Identification of “Unobservable” Cyber Data Attacks on Power Grids

Meng Wang[1], Member, IEEE, Pengzhi Gao,[1] Student Member, IEEE, Scott G. Ghiocel[1], Member, IEEE,
Joe H. Chow[1], Fellow, IEEE, Bruce Fardanesh[2], Fellow, IEEE, George Stefopoulos[2], Michael P. Razanousky[3]
[1]Department of Electrical, Computer, and Systems Engineering, Rensselaer Polytechnic Institute, Troy, NY, 12180, USA
[2]New York Power Authority, White Plains, NY, 10601, USA
[3]New York State Energy Research and Development Authority, Albany, NY, 12203.

***Abstract*—This paper presents a new framework of identifying cyber data attacks on synchrophasor measurements. We focus on detecting “unobservable” cyber data attacks that cannot be detected by any existing detection 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 unobservable cyber attack identification problem as a matrix decomposition problem where the observed data matrix is the sum of a low-rank matrix plus a linear projection of a column-sparse matrix. We propose a convex-optimization-based decomposition method and provide its theoretical guarantee in the attack identification. Numerical experiments on actual PMU data and synthetic data are conducted to verify the effectiveness of the proposed method.**

I. Introduction

The monitoring, dispatch, and scheduling of power systems can benefit a lot from the integration of cyber infrastructures into future smart grids. Such integration, however, makes the power systems more susceptible to cyber attacks. It is reported that cyber spies have penetrated U.S. electrical grid [24]. 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. It continuously updates the system operator about the operating state based on measurements over various locations of the system. Errors in the measurement can affect the state estimations and mislead the system operator. Therefore, many efforts have been devoted to develop methods that can identify the bad data, see e.g., [6], [14], [23], [25], [32].

Cyber data attacks are firstly studied in [21] and can be viewed as “the worst interacting bad data injected by an adversary”[17]. Malicious intruders 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 [17].

State estimation in the presence of cyber data attacks has attracted much research attention recently [3], [9], [17], [21], [27], [28]. 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], [16], as well as detectors designed for attacks in the observable regime [17]. Only one recent paper [28] considered the detection of unobservable attacks in Supervisory Control and Data Acquisition (SCADA) system and proposed a detection method based on statistical learning. The method in [28] has no theoretical guarantee and 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 experiencing some disturbances.

We propose a new method that can identify the unobservable cyber data attacks to PMUs. It has the theoretical guarantee of attack detection even when the system is under disturbance, provided that the attacker only. The intuition is that although these attacks are undetectable to detectors that rely only on instantaneous measurements, they can be identified by examining the temporal correlations in a sequence of measurements, as long as the intruders do not know the system dynamics.

Low-dimensional structure of PMU data matrix is recently observed in [7], [8], [12]. We formulate the identification problem as a decomposition problem of a low-rank matrix plus a linear projection of a column-sparse matrix. The matrix decomposition problem has attracted much research attention recently, see e.g., [4], [5], [26], [31], and have wide applications in areas like Internet monitoring [18], [22], [29], medical imaging [10], [11], image processing [2], etc. The situation that one component is a projection of a sparse matrix, howe.1(w)3.t-274.7e-

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

II. P

Fig. 4: π model of a transmission line

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

$$\bar{L} = X\bar{W}^T. \qquad (2)$$

The attack at time i is called unobservable[3] if and only if

$$M_{i,} \ = \bar{L}_{i,} \ + \bar{D}_{i,} \ = X_{i,} \ \bar{W}^T + \bar{D}_{i,} \ = (X_{i,} \ + \ \alpha^j)\bar{W}^T$$

holds for some nonzero row vector $\alpha^j \in \mathbb{C}^{1\times n}$. The attack, denoted by data injection $\bar{D}_{i,}$, is unobservable since no detector can differentiate $X_{i,}$ and $X_{i,} \ + \ \alpha^j$ based on $M_{i,}$. We consider the scenario that the attacks at all time instants are unobservable. The attack matrix can be represented by

$$\bar{D} = \begin{bmatrix} \alpha^1 \\ \alpha^2 \\ \vdots \\ \alpha^t \end{bmatrix} \bar{W}^T := \ \bar{} W^T \qquad (3)$$

where $W_j = \bar{W}_j / \ \bar{W}_j$. $\bar{}$ represents the additive error (up to a scaling factor) to bus voltages due to data attacks, i.e., $\bar{W}_j \quad \bar{}_j$ is the error to bus voltage V^j. Let $\bar{\mathcal{I}} \in [\![n]\!]$ denote the column support of $\bar{}$. We assume $\bar{}$ is column-sparse because intruders might only alter some of the state variables due to resource constraints.

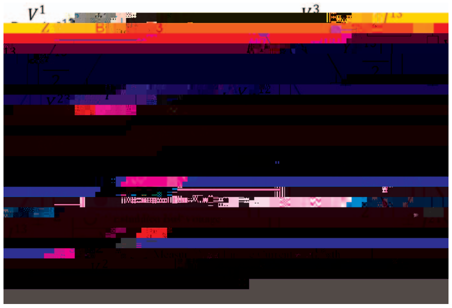

Fig. 5: Three-bus example

We use a three-bus network (Fig. 5) to illustrate the notations. Let $\mathbf{V}^1$, $\mathbf{V}^2$, $\mathbf{V}^3$, $\mathbf{I}^{12}$, $\mathbf{I}^{13}$, $\mathbf{I}^{21}$, $\mathbf{I}^{23} \in \mathbb{C}^{t\times 1}$ denote the bus voltages and line currents in t instants. Assume two PMUs are installed at bus 1 and bus 2. The PMU measurements without attacks are

$$\bar{L} = [\mathbf{V}^1, \mathbf{I}^{12}, \mathbf{I}^{13}, \mathbf{V}^2, \mathbf{I}^{21}, \mathbf{I}^{23}] = [\mathbf{V}^1, \mathbf{V}^2, \mathbf{V}^3]\bar{W}^T \qquad (4)$$

where $\bar{W}^T$ is shown as follows.

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

Suppose the intruder attacks all channels of PMU 1 and the channel of PMU 2 that measures $\mathbf{I}^{13}$ and manipulates these measurements so that the system operator would have the wrong estimation that the system states are $[\mathbf{V}^1 + \boldsymbol{\beta}^1, \mathbf{V}^2 + \boldsymbol{\beta}^2, \mathbf{V}^3]$ for any nonzero $\boldsymbol{\beta}^1$, $\boldsymbol{\beta}^2 \in \mathbb{C}^{t\times 1}$. In this case, the measurements under attacks should be

$$\begin{aligned} M &= [\mathbf{V}^1 + \boldsymbol{\beta}^1, \mathbf{V}^2, \mathbf{V}^3 + \boldsymbol{\beta}^2]\bar{W}^T \\ &= [\mathbf{V}^1 \overset{\text{D}}{+} \boldsymbol{\beta}^1, \mathbf{I}^{12} + \frac{\boldsymbol{\beta}^1}{Z^{12}} + \frac{\boldsymbol{\beta}^1 Y^{12}}{2}, \mathbf{I}^{13} + \frac{\boldsymbol{\beta}^1 - \boldsymbol{\beta}^2}{Z^{13}} + \frac{\boldsymbol{\beta}^1 Y^{12}}{2}, \\ &\qquad \mathbf{V}^2, \mathbf{I}^{21} - \boldsymbol{\beta}^1/Z^{12}, \mathbf{I}^{13} - \boldsymbol{\beta}^2/Z^{13}]. \end{aligned}$$

The additive errors due to attacks are

$$\bar{D} = M -$$

[3] [21] is centered 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 (2).

Method 1 Unobservable cyber attack identification method

```
Input: PMU measurements in $t$ instants, represented by $M$
  Find ($L$ , ), the optimum solution to the following optimization problem

$L \quad \mathbb{C}^{t\times p}, C \quad \mathbb{C}$
```

where $\bar{\mathcal{I}}$ is the column support of . From [31] we have

Lemma 2 (Lemma 4 and Lemma 5 of [31])**.**

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

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

$$U\ V^{\dagger} = \bar{U}V^{\dagger}. \tag{11}$$

Also, we have

$$_{T'} := \quad _{U'} + \quad _{V'} - \quad _{U'} \quad _{V'} = \quad _{\bar{U}} + \quad _{\hat{V}} - \quad _{\bar{U}} \quad _{\hat{V}} \cdot$$

The condition when a solution to Oracle problem (10) is also a solution to (6) is stated in the following lemma,

Lemma 3. An optimal solution $(L\ ,\ )$ to (10) is an optimal solution to (6) if there exists $\ \in \mathbb{C}^{t\times p}$ that satisfies

$$\begin{array}{ll} (\ )\ \ _{T'}(\ ) = U\ V^{\dagger}, & (\ )\ \ _{T'^{\perp}}(\ )\ \ \ 1, \\ (\ )(\ \ W)_{\bar{\mathcal{I}}}/\ \ \in \mathfrak{G}(\ ), & \text{and } (\ )\ \ (\ \ W)_{\bar{\mathcal{I}}^c}\ \ _{,2}\ \ \ . \end{array} \tag{12}$$

If both (b) and (d) are strict, and $\quad _{V'} = \ 0$, then any optimal solution $(L\ ,\ )$ to (6) satisfies $_{\bar{U}}(L\ ) = L$, $_{\bar{\mathcal{I}}}(\ ) = \ $.

The major technical step is to construct , called the dual certificate, that satisfies (12). Our construction method is as follows. Pick $\ \in \mathfrak{G}(\ )$ that satisfies

$$V^{\dagger}W_{\bar{\mathcal{I}}} = \ \bar{U}^{\dagger}\ \ . \tag{13}$$

Define

$$:= \quad (W_{\bar{\mathcal{I}}}^{\dagger}W_{\bar{\mathcal{I}}})^{-1}W_{\bar{\mathcal{I}}}^{\dagger}, \tag{14}$$

$$_1 := \ \ _{\bar{U}}(\ \ ),$$

$$_2 := \ \ _{\bar{U}^{\perp}}(I - \quad W$$