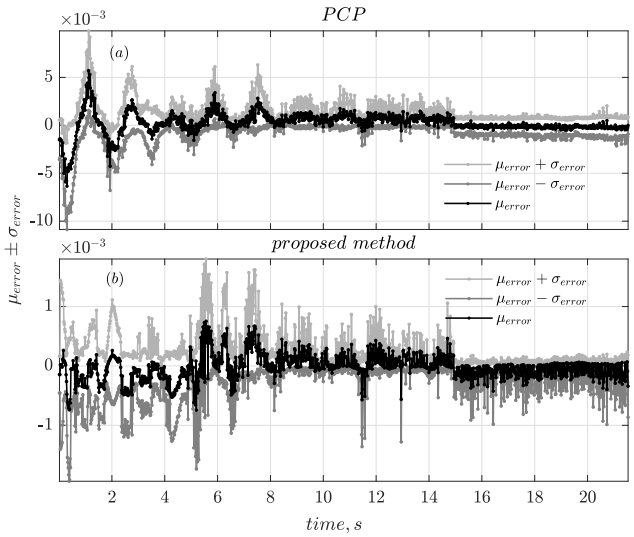

Figure 10. Case III: Mean error (μ_{error}) $\pm$ Standard deviation of the error (σ_{error}) obtained during reconstruction of $|V|$ signals with (a) PCP [27] and the (b) proposed method. The plots of $\mu_{error}+\sigma_{error}$ and $\mu_{error}-\sigma_{error}$ show statistical dispersion of reconstruction error obtained over 21 seconds.

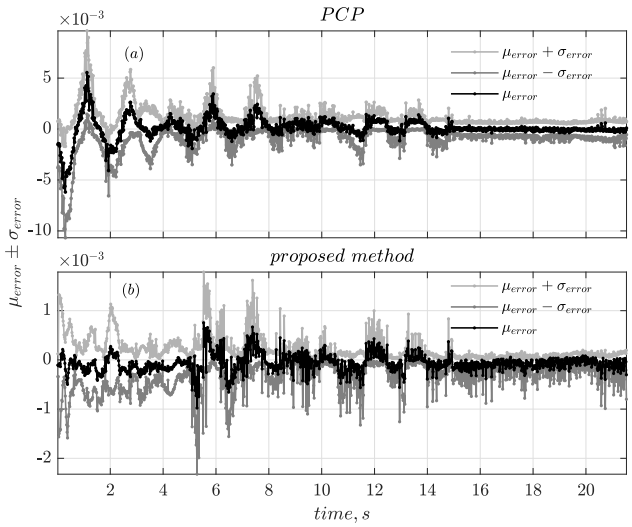

Figure 12. Case IV: Mean error (μ_{error}) $\pm$ Standard deviation of the error (σ_{error}) obtained during reconstruction of $|V|$ signals with (a) PCP [27] and the (b) proposed method. The plots of $\mu_{error}+\sigma_{error}$ and $\mu_{error}-\sigma_{error}$ show statistical dispersion of reconstruction error obtained over 21 seconds.

Similar to the ambient case studies, the proposed approach was compared with PCP for Case III and IV. A comparison of different statistical measures of reconstruction errors in Tables III and IV clearly shows superiority of the proposed method. Also, temporal variation of the central tendency and dispersion of this error in Figs 10 and 12 demonstrate lesser variation in error mean and standard deviation for the proposed approach.

Table III
CASE III: COMPARISON OF RECONSTRUCTION ERRORS BETWEEN PCP [27] AND PROPOSED ALGORITHM

Missing Data Attack	Average MSE	Standard deviation	Maximum MSE
PCP	2.9779e-06	0.0012	1.9120e-04
Proposed method	1.7713e-07	3.0069e-04	9.4739e-06

3) Comparison with Another Existing Method [29]: To evaluate the effectiveness of the proposed approach, we have compared another existing method based on low-rank Hankel structure, which was reported in [29]. This low-rank matrix block processing method is used for an initial estimate and then to identify and correct bad data as well as to fill in missing data in PMU measurements. We have shown results of the continuously correlated corrupted signals and corresponding reconstruction. As described in the Introduction, this method requires several hyperparameters, which needs to be learned in advance from historical data and tuned in real-time to improve its detection accuracy.

Here, the comparison is made for Case II and the threshold for each signal has been exhaustively tuned until the best result can be obtained with uncorrupted as well as corrupted data. The signal subspace was chosen following the procedure mentioned in [29]. We have studied the reconstruction with the

Table IV
CASE IV: COMPARISON OF RECONSTRUCTION ERRORS BETWEEN PCP [27] AND PROPOSED ALGORITHM

Data Repetition Attack	Average MSE	Standard deviation	Maximum MSE
PCP	2.7234e-06	0.0012	1.9866e-04
Proposed method	1.5524e-07	2.9266e-04	1.4379e-05

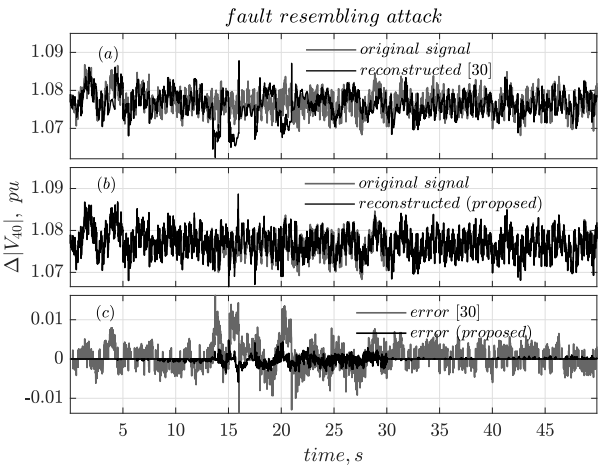

Figure 13. Case II: Comparison of reconstruction errors with an existing method [29] and proposed method for signal $|V_{40}|$.

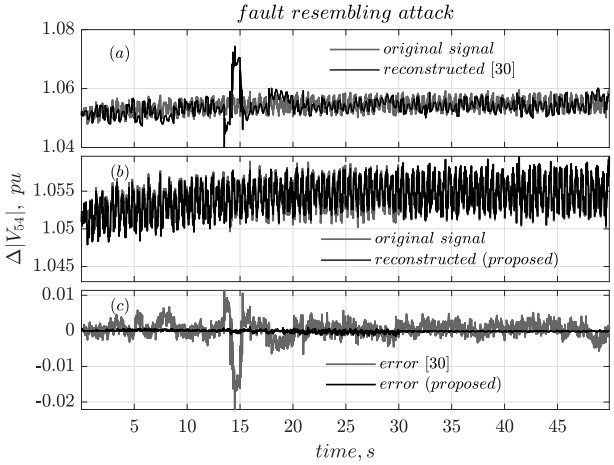

Figure 14. Case II: Comparison of reconstruction errors with an existing method [29] and proposed method for signal $|V_{54}|$.

fault injection attack (Case II) in 2 voltage magnitude signals $|V_{40}|$ and $|V_{54}|$ during ambient condition. Figures 13 and 14 show the plots of the original, corrupted, and reconstructed signals using the method in [29] and the proposed method. From Figs 13 and 14, it is evident that the proposed method is more efficient in detection as well as reconstruction as compared to [29] for fault resembling attacks.

We found that the threshold selection is quite challenging for the method in [29]. In addition, error in estimation in one instant with the Hankel matrix subspace can propagate through inaccurate subspace calculation to future estimates. On the contrary, the proposed approach uses only one threshold and utilizes a subspace library obtained from off-line simulations. The trade-off is that [29] is model-free, whereas the proposed approach needs models for off-line simulations.

B. Test under Off-nominal Operating Conditions

The purpose of this section is to illustrate the importance of selecting a specific subspace from the library to be used by the algorithm at any instant according to the current operating point of the system. This has been demonstrated by using a set of subspaces extracted from different operating conditions of the network. To that end, we conducted two experiments.

■ *Experiment I - No Corruption:* This experiment has been conducted across different conditions without any data corruption. For each condition, data reconstruction is performed using multiple subspaces taken from the library, which correspond to the following operating points:

1) $Op-1$: Nominal condition (subspace spanned by $\hat{U}_1$).
2) $Op-2$: One of the double-circuit tie-lines connecting buses $18-42$ out of service ($\hat{U}_2$).

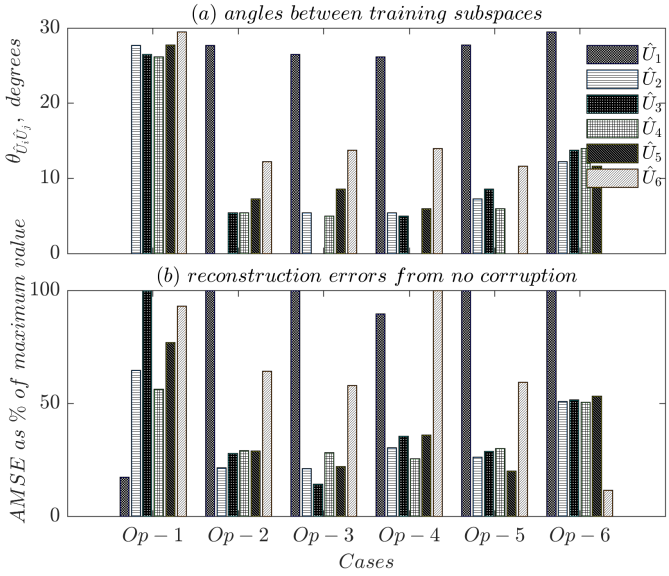

Figure 15. (a) Angles between different subspaces spanned by $\hat{U}_j$ used for reconstruction of the signals, (b) AMSE as a % of maximum value obtained from reconstruction of data with different subspaces spanned by $\hat{U}_j$ in absence of any corruption in the measurements.

3) $Op-3$: One of the double-circuit tie-lines connecting buses $18-49$ out of service ($\hat{U}_3$).
4) $Op-4$: One of the double-circuit tie-lines connecting buses $40-41$ out of service ($\hat{U}_4$).
5) $Op-5$: Nominal condition with a detuned PSS gain in G9 in Fig. 2 ($\hat{U}_5$).
6) $Op-6$: Nominal condition with PSS gain as in $Op-5$ and loads increased by 20% over nominal loading ($\hat{U}_6$).

We propose to use the angle between different subspaces as a measure of proximity of these subspaces. Any two subspaces represented by $\hat{U}_i$ and $\hat{U}_j$ consisting of a set of basis vectors form an angle, which can be calculated as follows [41].

$$\theta_{\hat{U}_i\hat{U}_j} = sin^{-1}\left(\left\|(I-\hat{U}_i\hat{U}_i')\hat{U}_j\right\|_2 \Big/ \left\|\hat{U}_j\right\|_2\right) \qquad (6)$$

The performance of different subspaces is evaluated by their reconstruction errors, which are the average mean square errors (AMSEs) during reconstruction over an interval $[T_0, T_c]$,

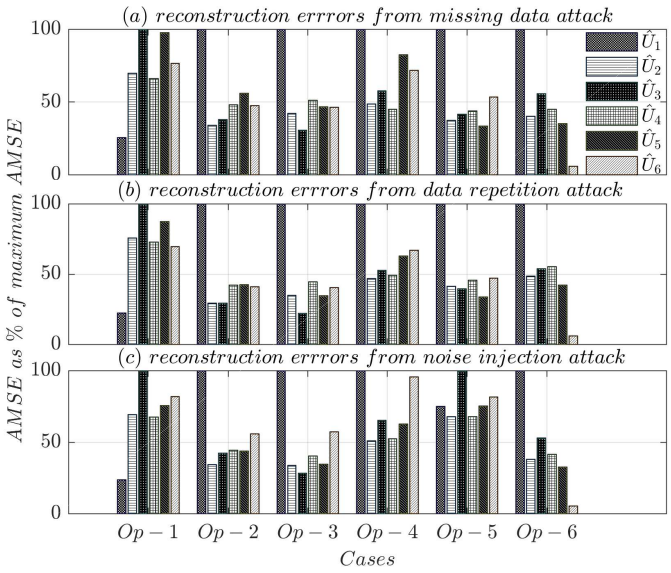

Figure 16. AMSE as a % of maximum value obtained from reconstruction of data with different subspaces spanned by $\hat{U}_j$ during different corruptions in the transient data. The data is generated by simulating a self-clearing fault under each condition.

and averaged over all signals (n_1) considered together.

$$AMSE_{[T_0,T_c]}(e_t) = [e_t' e_t]\, n_1^{-1}\, (T_c - T_0 + 1)^{-1} \qquad (7)$$

where e_t $(n \times 1)$ denotes the 'error' during reconstruction at any instant t. T_0 and T_c represent the starting and ending time instances of corruption interval, respectively. The goal is to show that for operating condition $Op-i$, when reconstruction is performed using subspace spanned by $\hat{U}_j$, the value of AMSE is smaller if $\theta_{\hat{U}_i\hat{U}_j}$ is smaller, and vice-versa.

The data collected at any particular operating condition is assumed to be free of corruption. *This ensures that the reconstruction error is purely caused by the choice of subspaces*.

In Fig. 15, the x-axis shows the operating conditions. For each condition $Op-i$, $i = 1, 2, ...6$; the y-axis of Fig. 15(a) shows the angle $\theta_{\hat{U}_i\hat{U}_j}$, $j = 1, 2, ...6$ and the y-axis of Fig. 15(b) shows the normalized AMSE when $\hat{U}_j$, $j = 1, 2, ...6$ is used as the subspace for reconstruction. The AMSEs are normalized with respect to the maximum AMSE for each operating point $Op-i$.

At each operating condition $Op-i$, the AMSE is minimum along with the corresponding angle $\theta_{\hat{U}_i\hat{U}_j}$ for $i = j$ (actually, $\theta_{\hat{U}_i\hat{U}_i} = 0$) and higher when $i \neq j$ as can be seen in Fig. 15. Also, higher angles largely correspond to higher AMSEs. This emphasizes the importance of selecting an appropriate subspace at any operating point - see remark under Section III(A).

■ *Experiment II - With Corruption:* Figure 16 shows various reconstruction errors for three different attacks on data during transient state. The transient data is obtained by simulating a self-clearing fault near bus 53. This is achieved by corrupting the test data with missing data attack in (a), data repetition attack in (b), and noise injection attack in (c). The corresponding reconstruction errors in terms of normalized AMSEs as a consequence of using different subspaces at each of six operating conditions are presented. As shown, for each of the operating conditions $Op-i$ in x-axis, the normalized AMSE is minimum when the corresponding subspace spanned by $\hat{U}_i$ is utilized for reconstruction. The error becomes higher for other subspaces spanned by $\hat{U}_j$, $j \neq i$.

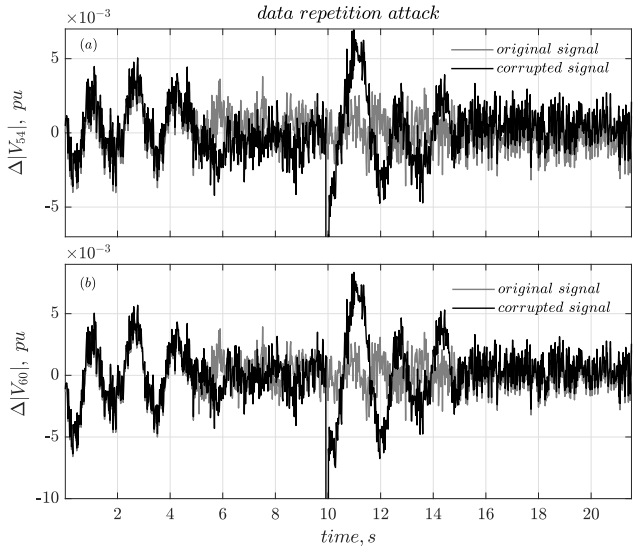

Figure 17. Case V: Data repetition attack in signals $|V_{54}|$ and $|V_{60}|$, for $Op-2$ following a self clearing fault near bus 53.

To demonstrate the effect on modal estimation, the following study has been conducted when the system operates under $Op-2$ and a self clearing fault is created near bus 53 to generate transient response. The set of subspaces spanned by $\hat{U}$ to be tested by the algorithm are $\hat{U}_1$ and $\hat{U}_2$.

Data repetition attack was performed on voltage magnitude signals $|V_{54}|$ and $|V_{60}|$ during the transient condition as shown in Fig. 17. The resulting frequency and damping estimates of original, corrupted, and reconstructed $|V_{54}|$ signal using subspace spanned by $\hat{U}_1$ and by $\hat{U}_2$ are demonstrated in Figs 18 and 19, respectively. As can be seen in Fig. 19, the estimations from reconstructed signal closely follow those of the original signal. This shows that the selection of an appropriate subspace spanned by $\hat{U}_2$ for the current operating condition $Op-2$ results in more accurate modal estimates as compared to the other subspace spanned by $\hat{U}_1$, which produces inferior estimates presented in Fig. 18.

C. Impact of Parameter 'q' and Higher Corruption

An experiment was performed during nominal operating condition ($Op-1$) for evaluating the performance of the algorithm for different values of threshold parameter q. In order to choose the fraction q in ω, we have presented an ROC analysis, which is a standard statistical method for selecting the discrimination threshold ω for a binary classification (corrupted or uncorrupted). An efficient detection can be obtained by selection of a threshold value from the knowledge of the data collected on true/false positive/negatives from different experiments. Data repetition attack and noise injection attack were performed for a corruption in 20% and 30% of the signals for a duration of 10s. Four indices were calculated in the corruption interval for each value of the parameter q: $0.01, 0.1, 0.2, 0.3, 0.4$, and 0.5.

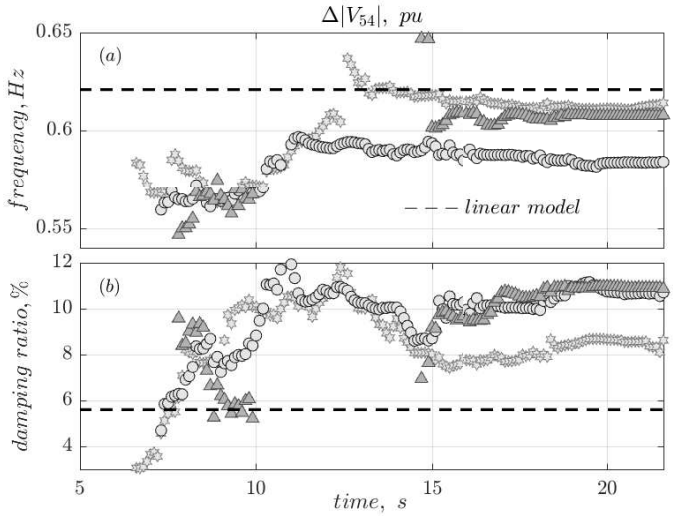

Figure 18. Case V: Estimated frequency and damping ratio from original **(light grey '$*$')**, corrupted **(dark grey'Δ')**, and reconstructed **(black 'o')** signal in $|V_{54}|$ under $Op-2$ following a self clearing fault. Subspace spanned by $\hat{U}_1$ is used for reconstruction.

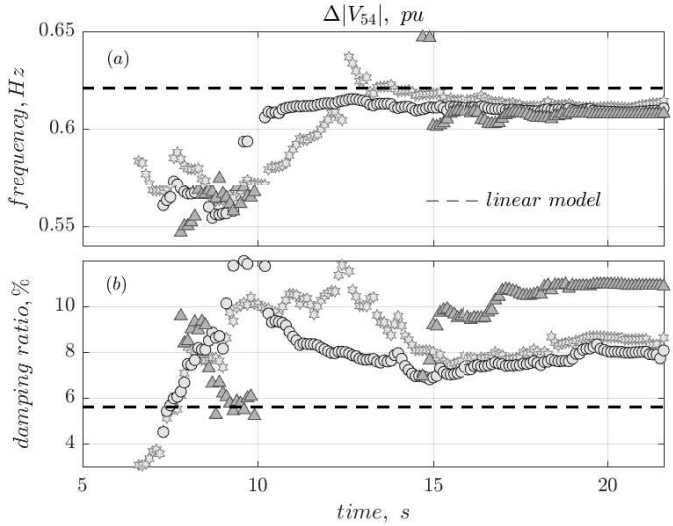

Figure 19. Case V: Estimated frequency and damping ratio from original **(light grey '$*$')**, corrupted **(dark grey'Δ')**, and reconstructed **(black 'o')** signal in $|V_{54}|$ under $Op-2$ following a self clearing fault. Subspace spanned by $\hat{U}_2$ is used for reconstruction.

- True Positive (TP): # of samples in the interval, which are 'actually corrupted' and 'labeled as corrupted' as detected by the algorithm.
- False Positive (FP): # of samples in the interval, which are 'actually uncorrupted' but 'labeled as corrupted' as detected by the algorithm.
- True Negative (TN): # of samples in the interval, which are 'actually uncorrupted' and 'labeled as uncorrupted' as detected by the algorithm.
- False Negative (FN): # of samples in the interval, which are 'actually corrupted' but 'labeled as uncorrupted' as detected by the algorithm.

In order to determine how good the algorithm is in picking out the corrupted samples, performance indicators such as sensitivity (S_n) and specificity (S_p) are calculated for each value of q as follows.

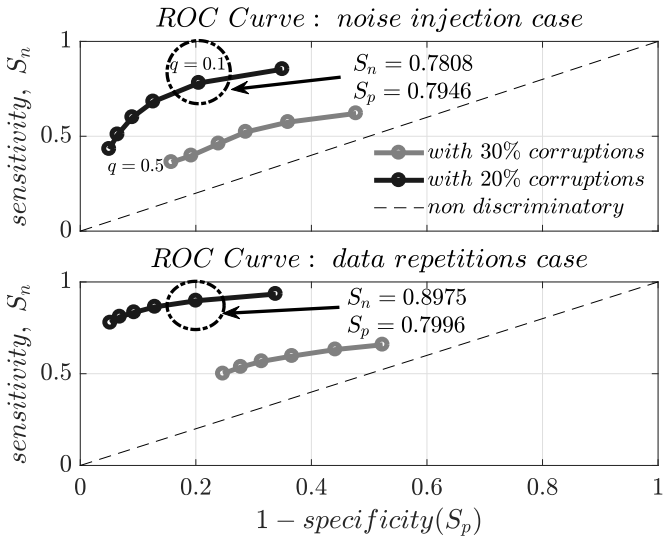

Figure 20. Receiver operating characteristic (ROC) curve for two attacks during nominal operating condition of the test system ($Op-1$) using the subspace spanned by $\hat{U}_1$.

$$S_n(q) = TP/(TP+FN),\ \ S_p(q) = TN/(TN+FP) \quad (8)$$

Figure 20 presents the effects of changing the threshold parameter q graphically by using a receiver operating characteristic (ROC) curve, which plots S_n on the y-axis and (1-S_p) on the x-axis. Each point in the graph indicates a threshold value of q used by the algorithm. ROC curves tend to go from the bottom left corner to the top right corner of the box as q reduces from 0.5 to 0.01. This represents the intuitive trade-off between sensitivity (rising as we move up) and specificity (dropping as we move right). Therefore, higher values of q makes the algorithm more specific but less sensitive, and vice versa. As described before, throughout the paper, we have selected $q = 0.1$ at which a reasonable sensitivity and specificity can be obtained by the proposed algorithm for correct classification of the corrupted samples.

■ *Remark on Limitation with Higher Corruption:* It can also be seen that the algorithm works more efficiently when corruption is present in 20% of the signals at any instant. For each value of q, when the corruption is increased to 30% of the signals at any instant, it leads to lesser sensitivity and specificity. Note that accuracy of detecting corruptions also depends on the noise levels present in the signals. Our present research is focused on improving the performance of the algorithm with higher corruption.

V. Conclusion

In this work, detection of malicious injections in PMU data was formulated as a LASSO problem. It was shown that the solution to this problem can be used to reconstruct the original data with sufficient accuracy from the corrupted signal when corruption is present in 20% of the total number of signals at any instant. Different types of attacks including continuous injection of correlated corruption were studied. It was also shown that the reconstructed signal can be used by a mode-metering algorithm to estimate modal damping and frequency with reasonable accuracy. Proximity between

different subspaces was shown using angles between those subspaces and the effect selecting different subspaces on the reconstruction error was demonstrated. It was observed that the reconstruction error is minimum when an appropriate low-rank subspace is selected by the algorithm for the reconstruction of the data. Also the impact of choosing different threshold values for detecting a corrupted samples was presented for evaluating the sensitivity and specificity performances of the algorithm.

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 Communications (SmartGridComm), 2012 IEEE Third International Conference on*. 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 Journal of Critical Infrastructure Protection*, 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 Networks*, 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," *Proceedings of the IEEE*, vol. 93, no. 5, pp. 980–996, May 2005.

[5] D. J. Trudnowski, J. W. Pierre, N. Zhou, J. F. Hauer, and M. Parashar, "Performance of three mode-meter block-processing algorithms for automated dynamic stability assessment," *IEEE Transactions on Power Systems*, vol. 23, no. 2, pp. 680–690, 2008.

[6] G. Liu, V. M. Venkatasubramanian, and J. R. Carroll, "Oscillation monitoring system using synchrophasors," in *Power & Energy Society General Meeting, 2009. PES'09. IEEE*. IEEE, 2009, pp. 1–4.

[7] S. Pan, T. Morris, and U. Adhikari, "Classification of disturbances and cyber-attacks in power systems using heterogeneous time-synchronized data," *IEEE Transactions on Industrial Informatics*, vol. 11, no. 3, pp. 650–662, June 2015.

[8] ——, "Developing a hybrid intrusion detection system using data mining for power systems," *IEEE Transactions on Smart Grid*, vol. 6, no. 6, pp. 3104–3113, Nov 2015.

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

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

[11] J. Valenzuela, J. Wang, and N. Bissinger, "Real-time intrusion detection in power system operations," *IEEE Transactions on Power Systems*, vol. 28, no. 2, pp. 1052–1062, May 2013.

[12] J. Zhao, L. Mili, and M. Wang, "A generalized false data injection attacks against power system nonlinear state estimator and countermeasures," *IEEE Transactions on Power Systems*, 2018.

[13] A. Ashok, M. Govindarasu, and V. Ajjarapu, "Online detection of stealthy false data injection attacks in power system state estimation," *IEEE Transactions on Smart Grid*, 2016.

[14] M. Netto and L. Mili, "Robust data filtering for estimating electromechanical modes of oscillation via the multichannel prony method," *IEEE Transactions on Power Systems*, vol. 33, no. 4, 2018.

[15] J. Zhao and L. Mili, "A framework for robust hybrid state estimation with unknown measurement noise statistics," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 5, pp. 1866–1875, 2018.

[16] 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 Transactions on Power Systems*, vol. 33, no. 4, pp. 4604–4613, 2018.

[17] J. Zhao, L. Mili, and F. Milano, "Robust frequency divider for power system online monitoring and control," *IEEE Transactions on Power Systems*, vol. 33, no. 4, 2018.

[18] J. Zhao and L. Mili, "Power system robust decentralized dynamic state estimation based on multiple hypothesis testing," *IEEE Transactions on Power Systems*, vol. 33, no. 4, 2018.

[19] A. S. Musleh, H. M. Khalid, S. Muyeen, and A. Al-Durra, "A prediction algorithm to enhance grid resilience toward cyber attacks in wamcs applications," *IEEE Systems Journal*, 2017.

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

[21] S. Pal, B. Sikdar, and J. Chow, "Classification and detection of PMU data manipulation attacks using transmission line parameters," *IEEE Transactions on Smart Grid*, vol. PP, no. 99, pp. 1–1, 2017.

[22] K. Mahapatra, N. R. Chaudhuri, R. Kavasseri, and S. Brahma, "Online analytical characterization of outliers in synchrophasor measurements: A singular value perturbation viewpoint," *IEEE Transactions on Power Systems*, vol. PP, no. 99, pp. 1–1, 2017.

[23] 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 Transactions on Signal Processing*, vol. 65, no. 20, pp. 5421–5436, 2015.

[24] 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 Transactions on Power Systems*, vol. 31, no. 2, pp. 1006–1013, 2016.

[25] 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 on*. IEEE, 2017, pp. 1–5.

[26] 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 Transactions on Signal Processing*, vol. 64, no. 21, pp. 5557–5570, 2016.

[27] K. Mahapatra and N. R. Chaudhuri, "Malicious corruption-resilient wide-area oscillation monitoring using principal component pursuit," *IEEE Transactions on Smart Grid*, vol. PP, no. 99, pp. 1–1, 2017.

[28] 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.

[29] Y. Hao, M. Wang, J. H. Chow, E. Farantatos, and M. Patel, "Model-less data quality improvement of streaming synchrophasor measurements by exploiting the low-rank hankel structure," *IEEE Transactions on Power Systems*, 2018.

[30] P. Gao, R. Wang, M. Wang, and J. H. Chow, "Low-rank matrix recovery from noisy, quantized, and erroneous measurements," *IEEE Transactions on Signal Processing*, vol. 66, no. 11, pp. 2918–2932, 2018.

[31] K. Mahapatra and N. R. Chaudhuri, "Malicious corruption-resilient wide-area oscillation monitoring using online robust PCA," in *IEEE Power & Energy Society General Meeting, 2018.* (accepted).

[32] R. Tibshirani, "Regression shrinkage and selection via the lasso," *Journal of the Royal Statistical Society. Series B (Methodological)*, pp. 267–288, 1996.

[33] E. J. Candès and M. B. Wakin, "An introduction to compressive sampling," *IEEE signal processing magazine*, vol. 25, no. 2, pp. 21–30, 2008.

[34] H. Guo, C. Qiu, and N. Vaswani, "An online algorithm for separating sparse and low-dimensional signal sequences from their sum," *IEEE Transactions on Signal Processing*, vol. 62, no. 16, pp. 4284–4297, 2014.

[35] L. Ljung, *System identification: theory for the user*, 2nd ed. Upper Saddle River, N.J.: Prentice Hall PTR; London : Prentice-Hall International, 1999.

[36] 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.

[37] G. V. Tim Roughgarden, "CS168: The modern algorithmic toolbox, lecture-9." [Online]. Available: http://theory.stanford.edu/∼tim/s15/l/l9.pdf

[38] M. Grant and S. Boyd, "CVX: Matlab software for disciplined convex programming, version 2.1," http://cvxr.com/cvx, Mar. 2014.

[39] ——, "Graph implementations for nonsmooth convex programs," in *Recent Advances in Learning and Control*, ser. Lecture Notes in Control and Information Sciences, V. Blondel, S. Boyd, and H. Kimura, Eds. Springer-Verlag Limited, 2008, pp. 95–110, http://stanford.edu/∼boyd/graph_dcp.html.

[40] B. Pal and B. Chaudhuri, *Robust control in power systems*, ser. Power electronics and power systems. New York: Springer, 2005.

[41] A. Björck and G. H. Golub, "Numerical methods for computing angles between linear subspaces," *Mathematics of computation*, vol. 27, no. 123, pp. 579–594, 1973.

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.

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.