Identification of Successive “Unobservable” Cyber Data Attacks in Power Systems Through Matrix Decomposition

Pengzhi Gao, *Student Member, IEEE*, Meng Wang, *Member, IEEE,* Joe H. Chow, *Fellow, IEEE,*
Scott G. Ghiocel, *Member, IEEE,* Bruce Fardanesh, *Fellow, IEEE,*
George Stefopoulos, *Member, IEEE*, and Michael P. Razanousky

***Abstract*—This paper presents a new framework of identifying a series of cyber data attacks on power system synchrophasor measurements. We focus on detecting “unobservable” cyber data attacks that cannot be detected by any existing method that purely relies on measurements received at one time instant. Leveraging the approximate low-rank property of phasor measurement unit (PMU) data, we formulate the identification problem of successive unobservable cyber attacks as a matrix decomposition problem of a low-rank matrix plus a transformed column-sparse matrix. We propose a convex-optimization-based method and provide its theoretical guarantee in the data identification. Numerical experiments on actual PMU data from the Central New York power system and synthetic data are conducted to verify the effectiveness of the proposed method.**

***Index Terms*—cyber data attacks, low-rank matrix, matrix decomposition, synchrophasor measurements.**

I. Introduction

THE integration of cyber infrastructures into future smart grids greatly enhances the monitoring, dispatch, and scheduling of power systems. Such integration, however, makes the power systems more susceptible to cyber attacks. It is reported that cyber spies have penetrated U.S. electrical grid [26]. Researchers have also launched an experimental cyber attack that caused a generator to self-destruct [15].

State estimation [1] is a critical component of power system monitoring. System state is estimated based on the obtained measurements across the system. Bad data can affect the state estimation and mislead the system operator. Many efforts have been devoted to develop methods that can identify bad data, see e.g., [6], [14], [25], [27], [35].

Cyber data attacks (firstly studied in [23]) can be viewed as “the worst interacting bad data injected by an adversary”[18]. Malicious intruders with system configuration information can simultaneously manipulate multiple measurements so that these attacks cannot be detected by any bad data detector. Because the removal of affected measurements would make the system unobservable, these attacks are termed as “unobservable attacks”[1] in [18].

State estimation in the presence of cyber data attacks has attracted much research attention recently [3], [9], [18], [22], [23], [29]–[31]. Existing approaches include protecting a small number of key measurement units such that the intruders cannot inject unobservable attacks without hacking protected units [3], [9], [17], as well as detectors designed for attacks in the observable regime [18]. The research on the detection of unobservable attacks is still limited. Refs. [22], [30] proposed different methods to detect unobservable attacks in Supervisory Control and Data Acquisition (SCADA) system. The method in [30] relies critically on the assumption that the measurements at different time instants are i.i.d. samples of random variables. This assumption might not hold when the system is under disturbance. Ref. [22] focused on the scenarios that an intruder attacks a different set of measurements at each time instant, and no theoretical analysis of the detection performance is provided in [22].

This paper considers cyber data attacks to PMU measurements. It focuses on the case when an intruder injects unobservable data attacks to the same set of PMUs constantly. Because PMUs under attack do not provide any accurate measurement at any time instant to the operator, the attack identification in this case is very challenging and has not been addressed before. We propose a method that can identify the successive unobservable cyber data attacks and provide the theoretical guarantee even when the system is under disturbance. The intuition is that even though an intruder can constantly inject data attacks that are consistent with each other at each time instant, as long as the intruder does not know the system dynamics, one can identify the attacks by comparing time series of different PMUs and locating the PMUs that exhibit abnormal dynamics.

Because PMU measurements are synchronized and correlated, the high-dimensional PMU data matrix exhibits low-rank property [7], [8], [12], [33]. We formulate the identification problem as a matrix decomposition problem of a low-rank matrix plus a transformed column-sparse matrix. The matrix decomposition problem has attracted much research

P. Gao, M. Wang and J. H. Chow are with the Dept. of Electrical, Computer, and Systems Engineering, Rensselaer Polytechnic Institute, Troy, NY. Email: {gaop, wangm7, chowj}@rpi.edu.

S. G. Ghiocel is with Exponent, New York, NY. Email: sghiocel@exponent.com.

B. Fardanesh, and G. Stefopoulos are with New York Power Authority, White Plains, NY. Email: {Bruce.Fardanesh, George.Stefopoulos}@nypa.gov.

M. P. Razanousky is with New York State Energy Research and Development Authority, Albany, NY. Email: mpr@nyserda.org.

Partial and preliminary results have appeared in [33].

[1] The term “unobservable” is used in this sense throughout the paper.

attention recently, see e.g., [4], [5], [28], [34], and have wide applications in areas like Internet monitoring [19], [24], [32], medical imaging [10], [11], and image processing [2]. The situation that one component is a transformed column-sparse matrix, however, has not been addressed before.

The contributions of this paper are threefold. (1) We propose the idea of exploiting spatial-temporal correlations in PMU measurements to identify unobservable data attacks. (2) We formulate the identification problem into a matrix decomposition problem and propose a computationally efficient method that does not require the modeling of power system dynamics. (3) We provide theoretical guarantees of attack detection, as well as the general matrix decomposition problem.

The rest of the paper is organized as follows. We formulate our problem and point out its connection to other applications in Section II. We describe our detection method and analyze its theoretical guarantee with both noiseless (Section III) and noisy measurements (Section IV). Section V records our numerical experiments. We conclude the paper in Section VI.

II. Problem Formulation and Related Work

A. Low-rankness of PMU measurements

Consider a n-bus power grid with PMUs installed on some buses. Let p denote the total number of PMU channels that measure bus voltage and line current phasors[2]. Phasors are expressed in Cartesian coordinates throughout the paper. Matrix $M \in \mathbb{C}^{t\times p}$ contains the collected phasor measurements in t synchronized time instants. $\bar{\mathcal{J}} \in [\![p]\!]$ denotes the set of PMU channels that are under data attacks. The observed measurement matrix can be presented as

$$M = \bar{L} + \bar{D} + N, \tag{1}$$

where $\bar{L} \in \mathbb{C}^{t\times p}$ represents the actual phasors without data attacks, $\bar{D} \in \mathbb{C}^{t\times p}$ represents the additive errors introduced by an intruder, and N represents the measurement noise.

High-dimensional PMU data matrices exhibit low-rank property [7], [8], [12], [33]. We analyzed actual PMU data from six multi-channel PMUs deployed in the Central New York (NY) Power System (Fig. 1). Six PMUs measure twenty-three voltage and current phasors, and the data rate is thirty samples per second per channel. Fig. 2 shows the current magnitudes of PMU data in twenty seconds. An event occurs around 2.5s. The obtained data are collected into a 600 × 23 matrix. Fig. 3 plots the singular values of the matrix with the ten largest ones being 832.8, 194.8, 35.1, 18.1, 4.3, 2.5, 2.1, 1.3, 1.2, 0.5. Therefore, we can approximate the 600 × 23 matrix by a low-rank matrix with little approximation error.

The Singular Value Decomposition (SVD) of $\bar{L}$ is

$$\bar{L} = \bar{U}\bar{\Sigma}\bar{V}^{\dagger}, \tag{2}$$

where $\bar{U} \in \mathbb{C}^{t\times r}$, $\bar{\Sigma} \in \mathbb{C}^{r\times r}$, $\bar{V} \in \mathbb{C}^{p\times r}$ $(r \ll t, p)$. We assume throughout the paper that nonzero columns of $\bar{D}$ do not lie in the column space of $\bar{L}$ $(\bar{D} \neq \bar{U}\bar{U}^{\dagger}\bar{D})$. It is a legitimate assumption when the intruders do not have full information about the system dynamics. The notations are summarized in Table I. Matrix A is *column-sparse* if it contains a small fraction of non-zero columns. We call the set of indices of nonzero columns the *column support* of A.

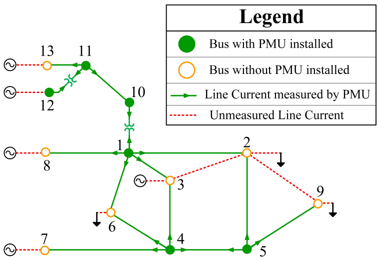


Fig. 1: PMUs in the Central NY Power System. (Circles and lines represent buses and transmission lines. A PMU measures the voltage phasor and the incident current phasors of the bus where it is located.)

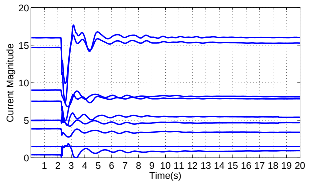


Fig. 2: Visualization of Partial PMU data (Magnitude of nine current phasors)

TABLE I: Notations

A_i, $A_{i,:}$	the ith column and the ith row of matrix A, respectively.
$A_{\mathcal{I}}$	the submatrix of A with column indices in set $\mathcal{I}$.
$A^{\ddagger}$, $A^{\dagger}$	the conjugate and conjugate transpose matrix of A.
$\mathcal{P}_{\mathcal{I}}(A)$	matrix obtained from A by setting A_i to zero for all $i \notin \mathcal{I}$.
$A \in \mathcal{P}_{\mathcal{I}}$	if and only if $\mathcal{P}_{\mathcal{I}}(A) = A$.
$\lVert A\rVert$, $\lVert A\rVert_F$	the spectral and Frobenius norm of A, respectively.
$\lVert A\rVert_*$	the nuclear norm of A, which is the sum of singular values.
$\lVert A\rVert_{1,2}$	the sum of ℓ_2 norms of the columns of A.
$\lVert A\rVert_{\infty,2}$	the largest ℓ_2 norm of the columns.
$\mathcal{P}_U(A)$	$:= UU^{\dagger}A$, the projection of A onto the column space of L.
$\mathcal{P}_V(A)$	$:= AVV^{\dagger}$, the projection of A onto the row space.
$\mathcal{P}_T(\cdot)$	$:= \mathcal{P}_U(\cdot) + \mathcal{P}_V(\cdot) - \mathcal{P}_U\mathcal{P}_V(\cdot)$.
$\mathcal{P}_{U^{\perp}}(A)$	$:= (I - UU^{\dagger})A$.
$\mathcal{P}_{V^{\perp}}(A)$	$:= A(I - VV^{\dagger})$.
$\mathcal{P}_{T^{\perp}}(A)$	$:= \mathcal{P}_{U^{\perp}}\mathcal{P}_{V^{\perp}}(A)$.
$A \in \mathcal{P}_T$	if and only if $\mathcal{P}_T(A) = A$.
$\mathcal{I}^c$	the complimentary set of set $\mathcal{I}$.

B. Unobservable cyber data attacks and problem formulation

We use bus voltage phasors as state variables, and let $X \in \mathbb{C}^{t\times n}$ contain the state variables at t instants. We use the π equivalent model to represent a transmission line (Fig. 4). Z^{ij} and Y^{ij} denote the impedance and admittance of the transmission line between bus i and bus j. Current I^{ij} from bus i to bus j is related to bus voltage V^i and V^j by

$$I^{ij} = \frac{V^i - V^j}{Z^{ij}} + V^i\frac{Y^{ij}}{2}. \tag{3}$$

We define $\bar{W} \in \mathbb{C}^{p\times n}$ as follows. If the kth PMU channel measures the voltage phasor of bus j, $\bar{W}_{kj} = 1$; if it measures the current phasor from bus i to bus j, then

[2] In three phase AC systems, a phasor is defined as a complex number that represents both the magnitude and phase angle of the sinusoidal waveforms.

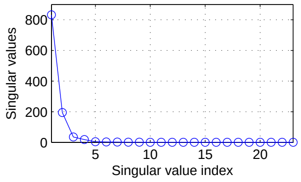


Fig. 3: Singular values of PMU data matrix in decreasing order

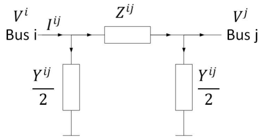


Fig. 4: π model of a transmission line

$\bar{W}_{ki} = 1/Z^{ij} + Y^{ij}/2$, $\bar{W}_{kj} = -1/Z^{ij}$; $\bar{W}_{kj} = 0$ otherwise. The PMU measurements and the state variables are related by

$$\bar{L} = X\bar{W}^T. \tag{4}$$

The attack at time t, denoted by data injection $\bar{D}_{t,:}$, is called *unobservable*[3] if and only if

$$\bar{D}_{t,:} = c^t \bar{W}^T \tag{5}$$

holds for some nonzero row vector $c^t \in \mathbb{C}^{1\times n}$. In this case,

$$\bar{L}_{t,:} + \bar{D}_{t,:} = (X_{t,:} + c^t)\bar{W}^T, \tag{6}$$

and the operator would have the wrong impression that the state is $X_{t,:} + c^t$. We focus on the cases that the attacks from time 1 to t are all unobservable[4], then we have

$$\bar{D} = \begin{bmatrix} c^1 \\ \vdots \\ c^t \end{bmatrix} \bar{W}^T := \bar{C}W^T, \tag{7}$$

where $W_j = \bar{W}_j/\|\bar{W}_j\|$. $\bar{C}$ represents the additive error (up to a scaling factor) to bus voltages due to data attacks, i.e., $\|\bar{W}_j\|\bar{C}_j$ is the error to bus voltage V^j. Let $\bar{\mathcal{I}} \in [\![n]\!]$ denote the column support of $\bar{C}$. We assume $\bar{C}$ is column-sparse because intruders might only alter some of the state variables due to resource constraints. With increasing installation of PMUs, we anticipate that the total number of PMU channels p will be larger than the number of buses n. The transform in (7) reduces the degree of freedom in $\bar{D}$. Combining (1) and (7), the obtained measurements under attack can be written as

$$M = \bar{L} + \bar{C}W^T + N. \tag{8}$$

The attack identification problem is formulated as follows. Given M and W, is it possible to separate $\bar{L}$ and $\bar{C}$? We assume noise level is bounded and given, i.e., $\|N\|_F \leq \eta$. We say a method can *identify* an unobservable attack if it successfully determines the set of PMU channels that are under attack and recovers measurements that are not attacked.

Although cannot be detected at a given time instant, the unobservable attacks can be detected if the time series in the affected PMU channels exhibit dynamics different from those of unaffected PMUs. Mathematically, the matrix decomposition is possible if columns in $\bar{D}$ do not belong to the column space of $\bar{L}$.

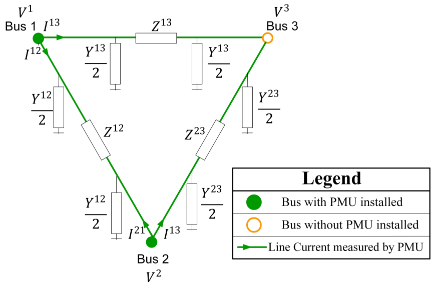


Fig. 5: Three-bus example. PMUs are installed at bus 1 and bus 2 measuring the corresponding voltage phasors and incident line current phasors.

We use a three-bus network (Fig. 5) to illustrate the notations. Let $\mathbf{V}^i$ and $\mathbf{I}^{ij}$ $(i, j \in \{1, 2, 3\})$ in $\mathbb{C}^{t\times 1}$ denote the bus voltages and line currents in t instants. Then

$$\bar{L} = [\mathbf{V}^1\ \mathbf{I}^{12}\ \mathbf{I}^{13}\ \mathbf{V}^2\ \mathbf{I}^{21}\ \mathbf{I}^{23}] = [\mathbf{V}^1\ \mathbf{V}^2\ \mathbf{V}^3]\bar{W}^T \tag{9}$$

where $\bar{W}^T$ is

$$\begin{bmatrix} 1 & \frac{1}{Z^{12}} + \frac{Y^{12}}{2} & \frac{1}{Z^{13}} + \frac{Y^{13}}{2} & 0 & -\frac{1}{Z^{12}} & 0 \\ 0 & -\frac{1}{Z^{12}} & 0 & 1 & \frac{1}{Z^{12}} + \frac{Y^{12}}{2} & \frac{1}{Z^{23}} + \frac{Y^{23}}{2} \\ 0 & 0 & -\frac{1}{Z^{13}} & 0 & 0 & -\frac{1}{Z^{23}} \end{bmatrix}.$$

Suppose the intruder manipulates measurements in all channels of PMU 1 and the channel of PMU 2 that measures $\mathbf{I}^{21}$ and $\mathbf{I}^{23}$ so that the system operator would have the wrong impression that the system states are $[\mathbf{V}^1 + \boldsymbol{\beta}^1\ \mathbf{V}^2\ \mathbf{V}^3 + \boldsymbol{\beta}^2]$ for any nonzero $\boldsymbol{\beta}^1$, $\boldsymbol{\beta}^2 \in \mathbb{C}^{t\times 1}$. In this case, the observed measurements under attacks when there is no noise are

$$\begin{aligned} M &= [\mathbf{V}^1 + \boldsymbol{\beta}^1\quad \mathbf{V}^2\quad \mathbf{V}^3 + \boldsymbol{\beta}^2]\bar{W}^T \\ &= [\mathbf{V}^1 + \boldsymbol{\beta}^1\quad \mathbf{I}^{12} + \frac{\boldsymbol{\beta}^1}{Z^{12}} + \frac{\boldsymbol{\beta}^1 Y^{12}}{2}\quad \mathbf{I}^{13} + \frac{\boldsymbol{\beta}^1 - \boldsymbol{\beta}^2}{Z^{13}} + \frac{\boldsymbol{\beta}^1 Y^{13}}{2} \\ &\quad \mathbf{V}^2\quad \mathbf{I}^{21} - \boldsymbol{\beta}^1/Z^{12}\quad \mathbf{I}^{23} - \boldsymbol{\beta}^2/Z^{23}]. \end{aligned} \tag{10}$$

The additive errors due to attacks are

$$\bar{D} = [\boldsymbol{\beta}^1\quad \mathbf{0}\quad \boldsymbol{\beta}^2]\bar{W}^T = [\|\bar{W}_1\|\boldsymbol{\beta}^1\quad \mathbf{0}\quad \|\bar{W}_3\|\boldsymbol{\beta}^2]W^T. \tag{11}$$

C. Connections to existing work

The detection of unobservable cyber data attacks has not been much addressed. [30] and [22] considered the detection of unobservable attacks to SCADA data and provided numerical results. [30] assumes the measurements across time are i.i.d. distributed and detects the attacks based on statistical learning. [22] assumes the SCADA measurements under DC power flow model are low-rank and proposes to detect the attacks by decomposing a low-rank matrix and a sparse matrix from their sum. Our work differs from [22] in that we assume the intruder constantly injects data attacks to the same set of PMUs, while [22] assumes the intruder attacks different

[3] [23] focuses on DC model where power measurements and state variables are approximately related by linear equations. Here PMU measurements and state variables are accurately related by linear equation (4).

[4] Our detection method can be extended to cases that both unobservable and observable attacks exist. See the beginning of Section III-A

Method 1 Unobservable cyber attack identification method

Input: PMU measurements M in t instants; coefficient η; the set Ω of the locations (i, j) of the observed entries.

Find (L^*, C^*), the optimum solution to the following optimization problem

$$\min_{L\in\mathbb{C}^{t\times p}, C\in\mathbb{C}^{t\times n}} \|L\|_* + \lambda\|C\|_{1,2} \tag{12}$$

$$\text{s.t.} \quad \sum_{i,j\in\Omega} |M_{ij} - L_{ij} - (CW^T)_{ij}|^2 \leq \frac{|\Omega|}{tp}\eta^2 \tag{13}$$

Compute the SVD of $L^* = U^*\Sigma^*V^{*\dagger}$.

Find column support of $D^* = C^*W^T$, denoted by $\mathcal{J}^*$.

Return: L^*, C^*, $L^*_{\mathcal{J}^{*c}}$, U^* and $\mathcal{J}^*$.

PMUs at different time instants. Furthermore, we provide the theoretical guarantee of our detection method.

Our problem formulation of matrix decomposition is closely related to those in [34] and [24]. When W is an identity matrix, our problem reduces to the one in [34]. The difference between our model and the one in [24] is that the sparse matrix $\bar{C}$ in [24] has nonzero entries located independent of each other, while $\bar{C}$ here is a column-sparse matrix. Our method and analysis are built up those in [34], but we consider a more general framework of matrix decomposition through the introduction of the transform matrix W.

The significance of our work is twofold. First, we for the first time consider the case that the additive error matrix $\bar{D}$ can be dense (i.e., W is a dense matrix), while the error matrices in [34] and [24] are sparse. We show through both theoretical analysis and numerical experiments that it is possible to achieve matrix decomposition with dense $\bar{D}$. Second, when $\bar{D}$ is a column-sparse matrix itself (i.e., W is sparse), our decomposition method outperforms those in [34] and [24] (see Section V-B and V-C) in the sense that our recovery method can tolerate a higher level of corruption (i.e., large support size of $\bar{D}$). This advance results from exploiting (7), which reduces the degree of freedom of $\bar{D}$.

Note that our method and analysis hold for an arbitrary W and can be applied to other domains that involve decomposing a matrix as in (8). As discussed in [24], applications include unveiling network traffic anomalies [19], [32], dynamic magnetic resonance imaging [10], [11], face recognition [2], and music analysis [20], [21].

III. Attack Identification without Noise

A. Identification method and guarantee

We first consider noiseless measurements ($\eta = 0$). We assume a complete set of measurements for analysis, but our method can be extended to cases when measurements are partially lost. Moreover, although we consider attack patterns in (7), our method can be generalized to detect combined attacks. In this case, $\bar{D}$ is generalized to

$$\bar{D} = \bar{C}W^T + \bar{S}, \tag{14}$$

where a sparse matrix $\bar{S}$ represents attacks (observable and/or unobservable) that have different locations across time. Then (12)-(13) are generalized to

$$\min_{L\in\mathbb{C}^{t\times p}, C\in\mathbb{C}^{t\times n}, S\in\mathbb{C}^{t\times p}} \|L\|_* + \lambda_1\|C\|_{1,2} + \lambda_2\sum_{ij}|S_{ij}| \tag{15}$$

$$\text{s.t.} \quad \sum_{i,j\in\Omega} |M_{ij} - L_{ij} - (CW^T)_{ij} - S_{ij}|^2 \leq \frac{|\Omega|}{tp}\eta^2, \tag{16}$$

with given positive constants λ_1, λ_2. We study this extension numerically in Section V-B.

To formally present the theoretical result, we need the following definitions. Given $\bar{L} = \bar{U}\bar{\Sigma}\bar{V}^\dagger$ and W, we define

$$\epsilon := \|\bar{V}^\dagger W^\ddagger\|_{\infty,2}, \ \mu := \max_{i\neq j}\|W_i^\dagger W_j\|, \tag{17}$$

$$\text{and } \sigma_k := \max_{\mathcal{I}:|\mathcal{I}|\leq k}\|(W_\mathcal{I}^\dagger W_\mathcal{I})^{-1}\|. \tag{18}$$

Note that $\sigma_1 = 1$ as W has unit-norm columns, and ϵ depends on the rank r of $\bar{L}$, since $\|\bar{V}\|_F^2 = r$.

Pick any constants $\tilde{\psi}$ and c in $(0, 1)$ such that

$$(2-\tilde{\psi})\sqrt{\tilde{\psi}/(1-\tilde{\psi})} \leq \sqrt{(1+c)/(1-c)}. \tag{19}$$

For any integer k, define

$$\lambda_{\min,k} = \frac{(1+(2-\tilde{\psi})^{-1})\epsilon}{1-(1+(2-\tilde{\psi})^{-1})k\sigma_k\mu} \tag{20}$$

$$\text{and } \lambda_{\max,k} = \sqrt{\tilde{\psi}/(k\sigma_k)}. \tag{21}$$

Our detection method is summarized in Method 1. (13) is a convex program and can be solved efficiently by generic solvers such as CVX[13]. Its recovery guarantee is as follows.

Theorem 1. *Suppose there exists nonzero $\tilde{k}$ such that*

$$\tilde{k}\mu \leq c, \ \text{and } \lambda_{\min,\tilde{k}} \leq \lambda_{\max,\tilde{k}}, \tag{22}$$

with c, $\lambda_{\min,\tilde{k}}$, and $\lambda_{\max,\tilde{k}}$ defined in (19)-(21). Then as long as the column support of $\bar{C}$ has size at most $\tilde{k}$, for any $\lambda \in [\lambda_{\min,\tilde{k}}, \lambda_{\max,\tilde{k}}]$, the output of Method 1 satisfies

$$U^*U^{*\dagger} = \bar{U}\bar{U}^\dagger, \tag{23}$$

$$\mathcal{J}^* = \bar{\mathcal{J}} \text{ and } L^*_{\mathcal{J}^{*c}} = \bar{L}_{\bar{\mathcal{J}}^c}.$$

Theorem 1 guarantees that the affected PMUs can be correctly located and thus, the "clean" PMU measurements could be identified. Furthermore, the subspace spanned by the actual phasors can be recovered. Since we do not obtain any actual measurements from PMUs that are under attack, it is impossible to recover the exact measurements in the affected PMUs without further regularization. Under the conditions of Theorem 1, the recovery is also successful when the column support of $\bar{C}$ is zero. Thus, the false alarm rate is zero.

Method 1 is motivated by [34]. In fact, after post-multiplying $W^\ddagger(W^TW^\ddagger)^{-1}$ to both sides of (1), we have

$$MW^\ddagger(W^TW^\ddagger)^{-1} = \bar{L}W^\ddagger(W^TW^\ddagger)^{-1} + \bar{C} + NW^\ddagger(W^TW^\ddagger)^{-1}$$

where the right-hand side is the sum of a low-rank matrix plus a column-sparse matrix and noise. Then, the results of [34] can be directly applied to our problem. We do not follow this path due to two reasons. First, $MW^{\ddagger}(W^TW^{\ddagger})^{-1}$ cannot be computed if some entries of M are missing, while Method 1 can be easily extended to scenarios with missing data by restricting the constraints in (13) to the observed measurements. Second, $(W^TW^{\ddagger})^{-1}$ does not exist when W is a flat matrix, i.e., $p < n$, while Method 1 and Theorem 1 can be applied to an arbitrary W.

B. Discussion of λ and $\tilde{k}$

We remark that due to the slackness in the proof, $\lambda \in [\lambda_{\min,\tilde{k}}, \lambda_{\max,\tilde{k}}]$ in Theorem 1 is sufficient but not necessary[5]. There may exist λ outside $[\lambda_{\min,\tilde{k}}, \lambda_{\max,\tilde{k}}]$ that can still lead to correct recovery. We observe from numerical experiments that recovery performance is generally much better than the bound in Theorem 1. Furthermore, when L is fixed, as $\tilde{k}$ decreases, $\lambda_{\min,\tilde{k}}$ decreases, and $\lambda_{\max,\tilde{k}}$ increases. Thus, intuitively, if the number of affected PMUs decreases, a wider range of λ is proper for Method 1. For a detailed discussion, we state the following lemma and defer its proof to the Appendix.

Lemma 1. *Suppose $k\mu < 1$, then $\sigma_k \le (1-(k-1)\mu)^{-1}$.*

Since σ_k increases in k, $\sigma_1 \ge 1$, and $k\mu \le c < 1$, together with Lemma 1, we know $\sigma_{\tilde{k}} = \Theta(1)$[6]. Since $\tilde{\psi}$ is a constant, one can check that $\lambda_{\min,\tilde{k}} = \Theta(\epsilon)$, and $\lambda_{\max,\tilde{k}} = \Theta(\sqrt{1/\tilde{k}})$.

Note that $\|\bar{V}^\dagger\|_F^2 = r$. We assume that $\|\bar{V}^\dagger\|$ is column-incoherent [34] with some positive constant $\rho > 1$, i.e.,

$$\|\bar{V}^\dagger\|_{\infty,2} \le \sqrt{\rho r/p}. \tag{24}$$

We assume the number of PMU channels incident to each bus is in the range of $[d, Cd]$ for some $d > 0$ and some constant C. This is also the number of nonzero entries in each column of W with unit column-norm. Then $p = \Theta(dn)$, and we have

$$\epsilon = \|\bar{V}^\dagger W^\ddagger\|_{\infty,2} \le \sqrt{\frac{\rho r}{p}} \max_i \sum_j |W_{ij}| = O(\sqrt{\frac{r}{n}}). \tag{25}$$

Therefore, as long as $\tilde{k} = O(n/r)$, when n is sufficiently large, $\lambda_{\min,\tilde{k}} \le \lambda_{\max,\tilde{k}}$. $\tilde{k}\mu \le c$ requires that $\tilde{k} = O(1/\mu)$. Note that $\mu = \Theta(\frac{1}{d})$. Thus, if both $\tilde{k} = O(n/r)$ and $\tilde{k} = O(d)$ hold, then a proper λ exists, and Theorem 1 holds.

In the case that $d = \Theta(n)$, $\tilde{k}$ could be $\Theta(n/r)$. If r is a constant, our method succeeds even when a constant fraction of bus voltages are corrupted. Also consider the case that $\tilde{k} = 1$. We pick $\tilde{\psi}$ and c in (19) arbitrarily close to one, then $\lambda = 1$ is a proper choice (see Fig. 16 for results on actual PMU data) provided that $\epsilon + \mu \le 0.5$. Since ϵ scales as $1/\sqrt{n}$ and μ scales as $1/d$, the condition will be met in large systems that are tightly connected. Intuitively, μ is small if the bus degree is high, and the line impedances are in the same range.

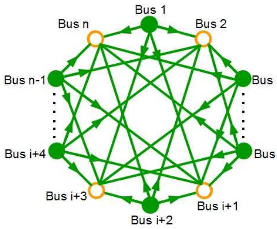


Fig. 6: n-bus ring network

We next use an example to illustrate the existence of proper λ. Consider an n-bus (n is even) ring network in Fig. 6. Each odd-numbered bus is connected to all even-numbered buses. There is no connection among odd buses and no connection among even-numbered buses. A PMU is installed on each odd bus and measures the corresponding voltage phasor and all incident line current phasors. For the simplicity of analysis, we assume $Z^{ij} = 1$ and $Y^{ij} = 0$ in this ring network. W is a $(\frac{n^2}{4} + \frac{n}{2}) \times n$ matrix with unit norm columns. Specifically, for every integer k,

$$W_{ij} = \begin{cases} \sqrt{2/(n+2)}, & \text{if } i \in \mathcal{I}_{k1} \text{ and } j = 2k-1 \\ -\sqrt{2/n}, & \text{if } i \in \mathcal{I}_{k2} \text{ and } j = 2k \\ 0, & \text{otherwise} \end{cases},$$

where

$$\mathcal{I}_{k1} := \left\{ k + (k-1)\frac{n}{2} + k' \mid \text{interger } k' = 0, 1, 2, ..., \frac{n}{2} \right\},$$

$$\mathcal{I}_{k2} := \left\{ k + 1 + (\frac{n}{2} + 1)k' \mid \text{interger } k' = 0, 1, 2, ..., \frac{n}{2} - 1 \right\}.$$

Note that $|\mathcal{I}_{k1}| = \frac{n}{2} + 1$, $|\mathcal{I}_{k2}| = \frac{n}{2}$ for all k. Here, $\mu = 2/\sqrt{n^2 + 2n}$. Then we have

$$(V^\dagger W^\ddagger)_j = \begin{cases} \sqrt{2/(n+2)} \sum_{i \in \mathcal{I}_{k1}} (V^\dagger)_i, & \text{if } j = 2k-1 \\ -\sqrt{2/n} \sum_{i \in \mathcal{I}_{k2}} (V^\dagger)_i, & \text{if } j = 2k \end{cases}, \tag{26}$$

where $V \in \mathbb{C}^{(\frac{n^2}{4} + \frac{n}{2}) \times r}$ contains the right singular vectors of the rank-r measurement matrix $\bar{L} \in \mathbb{C}^{t \times (\frac{n^2}{4} + \frac{n}{2})}$. If $\|\bar{V}^\dagger\|$ is column-incoherent [34] with some positive constant ρ, then

$$\begin{aligned} \epsilon = \|\bar{V}^\dagger W^\ddagger\|_{\infty,2} &\le \max\left(\sqrt{\frac{2}{n+2}}|\mathcal{I}_{k1}|, \sqrt{\frac{2}{n}}|\mathcal{I}_{k2}|\right) \cdot \|\bar{V}^\dagger\|_{\infty,2} \\ &\le \sqrt{\frac{n+2}{2}} \cdot \sqrt{\frac{\rho r}{(\frac{n}{2}+1)\frac{n}{2}}} \le \sqrt{\frac{2\rho r}{n}}, \end{aligned} \tag{27}$$

where the first inequality follows from (26), and the second inequality follows from (24).

To find λ, we pick $c = 1/4$ and $\tilde{\psi} = 1/8$. We choose $\tilde{k} = \frac{n}{48\rho r}$. One can check that (19) follows. Then

$$\tilde{k}\mu = \frac{n}{48\rho r} \times \frac{2}{\sqrt{n^2 + 2n}} \le \frac{1}{24\rho r} \le \frac{1}{24} \le \frac{1}{4} = c, \tag{28}$$

where the last inequality follows since $\rho > 1$ and $r \ge 1$. Then from Lemma 1, we have

$$\sigma_{\tilde{k}} \le (1 - (\tilde{k} - 1)\mu)^{-1} \le (1 - \tilde{k}\mu)^{-1} \le 24/23. \tag{29}$$

From (20) and (21),

$$\lambda_{\min,\tilde{k}} \le \frac{(1 + (2 - \tilde{\psi})^{-1})\epsilon}{1 - (1 + (2 - \tilde{\psi})^{-1})\tilde{k}\mu\sigma_{\tilde{k}}} \le \frac{23\epsilon}{14} \le \frac{23}{14}\sqrt{\frac{2\rho r}{n}}. \tag{30}$$

[5] Specially, the requirements on dual certificate in Lemma 4 are sufficient but not necessary. Furthermore, we use loose bounds in the proofs to simplify analysis. ϵ, μ, and σ_k are in turn defined based on worst-case scenarios.

[6] We use the notations $g(n) \in O(h(n))$, $g(n) \in \Omega(h(n))$, or $g(n) = \Theta(h(n))$ if as n goes to infinity, $g(n) \le c \cdot h(n)$, $g(n) \ge c \cdot h(n)$ or $c_1 \cdot h(n) \le g(n) \le c_2 \cdot h(n)$ eventually holds for some positive constants c, c_1 and c_2 respectively.

$$\lambda_{\max,\tilde{k}} = \sqrt{\frac{1/8}{\frac{n}{48\rho r}\sigma_{\tilde{k}}}} \geq \frac{1}{2}\sqrt{\frac{23\rho r}{n}}. \tag{31}$$

Since $\frac{23}{14}\sqrt{\frac{2\rho r}{n}} < \frac{1}{2}\sqrt{\frac{23\rho r}{n}}$, then $\lambda_{\min,\tilde{k}} < \lambda_{\max,\tilde{k}}$. Then there exists λ such that Method 1 correctly identifies the corruptions in up to $\tilde{k} = \frac{n}{48\rho r}$ bus voltages. In fact, any $\lambda \in [\frac{23}{14}\sqrt{\frac{2\rho r}{n}}, \frac{1}{2}\sqrt{\frac{23\rho r}{n}}]$ suffices. Note that for a constant r, $\tilde{k}$ is linear in n, the total number of buses.

C. Proof sketch of Theorem 1

The proof of Theorem 1 follows the same line as the proof of Theorem 1 in [34]. With the additional projection matrix W, our proof is more involved than the one in [34].

Like [34], we design the following Oracle Problem (32) by adding explicit constraints that the solution pair should have the correct column space of $\bar{L}$ and the correct column support of $\bar{C}$. The major step is to show that an optimal solution (L^*,C^*) to (13) is also an solution to the Oracle problem (32). Note that Oracle problem is only designed for analysis, since $\bar{U}$ and $\bar{\mathcal{I}}$ are unknown to the operator.

$$\begin{aligned} \text{Oracle Problem} \quad & \min_{L,C} \|L\|_* + \lambda\|C\|_{1,2} \\ & \text{s.t.} \quad M = L + CW^T \\ & \qquad \mathcal{P}_{\bar{U}}(L) = L,\, \mathcal{P}_{\bar{\mathcal{I}}}(C) = C. \end{aligned} \tag{32}$$

Let (L', C') be an optimal solution to the Oracle problem (32). We define $\mathcal{P}_{T'} := \mathcal{P}_{U'} + \mathcal{P}_{V'} - \mathcal{P}_{U'}\mathcal{P}_{V'}$, where the SVD of $L' = U'\Sigma' V'^{\dagger}$. Define

$$\begin{aligned} \mathfrak{G}(C') := \{H \in \mathbb{C}^{t\times k} \mid \forall i \in \mathcal{I}' : H_i = C'_i/\|C'_i\|; \\ \forall i \in \bar{\mathcal{I}} \cap (\mathcal{I}')^c : \|H_i\|_2 \leq 1\}, \end{aligned}$$

where $\mathcal{I}'$ is the column support of C'. We have

Lemma 2 (Lemma 4 and Lemma 5 of [34])**.**

$$U'U'^{\dagger} = \bar{U}\bar{U}^{\dagger}.$$

There exists an orthonormal matrix $\hat{V} \in \mathbb{C}^{t\times p}$ such that

$$U'V'^{\dagger} = \bar{U}\hat{V}^{\dagger}. \tag{33}$$

Also, we have

$$\mathcal{P}_{T'} := \mathcal{P}_{U'} + \mathcal{P}_{V'} - \mathcal{P}_{U'}\mathcal{P}_{V'} = \mathcal{P}_{\bar{U}} + \mathcal{P}_{\hat{V}} - \mathcal{P}_{\bar{U}}\mathcal{P}_{\hat{V}}.$$

The following lemma establishes that the solution to the Oracle problem (32) is also a solution to (13),

Lemma 3. *An optimal solution (L', C') to (32) is an optimal solution to (13) if there exists $Q \in \mathbb{C}^{t\times p}$ that satisfies*

$$\begin{aligned} & (a)\mathcal{P}_{T'}(Q) = U'V'^{\dagger}, \qquad (b)\|\mathcal{P}_{T'^{\perp}}(Q)\| \leq 1, \\ & (c)(QW^{\ddagger})_{\bar{\mathcal{I}}}/\lambda \in \mathfrak{G}(C'), \quad \textit{and } (d)\|(QW^{\ddagger})_{\bar{\mathcal{I}}^c}\|_{\infty,2} \leq \lambda. \end{aligned} \tag{34}$$

If both (b) and (d) are strict, and $\mathcal{P}_{\bar{\mathcal{J}}} \cap \mathcal{P}_{V'} = \{0\}$, then any optimal solution (L^*, C^*) to (13) satisfies $\mathcal{P}_{\bar{U}}(L^*) = L^*$, $\mathcal{P}_{\bar{\mathcal{I}}}(C^*) = C^*$.

The major technical step is to construct Q, called the *dual certificate*, that satisfies (34). Our construction method is as follows. Pick $\hat{H} \in \mathfrak{G}(C')$ that satisfies

$$\hat{V}^{\dagger}W^{\ddagger}_{\bar{\mathcal{I}}} = \lambda\bar{U}^{\dagger}\hat{H}. \tag{35}$$

Define

$$\Phi := \lambda\hat{H}(W^T_{\bar{\mathcal{I}}}W^{\ddagger}_{\bar{\mathcal{I}}})^{-1}W^T_{\bar{\mathcal{I}}},\ \Delta_1 := \mathcal{P}_{\bar{U}}(\Phi), \tag{36}$$

$$\Delta_2 := \mathcal{P}_{\bar{U}^{\perp}}(I - \mathcal{P}_{W_{\bar{\mathcal{I}}}})\mathcal{P}_{\hat{V}}(I + \sum_{i=1}^{\infty}(\mathcal{P}_{\hat{V}}\mathcal{P}_{W_{\bar{\mathcal{I}}}}\mathcal{P}_{\hat{V}})^i)\mathcal{P}_{\hat{V}}(\Phi), \tag{37}$$

$$\text{where } \mathcal{P}_{W_{\bar{\mathcal{I}}}}(X) := XW^{\ddagger}_{\bar{\mathcal{I}}}(W^T_{\bar{\mathcal{I}}}W^{\ddagger}_{\bar{\mathcal{I}}})^{-1}W^T_{\bar{\mathcal{I}}}. \tag{38}$$

$$Q := \bar{U}\hat{V}^{\dagger} + \Phi - \Delta_1 - \Delta_2. \tag{39}$$

We show that Q in (39) is well defined in Appendix-B. Lemma 4 shows that Q in (39) is the desired dual certificate.

Lemma 4. *Suppose there exists nonzero $\tilde{k}$ such that $\tilde{k}\mu \leq c$ for c in (19), and $\lambda_{\min,\tilde{k}} \leq \lambda_{\max,\tilde{k}}$ with $\lambda_{\min,\tilde{k}}$ and $\lambda_{\max,\tilde{k}}$ defined in (20) and (21). Then as long as the column support of $\bar{C}$ has size at most $\tilde{k}$, for any $\lambda \in [\lambda_{\min,\tilde{k}}, \lambda_{\max,\tilde{k}}]$, Q defined in (39) satisfies (34).*

Theorem 1 follows when we combine Lemmas 3 and 4. Please refer to the Appendix for the proofs.

IV. Attack Identification with Noise

We now analyze the detection performance when M contains noise ($N \neq 0$) with $\|N\|_F \leq \eta$. Given k, define

$$\lambda'_{\min,k} = \frac{(1 + (2-\tilde{\psi})^{-1})\epsilon}{1/2 - (1 + (2-\tilde{\psi})^{-1})k\sigma\mu}, \text{ and } \lambda'_{\max,k} = \frac{1}{2}\sqrt{\frac{\tilde{\psi}}{k\sigma_k}}.$$

Theorem 2. *Suppose there exists nonzero $\tilde{k}$ such that $\tilde{k}\mu \leq c$ for c in (19), and $\lambda'_{\min,\tilde{k}} \leq \lambda'_{\max,\tilde{k}}$. Then if column support size of $\bar{C}$ is at most $\tilde{k}$, for any $\lambda \in [\lambda'_{\min,\tilde{k}}, \lambda'_{\max,\tilde{k}}]$, there exists a pair $(\tilde{L}, \tilde{C})$, where $\tilde{L} + \tilde{C}W^T = \bar{L} + \bar{C}W^T$, $\mathcal{P}_{\bar{U}}(\tilde{L}) = \tilde{L}$ and $\mathcal{P}_{\bar{\mathcal{I}}}(\tilde{C}) = \tilde{C}$, such that the output of Method 1 satisfies*

$$\begin{aligned} & \|L^* - \tilde{L}\|_F \\ \leq & (2 - \tilde{\psi} + \frac{\lambda + (2-\tilde{\psi})\sqrt{1+(n-1)\mu}}{\lambda}\sqrt{\theta + 3r})\frac{2\eta}{1-\tilde{\psi}}, \end{aligned} \tag{40}$$

and $\|C^* - \tilde{C}\|_F$

$$\begin{aligned} \leq & (1 + (\frac{\lambda + \sqrt{1+(n-1)\mu}}{\lambda} + \frac{1-\tilde{\psi}}{\lambda\sigma_k\sqrt{1+(k-1)\mu}})\sqrt{\theta+3r}) \\ & \frac{2\eta\sigma_k\sqrt{1+(k-1)\mu}}{1-\tilde{\psi}}, \end{aligned} \tag{41}$$

where $\theta := \min(t, p)$.

The discussion of the existence of λ is very similar to the discussion for Theorem 1, so we skip it. If $\tilde{k}\mu \leq c$ and $\tilde{k} = O(n/r)$ hold, then a proper λ exists. Theorem 2 guarantees that (L^*, C^*) returned by Method 1 is "close" to a pair that has the correct column space and column support, and the distance measured by Frobenius norm is proportional to the noise level η. The proof of Theorem 2 follows the same line as the proof of Theorem 2 in [34] mostly with modifications to address the projection matrix W. We establish Lemma 5, a counterpart in the noisy case of Lemma 3, that demonstrates that Method 1 succeeds if there exists a dual certificate Q with tighter requirements than that in the noiseless case.

Lemma 5. *There exists* $(\tilde{L}, \tilde{C})$ *where* $\tilde{L}+\tilde{C}W^T = \bar{L}+\bar{C}W^T$, $\mathcal{P}_{\bar{U}}(\tilde{L}) = \tilde{L}$, $\mathcal{P}_{\bar{\mathcal{I}}}(\tilde{C}) = \tilde{C}$, *such that the output of Method 1 satisfies (40) and (41), if there exists* $Q \in \mathbb{C}^{t\times p}$ *that satisfies*

$$(a)\mathcal{P}_{\bar{T}}(Q) = \bar{U}\bar{V}^{\dagger}, \qquad (b)\|\mathcal{P}_{\bar{T}^{\perp}}(Q)\| \leq 1/2,$$
$$(c)(QW^{\ddagger})_{\bar{\mathcal{I}}}/\lambda \in \mathfrak{G}(\bar{C}), \quad \textit{and } (d)\|(QW^{\ddagger})_{\bar{\mathcal{I}}^c}\|_{\infty,2} \leq \lambda/2. \tag{42}$$

The construction of Q is the same as that in Section III (equations (35) to (39)). We show that Q is the desire dual certificate if λ belongs to $[\lambda'_{\min}, \lambda'_{\max}]$ in Lemma 6.

Lemma 6. *If the column support size of* $\bar{C}$ *is at most* $\tilde{k}$, *then for any* $\lambda \in [\lambda'_{\min}, \lambda'_{\max}]$, *Q defined in (39) satisfies (42).*

Theorem 2 follows when we combine Lemmas 5 and 6. Please refer to the Appendix for the proofs.

V. Simulation

We explore the performance of data attack identification methods on both synthetic data and actual PMU data from the Central NY power system. We use CVX [13] to solve (13). We identify a column of C^* to be nonzero if its ℓ_2 norm exceeds the predefined threshold ϵ_1. Method 1 succeeds if $\|U^*U^{*\dagger} - \bar{U}\bar{U}^{\dagger}\| \leq \epsilon_2$ for some small positive ϵ_2, and the column supports of $\bar{C}$ and C^* are the same.

A. Performance on synthetic data

Fix $t = p = 50$. Given rank r, we generate matrices $A \in \mathbb{R}^{t\times r}$ and $B \in \mathbb{R}^{p\times r}$ with each entry independently drawn from Gaussian $\mathcal{N}(0, 1)$ and set $\bar{L} := AB^T$. We generate matrix $W \in \mathbb{R}^{p\times n}$ with independent $\mathcal{N}(0, 1)$ entries. To generate a column-sparse matrix $\bar{C} \in \mathbb{R}^{t\times n}$, we randomly select the column support and set the nonzero entries to be independent $\mathcal{N}(0, 1)$. We vary r and the number of corrupted columns, and take 100 runs for each case. λ is set to be 0.95.

1) Noiseless formulation: We simulate the observed measurement matrix M according to (8) with $N = 0$. We apply Method 1 to obtain the estimation (L^*, C^*). We set ϵ_1 and ϵ_2 to be 0.002 and 0.01, respectively. Fig. 7 shows the transition property of Method 1 in gray scale. White stands for 100% success while black denotes 100% failure. When n is 25, W is a tall matrix ($p > n$). When n is 100, W is a flat matrix ($p < n$). For both simulations, the identification is successful even when rank r is six, and $\bar{C}$ has two nonzero columns.

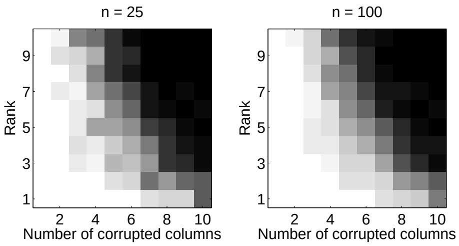


Fig. 7: Matrix decomposition performance for different n

We further assume some of the observations are missing. We generate M as before and then delete some randomly selected entries. Fig. 8 shows the decomposition performance of Method 1 for partial observation. We can see that the successful decomposition rate is close to the complete observation case even only 80% of the entries are observed.

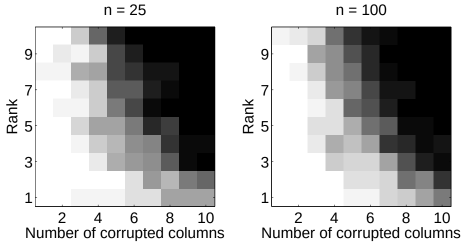


Fig. 8: Matrix decomposition performance for different n with 80% observed entries

2) Noisy formulation: We generate matrix $N \in \mathbb{R}^{t\times p}$ with independent Gaussian $\mathcal{N}(0, \sigma^2)$ entries. We fix the matrix rank r to be 3 and the number of corrupted columns to be 3. We simulate the observed measurement matrix M according to (8). We set η to be $\|N\|_F$ and apply Method 1 to obtain the estimation (L^*, C^*). ϵ_1 is set to be 0.001.

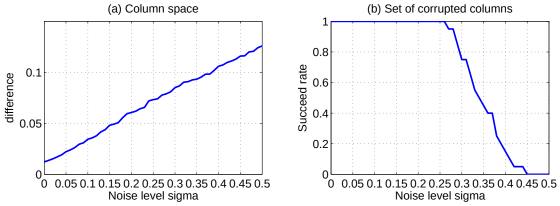


Fig. 9: Performance of Method 1 for different noise level σ

Fig. 9 shows the difference between the original and reconstructed column space ($\|U^*U^{*\dagger} - \bar{U}\bar{U}^{\dagger}\|$) and the succeed rate for determining the set of corrupted columns according to different noise level σ. We can see that Method 1 can successfully identify the corrupted columns when the noise level σ is below 0.25. Method 1 can recover the column space with small errors when σ is smaller than 0.1.

B. Comparison with other methods on synthetic data

1) $\bar{D} = \bar{C}W^T$ *is column-sparse:* Refs. [34] [22] considered matrix decomposition problem when $\bar{D}$ is column-sparse and scattered-sparse, respectively. We compare our method with them in the special case that $\bar{D} = \bar{C}W^T$ is column-sparse. Fix $t = p = 50$, $n = 20$, and $r = 2$. We generate $\bar{L}$ and $\bar{C}$ with the same rules as in Section V-A. We generate a binary matrix $W \in \mathbb{R}^{p\times n}$ with two '1's each row and five '1's each column. Then the ratio of support sizes of $\bar{D}$ and $\bar{C}$ is about five. $\bar{D}$ is column-sparse when $\bar{C}$ is column-sparse. We simulate the measurement matrix M according to (8) with $N = 0$. λ in our method is set to be 0.9. λ's in methods of [34] and [22] are set to be 0.5 and 0.1, respectively.

Fig. 10 shows the success rates of three methods with different support sizes of $\bar{C}$. Our method performs the best since we exploit the structure $\bar{D} = \bar{C}W^T$ besides sparsity. The false alarm rate of our method is zero.

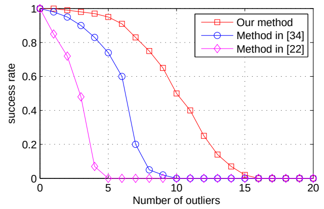


Fig. 10: Success rates when $\bar{D} = \bar{C}W^T$ is column-sparse.

2) Combination of attack patterns.: We consider the general case that the attacks satisfy (14). We use the generalized version in (15)-(16) to detect combined attacks. λ_1 and λ_2 in (15) are set to be 1 and 0.1, respectively. λ's in methods of [34] and [22] are set to be 0.5 and 0.1, respectively. $\bar{L}$, $\bar{C}$, and W are generated the same as above. $\bar{S}$ is a sparse matrix with nonzero entries independently drawn from $\mathcal{N}(0, 1)$. We define the correct estimation of the column space of $\bar{L}$ as a successful recovery. Fig. 11 compares the methods when $\bar{C}$ is a zero matrix. The attacks are scattered-sparse, and our method performs as well as that in [22]. Fig. 12 compares the methods when both column-sparse and scattered-sparse attacks exist. Besides a sparse $\bar{S}$, we randomly select two columns in $\bar{C}$ and select their entries independently from $\mathcal{N}(0, 1)$. Only our method succeeds when both attacks exist.

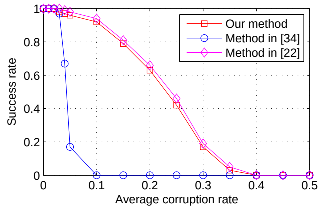


Fig. 11: Success rates when $\bar{D} = \bar{S}$ is scattered-sparse.

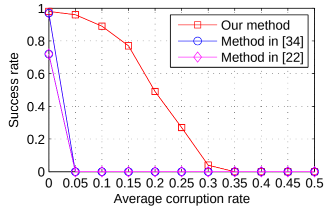


Fig. 12: Success rates when $\bar{D} = \bar{C}W^T + \bar{S}$.

C. Performance comparison on actual PMU data

We consider the PMU data shown in Section II-A. Two two-second PMU datasets are tested. One contains ambient data, and the other contains an abnormal event ($t = 17 - 19s$ and $t = 2 - 4s$ in Fig. 2, respectively). We first inject data attacks as an intruder and then use Method 1 to detect the attacks.

We consider the scenario that an intruder alters the PMU channels that measure I^{12},I^{52},I^{13} and I^{43} in order to corrupt voltage estimations of Buses 2 and 3. Fig. 13 visualizes the actual PMU data and the data after the injection of attacks for two 2-second datasets. η and λ are set to be 5 and 1 respectively in Method 1. Fig. 14 shows the ℓ_2 norm of each column of the resulting $\bar{D}$ matrix. The columns with significant ℓ_2 norm correspond to channels that measure I^{12},I^{52},I^{13} and I^{43}. Therefore, our method successfully identifies the four PMU channels under attack. We repeat the same experiment when an intruder alters the channels that measure V^5, I^{52}, I^{54}, I^{59}, and I^{45} to corrupt voltage estimation of Buses 5. Fig. 15 shows the ℓ_2 norm of each column of the resulting $\bar{C}$ matrix in this case. The column with significant ℓ_2 norm corresponds Bus 5. Thus the recovery is also successful.

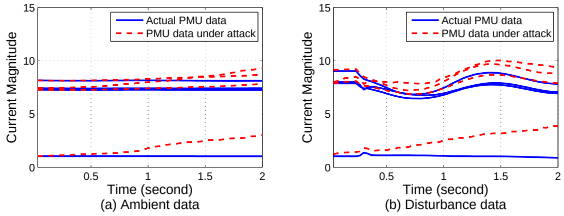


Fig. 13: The actual PMU data and PMU data under attack

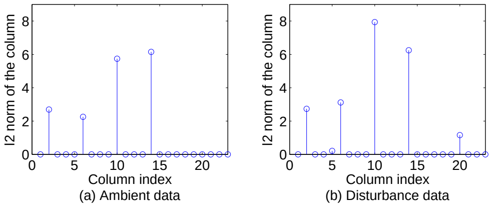


Fig. 14: ℓ_2 norm of each column of $\bar{D}$

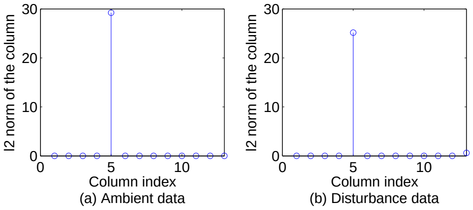


Fig. 15: ℓ_2 norm of each column of $\bar{C}$

Fig. 16 compares our method and that in [34] on the ambient PMU data. Given support size of $\bar{C}$, the result is averaged over all possible attack locations. Our method outperforms [34] because we exploit (7) to reduce the degree of freedom in $\bar{D}$. For example, 7 out of 23 channels needs to be attacked to change the state of Bus 1. That means 30% of the columns of $\bar{D}$ are nonzero. This high percentage of corruption in $\bar{D}$ cannot be handedly by [34].

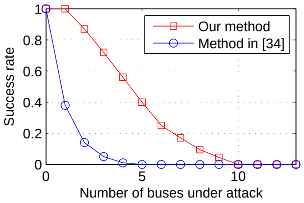


Fig. 16: Success rates with varying support size of $\bar{C}$, or equivalently, the number of affected system states.

VI. Conclusion

We address the problem of detecting successive unobservable cyber data attacks to PMU measurements. We formulate the identification problem as a matrix decomposition problem of a low-rank matrix and a transformed column-sparse matrix. We propose a convex-optimization-based method and provide its theoretical guarantee. Although motivated by power system monitoring, our results on matrix decomposition can be applied to other scenarios. One future direction is the analysis of the detection performance when some of the measurements are lost during the communication to the central operator.

Acknowledgement

We thank New York Power Authority for providing PMU data for the Central NY Power System. This research is supported in part by the ERC Program of NSF and DoE under the supplement to NSF Award EEC-1041877 and the CURENT Industry Partnership Program, and in part by NSF Grant 1508875, NYSERDA Grants #36653 and #28815.

References

[1] A. Abur and A. G. Exposito, *Power system state estimation: theory and implementation*. CRC Press, 2004.

[2] R. Basri and D. W. Jacobs, "Lambertian reflectance and linear subspaces," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 25, no. 2, pp. 218–233, 2003.

[3] R. B. Bobba, K. M. Rogers, Q. Wang, H. Khurana, K. Nahrstedt, and T. J. Overbye, "Detecting false data injection attacks on DC state estimation," in *Proc. the First Workshop on Secure Control Systems (SCS)*, 2010.

[4] E. J. Candès, X. Li, Y. Ma, and J. Wright, "Robust principal component analysis?" *Journal of the ACM (JACM)*, vol. 58, no. 3, p. 11, 2011.

[5] V. Chandrasekaran, S. Sanghavi, P. A. Parrilo, and A. S. Willsky, "Rank-sparsity incoherence for matrix decomposition," *SIAM Journal on Optimization*, vol. 21, no. 2, pp. 572–596, 2011.

[6] J. Chen and A. Abur, "Placement of PMUs to enable bad data detection in state estimation," *IEEE Trans. Power Syst.*, vol. 21, no. 4, pp. 1608–1615, 2006.

[7] Y. Chen, L. Xie, and P. Kumar, "Dimensionality reduction and early event detection using online synchrophasor data," in *Proc. IEEE Power and Energy Society General Meeting*, 2013, pp. 1–5.

[8] N. Dahal, R. L. King, and V. Madani, "Online dimension reduction of synchrophasor data," in *Proc. IEEE PES Transmission and Distribution Conference and Exposition (T&D)*, 2012, pp. 1–7.

[9] G. Dán and H. Sandberg, "Stealth attacks and protection schemes for state estimators in power systems," in *Proc. IEEE International Conference on Smart Grid Communications (SmartGridComm)*, 2010, pp. 214–219.

[10] J. P. Finn, K. Nael, V. Deshpande, O. Ratib, and G. Laub, "Cardiac MR imaging: State of the technology1," *Radiology*, vol. 241, no. 2, pp. 338–354, 2006.

[11] H. Gao, J.-F. Cai, Z. Shen, and H. Zhao, "Robust principal component analysis-based four-dimensional computed tomography," *Physics in medicine and biology*, vol. 56, no. 11, p. 3181, 2011.

[12] P. Gao, M. Wang, S. Ghiocel, and J. H. Chow, "Modeless reconstruction of missing synchrophasor measurements," in *Proc. IEEE PES General Meeting (selected in Best Papers Sessions)*, 2014.

[13] M. Grant and S. Boyd, "CVX: Matlab software for disciplined convex programming, version 1.21," http://cvxr.com/, Oct. 2010.

[14] E. Handschin, F. Schweppe, J. Kohlas, and A. Fiechter, "Bad data analysis for power system state estimation," *IEEE Trans. Power App. Syst.*, vol. 94, no. 2, pp. 329–337, 1975.

[15] C. Herridge, M. Levine, M. Emanuel, and M. Oinounou, "Sources: Staged cyber attack reveals vulnerability in power grid," http://www.foxnews.com/politics/2009/04/08/cyberspies-penetrate-power-grid-leave-software-disrupt/, 2009.

[16] R. A. Horn and C. R. Johnson, *Matrix analysis*. Cambridge university press, 2012.

[17] T. Kim and H. Poor, "Strategic protection against data injection attacks on power grids," *IEEE Trans. Smart Grid*, vol. 2, no. 2, pp. 326–333, 2011.

[18] O. Kosut, L. Jia, R. Thomas, and L. Tong, "Malicious data attacks on smart grid state estimation: Attack strategies and countermeasures," in *Proc. IEEE International Conference on Smart Grid Communications (SmartGridComm)*, 2010, pp. 220–225.

[19] A. Lakhina, M. Crovella, and C. Diot, "Diagnosing network-wide traffic anomalies," in *ACM SIGCOMM Computer Communication Review*, vol. 34, no. 4, 2004, pp. 219–230.

[20] Y. Li and D. Wang, "Separation of singing voice from music accompaniment for monaural recordings," *IEEE Trans. Audio, Speech, Language Process.*, vol. 15, no. 4, pp. 1475–1487, 2007.

[21] Z. Lin, A. Ganesh, J. Wright, L. Wu, M. Chen, and Y. Ma, "Fast convex optimization algorithms for exact recovery of a corrupted low-rank matrix," *Computational Advances in Multi-Sensor Adaptive Processing (CAMSAP)*, vol. 61, 2009.

[22] L. Liu, M. Esmalifalak, Q. Ding, V. A. Emesih, and Z. Han, "Detecting false data injection attacks on power grid by sparse optimization," *IEEE Trans. Smart Grid*, vol. 5, no. 2, pp. 612–621, 2014.

[23] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Transactions on Information and System Security (TISSEC)*, vol. 14, no. 1, p. 13, 2011.

[24] M. Mardani, G. Mateos, and G. Giannakis, "Recovery of low-rank plus compressed sparse matrices with application to unveiling traffic anomalies," *IEEE Trans. Inf. Theory*, vol. 59, no. 8, pp. 5186–5205, 2013.

[25] H. M. Merrill and F. C. Schweppe, "Bad data suppression in power system static state estimation," *IEEE Trans. Power App. Syst.*, no. 6, pp. 2718–2725, 1971.

[26] J. Meserve, "Sources: Staged cyber attack reveals vulnerability in power grid," http://www.cnn.com/2007/US/09/26/power.at.risk/, 2007.

[27] A. Monticelli and A. Garcia, "Reliable bad data processing for real-time state estimation," *IEEE Trans. Power App. Syst.*, no. 5, pp. 1126–1139, 1983.

[28] B. Recht, M. Fazel, and P. A. Parrilo, "Guaranteed minimum-rank solutions of linear matrix equations via nuclear norm minimization," *SIAM Rev.*, vol. 52, no. 3, pp. 471–501, 2010.

[29] H. Sandberg, A. Teixeira, and K. H. Johansson, "On security indices for state estimators in power networks," in *Proc. the First Workshop on Secure Control Systems (SCS)*, 2010.

[30] H. Sedghi and E. Jonckheere, "Statistical structure learning of smart grid for detection of false data injection," in *Proc. IEEE Power and Energy Society General Meeting (PES)*, 2013, pp. 1–5.

[31] A. Tajer, S. Kar, H. V. Poor, and S. Cui, "Distributed joint cyber attack detection and state recovery in smart grids," in *Proc. IEEE International Conference on Smart Grid Communications (SmartGridComm)*, 2011, pp. 202–207.

[32] M. Thottan and C. Ji, "Anomaly detection in IP networks," *IEEE Trans. Signal Process.*, vol. 51, no. 8, pp. 2191–2204, 2003.

[33] M. Wang, P. Gao, S. Ghiocel, J. H. Chow, B. Fardanesh, G. Stefopoulos, and M. P. Razanousky, "Identification of "unobservable" cyber data attacks on power grids," in *Proc. IEEE SmartGridComm*, 2014.

[34] H. Xu, C. Caramanis, and S. Sanghavi, "Robust PCA via outlier pursuit," *IEEE Trans. Inf. Theory*, vol. 58, no. 5, pp. 3047–3064, May 2012.

[35] W. Xu, M. Wang, J. Cai, and A. Tang, "Sparse error correction from nonlinear measurements with applications in bad data detection for power networks," *IEEE Trans. Signal Process.*, vol. 61, no. 24, pp. 6175–6187, 2013.

Appendix

A. Proof of Lemma 1

Proof: We first state the following result that will be used in the proof.

Lemma 7 (Geršhgorin circle theorem [16])**.** *Let A be a complex $n \times n$ matrix, with entries a_{ij}. Then, every eigenvalue of A lies within at least one of the Geršhgorin discs $D_i(A) (i = 1, ..., n)$, where $D_i(A) := \{z \in \mathbb{C} : |z - a_{ii}| \leq \sum_{j \neq i} |a_{ij}|\}$.*

For any given $\mathcal{I}$ with $|\mathcal{I}| \leq k$, since W has unit-norm columns, and $|W_i^\dagger W_j| \leq \mu$ for all $i \neq j$, from Geršhgorin circle theorem, we have $\|I - W_{\mathcal{I}}^\dagger W_{\mathcal{I}}\| \leq (k-1)\mu < 1$, where the last inequality follows from $k\mu < 1$. Then,

$$\begin{aligned}\|(W_{\mathcal{I}}^\dagger W_{\mathcal{I}})^{-1}\| =& \| \sum_{i=0}^{\infty} (I - W_{\mathcal{I}}^\dagger W_{\mathcal{I}})^i \| \leq \sum_{i=0}^{\infty} \|(I - W_{\mathcal{I}}^\dagger W_{\mathcal{I}})^i\| \\ \leq& 1/(1-(k-1)\mu).\end{aligned}$$

The lemma follows from the definition of σ_k. ■

B. Proof of Lemma 3

Proof: For any $\Delta \in \mathbb{C}^{t\times n}$, $\langle L' + \Delta W^T, C' - \Delta\rangle$ is feasible to (13). Let G be such that $\|G\| = 1$, $\left\langle G, \mathcal{P}_{T'^{\perp}}(\Delta W^T)\right\rangle = \|\mathcal{P}_{T'^{\perp}}(\Delta W^T)\|_*$ and $\mathcal{P}_{T'}(G) = 0$. Then $\mathcal{P}_{T'}(Q) + G$ is a subgradient of $\|L'\|_*$. Let F be such that $F_i = -\Delta_i/\|\Delta_i\|_2$ if $i \in \bar{\mathcal{I}}^c$ and $\Delta_i \neq \mathbf{0}$, and $F_i = \mathbf{0}$ otherwise. Then $\mathcal{P}_{\bar{\mathcal{I}}}(QW^{\ddagger})/\lambda + F$ is a subgradient of $\|C'\|_{1,2}$. Then

$$\begin{aligned}
&\|L' + \Delta W^T\|_* + \lambda\|C' - \Delta\|_{1,2} - \|L'\|_* - \lambda\|C'\|_{1,2}\\
\geq&\langle \mathcal{P}_{T'}(Q) + G, \Delta W^T\rangle - \lambda\langle \mathcal{P}_{\bar{\mathcal{I}}}(QW^{\ddagger})/\lambda + F, \Delta\rangle\\
=&\|\mathcal{P}_{T'^{\perp}}(\Delta W^T)\|_* + \lambda\|\mathcal{P}_{\bar{\mathcal{I}}^c}(\Delta)\|_{1,2} + \langle Q - \mathcal{P}_{T'^{\perp}}(Q), \Delta W^T\rangle\\
&- \langle QW^{\ddagger} - \mathcal{P}_{\bar{\mathcal{I}}^c}(QW^{\ddagger}), \Delta\rangle\\
\geq&(1 - \|\mathcal{P}_{T'^{\perp}}(Q)\|)\|\mathcal{P}_{T'^{\perp}}(\Delta W^T)\|_*\\
&+ (\lambda - \|(QW^{\ddagger})_{\bar{\mathcal{I}}^c}\|_{\infty,2})\|\mathcal{P}_{\bar{\mathcal{I}}^c}(\Delta)\|_{1,2}\\
\geq&0
\end{aligned} \tag{43}$$

From (43), $\langle L', C'\rangle$ is an optimal solution to (13). If (34) holds with strict inequality, the last inequality of (43) is strict unless

$$\|\mathcal{P}_{T'^{\perp}}(\Delta W^T)\|_* = \|\mathcal{P}_{\bar{\mathcal{I}}^c}(\Delta)\|_{1,2} = 0. \tag{44}$$

(44) implies that $\Delta W^T \in \mathcal{P}_{T'}$ and $\Delta \in \mathcal{P}_{\bar{\mathcal{I}}}$. Note that $\Delta \in \mathcal{P}_{\bar{\mathcal{I}}}$ implies that $\Delta W^T \in \mathcal{P}_{\bar{\mathcal{J}}}$. Then

$$\begin{aligned}
\mathcal{P}_{\bar{\mathcal{J}}}(\Delta W^T) = \Delta W^T &= \mathcal{P}_{T'}(\Delta W^T)\\
&= \mathcal{P}_{U'}(\Delta W^T) + \mathcal{P}_{V'}\mathcal{P}_{U'^{\perp}}(\Delta W^T)\\
&= \mathcal{P}_{\bar{\mathcal{J}}}\mathcal{P}_{U'}(\Delta W^T) + \mathcal{P}_{V'}\mathcal{P}_{U'^{\perp}}(\Delta W^T),
\end{aligned} \tag{45}$$

where the last equality holds since $\mathcal{P}_{\bar{\mathcal{J}}}(\Delta W^T) = \Delta W^T$. Thus, from (45) we have $\mathcal{P}_{\bar{\mathcal{J}}}\mathcal{P}_{U'^{\perp}}(\Delta W^T) = \mathcal{P}_{V'}\mathcal{P}_{U'^{\perp}}(\Delta W^T)$, which means $\mathcal{P}_{U'^{\perp}}(\Delta W^T) \in \mathcal{P}_{\bar{\mathcal{J}}} \cap \mathcal{P}_{V'}$. Then $\mathcal{P}_{U'^{\perp}}(\Delta W^T)$ is 0 from the assumption. Then, $\mathcal{P}_{\bar{U}}(\Delta W^T) = \mathcal{P}_{U'}(\Delta W^T) = \Delta W^T$, where the first equality holds from (33). Therefore, for any optimal solution $\langle L' + \Delta W^T, C' - \Delta\rangle$ for some $\Delta \neq 0$ to (13), $\Delta W^T \in \mathcal{P}_{\bar{U}}$, and $\Delta \in \mathcal{P}_{\bar{\mathcal{I}}}$. The claim follows. ■

C. Construction of Q

Here we demonstrate that Q in (39) is well defined. The key is to show (a) there exists $\hat{H} \in \mathfrak{G}(C')$ such that (35) holds, and (b) the infinite sum in (37) converges. We prove these two properties through the following lemmas.

Lemma 8. *There exists $\hat{H} \in \mathfrak{G}(C')$ such that (35) holds.*

Proof. Since $\langle L', C'\rangle$ is an optimal solution to the Oracle problem (32), there exists $G', A' \in \mathbb{C}^{t\times p}$, $B', Z \in \mathbb{C}^{t\times n}$, and some $\hat{H} \in \mathfrak{G}(C)$ such that

$$(\bar{U}\hat{V}^{\dagger} + G' + \mathcal{P}_{\bar{U}^{\perp}}(A'))W^{\ddagger} = \lambda(\hat{H} + Z) + \mathcal{P}_{\mathcal{I}^c}(B'), \tag{46}$$

where $\mathcal{P}_{T'^{\perp}}(G') = 0$ and $\mathcal{P}_{\mathcal{I}}(Z) = 0$. Then

$$\mathcal{P}_{\bar{U}}\mathcal{P}_{\bar{\mathcal{I}}}(((\bar{U}\hat{V}^{\dagger} + G' + \mathcal{P}_{\bar{U}^{\perp}}(A'))W^{\ddagger}) = \bar{U}\hat{V}^{\dagger}W^{\ddagger}_{\bar{\mathcal{I}}}, \tag{47}$$

$$\mathcal{P}_{\bar{U}}\mathcal{P}_{\bar{\mathcal{I}}}(\lambda(\hat{H}+Z)+\mathcal{P}_{\mathcal{I}^c}(B')) = \lambda\mathcal{P}_{\bar{U}}\mathcal{P}_{\bar{\mathcal{I}}}(\hat{H}) = \lambda\bar{U}\bar{U}^{\dagger}\hat{H} \tag{48}$$

Combining (46)-(48), we have

$$\bar{U}\hat{V}^{\dagger}W^{\ddagger}_{\bar{\mathcal{I}}} = \lambda\bar{U}\bar{U}^{\dagger}\hat{H}. \tag{49}$$

By multiplying $\bar{U}^{\dagger}$ to both sides of (49), we obtain Lemma 8. □

Lemma 9.

$$\psi := \|\mathcal{P}_{\hat{V}}\mathcal{P}_{W_{\bar{\mathcal{I}}}}\mathcal{P}_{\hat{V}}\| \leq \tilde{\psi} < 1$$

Proof.

$$\begin{aligned}
&\|\mathcal{P}_{\hat{V}}\mathcal{P}_{W_{\bar{\mathcal{I}}}}\mathcal{P}_{\hat{V}}(X)\|\\
=&\|X\hat{V}\hat{V}^{\dagger}W^{\ddagger}_{\bar{\mathcal{I}}}(W^T_{\bar{\mathcal{I}}}W^{\ddagger}_{\bar{\mathcal{I}}})^{-1}W^T_{\bar{\mathcal{I}}}\hat{V}\hat{V}^{\dagger}\|\\
\overset{\text{(a)}}{=}&\|X\hat{V}(\lambda\bar{U}^{\dagger}\hat{H})(W^T_{\bar{\mathcal{I}}}W^{\ddagger}_{\bar{\mathcal{I}}})^{-1}(\lambda\bar{U}^{\dagger}\hat{H})^{\dagger}\hat{V}^{\dagger}\|\\
\leq&\|X\|\|\hat{V}\bar{U}^{\dagger}\|\|\lambda\hat{H}\|\|(W^{\dagger}_{\bar{\mathcal{I}}}W_{\bar{\mathcal{I}}})^{-1}\|\|\lambda\hat{H}^{\dagger}\|\|\bar{U}\hat{V}^{\dagger}\|\\
\overset{\text{(b)}}{\leq}&\|X\| \cdot 1 \cdot \lambda\sqrt{k} \cdot \sigma_k \cdot \lambda\sqrt{k} \cdot 1\\
\overset{\text{(c)}}{\leq}&\|X\|\lambda_{\max}\tilde{k}\sigma_{\tilde{k}} \overset{\text{(d)}}{=} \|X\|\tilde{\psi},
\end{aligned}$$

where (a) follows from Lemma 8, (b) follows from the fact that $\hat{H}$ has at most k nonzero columns with unit-norm, (c) follows from the property that $\lambda \leq \lambda_{\max}$, $k \leq \tilde{k}$ and $\sigma_k \leq \sigma_{\tilde{k}}$, and (d) follows from the definition of $\tilde{\psi}$. Then Lemma 9 follows. □

Lemma 10. *$\mathcal{P}_{\hat{V}}(I - \mathcal{P}_{W_{\bar{\mathcal{I}}}})\mathcal{P}_{\hat{V}}$ is an injection from $\mathcal{P}_{\hat{V}}$ to $\mathcal{P}_{\hat{V}}$, and its inverse operation is $(I + \sum_{i=1}^{\infty}(\mathcal{P}_{\hat{V}}\mathcal{P}_{W_{\bar{\mathcal{I}}}}\mathcal{P}_{\hat{V}})^i)$.*

Proof. Since $\|\mathcal{P}_{\hat{V}}\mathcal{P}_{W_{\bar{\mathcal{I}}}}\mathcal{P}_{\hat{V}}\| < 1$ from Lemma 9, then $(I + \sum_{i=1}^{\infty}(\mathcal{P}_{\hat{V}}\mathcal{P}_{W_{\bar{\mathcal{I}}}}\mathcal{P}_{\hat{V}})^i)$ is well defined. For any $X \in \mathcal{P}_{\hat{V}}$, we have

$$\begin{aligned}
&\mathcal{P}_{\hat{V}}(I - \mathcal{P}_{W_{\bar{\mathcal{I}}}})\mathcal{P}_{\hat{V}}(I + \sum_{i=1}^{\infty}(\mathcal{P}_{\hat{V}}\mathcal{P}_{W_{\bar{\mathcal{I}}}}\mathcal{P}_{\hat{V}})^i)(X)\\
=&\mathcal{P}_{\hat{V}}(I - \mathcal{P}_{\hat{V}}\mathcal{P}_{W_{\bar{\mathcal{I}}}}\mathcal{P}_{\hat{V}})(I + \sum_{i=1}^{\infty}(\mathcal{P}_{\hat{V}}\mathcal{P}_{W_{\bar{\mathcal{I}}}}\mathcal{P}_{\hat{V}})^i)(X)\\
=&\mathcal{P}_{\hat{V}}(X) = X.
\end{aligned} \tag{50}$$

Then the lemma follows. □

D. Proof of Lemma 4

Proof. We need to show that Q defined in (39) satisfies all the conditions in (34). We first summarize some properties that will be used in the proof. Since W has unit-norm columns, $|W_i^{\dagger}W_j| \leq \mu$ for all $i \neq j$, and $|\bar{\mathcal{I}}| \leq k$, we have

$$\|W_{\bar{\mathcal{I}}}\| = \sqrt{\lambda_{\max}(W^{\dagger}_{\bar{\mathcal{I}}}W_{\bar{\mathcal{I}}})} \leq \sqrt{1 + (k-1)\mu}, \tag{51}$$

where the inequality follows from the Geršhgorin circle theorem. From $|\bar{\mathcal{I}}| \leq k$ and $|W_i^{\dagger}W_j| \leq \mu$ for all $i \neq j$, we have $\|(W^{\dagger}_{\bar{\mathcal{I}}}W_{\bar{\mathcal{I}}^c})\|_{\infty,2} \leq \sqrt{k}\mu$. Since $\hat{H}$ has at most k unit-norm columns while other columns are zero, we have

$$\|\lambda\hat{H}\| \leq \lambda\sqrt{k}. \tag{52}$$

Step 1: verification of (a) of (34).

$$\mathcal{P}_{U'}(Q) \overset{\text{(a)}}{=} \mathcal{P}_{\bar{U}}(Q) = \bar{U}\hat{V}^{\dagger} + \mathcal{P}_{\bar{U}}(\Phi) - \mathcal{P}_{\bar{U}}(\Phi) - 0 = \bar{U}\hat{V}^{\dagger}, \tag{53}$$

where (a) follows from (23). From (33), we have

$$\hat{V}\hat{V}^\dagger = V'U'^\dagger\bar{U}\bar{U}^\dagger U'V'^\dagger \overset{\text{(b)}}{=} V'U'^\dagger U'U'^\dagger U'V'^\dagger = V'V'^\dagger,$$

where (b) follows from (33). Thus, $\mathcal{P}_{V'}(\cdot) = \mathcal{P}_{\hat{V}}(\cdot)$. Then

$$\begin{aligned}\mathcal{P}_{V'}(Q) = \mathcal{P}_{\hat{V}}(Q) &\overset{\text{(c)}}{=} \bar{U}\hat{V}^\dagger + \mathcal{P}_{\hat{V}}(\Phi) - \mathcal{P}_{\hat{V}}\mathcal{P}_{\bar{U}}(\Phi)\\ &- \mathcal{P}_{\hat{V}}(I - \mathcal{P}_{W_{\bar{\mathcal{I}}}})\mathcal{P}_{\hat{V}}(I + \sum_{i=1}^{\infty}(\mathcal{P}_{\hat{V}}\mathcal{P}_{W_{\bar{\mathcal{I}}}}\\ &\mathcal{P}_{\hat{V}})^i)\mathcal{P}_{\hat{V}}\mathcal{P}_{\bar{U}^\perp}(\Phi)\\ &\overset{\text{(d)}}{=} \bar{U}\hat{V}^\dagger + \mathcal{P}_{\hat{V}}(\Phi) - \mathcal{P}_{\hat{V}}\mathcal{P}_{\bar{U}}(\Phi) - \mathcal{P}_{\hat{V}}\mathcal{P}_{\bar{U}^\perp}(\Phi)\\ &= \bar{U}\hat{V}^\dagger. \end{aligned} \tag{54}$$

(c) follows since $\mathcal{P}_{W_{\bar{\mathcal{I}}}}$, $\mathcal{P}_{\hat{V}}$, and $\mathcal{P}_{\hat{V}}\mathcal{P}_{W_{\bar{\mathcal{I}}}}\mathcal{P}_{\hat{V}}$ are all given by right matrix multiplication, while $\mathcal{P}_{\bar{U}^\perp}$ is given by left matrix multiplication. (d) follows from Lemma 10. Combining (53) and (54), we obtain that (a) of (34) holds.

Step 2: verification of (b) of (34).

$$\begin{aligned}&\|\mathcal{P}_{T'^\perp}(Q)\| = \|\mathcal{P}_{\hat{V}^\perp}\mathcal{P}_{\bar{U}^\perp}(\Phi) -\\ &\quad\mathcal{P}_{\bar{U}^\perp}\mathcal{P}_{\hat{V}^\perp}(I - \mathcal{P}_{W_{\bar{\mathcal{I}}}})\mathcal{P}_{\hat{V}}(I + \sum_{i=1}^{\infty}(\mathcal{P}_{\hat{V}}\mathcal{P}_{W_{\bar{\mathcal{I}}}}\mathcal{P}_{\hat{V}})^i)\mathcal{P}_{\hat{V}}(\Phi)\|\\ &\le\|\Phi\| + (1 + \sum_{i=1}^{\infty}\psi^i)\|\Phi\| = \frac{2-\psi}{1-\psi}\|\Phi\|\\ &\overset{\text{(e)}}{\le}\frac{2-\psi}{1-\psi}\|\lambda\hat{H}\|\|(W_{\bar{\mathcal{I}}}^\dagger W_{\bar{\mathcal{I}}})^{-1}\|\|W_{\bar{\mathcal{I}}}^T\|\\ &\overset{\text{(f)}}{\le}\frac{2-\psi}{1-\psi}\lambda\sqrt{k}\sigma_k\sqrt{1+(k-1)\mu} &(55)\\ &\overset{\text{(g)}}{\le}\frac{2-\tilde{\psi}}{1-\tilde{\psi}}\sqrt{\frac{\tilde{\psi}}{\tilde{k}\sigma_{\tilde{k}}}}\sqrt{\tilde{k}}\sigma_{\tilde{k}}\sqrt{1+(\tilde{k}-1)\mu} &(56)\\ &\overset{\text{(h)}}{\le}\frac{2-\tilde{\psi}}{1-\tilde{\psi}}\sqrt{\tilde{\psi}}\sqrt{\frac{1+(\tilde{k}-1)\mu}{1-(\tilde{k}-1)\mu}} &(57)\\ &\overset{\text{(i)}}{\le}\frac{2-\tilde{\psi}}{1-\tilde{\psi}}\sqrt{\tilde{\psi}}\sqrt{\frac{1+c}{1-c}}\overset{\text{(j)}}{\le}1.\end{aligned}$$

where (e) follows from the definition of Φ, and (f) follows from (51) and (52). (g) follows from the property that $\psi \le \tilde{\psi}$, $1 \le k \le \tilde{k}$, $\lambda \le \lambda_{\max,\tilde{k}}$, and $\sigma_k \le \sigma_{\tilde{k}}$. (h) follows from Lemma 1. (i) follow from $\tilde{k}\mu \le c$, and (j) follows from (19). Then (b) of (34) holds.

Step 3: verification of (c) of (34). First consider

$$\begin{aligned}&(\Delta_2 W^\ddagger)_{\bar{\mathcal{I}}}\\ =&(\mathcal{P}_{\bar{U}^\perp}(I - \mathcal{P}_{W_{\bar{\mathcal{I}}}})\mathcal{P}_{\hat{V}}(I + \sum_{i=1}^{\infty}(\mathcal{P}_{\hat{V}}\mathcal{P}_{W_{\bar{\mathcal{I}}}}\mathcal{P}_{\hat{V}})^i)\mathcal{P}_{\hat{V}}(\Phi)W^\ddagger)_{\bar{\mathcal{I}}}\\ \overset{\text{(k)}}{=}&(\mathcal{P}_{\bar{U}^\perp}\mathcal{P}_{\hat{V}}(I + \sum_{i=1}^{\infty}(\mathcal{P}_{\hat{V}}\mathcal{P}_{W_{\bar{\mathcal{I}}}}\mathcal{P}_{\hat{V}})^i)\mathcal{P}_{\hat{V}}(\Phi))(I -\\ &W_{\bar{\mathcal{I}}}^\ddagger(W_{\bar{\mathcal{I}}}^T W_{\bar{\mathcal{I}}}^\ddagger)^{-1}W_{\bar{\mathcal{I}}}^T)W_{\bar{\mathcal{I}}}^\ddagger = 0\end{aligned}$$

where (k) holds since $\mathcal{P}_{W_{\bar{\mathcal{I}}}}$, $\mathcal{P}_{\hat{V}}$, and $\mathcal{P}_{\hat{V}}\mathcal{P}_{W_{\bar{\mathcal{I}}}}\mathcal{P}_{\hat{V}}$ are all given by right matrix multiplication, while $\mathcal{P}_{\bar{U}^\perp}$ is given by left matrix multiplication. Then

$$\begin{aligned}(QW^\ddagger)_{\bar{\mathcal{I}}} &= (\bar{U}\hat{V}W^\ddagger + \Phi W^\ddagger - \mathcal{P}_{\bar{U}}(\Phi)W^\ddagger)_{\bar{\mathcal{I}}} - (\Delta_2 W^\ddagger)_{\bar{\mathcal{I}}}\\ &= \bar{U}\hat{V}W_{\bar{\mathcal{I}}}^\ddagger + \Phi W_{\bar{\mathcal{I}}}^\ddagger - \mathcal{P}_{\bar{U}}(\Phi)W_{\bar{\mathcal{I}}}^\ddagger - 0\\ &\overset{\text{(l)}}{=} \lambda\bar{U}\bar{U}^\dagger\hat{H} + \lambda\hat{H} - \lambda\bar{U}\bar{U}^\dagger\hat{H}\\ &= \lambda\hat{H} \in \lambda\mathfrak{G}(C'),\end{aligned} \tag{58}$$

where (l) follows from Lemma 8 and the definition of Φ in (36). Then (c) of (34) holds.

Step 4: verification of (d) of (34). First consider

$$\begin{aligned}&\|(\Delta_2 W^\ddagger)_{\bar{\mathcal{I}}^c}\|_{\infty,2}\\ =&\|\mathcal{P}_{\bar{U}^\perp}\mathcal{P}_{\hat{V}}(I + \sum_{i=1}^{\infty}(\mathcal{P}_{\hat{V}}\mathcal{P}_{W_{\bar{\mathcal{I}}}}\mathcal{P}_{\hat{V}})^i)\\ &\cdot\Phi\hat{V}\hat{V}^\dagger(I - W_{\bar{\mathcal{I}}}^\ddagger(W_{\bar{\mathcal{I}}}^T W_{\bar{\mathcal{I}}}^\ddagger)^{-1}W_{\bar{\mathcal{I}}}^T)W_{\bar{\mathcal{I}}^c}^\ddagger\|_{\infty,2}\\ =&\|\mathcal{P}_{\bar{U}^\perp}\mathcal{P}_{\hat{V}}(I + \sum_{i=1}^{\infty}(\mathcal{P}_{\hat{V}}\mathcal{P}_{W_{\bar{\mathcal{I}}}}\mathcal{P}_{\hat{V}})^i)\Phi(\hat{V}\hat{V}^\dagger W_{\bar{\mathcal{I}}^c}^\ddagger -\\ &\hat{V}\hat{V}^\dagger W_{\bar{\mathcal{I}}}^\ddagger(W_{\bar{\mathcal{I}}}^T W_{\bar{\mathcal{I}}}^\ddagger)^{-1}W_{\bar{\mathcal{I}}}^T)W_{\bar{\mathcal{I}}^c}^\ddagger\|_{\infty,2}\\ \le&\|I + \sum_{i=1}^{\infty}(\mathcal{P}_{\hat{V}}\mathcal{P}_{W_{\bar{\mathcal{I}}}}\mathcal{P}_{\hat{V}})^i\|\|\Phi\|\Big(\|\hat{V}\|\|\hat{V}W_{\bar{\mathcal{I}}^c}^\ddagger\|_{\infty,2}\\ &+\|\hat{V}\|\hat{V}^\dagger W_{\bar{\mathcal{I}}}^\ddagger\|\|(W_{\bar{\mathcal{I}}}^\dagger W_{\bar{\mathcal{I}}})^{-1}\|\|W_{\bar{\mathcal{I}}}^T W_{\bar{\mathcal{I}}^c}^\ddagger\|_{\infty,2}\Big)\\ \le&\frac{\|\Phi\|(\epsilon + \lambda\sqrt{k}\sigma_k\sqrt{k}\mu)}{1-\psi} \le \frac{\epsilon + \lambda k\sigma_k\mu}{2-\psi} \le \frac{\epsilon + \lambda k\sigma_k\mu}{2-\tilde{\psi}},\end{aligned}$$

where the second to last inequality follows from (e) to (j) in step 2.

$$\begin{aligned}&\|(QW^\ddagger)_{\bar{\mathcal{I}}^c}\|_{\infty,2}\\ =&\|(\bar{U}\hat{V}W^\ddagger + \Phi W^\ddagger - \mathcal{P}_{\bar{U}}(\Phi)W^\ddagger - \Delta_2 W^\ddagger)_{\bar{\mathcal{I}}^c}\|_{\infty,2}\\ =&\|\bar{U}\hat{V}W_{\bar{\mathcal{I}}^c}^\ddagger + \mathcal{P}_{\bar{U}^\perp}(\Phi)W_{\bar{\mathcal{I}}^c}^\ddagger - (\Delta_2 W^\ddagger)_{\bar{\mathcal{I}}^c}\|_{\infty,2}\\ \le&\|\bar{U}\hat{V}W_{\bar{\mathcal{I}}^c}^\ddagger\|_{\infty,2} + \|(I - \bar{U}\bar{U})^\dagger\lambda\hat{H}(W_{\bar{\mathcal{I}}}^T W_{\bar{\mathcal{I}}}^\ddagger)^{-1}W_{\bar{\mathcal{I}}}^T W_{\bar{\mathcal{I}}^c}^\ddagger\|_{\infty,2}\\ &+\|(\Delta_2 W^\ddagger)_{\bar{\mathcal{I}}^c}\|_{\infty,2}\\ \le&\|\bar{U}\|\|\hat{V}W_{\bar{\mathcal{I}}^c}^\ddagger\|_{\infty,2}+\\ &\|(I - \bar{U}\bar{U})^\dagger\|\|\lambda\hat{H}\|\|(W_{\bar{\mathcal{I}}}^\dagger W_{\bar{\mathcal{I}}})^{-1}\|\|W_{\bar{\mathcal{I}}}^T W_{\bar{\mathcal{I}}^c}^\ddagger\|_{\infty,2}+\\ &\|(\Delta_2 W^\ddagger)_{\bar{\mathcal{I}}^c}\|_{\infty,2}\\ \le&\epsilon + \lambda\sqrt{k}\sigma_k\sqrt{k}\mu+\\ &\frac{\lambda\sigma_k\sqrt{k+(k^2-k)\mu}(\epsilon + \sigma_k\mu\sqrt{k+(k^2-k)\mu})}{1-\psi}\\ \le&(1 + \frac{1}{2-\tilde{\psi}})(\epsilon + \lambda k\sigma_k\mu),\\ \le&(1 + \frac{1}{2-\tilde{\psi}})(\epsilon + \lambda\tilde{k}\sigma_{\tilde{k}}\mu), &(59)\\ \le&\lambda,\end{aligned}$$

where the last inequality follows from $\lambda \ge \lambda_{\min,\tilde{k}}$. Then (d) of (34) holds. □

E. Proof of Lemma 5

Proof. We define

$\tilde{C} = \bar{C} + \mathcal{P}_{\bar{\mathcal{I}}}\mathcal{P}_{\bar{U}}(C^* - \bar{C})$ and $\tilde{L} = \bar{L} - \mathcal{P}_{\bar{\mathcal{I}}}\mathcal{P}_{\bar{U}}(C^* - \bar{C})W^T$.

Note that $\mathcal{P}_{\bar{U}}(\tilde{L}) = \tilde{L}$, $\mathcal{P}_{\bar{\mathcal{I}}}(\tilde{C}) = \tilde{C}$ and $\bar{L} + \bar{C}W^T = \tilde{L} + \tilde{C}W^T$. We further define $N_L = L^* - \bar{L}$, $N_C = C^* - \bar{C}$, and $N_C^+ = C^* - \tilde{C}$. Note that $\mathcal{P}_{\bar{\mathcal{I}}^c}(N_C^+) = \mathcal{P}_{\bar{\mathcal{I}}^c}(N_C)$ from the definition of N_C^+. Let $E = N_L + N_C W^T$. We have

$$\begin{aligned}\|E\|_F &= \|L^* + C^*W^T - (\bar{L} + \bar{C}W^T)\|_F \\ \leq& \|L^* + C^*W^T - M\|_F + \|N\|_F \leq 2\eta,\end{aligned} \tag{60}$$

where the last inequality holds since (L^*, C^*) is the solution to (13) and $\|N\|_F \leq \eta$. Let G be such that $\|G\| = 1$, $\langle G, \mathcal{P}_{T^{*\perp}}(\Delta W^T)\rangle = \|\mathcal{P}_{T^{*\perp}}(\Delta W^T)\|_*$ and $\mathcal{P}_{T^*}(G) = 0$. Let F be such that $F_i = \Delta_i / \|\Delta_i\|_2$ if $i \in \bar{\mathcal{I}}$ and $\Delta_i \neq 0$, and $F_i = 0$ otherwise. Then

$$\begin{aligned}&\|\bar{L}\|_* + \lambda\|\bar{C}\|_{1,2} \overset{\text{(m)}}{\geq} \|L^*\|_* + \lambda\|C^*\|_{1,2} \\ \overset{\text{(n)}}{\geq}& \|\bar{L}\|_* + \lambda\|\bar{C}\|_{1,2} + \langle \mathcal{P}_{\bar{T}}(Q) + G, N_L\rangle + \lambda\langle \mathcal{P}_{\bar{\mathcal{I}}}(QW^\ddagger)/\lambda \\ &+ F, N_C\rangle \\ =& \|\bar{L}\|_* + \lambda\|\bar{C}\|_{1,2} + \|\mathcal{P}_{\bar{T}^\perp}(N_L)\|_* + \langle \mathcal{P}_{\bar{T}}(Q), N_L\rangle \\ &+ \lambda\|\mathcal{P}_{\bar{\mathcal{I}}^c}(N_C)\|_{1,2} + \langle \mathcal{P}_{\bar{\mathcal{I}}}(QW^\ddagger), N_C\rangle \\ =& \|\bar{L}\|_* + \lambda\|\bar{C}\|_{1,2} + \|\mathcal{P}_{\bar{T}^\perp}(N_L)\|_* + \lambda\|\mathcal{P}_{\bar{\mathcal{I}}^c}(N_C)\|_{1,2} \\ &- \langle \mathcal{P}_{\bar{T}^\perp}(Q), N_L\rangle - \langle \mathcal{P}_{\bar{\mathcal{I}}^c}(QW^\ddagger), N_C\rangle + \langle Q, N_L + N_C W^T\rangle \\ \geq& \|\bar{L}\|_* + \lambda\|\bar{C}\|_{1,2} + (1 - \|\mathcal{P}_{\bar{T}^\perp}(Q)\|)\|\mathcal{P}_{\bar{T}^\perp}(N_L)\|_* \\ &+ (\lambda - \|\mathcal{P}_{\bar{\mathcal{I}}^c}(QW^\ddagger)\|_{\infty,2})\|\mathcal{P}_{\bar{\mathcal{I}}^c}(N_C)\|_{1,2} + \langle Q, E\rangle \\ \geq& \|\bar{L}\|_* + \lambda\|\bar{C}\|_{1,2} + \frac{1}{2}\|\mathcal{P}_{\bar{T}^\perp}(N_L)\|_* + \frac{\lambda}{2}\|\mathcal{P}_{\bar{\mathcal{I}}^c}(N_C)\|_{1,2} \\ &- 2\eta\|Q\|_F,\end{aligned} \tag{61}$$

where (m) holds because of the optimality of (L^*, C^*) and (n) holds because of the convexity of the objective function of (13). We can see that the last inequality of (61) follows from (b) and (d) of (42). Then we have

$$\frac{1}{2}\|\mathcal{P}_{\bar{T}^\perp}(N_L)\|_* + \frac{\lambda}{2}\|\mathcal{P}_{\bar{\mathcal{I}}^c}(N_C)\|_{1,2} - 2\eta\|Q\|_F \leq 0. \tag{62}$$

Note that

$$\begin{aligned}&\|Q\|_F = \|\mathcal{P}_{\bar{T}}(Q) + \mathcal{P}_{\bar{T}^\perp}(Q)\|_F \\ =& \sqrt{\|\mathcal{P}_{\bar{T}}(Q)\|_F^2 + \|\mathcal{P}_{\bar{T}^\perp}(Q)\|_F^2} \\ =& \sqrt{\|\bar{U}\bar{V}^\dagger\|_F^2 + \|\mathcal{P}_{\bar{T}^\perp}(Q)\|_F^2} \overset{\text{(o)}}{\leq} \frac{1}{2}\sqrt{\min(t,p) + 3r},\end{aligned} \tag{63}$$

where the last equality follows from (a) of (42). The inequality (o) holds from $\|\bar{U}\bar{V}^\dagger\|_F = \sqrt{\mathrm{trace}(\mathrm{\bar{V}\bar{U}^\dagger\bar{U}\bar{V}^\dagger})} = \sqrt{r}$, and

$$\|\mathcal{P}_{\bar{T}^\perp}(Q)\|_F \leq \mathrm{rank}(\mathcal{P}_{\bar{T}^\perp}(Q)) \cdot \|\mathcal{P}_{\bar{T}^\perp}(Q)\| \leq \frac{\sqrt{\min(t,p) - r}}{2}.$$

Since $\theta = \min(t,p)$, combining (62) and (63), we have

$$\|\mathcal{P}_{\bar{T}^\perp}(N_L)\|_F \leq \|\mathcal{P}_{\bar{T}^\perp}(N_L)\|_* \leq 2\eta\sqrt{\theta + 3r}, \tag{64}$$

$$\|\mathcal{P}_{\bar{\mathcal{I}}^c}(N_C)\|_F \leq \|\mathcal{P}_{\bar{\mathcal{I}}^c}(N_C)\|_{1,2} \leq \frac{2}{\lambda}\eta\sqrt{\theta + 3r}. \tag{65}$$

From the definition of $\mathcal{P}_{W_{\bar{\mathcal{I}}}}$ in (38), one can check that

$$\mathcal{P}_{W_{\bar{\mathcal{I}}}}(\mathcal{P}_{\bar{\mathcal{I}}}(W)^T) = \mathcal{P}_{\bar{\mathcal{I}}}(W)^T. \tag{66}$$

Then we have

$$\begin{aligned}&\mathcal{P}_{\bar{\mathcal{I}}}(N_C^+)W^T = \mathcal{P}_{\bar{\mathcal{I}}}(N_C^+)\mathcal{P}_{\bar{\mathcal{I}}}(W)^T \\ =& \mathcal{P}_{\bar{\mathcal{I}}}(N_C^+)\mathcal{P}_{W_{\bar{\mathcal{I}}}}(\mathcal{P}_{\bar{\mathcal{I}}}(W)^T) = \mathcal{P}_{\bar{\mathcal{I}}}(N_C^+)\mathcal{P}_{W_{\bar{\mathcal{I}}}}(W^T) \\ =& \mathcal{P}_{W_{\bar{\mathcal{I}}}}(N_C^+W^T - \mathcal{P}_{\bar{\mathcal{I}}^c}(N_C^+)W^T) \\ \overset{\text{(p)}}{=}& \mathcal{P}_{W_{\bar{\mathcal{I}}}}(E - \mathcal{P}_{\bar{T}^\perp}(N_L) - \mathcal{P}_{\bar{T}}(N_L) - \mathcal{P}_{\bar{\mathcal{I}}}\mathcal{P}_{\bar{U}}(N_C)W^T \\ &- \mathcal{P}_{\bar{\mathcal{I}}^c}(N_C^+)W^T) \\ \overset{\text{(q)}}{=}& \mathcal{P}_{W_{\bar{\mathcal{I}}}}(E - \mathcal{P}_{\bar{T}^\perp}(N_L) - \mathcal{P}_{\bar{T}}(E) + \mathcal{P}_{\bar{T}}(N_C W^T) \\ &- \mathcal{P}_{\bar{\mathcal{I}}}\mathcal{P}_{\bar{U}}(N_C)W^T - \mathcal{P}_{\bar{\mathcal{I}}^c}(N_C^+)W^T) \\ =& \mathcal{P}_{W_{\bar{\mathcal{I}}}}(\mathcal{P}_{\bar{T}^\perp}(E) - \mathcal{P}_{\bar{T}^\perp}(N_L) - \mathcal{P}_{\bar{\mathcal{I}}^c}(N_C)W^T \\ &+ \mathcal{P}_{\bar{T}}(\mathcal{P}_{\bar{\mathcal{I}}}(N_C)W^T) + \mathcal{P}_{\bar{T}}(\mathcal{P}_{\bar{\mathcal{I}}^c}(N_C)W^T) \\ &- \mathcal{P}_{\bar{\mathcal{I}}}\mathcal{P}_{\bar{U}}(N_C)W^T) \\ \overset{\text{(r)}}{=}& \mathcal{P}_{W_{\bar{\mathcal{I}}}}(\mathcal{P}_{\bar{T}^\perp}(E) - \mathcal{P}_{\bar{T}^\perp}(N_L) - \mathcal{P}_{\bar{\mathcal{I}}^c}(N_C)W^T + \\ &\mathcal{P}_{\bar{T}}(\mathcal{P}_{\bar{\mathcal{I}}^c}(N_C)W^T) + \mathcal{P}_{\bar{U}}(\mathcal{P}_{\bar{\mathcal{I}}}(N_C)W^T) + \\ &\mathcal{P}_{\bar{V}}(\mathcal{P}_{\bar{\mathcal{I}}}(N_C)\mathcal{P}_{\bar{\mathcal{I}}}(W)^T) - \mathcal{P}_{\bar{U}}\mathcal{P}_{\bar{V}}(\mathcal{P}_{\bar{\mathcal{I}}}(N_C)W^T) \\ &- \mathcal{P}_{\bar{\mathcal{I}}}\mathcal{P}_{\bar{U}}(N_C)W^T) \\ \overset{\text{(s)}}{=}& \mathcal{P}_{W_{\bar{\mathcal{I}}}}(\mathcal{P}_{\bar{T}^\perp}(E) - \mathcal{P}_{\bar{T}^\perp}(N_L) - \mathcal{P}_{\bar{\mathcal{I}}^c}(N_C)W^T + \\ &\mathcal{P}_{\bar{T}}(\mathcal{P}_{\bar{\mathcal{I}}^c}(N_C)W^T) + \mathcal{P}_{\bar{V}}(N_C\mathcal{P}_{\bar{\mathcal{I}}}(W)^T) - \mathcal{P}_{\bar{V}}(\mathcal{P}_{\bar{\mathcal{I}}^c}(N_C) \\ &\mathcal{P}_{\bar{\mathcal{I}}}(W)^T) - \mathcal{P}_{\bar{U}}\mathcal{P}_{\bar{V}}(\mathcal{P}_{\bar{\mathcal{I}}}(N_C)W^T)) \\ \overset{\text{(t)}}{=}& \mathcal{P}_{W_{\bar{\mathcal{I}}}}(\mathcal{P}_{\bar{T}^\perp}(E) - \mathcal{P}_{\bar{T}^\perp}(N_L) - \mathcal{P}_{\bar{\mathcal{I}}^c}(N_C)W^T + \\ &\mathcal{P}_{\bar{T}}(\mathcal{P}_{\bar{\mathcal{I}}^c}(N_C)W^T) + \mathcal{P}_{\bar{V}}(N_C^+\mathcal{P}_{\bar{\mathcal{I}}}(W)^T)).\end{aligned} \tag{67}$$

where (p) and (q) follow from the definition $E = N_L + N_C W^T$ and $N_C^+ = N_C - \mathcal{P}_{\bar{\mathcal{I}}}\mathcal{P}_{\bar{U}}(N_C)$. (r) follows the definition of $\mathcal{P}_{\bar{T}}$. (s) holds because $\mathcal{P}_{\bar{U}}(\mathcal{P}_{\bar{\mathcal{I}}}(N_C)W^T) = \mathcal{P}_{\bar{\mathcal{I}}}\mathcal{P}_{\bar{U}}(N_C)W^T$. (t) holds because of the equality (68) shown as follows:

$$\begin{aligned}&\mathcal{P}_{\bar{V}}(N_C\mathcal{P}_{\bar{\mathcal{I}}}(W)^T) - \mathcal{P}_{\bar{U}}\mathcal{P}_{\bar{V}}(\mathcal{P}_{\bar{\mathcal{I}}}(N_C)\mathcal{P}_{\bar{\mathcal{I}}}(W)^T) \\ =& \mathcal{P}_{\bar{V}}(N_C\mathcal{P}_{\bar{\mathcal{I}}}(W)^T - \mathcal{P}_{\bar{\mathcal{I}}}\mathcal{P}_{\bar{U}}(N_C)\mathcal{P}_{\bar{\mathcal{I}}}(W)^T) \\ =& \mathcal{P}_{\bar{V}}(N_C^+\mathcal{P}_{\bar{\mathcal{I}}}(W)^T)\end{aligned} \tag{68}$$

Note that

$$\begin{aligned}&\|\mathcal{P}_{W_{\bar{\mathcal{I}}}}\mathcal{P}_{\bar{V}}(N_C^+\mathcal{P}_{\bar{\mathcal{I}}}(W)^T)\|_F \\ =& \|\mathcal{P}_{W_{\bar{\mathcal{I}}}}\mathcal{P}_{\bar{V}}(N_C^+\mathcal{P}_{W_{\bar{\mathcal{I}}}}\mathcal{P}_{\bar{\mathcal{I}}}(W)^T)\|_F \\ =& \|N_C^+\mathcal{P}_{\bar{\mathcal{I}}}(W)^T W_{\bar{\mathcal{I}}}^\ddagger(W_{\bar{\mathcal{I}}}^T W_{\bar{\mathcal{I}}}^\ddagger)^{-1}W_{\bar{\mathcal{I}}}^T\bar{V}\bar{V}^\dagger W_{\bar{\mathcal{I}}}^\ddagger(W_{\bar{\mathcal{I}}}^T W_{\bar{\mathcal{I}}}^\ddagger)^{-1}W_{\bar{\mathcal{I}}}^T\|_F \\ \overset{\text{(u)}}{\leq}& \|N_C^+\mathcal{P}_{\bar{\mathcal{I}}}(W)^T\|_F\|\bar{V}^\dagger W_{\bar{\mathcal{I}}}^\ddagger(W_{\bar{\mathcal{I}}}^T W_{\bar{\mathcal{I}}}^\ddagger)^{-1}W_{\bar{\mathcal{I}}}^T\bar{V}\| \\ =& \|N_C^+\mathcal{P}_{\bar{\mathcal{I}}}(W)^T\|_F\|\bar{V}\bar{V}^\dagger W_{\bar{\mathcal{I}}}^\ddagger(W_{\bar{\mathcal{I}}}^T W_{\bar{\mathcal{I}}}^\ddagger)^{-1}W_{\bar{\mathcal{I}}}^T\bar{V}\bar{V}^\dagger\| \\ =& \psi\|\mathcal{P}_{\bar{\mathcal{I}}}(N_C^+)W^T\|_F \leq \tilde{\psi}\|\mathcal{P}_{\bar{\mathcal{I}}}(N_C^+)W^T\|_F,\end{aligned}$$

where the first equality holds from (66), and (u) holds because $\|AB\|_F \leq \|A\|_F\|B\|$ and $\|A^\dagger A\| = \|AA^\dagger\|$ for matrices A and B. From (67), we have

$$\begin{aligned}&\|\mathcal{P}_{\bar{\mathcal{I}}}(N_C^+)W^T\|_F \\ \leq& (\|\mathcal{P}_{\bar{T}^\perp}(E)\|_F + \|\mathcal{P}_{\bar{T}^\perp}(N_L)\|_F + \|\mathcal{P}_{\bar{T}^\perp}(\mathcal{P}_{\bar{\mathcal{I}}^c}(N_C)W^T)\|_F) \\ &\|W_{\bar{\mathcal{I}}}^\ddagger(W_{\bar{\mathcal{I}}}^T W_{\bar{\mathcal{I}}}^\ddagger)^{-1}W_{\bar{\mathcal{I}}}^T\| + \tilde{\psi}\|\mathcal{P}_{\bar{\mathcal{I}}}(N_C^+)W^T\|_F \\ \leq& \|E\|_F + \|\mathcal{P}_{\bar{T}^\perp}(N_L)\|_F + \|\mathcal{P}_{\bar{\mathcal{I}}^c}(N_C)\|_F\|W\| + \\ &\tilde{\psi}\|\mathcal{P}_{\bar{\mathcal{I}}}(N_C^+)W^T\|_F,\end{aligned} \tag{69}$$

where the last inequality uses the property that $\|W_{\bar{\mathcal{I}}}^{\ddagger}(W_{\bar{\mathcal{I}}}^{T}W_{\bar{\mathcal{I}}}^{\ddagger})^{-1}W_{\bar{\mathcal{I}}}^{T}\| = 1$. From similar arguments as in (51), we have $\|W\| \leq \sqrt{1+(n-1)\mu}$. Then combining (60), (64), (65), and (69), we obtain

$$\|\mathcal{P}_{\bar{\mathcal{I}}}(N_C^{+})W^T\|_F \leq (1+\frac{\lambda+\sqrt{1+(n-1)\mu}}{\lambda}\sqrt{\theta+3r})\frac{2\eta}{1-\tilde{\psi}}. \tag{70}$$

Furthermore,

$$\begin{aligned}
&\|\mathcal{P}_{\bar{\mathcal{I}}}(N_C^{+})\|_F = \|\mathcal{P}_{\bar{\mathcal{I}}}(N_C^{+})W^TW_{\bar{\mathcal{I}}}^{\ddagger}(W_{\bar{\mathcal{I}}}^{T}W_{\bar{\mathcal{I}}}^{\ddagger})^{-1}\|_F \\
\leq&\|\mathcal{P}_{\bar{\mathcal{I}}}(N_C^{+})W^T\|_F\|W_{\bar{\mathcal{I}}}^{\ddagger}\|\|(W_{\bar{\mathcal{I}}}^{T}W_{\bar{\mathcal{I}}}^{\ddagger})^{-1}\| \\
\leq&(1+\frac{\lambda+\sqrt{1+(n-1)\mu}}{\lambda}\sqrt{\theta+3r})\frac{2\eta\sigma_k\sqrt{1+(k-1)\mu}}{1-\tilde{\psi}},
\end{aligned}$$

where the last inequality follows from (70), (51), and (18). We also have

$$\begin{aligned}
&\|N_C^{+}W^T\|_F = \|\mathcal{P}_{\bar{\mathcal{I}}^c}(N_C)W^T + \mathcal{P}_{\bar{\mathcal{I}}}(N_C^{+})W^T\|_F \\
\leq&\|\mathcal{P}_{\bar{\mathcal{I}}^c}(N_C)W^T\|_F + \|\mathcal{P}_{\bar{\mathcal{I}}}(N_C^{+})W^T\|_F \\
\leq&\|\mathcal{P}_{\bar{\mathcal{I}}^c}(N_C)\|_F\|W\| + \|\mathcal{P}_{\bar{\mathcal{I}}}(N_C^{+})W^T\|_F \\
\leq&(1+\frac{\lambda+(2-\tilde{\psi})\sqrt{1+(n-1)\mu}}{\lambda}\sqrt{\theta+3r})\frac{2\eta}{1-\tilde{\psi}}.
\end{aligned}$$

Finally, we have

$$\begin{aligned}
&\|C^* - \tilde{C}\|_F = \|\mathcal{P}_{\bar{\mathcal{I}}^c}(N_C) + \mathcal{P}_{\bar{\mathcal{I}}}(N_C^{+})\|_F \\
\leq&\|\mathcal{P}_{\bar{\mathcal{I}}^c}(N_C)\|_F + \|\mathcal{P}_{\bar{\mathcal{I}}}(N_C^{+})\|_F \\
\leq&(1+(\frac{\lambda+\sqrt{1+(n-1)\mu}}{\lambda}+\frac{1-\tilde{\psi}}{\lambda\sigma_k\sqrt{1+(k-1)\mu}})\sqrt{\theta+3r}) \\
&\frac{2\eta\sigma_k\sqrt{1+(k-1)\mu}}{1-\tilde{\psi}},
\end{aligned}$$

and

$$\begin{aligned}
&\|L^* - \tilde{L}\|_F = \|L^* - \bar{L} + \tilde{C}W^T - \bar{C}W^T\|_F \\
=&\|L^* - \bar{L} + C^*W^T - \bar{C}W^T + \tilde{C}W^T - C^*W^T\|_F \\
=&\|E - N_C^{+}W^T\|_F \leq \|E\|_F + \|N_C^{+}W^T\|_F \\
\leq&(2-\tilde{\psi}+\frac{\lambda+(2-\tilde{\psi})\sqrt{1+(n-1)\mu}}{\lambda}\sqrt{\theta+3r})\frac{2\eta}{1-\tilde{\psi}}.
\end{aligned}$$

□

F. Proof of Lemma 6

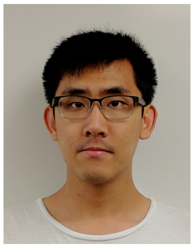
Proof. Since equalities (a) and (c) of (42) are the same as those in (34) and the construction of Q remains the same, then (a) and (c) of (42) have been proved in step 1 and 3 of the proof of Lemma 4. We only need to show that (b) and (d) hold when λ belongs to $[\lambda'_{\text{min},\tilde{k}}, \lambda'_{\text{max},\tilde{k}}]$. From (55), that is proved in the proof of Lemma 4, and $\lambda \leq \lambda'_{\text{max},\tilde{k}}$, we have

$$\|\mathcal{P}_{T'^{\perp}}(Q)\| \leq \frac{2-\tilde{\psi}}{1-\tilde{\psi}}\lambda\sigma_{\tilde{k}}\sqrt{\tilde{k}+(\tilde{k}^2-\tilde{k})\mu} \leq \frac{1}{2}.$$

From (59) and $\lambda \geq \lambda'_{\text{min},\tilde{k}}$, we have

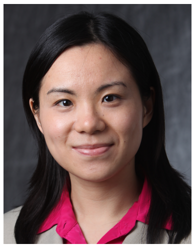
$$\|(QW^{\ddagger})_{\bar{\mathcal{I}}^c}\|_{\infty,2} \leq (1+\frac{1}{2-\tilde{\psi}})(\epsilon+\lambda\tilde{k}\sigma_{\tilde{k}}\mu) \leq \frac{\lambda}{2}.$$

□



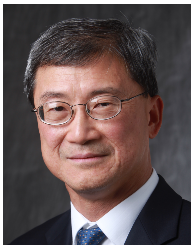
Pengzhi Gao (S'14) received the B.E. degree from Xidian University, Xian, China, in 2011 and the M.S. degree in electrical engineering from University of Pennsylvania, Philadelphia, PA, in 2013.

He is pursuing the Ph.D. degree in electrical engineering at Rensselaer Polytechnic Institute, Troy, NY. His research interests include signal processing, compressive sensing, low-rank matrix recovery, and power networks.



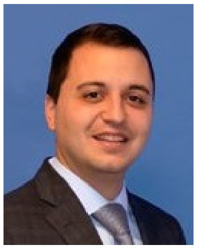
Meng Wang (M'12) received the Ph.D. degree from Cornell University, Ithaca, NY, USA, in 2012.

She is an Assistant Professor in the department of Electrical, Computer, and Systems Engineering at Rensselaer Polytechnic Institute. Her research interests include high dimensional data analysis and their applications in power systems monitoring and network inference.



Joe H. Chow (F'92) received the M.S. and Ph.D. degrees from the University of Illinois, Urbana-Champaign, Urbana, IL, USA.

After working in the General Electric power system business in Schenectady, NY, USA, he joined Rensselaer Polytechnic Institute, Troy, NY, USA, in 1987, where he is a Professor of Electrical, Computer, and Systems Engineering. His research interests include multivariable control, power system dynamics and control, FACTS controllers, and synchronized phasor data.



Scott G. Ghiocel (S'08) received the Ph.D. degree in electrical engineering from Rensselaer Polytechnic Institute, Troy, NY, USA, in 2013.

He is a technical consultant at Exponent. His research interests include synchrophasor measurements, voltage stability, and power system dynamics.

Bruce Fardanesh (F'13) received his Doctor of Engineering degree in Electrical Engineering from Cleveland State University in 1985.

He joined New York Power Authority in 1991, where he is the Chief Electrical Engineer. His research areas of interest are power system analysis, modeling, dynamics, operation, and control.

George Stefopoulos (M'08) received his Ph.D. degree in Electrical Engineering from the Georgia Institute of Technology in 2009.

He is a Research and Technology Development Engineer with the New York Power Authority. His research interests include power system state estimation, synchrophasor technology applications, and modeling and simulation of power systems.

Michael Razanousky received the B.S. degree in electric power engineering from Rensselaer Polytechnic Institute, Troy, NY, USA, in 1989 and the M.S. degree from the University of Albany, Albany, NY, USA, in 2005.

He is presently a project manager at the New York State Energy and Research Development Authority (NYSERDA).