Malicious Corruption-Resilient Wide-Area Oscillation Monitoring using Online Robust PCA

Kaveri Mahapatra
Department of Electrical Engineering
The Pennsylvania State University
University Park, PA 16802
Email: kzm221@psu.edu

Nilanjan Ray Chaudhuri
Department of Electrical Engineering
The Pennsylvania State University
University Park, PA 16802
Email: nuc88@psu.edu

***Abstract*—Presence of malicious injection originating from cyber attacks in PMU measurements can potentially affect the operation and stability of power system. This paper presents a method for detecting malicious data injections in PMU measurements. The problem of detection of malicious injections is formulated as a compressed sensing problem and the corrupted signals are recovered using a robust 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 a wide-area oscillation monitoring application. Data from a 16-machine, 5-area New England-New York system is used along with a recursive oscillation monitoring algorithm to test and validate the effectiveness of the proposed approach on correct detection and reconstruction of the PMU signals under both 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 communication and information technologies. An example being 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 cyberattacks. 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 cause inappropriate control decisions leading to instability and physical damage to the network.

In this work, our focus is on modal estimation using synchrophasor data, which is already operational in control centers of many utilities including California ISO, PG&E, BPA [5], and TVA [6], and a corresponding web-based version is deployed in 7 operations centers and 11 reliability coordinators in the Eastern Interconnection [5] for quite some time. Literature on detection of bad data originated by cyber-attacks in PMU dynamic data samples include a common path algorithm [7], a hybrid intrusion detection system [8], and a Bayesian-based approximation filter proposed in [9]. Most of the work on bad data or cyber intrusion detection are based on state estimation. However, to the best of our knowledge, PMU-enabled state estimators are yet to be integrated with the WAMS-based oscillation monitoring application. Therefore, detection techniques specific to state estimation are not applicable here. Our goal is to detect malicious injection present in PMU data and correct the data vector for real time oscillation monitoring application.

Not many papers exist that focused on cyber-attack detection for the oscillation monitoring application in power systems. Reference [9] applied a Baysian-based Approximated Filter (BAF) to extract modal damping and frequencies from corrupted data. In contrast to [9] and prior works focused on cyber intrusion detection in PMU data, this paper proposes an interface layer based on a robust principal component analysis (RPCA) technique for solving traditional compressed sensing (CS)/sparse recovery [10]–[12] problem. It pre-processes a vector of data samples from a set of signals at any time-step to detect data corruption stemming from cyberattack or otherwise and reconstructs the data vector for wide-area monitoring applications. This paper demonstrates the effectiveness of the proposed approach when different types of carefully designed cyber-attacks [9] corrupt PMU data during ambient and transient conditions. Attack on a single stream of PMU data among a set of PMU signals is considered and the reconstruction of the original PMU data from the corrupted data is demonstrated. A simple Recursive Least Squares (RLS)-based algorithm [13] has been applied as an example of mode metering technique to estimate the modal damping ratio and frequency from reconstructed data.

II. Proposed Architecture

An architecture for malicious corruption resilient wide-area monitoring is proposed in this work as shown in Fig. 1. The proposed framework introduces a data pre-processor block based on online RPCA for phasor data received from different PMUs. Phasor Data Concentrators (PDCs) situated at the control center align the data packets received from PMUs located at remote buses and pass on the data streams to the data pre-processor. Any malicious injections through cyberattacks is assumed to take place before the data arrives at the control

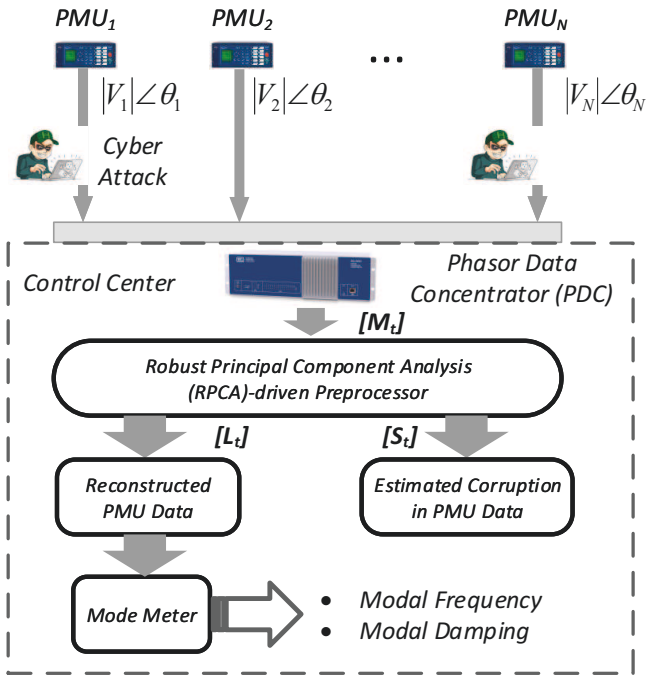

Figure 1. Proposed architecture for malicious corruption-resilient wide-area oscillation monitoring algorithm.

center by overcoming communication layer security and that the control center is assumed to be secure from such attacks.

We consider the following types of attacks -

1. Parameter manipulation attack - Inject signals with altered modal characteristics.

2. Fault-resembling injection attack - Inject signals from fault recordings.

3. Missing data attack - Stop data samples from reaching the control center. PDC produces the latest available data sample repeatedly unless fresh samples appear.

4. Data repetition attack - Extract a block of data from the past and repeat that in the transient condition.

III. Problem Formulation

The goal here is to identify the corrupted signals and quantify the amount of corruption present in the signal samples at any instant by using efficient convex optimization algorithms. This problem assumes corruption is present in less than 20% of the samples considered at an instant.

The measurements coming from PMUs are time-stamped samples of different phasor signals, which are highly correlated in the sense that all are governed by the system dynamics. Therefore, at any instant the values of all signals 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. The objective of the proposed model is to recover a time-sequence of sparse vectors S_t of dimension nx1 and a time-sequence of dense vectors L_t of dimension nx1 from their sum as follows.

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

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

In other words, this is a problem of recovering a sparse corruption in signal samples S_t at any instant. In literature, 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) [12] method-based algorithm is proposed to solve the above problem, which assumes no change in subspace. The algorithm uses a dynamic sequence of measurements M_{Train}=[M_t;$0 \leq t \leq t_{Train}$], under a nominal operating condition, which is free of corruption, i.e. M_t=L_t, to estimate the underlying subspace, U. At every time step t, both L_t and S_t are estimated such that L_t lies in this training subspace and S_t is the corruptions added to L_t to form M_t.

■ *Preparation of the data:* The empirical mean vector, μ consisting of mean of each signal in the raw training data M^{raw}_{Train}, is first calculated and subtracted from each sample vector of the raw training sequence of corresponding signals to prepare M_{Train}. Similarly, before passing any test data vector M^{raw}_t to the proposed algorithm, the μ vector is first subtracted from M^{raw}_t, to prepare M_t. Also, after obtaining estimates for the dense vector $\hat{L}_t$, and sparse vector $\hat{S}_t$, the uncorrupted values of the signals are obtained by adding the μ to L_t. ■

The subspace of the signals is considered to be constant throughout the simulation assuming that the operating point does not deviate far from the nominal condition. Given a set a measurements of voltage magnitudes and phase angles, a good candidate for the subspace, which satisfactorily represents the correlations between signals and does not contain any sparse vector is selected by choosing data samples M^{raw}_{Train} during a power system dynamical event such as a fault. Given a set of training data set $M_{Train} \in \mathbb{R}^{n_1 \times n_2}$ containing n_1 signals with n_2 samples, the singular value decomposition (SVD) is given by

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

where, 'r' represents the true rank of the matrix M_{Train}. σ_1,...σ_r denote the '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 $\hat{U}$ matrix for estimating 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 [14]. This process takes basis vectors corresponding to a certain number r_{approx} of higher singular vectors to form the approximate basis, $\hat{U} = [u_1, \ldots, u_{rapprox}]$.

The key idea is to project any new measurement vector M_t into a subspace, which is orthogonal to the low rank signal

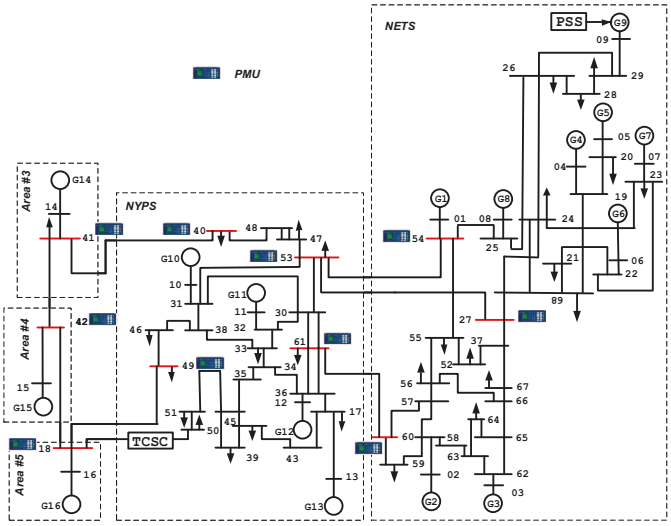

Figure 2. Single-line diagram of 16-machine, 5-area New England-New York system with PMUs installed at major inter-tie buses highlighted in red.

subspace $\hat{U}$ 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 [12]. Here β_t is interpreted as small noise. This leads to a traditional compressed sensing/sparse recovery problem [10]–[12] called as the "least absolute shrinkage and selection operator (LASSO)" which tries to recover the sparse S_t from y_t. The problem can now be formulated as follows.

$$\min_x \|x\|_1 \; s.t. \; \|y_t - \Phi_t x_t\| \leq \xi \tag{4}$$

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 x=$\hat{S}_t^x$ to the above minimization problem is an estimate of sparse vector $\hat{S}_t$. 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. In this work, 'YALL1' solver from l_1 minimization toolbox [15] is used for which code is available at [16].

The corrupted positions or support of $\hat{S}_t$ can be determined by thresholding the $\hat{S}_t^x$ by a small positive number, ω. The estimate of $\hat{S}_t$ can be obtained on this determined support using least squares (LS) method. This estimate of $\hat{S}_t$ is used to find the estimate of $\hat{L}_t = M_t$ - $\hat{S}_t$. By recovering S_t correctly, an accurate L_t can be recovered from M_t.

A. Proposed Algorithm

We present a modified version of the algorithm proposed in [12] to suite the problem of detecting corruptions in PMU measurements. The following describes the procedure derived from [12] to recover the correct signal vector from a set of corrupted signal measurements when only one signal is affected by anomalous injections at any instant. M_t, $\hat{T}_t$, $\hat{S}_t$, $\hat{L}_t$ are of size (n_1x1) where n_1 denotes the number of signals considered.

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

Initialization

- Apply SVD on M_{Train} to get U and Σ.
- Set r_{approx} and determine approximate subspace $\hat{U}$.
- Set the initial Support $\hat{S}$ = [.].

While $t \geq t_0$,

1) Perpendicular projection: Compute y_t= $\phi_t M_t$ where $\phi_t \leftarrow (I\text{-}\hat{U}\hat{U}')$.
2) 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 $t \geq 0$.
3) Compute $\hat{S}_t^x$ as a solution to equation (4) using YALL1 solver.
4) Calculate $\omega = q\sqrt{\|M_t\|^2/n}$ for $t = 0$ for the first sample and $\omega = q\sqrt{\|L_{t-1}\|^2/n}$ for $t \geq 0$.
5) Compute the support set $\hat{T}_t$ by thresholding $\hat{S}_t^x$ where $\hat{T}_t = \left\{i : \left|\hat{S}_t^x\right| \geq \omega\right\}$.
6) Compute $\hat{S}_t \leftarrow LS(y_t, \phi_t, \hat{T}_t)$ where $\hat{x} \leftarrow LS(y, A, T)$ means that $\hat{x}_T = \left(A_T' A_T\right)^{-1} A_T' y$ and $\hat{x}_T^c = 0$. Here A_T denotes a submatrix of matrix A containing the columns with indices in the set T.
7) Estimate $L_t \leftarrow M_t - \hat{S}_t$.
8) Increment t by sampling time duration and go to step 1.

B. Modal Estimation

As described in the Introduction, different algorithms can be used for modal estimation. In this work, we have applied a variable forgetting factor-based Recursive Least Squares (RLS) algorithm [13] which is well-known and is not repeated here.

C. 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 [17] 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 (i.e. 10 signals) were considered in this study and de-trending was performed on all signals. A fault near bus 53 is created in the system and the post-fault samples were collected as the raw training data M_{Train}^{raw}. The training subspace is a low rank approximation of the training data, which is obtained by applying SVD on M_{Train} and retaining the first 4 (r_{approx}=4) left singular vectors corresponding to higher singular values to represent subspace $\hat{U}$ for the system. In our case studies, one signal out of 10 is assumed to be corrupted at any instant. Algorithm parameter q can be chosen as a small positive number such as 0.25. Only the corrupted sample is recovered at each instant using LS estimation, see step (6) in the proposed algorithm. The recovered samples at any instant are utilized by an RLS-based mode metering algorithm. Due to space restrictions, we show mode-meter output for two cases - each one under ambient and transient conditions.

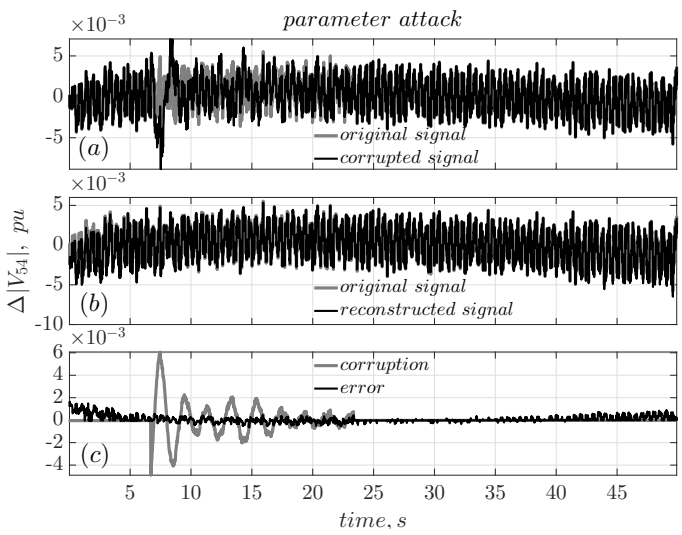

Figure 3. Case I: Parameter manipulation attack in signal $|V_{54}|$ under ambient condition. Corruption: difference between original and corrupted signal, Error: difference between original and reconstructed signal.

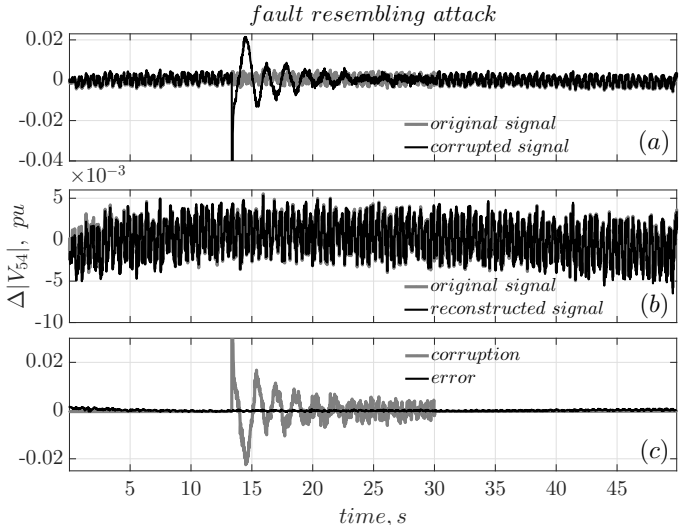

Figure 4. Case II: Fault-resembling injection attack in signal $|V_{54}|$ under ambient condition. Corruption: difference between original and corrupted signal, Error: difference between original and reconstructed signal.

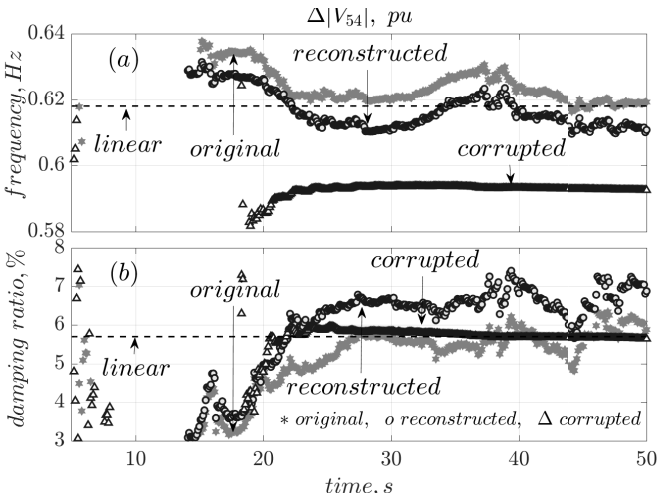

Figure 5. Case II: Estimated frequency and damping ratio from corrupted **('Δ')** signal is misleading. Reconstruction **('o')** produces reasonable accuracy as compared to original **(grey '∗')**.

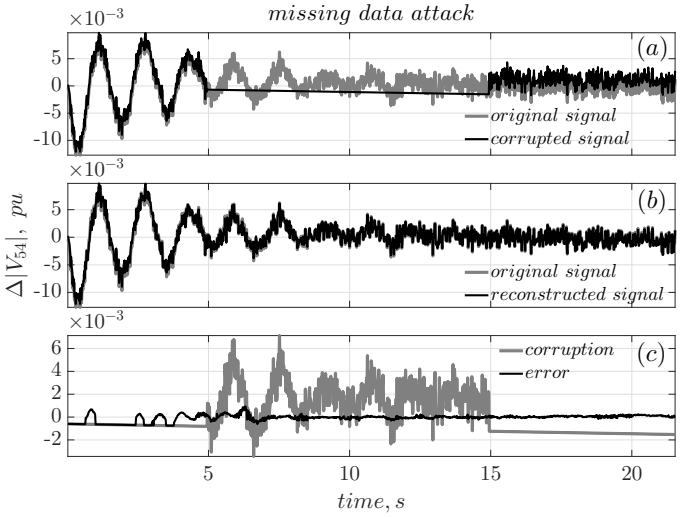

Figure 6. Case III: Missing data attack in signal $|V_{54}|$ under transient condition. Corruption: difference between original and corrupted signal, Error: difference between original and reconstructed signal.

1) Ambient Condition: To simulate the ambient condition, band-limited zero-mean gaussian noise was injected in load terminals of the power system.

■ *Case I: Parameter Manipulation Attack on One Signal:* Figure 3 shows the parameter manipulation attack in signal $|V_{54}|$ for 1000 samples. Unless otherwise stated, only deviation in the signals from nominal condition are shown. The attack model uses the 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(c) 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 good quality of reconstruction.

■ *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 a signal $|V_{54}|$ as shown in Figs 4. The quality of reconstruction is very good and is reflected in the estimated frequency and damping ratios in Fig. 5. Since the injected signals are actual transient response from the system, estimates from the corrupted signals finally tend to converge to original values. However, due to transient signal injection, a large deviation is witnessed in all estimates obtained from corrupted signal.

2) Transient Condition: A self-clearing three-phase fault near bus 53 was considered. The first half-cycle of oscillatory data immediately after fault is disregarded in our analysis to avoid the effect of higher nonlinearity. This is acceptable since the accuracy of most of the mode-metering algorithms is poor

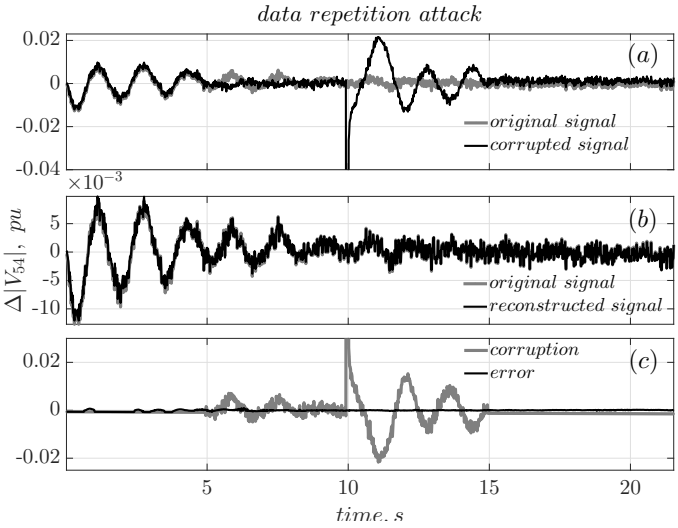

Figure 7. Case IV: Data repetition attack in signal $|V_{54}|$ under transient condition. Corruption: difference between original and corrupted signal, Error: difference between original and reconstructed signal.

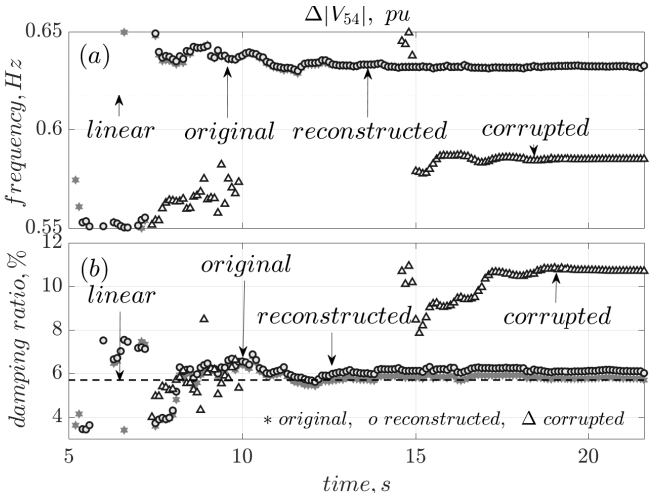

Figure 8. Case IV: Estimated frequency and damping ratio from corrupted **('Δ')** signal is misleading. Reconstruction **('o')** produces reasonable accuracy as compared to original **(grey '∗')**.

in this region.

■ *Case III: Missing Data Attack:* We consider a missing data attack on signal $|V_{54}|$. The effectiveness of the proposed pre-processor in data reconstruction is shown in Fig. 6. Like previous cases, 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 are repeated in signal $|V_{54}|$ as shown in Fig. 7, which resembles a consecutive fault in the system. It can be seen from Fig. 8 that the corruption in data consistently led to an increase in estimated damping ratio. The frequency and the damping estimates from the reconstructed signal appear to reasonably follow those obtained from the original signals.

IV. 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 reconstruct the original data with sufficient accuracy from the corrupted signal when corruption is present in 10% of the total number of signals. 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.

V. Acknowledgment

This work was supported by funding from NSF Award Number: CNS 1544621 and CNS 1739206.

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

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

[12] 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.

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

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

[15] J. Yang and Y. Zhang, "Alternating direction algorithms for l_1-problems in compressive sensing," *SIAM journal on scientific computing*, vol. 33, no. 1, pp. 250–278, 2011.

[16] J. Y. W. Y. Yin Zhang, Wei Deng, "Yall1." [Online]. Available: http://yall1.blogs.rice.edu/

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