Detecting False Data Injection Attacks on Power Grid by Sparse Optimization

Lanchao Liu, *Student Member, IEEE*, Mohammad Esmalifalak, *Student Member, IEEE*, Qifeng Ding, Valentine A. Emesih, and Zhu Han, *Fellow, IEEE*

***Abstract*—State estimation in electric power grid is vulnerable to false data injection attacks, and diagnosing such kind of malicious attacks has significant impacts on ensuring reliable operations for power systems. In this paper, the false data detection problem is viewed as a matrix separation problem. By noticing the intrinsic low dimensionality of temporal measurements of power grid states as well as the sparse nature of false data injection attacks, a novel false data detection mechanism is proposed based on the separation of nominal power grid states and anomalies. Two methods, the nuclear norm minimization and low rank matrix factorization, are presented to solve this problem. It is shown that proposed methods are able to identify proper power system operation states as well as detect the malicious attacks, even under the situation that collected measurement data is incomplete. Numerical simulation results both on the synthetic and real data validate the effectiveness of the proposed mechanism.**

***Index Terms*—False data injection attacks, power grid security, sparsity and low rank optimization, state estimation.**

I. Introduction

IN THE electric power grid we are observing more and more integration between cyber assets and physical infrastructure for generation, transmission, and distribution control. The ever-increasing demand for reliable, sustainable and economical electricity services necessitate near real-time monitoring and control in power system operations [1]. However, the security and reliability of power grid are not guaranteed at all the times and some failures can cause significant problems for the producers and consumers of electricity. For example, the 2003 Northeast power blackout [2] showed that even a small failure in a part of the grid (In this case, a single transmission line outage in northern Ohio) has cascading effects causing billions of dollars in economic losses. Nowadays, the integration of physical and cyber components gives rise to cyber-attack threats in a power grid, which can result into power outages and even system blackouts [3], or huge economical loss due to non-optimal operations of the power grid.

State estimation [4], which estimates the power system operation state based on a real-time electric network model, is a key function of the Energy Management System (EMS). A linearized measurement model is often used to estimate the states in the power system based on the measurements from remote meters on buses or transmission lines. Specifically, every several seconds or minutes, the Energy Control Center (ECC) collects active/reactive power flows and injections from transmission lines and buses around the power system as measurement data via a Supervisory Control and Data Acquisition (SCADA) system. The state estimation results reflect the real-time power grid operation state and are essential for operators to make decisions in order to maintain security and stability of the system.

The accuracy of state estimation can be affected by bad measurements in the electric power grid. Bad data could be due to topology errors in the grid, untended measurement abnormalities caused by meter failures, and malicious attacks. To detect and identify bad measurements in the power grid state, techniques based on the statistical test on measurement residuals [4] are developed and widely used. However, [5] reveals the fact that false data injection attacks are able to circumvent traditional detection methods based on residual testing. By exploiting the configuration of a power system, synchronized data injection attacks on meters can be launched to tamper with their measurements. What's more, attack vectors can be systematically and efficiently constructed even when the attacker is limited in the resources required to comprise meters, which will mislead the state estimation process, and thus affect the power grid control algorithms. Hence, sufficient attention should be paid to the vulnerability of state estimation to false data injection attacks, which may cause catastrophic consequences in power gird.

Unveiling false data injection attacks is crucial to the security and reliability of power systems. This task is challenging, since attackers may be able to construct false data attack vectors against the protection scheme, and inject attack vectors into power grid that can bypass the traditional methods for bad measurement detection. Furthermore, the incomplete measurement data due to intended attacks or meter failures complicate the task of malicious attack detection, and thus make state estimation even more difficult. The effects of false data injection attacks have been studied in [5]–[7]. False data injection attacks are presented in [5] against state estimation in electric power grid. By capitalizing the configuration of power system, malicious attacks can be launched to bypass the existing bad measurement detection techniques and manipulate the results of state

Manuscript received March 26, 2013; revised August 07, 2013; accepted September 17, 2013. Date of current version February 14, 2014. This work is partially supported by Electric Power Analytics Consortium, funded by CenterPoint Energy, and US NSF ECCS-1028782. Paper no. TSG-00254-2013.

L. Liu, M. Esmalifalak, and Z. Han are with the Department of Electrical and Computer Engineering, University of Houston, Houston, TX 77004 USA (e-mail: lliu10@uh.edu; mesmalifalak@uh.edu; zhan2@uh.edu).

Q. Ding and V. A. Emesih are with CenterPoint Energy, Houston, TX 77002 USA (e-mail: kevin.ding@centerpointenergy.com; valentine.emesih@centerpointenergy.com).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TSG.2013.2284438

estimation arbitrarily. [6], [7] demonstrated that false data injection attacks are able to circumvent the bad data identification techniques equipped in an EMS, and could lead to congestion of transmission lines as well as profitable financial misconduct in the power market. [8]–[10] also consider the false information injection attack in power systems. [8] and [10] consider the time synchronization attack in smart grid, and [9] investigates the load distribution attacks in power system.

On the other hand, the protection scheme against false data injection attacks are investigated in [11]–[18]. [11] introduces two security indices to describe the difficulty of performing a successful false data injection attack against particular physical topology of power grid and available measurements. [12] proposes an efficient method for computing the security index for sparse attack vectors, and describes a protection scheme to strengthen system security by placing encrypted devices in the electric power grid appropriately. [13] models and analyzes this situation as a zero-sum game between the attacker and defender. [14] characterizes two kinds of malicious attacks on electric power grid: the strong attack regime, in which false data injection attacks exist, and the weak attack regime, in which the generalized likelihood radio test can be used as a detector. [15] formulates the bad data detection problem as low-rank matrix recovery problem, which is solved by convex optimization that minimizes a combination of the nuclear norm and the $l1$ norm. However, [15] just proposed the nuclear norm minimization approach to solve the problem and did not take the effect of incomplete measurement into consideration. In [16], a low-complexity attacking strategy is designed to construct sparse false data injection attack vectors, and strategic protection schemes are also proposed based on greedy approaches. [17] gives a thorough survey of existing detection methods for false data injection attacks on smart power gird, and [18] studies the fundamental limits of cyber-physical security in presence of false data injection attacks in the system.

In this paper, instead of considering the measurement of electric grid states at an isolated time instance, a novel mechanism is presented to determine false data injection attacks in electric power grid. Two characteristics of power grid states are exploited in the proposed mechanism. Firstly, the attack-free power grid states are inherently of a low dimension structure due to the intrinsic temporal correlations of measurement. Secondly, the false data injection attack vectors are sparse because attackers are either constrained to some specific measurement meters or limited in the resources required to compromise the meters persistently. Hence, the problem of detecting false data injection attacks can be formulated as a matrix separation problem. Two methods are proposed to solve this problem: the nuclear norm minimization method, which offers provable optimality and convergence rate, and the low rank matrix factorization approach, which provides better scalability. The proposed algorithms are bad data detection methods and can be integrated in the main bad data detection routine of the state estimator. Every time the EMS performs the state estimation task, the state estimator of the system will launch the bad data detection routine, in which the proposed algorithms can be used to detect and identify malicious attacks, even with partial collected measurements. Numerical tests on both synthetic and real data are performed on the proposed algorithm. The proposed detection algorithm is tested on both IEEE case studies and Polish networks [19] during winter 2007–2008 evening peak conditions.

The rest of the paper is organized as follows. The system model and false data injection attcks are addressed in Section II. Section III formulates the malicious attack detection problem and adopts two proposed methods to solve it. The numerical results are given in Section IV. Finally, conclusion closes the paper in Section V.

II. System Model

A. State Estimation in Power Systems

A power system can be divided into three parts: generation, transmission, and distribution. In an electric power grid, the control center needs to monitor the voltage phase angles of all buses to make real-time decisions on operations. However, it is impractical to directly measuring all bus voltage phase angles. In this regard, the control center collects the readings from remote electric meters to estimate the system operation state. Specific measurement data include branch active power flows and bus active power injections, which can be used to estimate bus voltage angles in the system.

Generally, let $\boldsymbol{\theta} = (\theta_1, \theta_2, \ldots, \theta_n)^\top$ denote the power system state variables. The measurement at the control center is expressed as $\mathbf{z} = (z_1, z_2, \ldots, z_m)^\top$ and related to $\boldsymbol{\theta}$ by

$$\mathbf{z} = \mathbf{h}(\boldsymbol{\theta}) + \mathbf{e}, \tag{1}$$

where $\mathbf{h}(\boldsymbol{\theta}) = (h_1(\boldsymbol{\theta}), h_2(\boldsymbol{\theta}), \ldots, h_m(\boldsymbol{\theta}))^\top$, and $h_i(\boldsymbol{\theta})$ is a nonlinear function relating the ith measurement to the state vector $\boldsymbol{\theta}$. The vector $\mathbf{e}$ stands for the independent Gaussian measurement errors with zero mean and known covariance $\mathbf{R}$.

To analyze the efficiency of various state estimation methods solely related to the measurement configuration in a power system, a simplified DC approximation model is utilized. Assuming that the bus voltage magnitudes are already known and normalized, and neglecting all shunt elements and branch resistances, the active power flow from bus i to bus j can be approximated[1] [20] by the first order Taylor expansion as:

$$P_{ij} = \frac{\theta_i - \theta_j}{X_{ij}} + \omega, \tag{2}$$

where X_{ij} is the reactance of the of the transmission line between bus i and bus j, θ_i is the phase angle at bus i, and ω is the measurement error. Similarly, a power injection measurement at a give bus i can be expressed as:

$$P_i = \sum_j P_{ij} + \nu, \tag{3}$$

where ν stands for the measurement error.

[1]In general, one can approximate the impedance of a transmission line with its reactance due to the high reactance over resistance (X/R ratio)

Hence, the DC model for the real power measurement can be written in a linear matrix form as:

$$\mathbf{z} = \mathbf{H}\boldsymbol{\theta} + \mathbf{e}, \tag{4}$$

where $\mathbf{z}$ is the measurement vector includes active power flows and injection measurement, and $\mathbf{H} \in \mathbb{R}^{m \times n}$ is the Jacobian matrix of power system known to the independent system operator (ISO).

The measurements used for state estimation are obtained by the electric meters and collected by the energy control center. Suppose the measurement errors $\mathbf{e}$ in (4) are not correlated, and thus the covariance matrix $\mathbf{R}$ is a diagonal matrix. The Weighted Least Square estimator of the linearized state vector $\boldsymbol{\theta}$ is given by:

$$\hat{\boldsymbol{\theta}} = (\mathbf{H}^\top \mathbf{R}^{-1} \mathbf{H})^{-1} \mathbf{H}^\top \mathbf{R}^{-1} \mathbf{z}. \tag{5}$$

Let $\mathbf{K} = (\mathbf{H}^\top \mathbf{R}^{-1} \mathbf{H})^{-1} \mathbf{H}^\top \mathbf{R}^{-1}$, and then the measurement residuals can be expressed as:

$$\mathbf{r} = \mathbf{z} - \mathbf{H}\hat{\boldsymbol{\theta}} = (\mathbf{I} - \mathbf{K})(\mathbf{H}\boldsymbol{\theta} + \mathbf{e}) = (\mathbf{I} - \mathbf{K})\mathbf{e}, \tag{6}$$

where $\mathbf{I}$ is the identity matrix and the matrix (I-K) is called the residual sensitivity matrix.

The detection and identification of bad data in measurements can be accomplished by processing of the measurement residuals. Specifically, the χ^2-Test can be applied on the measurement residuals to detect bad data. Upon detection of bad data, two kinds of methods, named the largest normalized residual test and hypothesis testing identification method, can be used to identify the specific measurement data that actually contain bad data [4].

B. False Data Injection Attacks

The malicious attack vectors are able to circumvent existing statistical tests for bad data detection if the measurement residuals are unchanged. One such example is the false data injection attack, which is defined as follows:

Definition 1: (False Data Injection Attack) [5]: The malicious attack vector $\mathbf{a} = (a_1, a_2, \ldots, a_m)^\top$ is called the false data injection attack if and only if $\mathbf{a}$ can be expressed as a linear combination of the columns of $\mathbf{H}$ as $\mathbf{a} = \mathbf{H}\mathbf{c}$.

Once the false data injection attacks are applies to the power system, the collected measurements at the ISO can be expressed as:

$$\mathbf{z_a} = \mathbf{z_0} + \mathbf{a} = \mathbf{H}(\boldsymbol{\theta} + \mathbf{c}) + \mathbf{e}. \tag{7}$$

Suppose the state estimate using the malicious measurement $\mathbf{z_a}$ is $\boldsymbol{\theta_a}$, the measurement residuals $\|\mathbf{z_a} - \mathbf{H}\boldsymbol{\theta_a}\|$ in this case is:

$$\|\mathbf{z_a} - \mathbf{H}\boldsymbol{\theta_a}\| = \|\mathbf{z_0} + \mathbf{a} - \mathbf{H}(\boldsymbol{\theta} + \mathbf{c})\| = \|\mathbf{z_0} - \mathbf{H}\boldsymbol{\theta}\|, \tag{8}$$

which means measurement residuals are unaffected by the injection attack vector $\mathbf{a}$, and the attacker successfully trick the system into believing that the true state is $\boldsymbol{\theta_a} = \boldsymbol{\theta} + \mathbf{c}$ instead of $\boldsymbol{\theta}$. Note that $\mathbf{a}$ is the attack vector that under the control of attackers, and $\mathbf{c}$ reflects the estimation error induced by $\mathbf{a}$. A unified formulation for constructing attack vectors of this problem can be found in [16].

In practice, the attacker is either constrained to some specific measurement meters or limited in the resources required to compromise the meters persistently, which will result in a sparse attack vector a. Moreover, the power system is maintained regularly, which makes the attack to a great amount of meters impractical. Furthermore, the utilization of phasor measurement units (PMU) can improve the performance of false data injection detection. On one hand, PMUs can provide accurate measurements of bus voltage angles and power flows to the control center. On the other hand, they can reduce the number of comprised measurements in the grid, which will result in a sparse attack vector a. These also make it possible for the proposed formulation to be extended to a more general framework for detecting false data injection attacks in power grid. In this paper, we focus on the detection and identification of sparse false data injection attacks.

III. Proposed Algorithm

In this section, we show that the detection and identification of false data injection attacks in electric power grid can be formulated as a low rank matrix separation problem. Two methods, the nuclear norm minimization and low rank matrix factorization, are proposed to solve this problem.

A. Sparse Optimization Problem Formulation

Assume the measurement of the electric power system observed by the ISO at time k is denoted as $\mathbf{z}_k$. In presence of false data injection attacks, the measurement $\mathbf{z_k}$ is contaminated by the attack vector $\mathbf{a_k}$. Denote $\mathbf{Z_0} = [\mathbf{z_1}, \mathbf{z_2}, \ldots, \mathbf{z_t}] \in \mathbb{R}^{m \times t}$ as the measurement of the power state for a time period of t, and $\mathbf{A} = [\mathbf{a_1}, \mathbf{a_2}, \ldots, \mathbf{a_t}] \in \mathbb{R}^{m \times t}$ as the false data attacks matrix. The obtained temporal observations $\mathbf{Z_a}$ can be expressed as:

$$\mathbf{Z_a} = \mathbf{Z_0} + \mathbf{A}. \tag{9}$$

Remark that gradually changing power system state variables will typically lead to a low-rank measurement matrix $\mathbf{Z_0}$. In addition, due to the capability limitation of the attacker, the attacks are either constrained to some specific measurement meters or unable to compromise measurement meters persistently. Hence, only a small fraction of the observations are supposed to be anomalous at a given time instant. These imply that the false data injection matrix $\mathbf{A}$ is sparse across both rows and columns. By a little abuse of notation, we use $\mathrm{Rank}(\mathbf{Z_0})$ stands for the rank of matrix $\mathbf{Z_0}$, and $\|\mathbf{A}\|_0$ represents the number of nonzero entries of matrix $\mathbf{A}$. Noticing the intrinsic structures of $\mathbf{Z_0}$ and $\mathbf{A}$, the detection and identification of false data injection attacks can be converted to a matrix separation problem as:

$$\min_{\mathbf{Z_0}, \mathbf{A}} \mathrm{Rank}(\mathbf{Z_0}) + \|\mathbf{A}\|_0, \quad s.t. \quad \mathbf{Z_a} = \mathbf{Z_0} + \mathbf{A}, \tag{10}$$

Solving (10) distinguishes the power state measurement matrix $\mathbf{Z_0}$ and sparse attack matrix $\mathbf{A}$ from their sum $\mathbf{Z_a}$. Considering the missing measurements due to the meter failures or communication links outage in practical applications, (10) can be formulated as:

$$\min_{\mathbf{Z_0}, \mathbf{A}} \mathrm{Rank}(\mathbf{Z_0}) + \|\mathbf{A}\|_0, \quad s.t. \quad \boldsymbol{\mathcal{P}}_{\boldsymbol{\Omega}}(\mathbf{Z_a}) = \boldsymbol{\mathcal{P}}_{\boldsymbol{\Omega}}(\mathbf{Z_0} + \mathbf{A}), \tag{11}$$

where $\mathbf{\Omega}$ is an index subset, and $\boldsymbol{\mathcal{P}}_{\mathbf{\Omega}}(\cdot)$ is the projection operator. Specifically, $\boldsymbol{\mathcal{P}}_{\mathbf{\Omega}}(M)$ is the projection of a matrix $\mathbf{M}$ onto the subspace of matrices whose non-zeros entries are restricted to $\mathbf{\Omega}$ as:

$$[\boldsymbol{\mathcal{P}}_{\mathbf{\Omega}}(\mathbf{M})]_{ij} = 0, \quad \forall (i,j) \notin \mathbf{\Omega}. \tag{12}$$

In the next two subsections, we propose two methods to solve this problem.

B. Nuclear Norm Minimization

The optimization problem in (10) characterizes the low rank property of anomaly power state measurement matrix $\mathbf{Z_0}$ as well as sparse nature of malicious attacks $\mathbf{A_0}$. However, it is known impractical to directly solve (10). One possible approach is replacing $\mathrm{Rank}(\mathbf{Z_0})$ and $\|\mathbf{A}\|_0$ with their their convex relaxation, $\|\mathbf{Z_0}\|_*$ and $\|\mathbf{A}\|_1$, respectively. $\|\mathbf{Z_0}\|_*$ is the nuclear norm of $\mathbf{Z_0}$, which is the sum of its singular values, and $\|\mathbf{A}\|_1$ is the l_1 norm of $\mathbf{A}$, which is the sum of absolute values of its entries. Hence, (10) is reformulated as the following convex optimization problem:

$$\min_{\mathbf{Z_0},\mathbf{A}} \|\mathbf{Z_0}\|_* + \lambda \|\mathbf{A}\|_1, \quad s.t. \quad \mathbf{Z_a} = \mathbf{Z_0} + \mathbf{A}, \tag{13}$$

where λ is a regularization parameter. Correspondingly, (11) can be formulated as:

$$\min_{\mathbf{Z_0},\mathbf{A}} \|\mathbf{Z_0}\|_* + \lambda \|\mathbf{A}\|_1, \quad s.t. \quad \boldsymbol{\mathcal{P}}_{\mathbf{\Omega}}(\mathbf{Z_a}) = \boldsymbol{\mathcal{P}}_{\mathbf{\Omega}}(\mathbf{Z_0} + \mathbf{A}). \tag{14}$$

Algorithm 1 Nuclear Norm Minimization Approach

Input: $\mathbf{Z_a} \in \mathbb{R}^{m \times t}$; $\lambda = 1/\sqrt{\max(m,t)}$;
Initialize: $\mathbf{Y}_{[0]} = 0$; $\mathbf{Z_0}_{[0]} = 0$; $\mathbf{A}_{[0]} = 0$; $\mu_{[0]} > 0$; $\alpha > 0$; $k = 0$;
while not converge **do**
  $\mathbf{Z_0}_{[k+1]} = \mathbf{Z_0}_{[k]}$; $\mathbf{A}_{[k+1]} = \mathbf{A}_{[k]}$; $j = 0$;
  while not converge **do**
    $\mathbf{A}_{[k+1]}^{[j+1]} = \mathcal{S}_{\lambda u_{[k]}^{-1}}\{\mathbf{Z_a} - \mathbf{Z_0}_{[k+1]}^{[j]} + u_{[k]}^{-1}\mathbf{Y}_{[k]}\}$;
    $(\mathbf{Z_a} - \mathbf{A}_{[k+1]} + u_{[k]}^{-1}\mathbf{Y}_{[k]}) = \mathbf{USV}^\top$;
    Obtain $[\mathbf{U}, \mathbf{S}, \mathbf{V}]$;
    $\mathbf{Z_0}_{[k+1]}^{[j+1]} = \mathbf{U}\mathcal{S}_{u_{[k]}^{-1}}\{\mathbf{S}\}\mathbf{V}^\top$;
    $j = j + 1$;
  end while
  $\mathbf{Y}_{[k+1]} = \mathbf{Y}_{[k]} + u_{[k]}(\mathbf{Z_a} - \mathbf{Z_0}_{[k+1]} - \mathbf{A}_{[k+1]})$;
  $\mu_{[k+1]} = \alpha \mu_{[k]}$;
  $k = k + 1$;
end while
return $\mathbf{Z_0}_{[k]}$; $\mathbf{A}_{[k]}$;
Output $\mathbf{Z_0}_{[k]}$; $\mathbf{A}_{[k]}$;

The optimization problem in (14) has been extensively studied in the fields of compressive sensing [21] and matrix completion [22], [23], and can be solved by many off-the-shelf convex optimization algorithms. Motivated by [24], an algorithm applies the techniques of the augmented Lagrange multipliers is utilized here to detect the false data matrix $\mathbf{A}$ as well as recover the measurement matrix $\mathbf{Z_0}$.

The augmented Lagrange multipliers are used to solve the constrained optimization problems as follows:

$$\min f(\mathbf{X}), \quad s.t. \quad \mathbf{h}(\mathbf{X}) = 0, \tag{15}$$

where $f : \mathbb{R}^n \to \mathbb{R}$ and $h : \mathbb{R}^n \to \mathbb{R}^m$. The augmented Lagrangian function is defined as

$$\mathbf{L}(\mathbf{X}, \mathbf{Y}, \boldsymbol{\mu}) = \mathbf{f}(\mathbf{X}) + \langle \mathbf{Y}, \mathbf{h}(\mathbf{X}) \rangle + \frac{\mu}{2} \|\mathbf{h}(\mathbf{X})\|_2^2, \tag{16}$$

where μ is a positive scalar, and $\mathbf{Y}$ is the Lagrangian multipliers. $\langle \mathbf{Y}, \mathbf{h}(\mathbf{X}) \rangle$ denotes the trace of $\mathbf{Y}^\top \mathbf{h}(\mathbf{X})$. The optimization problem in (15) can be solved in an iterative way via the method of augmented Lagrange multipliers. More details about the augmented Lagrange multipliers technique can be found in [25].

For the optimization problem in (14), the Lagrangian function is expressed as:

$$L(\mathbf{Z_0}, \mathbf{A}, \mathbf{Y}, \mu) = \|\mathbf{Z_0}\|_* + \lambda \|\mathbf{A}\|_1 + \langle \mathbf{Y}, \boldsymbol{\mathcal{P}}_{\mathbf{\Omega}}(\mathbf{Z_a} - \mathbf{Z_0} - \mathbf{A}) \rangle + \frac{\mu}{2} \|\boldsymbol{\mathcal{P}}_{\mathbf{\Omega}}(\mathbf{Z_a} - \mathbf{Z_0} - \mathbf{A})\|_2^2. \tag{17}$$

The value of λ is set to $1/\sqrt{\max(m,t)}$, where m and t are dimensions of measurement matrix $\mathbf{Z_a}$. With $k = 1, 2, \ldots,$ indexing iterations, $\mathbf{Z_0}$ and $\mathbf{A}$ are optimized according to:

$$\mathbf{A}_{[k+1]} = \arg\min_{\mathbf{A}} L\left(\mathbf{Z_0}_{[k]}, \mathbf{A}, u_{[k]}, \mathbf{Y}_{[k]}\right), \tag{18}$$

$$\mathbf{Z_0}_{[k+1]} = \arg\min_{\mathbf{Z_0}} L\left(\mathbf{Z_0}, \mathbf{A}_{[k]}, u_{[k]}, \mathbf{Y}_{[k]}\right), \tag{19}$$

where (18) can be explicitly computed from the soft-shrinkage formula, and (19) can be solved via the singular value shrinkage operator [26]. Specifically, define the operator $\mathcal{S}_\tau\{x\} = \mathrm{sgn}(x)\max(|x| - \tau, 0)$ for variable x, where sgn is the sign function. This operator can be extended to vectors and matrices by applying it element-wise. (18) is solved by:

$$\mathbf{A}_{[k+1]} = \mathcal{S}_{\lambda u_{[k]}^{-1}}\left\{\mathbf{Z_a} - \mathbf{Z_0}_{[k]} + u_{[k]}^{-1}\mathbf{Y}_{[k]}\right\}. \tag{20}$$

To solve (19), a singular value decomposition (SVD) is applied on the matrix $\mathbf{Z_a} - \mathbf{A}_{[k+1]} + u_{[k]}^{-1}\mathbf{Y}_{[k]}$:

$$\left(\mathbf{Z_a} - \mathbf{A}_{[k+1]} + u_{[k]}^{-1}\mathbf{Y}_{[k]}\right) = \mathbf{USV}^\top \tag{21}$$

where $\mathbf{U} \in \mathbb{R}^{m \times m}$ and $\mathbf{V} \in \mathbb{R}^{t \times t}$ are unitary matrices. $\mathbf{S} \in \mathbb{R}^{m \times t}$ is diagonal matrix containing the singular values of $(\mathbf{Z_a} - \mathbf{A}_{[k+1]} + u_{[k]}^{-1}\mathbf{Y}_{[k]})$. Typically the singular values are arranged in a decreasing order. The $\mathbf{Z_0}$ is updated by:

$$\mathbf{Z_0}_{[k+1]} = \mathbf{U}\mathcal{S}_{u_{[k]}^{-1}}\{\mathbf{S}\}\mathbf{V}^\top, \tag{22}$$

During each iteration of the optimization, both the Lagrangian multipliers $\mathbf{Y}$ and μ are updated, which improves the performance of the algorithm.

$$\mathbf{Y}_{[k+1]} = \mathbf{Y}_{[k]} + u_{[k]} \left(\mathbf{Z_a} - \mathbf{Z_0}_{[k+1]} - \mathbf{A}_{[k+1]} \right), \quad (23)$$

$$\mu_{[k+1]} = \alpha \mu_{[k]}, \quad (24)$$

where α is a positive constant. The proposed algorithm is illustrated in Algorithm 1.

It has been proved in [27] that the method of augmented Lagrange multipliers has a Q-liner converges speed. Also, to achieve the optimal solution, it is unnecessary to make the penalty parameter μ to approach infinity. The analysis of the convergence of proposed algorithm can be found in [24] and we include it here for completeness.

Theorem 1: For Algorithm 1, any accumulation point $(\mathbf{Z_0}^*, \mathbf{A}^*)$ of $(\mathbf{Z_0}^*_{[k]}, \mathbf{A}^*_{[k]})$ is an optimal solution to problem (13), and the convergence rate is at least $\mathcal{O}(\mu^{-1}_{[k]})$ in the sense that

$$\left| \left\| \mathbf{Z_0}^*_{[k]} \right\|_* + \lambda \left\| \mathbf{A}^*_{[k]} \right\|_1 - f^* \right| = \mathcal{O}\left(\mu^{-1}_{[k-1]} \right), \quad (25)$$

where f^* is the optimal value of problem (13).

C. Low Rank Matrix Factorization

The speed and scalability of the nuclear norm minimization approach are limited by the computational complexity of singular value decomposition. When the matrix size and rank increase, the computation operations for singular value decomposition will become quite expensive. To improve the scalability of solving large-scale problems of malicious attacks detection in power systems, an low rank matrix factorization approach is proposed in this part.

Algorithm 2 Low Rank Matrix Factorization

Input: $\mathbf{Z_a} \in \mathbb{R}^{m \times t}$; Initial rank estimate r.

Initialize: $\mathbf{U} \in \mathbb{R}^{m \times r}$; $\mathbf{V} \in \mathbb{R}^{r \times t}$; $\mathbf{Z_0}_{[0]} = U * V$; $\mathbf{Y}_{[0]} = 0$; $\mu_{[0]} > 0$; $\alpha > 0$; $k = 0$.

while not converge **do**

$\mathbf{U}_{[k+1]} = (\mathbf{Z_0} - u^{-1}_{[k]} \mathbf{Y}_{[k]}) \mathbf{V}^\top (\mathbf{V}\mathbf{V}^\top)^{-1}$;

$\mathbf{V}_{[k+1]} = (\mathbf{U}^\top \mathbf{U})^{-1} \mathbf{U}^\top (\mathbf{Z_0} - u^{-1}_{[k]} \mathbf{Y}_{[k]})$;

$\mathbf{Z_0}_{[k+1]} = \mathcal{S}_{u^{-1}_{[k]}} \{ \mathbf{U}_{[k+1]} \mathbf{V}_{[k+1]} - \mathbf{Z_a} + u^{-1}_{[k]} \mathbf{Y}_{[k]} \}$;

$\mathbf{Y}_{[k+1]} = \mathbf{Y}_{[k]} + u_{[k]} (\mathbf{U}_{[k+1]} \mathbf{V}_{[k+1]} - \mathbf{Z_0}_{[k+1]})$;

$\mu_{[k+1]} = \alpha \mu_{[k]}$;

$k = k + 1$;

Check r, possibly re-estimate r and adjust sizes of the iterates;

end while

return $\mathbf{Z_0}_{[k]}$;

Output $\mathbf{Z_0}_{[k]}$; $\mathbf{Z_a} - \mathbf{Z_0}_{[k]}$;

Given the observations $\mathbf{Z_a}$ at the ISO, the measurements $\mathbf{Z_0}$ and false data injection attacks matrix $\mathbf{A}$ can be separated by the following minimization problem:

$$\min_{\mathbf{U},\mathbf{V},\mathbf{Z_0}} \|\mathbf{Z_a} - \mathbf{Z_0}\|_1, \quad s.t. \quad \mathbf{UV} - \mathbf{Z_0} = \mathbf{0}, \quad (26)$$

where low rank matrix $\mathbf{Z_0}$ is expressed as a product of $\mathbf{U} \in \mathbb{R}^{m \times r}$ and $\mathbf{V} \in \mathbb{R}^{r \times n}$ for some adjustable rank estimate r. Correspondingly, (14) can be rewritten as:

$$\min_{\mathbf{U},\mathbf{V},\mathbf{Z_0}} \|\boldsymbol{\mathcal{P}}_{\boldsymbol{\Omega}}(\mathbf{Z_a} - \mathbf{Z_0})\|_1, \quad s.t. \quad \mathbf{UV} - \mathbf{Z_0} = \mathbf{0}. \quad (27)$$

Note that a low-rank matrix factorization is explicitly applied to $\mathbf{Z_0}$ instead of minimizing its nuclear norm as in (14), which avoids singular value decomposition completely. To solve the minimization problem in (27), the augmented Lagrangian function is expressed as:

$$L(\mathbf{U},\mathbf{V},\mathbf{Z_0},\mathbf{Y},\mu) = \|\boldsymbol{\mathcal{P}}_{\boldsymbol{\Omega}}(\mathbf{Z_a} - \mathbf{Z_0})\|_1 + \langle \mathbf{Y}, \mathbf{UV} - \mathbf{Z_0} \rangle + \frac{\mu}{2} \|\mathbf{UV} - \mathbf{Z_0}\|_2^2, \quad (28)$$

where μ is a penalty parameter and $\mathbf{Y}$ is the Lagrange multiplier corresponding to the constraint $\mathbf{UV} - \mathbf{Z_0} = \mathbf{0}$. Motivated by the idea in the alternating direction method for convex optimization, the augmented Lagrangian function can be minimized with respect to block variables $\mathbf{U}, \mathbf{V}, \mathbf{Z_0}$ individually as the following framework in each iteration k [28]:

$$\mathbf{U}_{[k+1]} = \arg\min_{\mathbf{U}} L\left(\mathbf{U}, \mathbf{V}_{[k]}, \mathbf{Z_0}_{[k]}, \mathbf{Y}_{[k]}, \mu_{[k]}\right), \quad (29)$$

$$\mathbf{V}_{[k+1]} = \arg\min_{\mathbf{V}} L\left(\mathbf{U}_{[k+1]}, \mathbf{V}, \mathbf{Z_0}_{[k]}, \mathbf{Y}_{[k]}, \mu_{[k]}\right), \quad (30)$$

$$\mathbf{Z_0}_{[k+1]} = \arg\min_{\mathbf{Z_0}} L\left(\mathbf{U}_{[k+1]}, \mathbf{V}_{[k+1]}, \mathbf{Z_0}, \mathbf{Y}_{[k]}, \mu_{[k]}\right), \quad (31)$$

where (29) and (30) are least squares problems:

$$\mathbf{U}_{[k+1]} = \left(\mathbf{Z_0} - u^{-1}_{[k]} \mathbf{Y}_{[k]}\right) \mathbf{V}^\top (\mathbf{V}\mathbf{V}^\top)^{-1}, \quad (32)$$

$$\mathbf{V}_{[k+1]} = (\mathbf{U}^\top \mathbf{U})^{-1} \mathbf{U}^\top \left(\mathbf{Z_0} - u^{-1}_{[k]} \mathbf{Y}_{[k]}\right). \quad (33)$$

(31) can be solved by the shrinkage formula.

$$\mathcal{P}_\Omega\left(\mathbf{Z_0}_{[k+1]}\right) = \mathcal{P}_\Omega\left(\mathcal{S}_{u^{-1}_{[k]}}\left\{\mathbf{U}_{[k+1]}\mathbf{V}_{[k+1]} - \mathbf{Z_a} + u^{-1}_{[k]}\mathbf{Y}_{[k]}\right\}\right). \quad (34)$$

The Lagrangian multipliers $\mathbf{Y}$ and μ are updated during each iteration as:

$$\mathbf{Y}_{[k+1]} = \mathbf{Y}_{[k]} + u_{[k]} \left(\mathbf{U}_{[k+1]} \mathbf{V}_{[k+1]} - \mathbf{Z_0}_{[k+1]} \right), \quad (35)$$

$$\mu_{[k+1]} = \alpha \mu_{[k]}, \quad (36)$$

where α is a positive constant. At the end of each iteration, a rank estimation strategy [29] is applied to update r to ensure the success of the algorithm. The proposed algorithm is illustrated in Algorithm 2.

Remark that despite non-convexity in the factorization model in (27), Algorithm 2 has a significant advantage over the nu-

clear-norm minimization in terms of computational efficiency for removing SVD computation, yielding a much improved scalability for solving large-scale problems. Moreover, Algorithm 2 complements well the nuclear-norm minimization model in terms of recoverability. The convergence issue of Algorithm 2 has been investigated in [28], and include here for completeness.

Theorem 2: Let $\mathbf{X} = (\mathbf{U}, \mathbf{V}, \mathbf{Z_0}, \mathbf{Y})$ and $\{\mathbf{X}_{[k]}\}_{k=1}^{\infty}$ be generated by Algorithm 2. Assume that $\{\mathbf{X}_{[k]}\}_{k=1}^{\infty}$ is bounded and $\lim_{k\to\infty}(\mathbf{X}_{[k+1]} - \mathbf{X}_{[k]}) = 0$. Then any accumulation point of $\{\mathbf{X}_{[k]}\}_{k=1}^{\infty}$ satisfies the KKT conditions of problem (26). In particular, whenever $\{\mathbf{X}_{[k]}\}_{k=1}^{\infty}$ convergence, it converges to a KKT point of problem (26).

IV. Numerical Results

In this section, numerical simulations are given to evaluate the performance of the proposed algorithms. Power flow data for IEEE 57 bus and IEEE 118 bus test cases are used, and the power flow data for Polish system during winter evening peak conditions, 2007–2008 are also used for the scalability test of proposed algorithms.

Assume the loads on each bus in the power system are uniformly distributed between 50% and 150% of its base load. When the state estimation measurements are collected, a small portion ϵ of the measurement data are compromised by malicious attackers with an arbitrary amount of injection data, and ϵ is defined as the attack ratio here. The methods for false data injection attacks construction can be found in [14], [16]. Here, we focus on the protection scheme and suppose the locations of the attack are chosen randomly and last a period of Δt.[2] Totally a number of T time instances measurements are obtained for analysis. The receiver operating characteristic analysis is first given, where the true positive rate and false alarm rate are defined, respectively, as follows:

$$p_d = \frac{N_{Hit}}{N_{Hit} + N_{Miss}}, \quad \text{and} \quad p_f = \frac{N_{False}}{N_{False} + N_{Correct}},$$

where N_{Hit} is the number of successful detections of malicious attacks, N_{Miss} is the number of miss detections. N_{False} is the number of false alarms, and $N_{Correct}$ is the number of correct reports of no attack. Then, we investigate the performance of proposed algorithms under different missing measurement ratios as well as attack ratios. Finally, we evaluate the scalability of the algorithm.

A. Receiver Operating Characteristic Analysis

First we analyze the receiver operating characteristics (ROC) of the proposed algorithms, and compare their performances with the principle component analysis (PCA)[3] based detection method. In this part, the attack ratio is fixed at $\epsilon = 0.1$ and $\mathrm{SNR} = 10$ dB.

[2]Note that the attack vectors used in this paper are more general compare to [14], [16] and will not affect the efficiency of the proposed algorithms.

[3]For PCA, we remain the largest K singular values of the matrix such that $(\sum_1^K s_i / \sum_1^N s_i) > 95\%$.

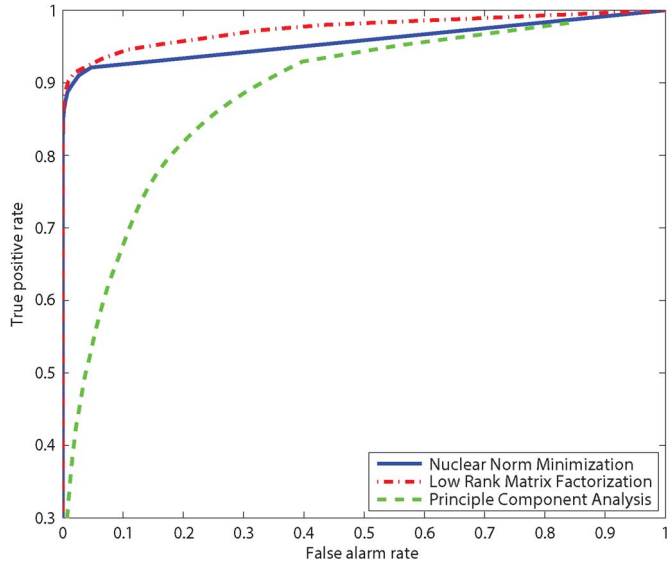


Fig. 1. Performance for case IEEE 57 bus. ROC curves of the proposed nuclear norm minimization and low rank matrix factorization algorithms versus PCA-base method. $\mathrm{SNR} = 10$ dB.

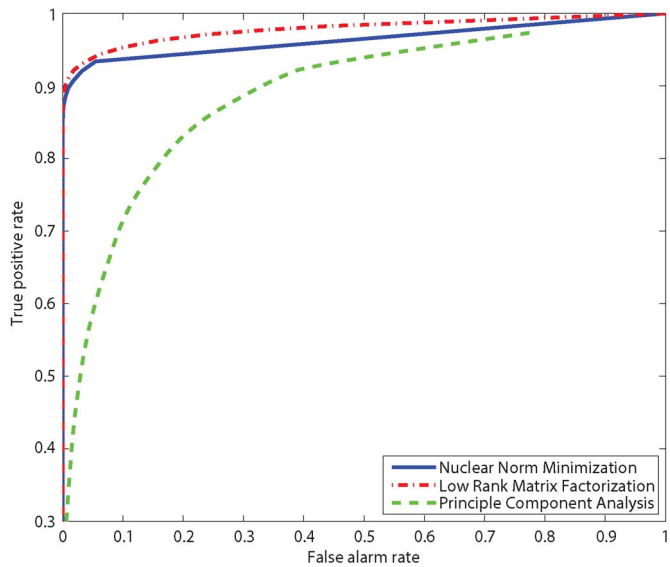


Fig. 2. Performance for case IEEE 118 bus. ROC curves of the proposed nuclear norm minimization and low rank matrix factorization algorithms versus PCA-base method. $\mathrm{SNR} = 10$ dB.

The ROC curves for IEEE 57 bus and IEEE 118 bus cases are depicted in Fig. 1 and Fig. 2, respectively. From the figures, it is apparent that the proposed algorithms can detect the false data accurately at a low false alarm rate. For example in case IEEE 57 bus system, the true positive rate of nuclear norm minimization is 93% and 95% for low rank matrix factorization when false alarm rate $p_f = 10\%$. Tests in case IEEE 118 bus system have similar results. Moreover, the low rank matrix factorization approach performs slightly better than the nuclear norm minimization method. The reason for this phenomena is model-related, and in this case, the sparse attack matrix is not the dominant part in measurements, which makes the low rank matrix factorization approach more suitable. Fig. 1 and in Fig. 2 show that the proposed algorithms outperform the PCA-based approach

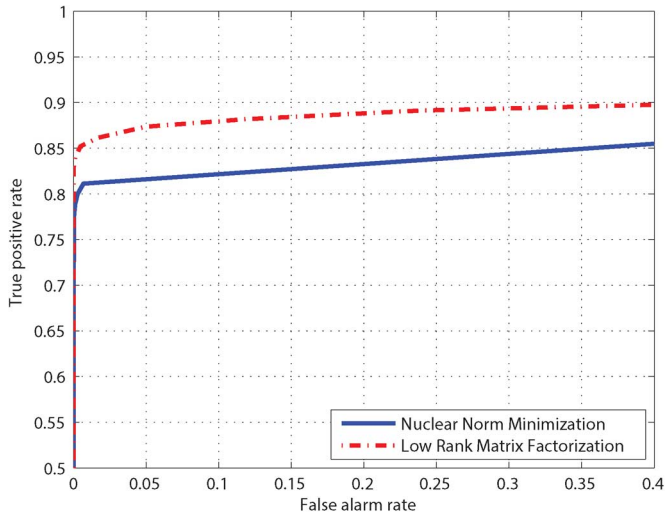


Fig. 3. ROC curves of the proposed algorithms for IEEE 118 bus. 10% measurement are missing and $\mathrm{SNR} = 10$ dB.

much. The PCA method do not take the corruptions of malicious attacks in to consideration. Even though the matrix $\mathbf{Z_0}$ is low rank, the sum of $\mathbf{Z_0}$ and $\mathbf{A}$ will not be low rank any more. Directly apply the PCA method will result in a poor performance. Different from the PCA, proposed algorithms exploits the low rank structure of the anomaly-free measurement matrix, and the fact that malicious attacks are quite sparse, which renders a better performance.

B. Performance vs. Missing Measurement Ratio

In this part, we assume a portion of the measurements collected at the control center is missing due to the meter failures or communication links outage, and evaluate the performance of proposed algorithms under different missing measurement ratios till 10% on IEEE 118 bus system. The attack ratio is fixed at $\epsilon = 0.1$ and $\mathrm{SNR} = 10$ dB.

The ROC curves for IEEE 118 bus case are depicted in Fig. 3. From the figure we can see that with 10% missing measurements, the proposed algorithms are still able to detect the malicious attacks in power system at acceptable true positive rates, and the low rank matrix factorization method performs slightly better. Compare with Fig. 2, we can see the missing measurements actually deteriorate the performance of proposed algorithms. Since the PCA-based method is unable to detect the anomalies in this case, we omitted the simulation result here. Note that the existence of missing entries will result in an incorrect estimation of low-dimensional space of matrix $\mathbf{Z_0}$, which leads to the failure of PCA.

To investigate the performance under different missing measurement ratios, the percentage of missing measurements is varied from 0% (no missing measurements) to 10%, and the results are shown in Fig. 4. The true positive rates are calculated for both algorithms when the false alarm rate equals 10%. It is shown that the performance is monotonously improved as more and more measurements are collected. At the worst case when 10% of measurements are missing, the proposed algorithms can still achieve a true positive rate of 85% and 90% for nuclear norm minimization and low rank matrix factorization, respectively.

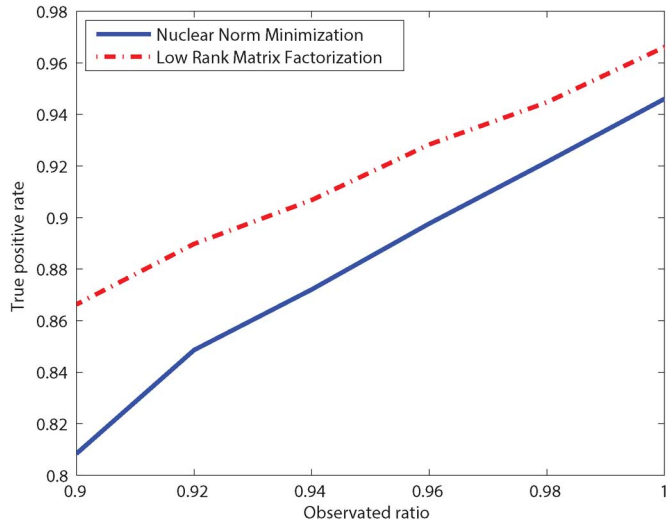


Fig. 4. Performance of proposed algorithms under different missing ratios for IEEE 118 bus. The false alarm rate is 10% and $\mathrm{SNR} = 10$ dB.

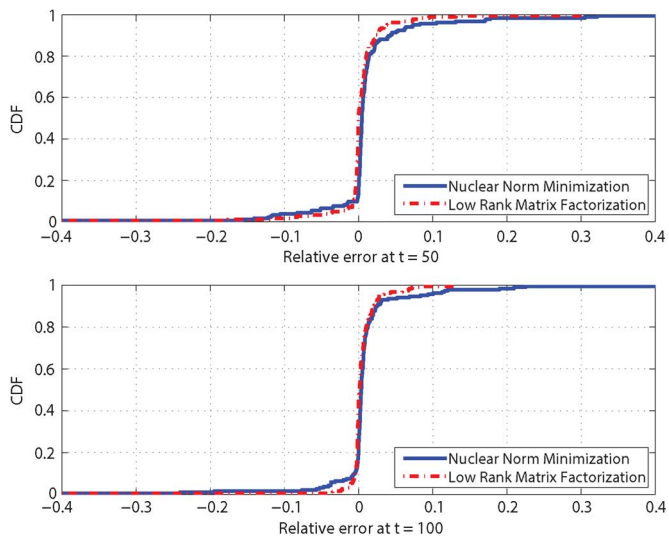


Fig. 5. Power state reconstruction performance of proposed algorithms at specific time instance $t = 50$ and $t = 100$. 10% measurements are missing and $\mathrm{SNR} = 10$ dB.

A more detailed demonstration of the proposed algorithms' recoverability for power system states is shown in Fig. 5. Assume 10% measurements are missing and $\mathrm{SNR} = 10$ dB, the cumulative distribution functions of relative reconstruction errors at $t = 50$ and $t = 100$ are calculated. The relative reconstruction error is defined as:

$$\boldsymbol{\varepsilon} = (\hat{\boldsymbol{\theta}} - \boldsymbol{\theta})./|\boldsymbol{\theta}|, \tag{37}$$

where $./$ denotes the componentwise division, and $|\boldsymbol{\theta}|$ calculates the absolute value of each element in vector $\boldsymbol{\theta}$. The $\boldsymbol{\theta}$ is in radian units which is obtained from the recovered $\mathbf{Z_0}$, and the vector $\boldsymbol{\varepsilon}$ calculates the relative error of each component in the state vector $\boldsymbol{\theta}$. We calculate the relative error for each bus in the system, and plot the cumulative distribution function. From the figures we can see that the proposed algorithms are able to reconstruct the power system states quite accurately. At $t = 50$, majority of the relative errors focus between interval $[-0.1\ 0.1]$, and similar results are shown at $t = 100$. These imply that the

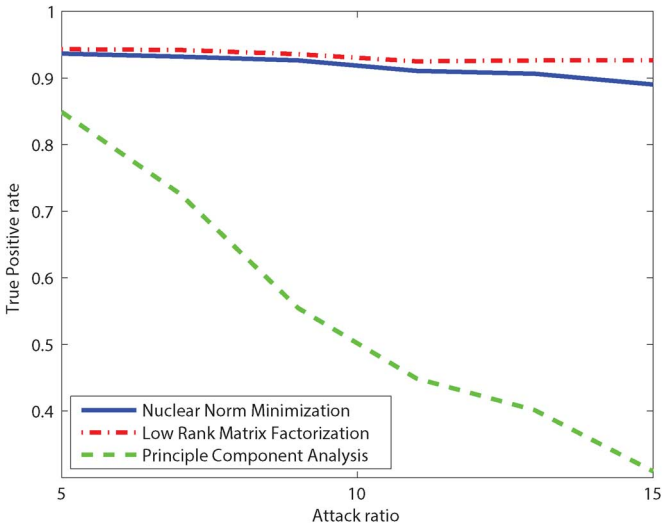


Fig. 6. Performance of proposed algorithms under different attack ratios for IEEE 118 bus. The false alarm rate is 10% and $\mathrm{SNR} = 10$ dB.

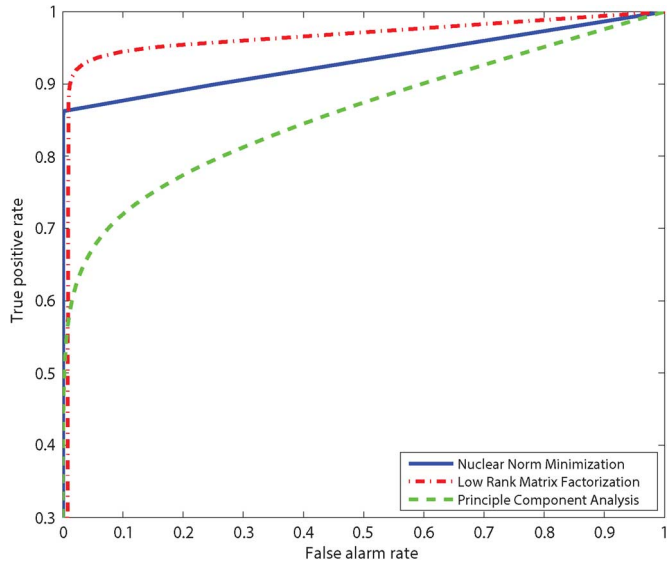


Fig. 7. Performance for on power flow data for Polish system during winter peak conditions, 2007–2008. ROC curves of the proposed nuclear norm minimization and low rank matrix factorization algorithms versus PCA-base method. $\mathrm{SNR} = 10$ dB.

proposed algorithms are able to precisely detect the malicious attacks as well as accurately estimate power system states, even under the severe situation of partial measurements.

C. Performance vs. Attack Ratio

In this section, the attack ratio ϵ of attack vector $\mathbf{a}$ is varied to evaluate the performance of proposed algorithms in IEEE 118 bus system. The ϵ is varied from 5% to 15%, and $\mathrm{SNR} = 10$ dB.

From Fig. 6, the true positive rate is quite high at low sparsity ratio for both proposed algorithms. Particularly, when the sparsity ratio is 5%, the true positive rates are 93.6% and 94.3% at $f_a = 10\%$ for nuclear norm minimization and low rank matrix factorization, respectively. Compared with the PCA-based method, the performance of the proposed algorithms are quite stable as the attack ratio increases. When the attack ratio reaches 15%, the true positive rates for both algorithms are still around 90%. The true positive rates of proposed algorithms will decrease dramatically when attackers attack the power system massively. It is because that when the attack matrix are not sparse enough, the mixed-norm minimization is not able to separate the low rank anomaly-free matrix and attack matrix.

D. Performance on Large Scale System

Finally we analyze the scalability and computational efficiency of proposed algorithms on power flow data for Polish system during winter peak conditions 2007–2008, and compare their performances with the PCA-based detection method. In this part, the attack ratio is fixed at $\epsilon = 0.1$ and $\mathrm{SNR} = 10$ dB.

The ROC curve is shown in Fig. 7. It is shown in the figure that the performance of proposed algorithms is quite stable on the large scale system compare to the IEEE 57 bus system and IEEE 118 bus system. The comparison on the computational efficiency of two proposed algorithms are shown in Fig. 8. The data matrix row dimension m is varied from 100 to 3400, and is increased by 300 rows each time. The proposed algorithms are performed on the subset of the measurement matrix each time, and the CPU computation time is logged. It is shown in Fig. 8 that as the dimension of the measurement matrix increases, the CPU time for computation will increase, and the low rank matrix

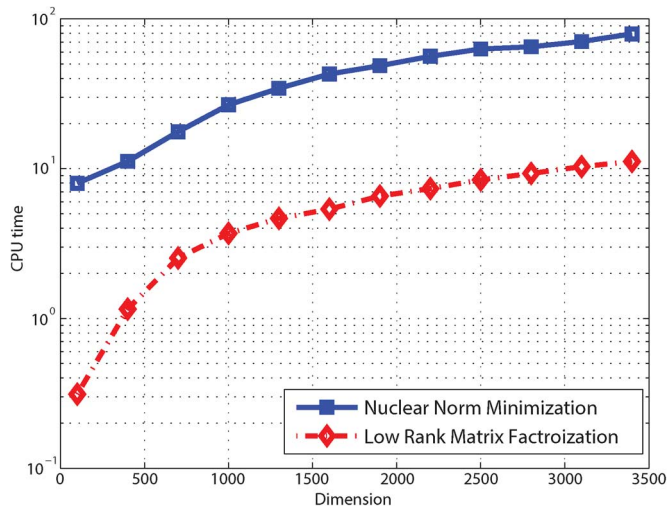


Fig. 8. CPU time versus matrix dimension for proposed nuclear norm minimization and low rank matrix factorization algorithms.

factorization approach performs better than the nuclear norm minimization method, which demonstrates a better scalability to large problems.

The numerical results validate the effectiveness of proposed algorithm. According to the simulation results, Both the low rank matrix factorization technique and nuclear norm minimization technique can solve the matrix separation problem, and the performance of the low rank matrix factorization is slightly better than nuclear norm minimization technique. From the perspective of recoverability, since the false data attack matrix $\mathbf{A}$ is not the dominant part compared with $\mathbf{Z_0}$ in this setting, the performance of ow rank matrix factorization technique is better. From the perspective of computation time, the low rank matrix factorization technique possesses a solution speed much faster than the nuclear-norm minimization due to its SVD-free feature. A detailed comparison of two algorithms is out the scope of this paper. A detail discussion can be found in reference [28].

V. Conclusion

In this paper, we propose a mechanism that exploits the temporal correlation of the time-series state measurements, as well as the sparse nature of the malicious attacks, to detect the false data injection in power grid. The false data detection problem is formulated as the matrix separation problem. Two methods, the nuclear norm minimization method and low rank matrix factorization method, are proposed to recover the electric power states as well as detect the malicious attacks in the power grid. The proposed methods can also deal with missing measurements. Numerical simulations are performed to evaluate the performance of proposed algorithms. The effects of the missing measurement ratio, attack ratio and dimension of measurements are also analyzed. Simulation results are compared with the PCA-based detection method and validate the effectiveness of proposed algorithms.

References

[1] E. Hossain, Z. Han, and H. V. Poor, *Smart Grid Communications and Networking*. Cambridge, U.K.: Cambridge Univ. Press, 2012.

[2] "Final report on the August 14, 2003 blackout in the United States and Canada: Causes and recommendations," U.S.-Canada Power System Outage Task Force, Apr. 2004.

[3] S. Gorman, "Effect of stealthy bad data injection on network congestion in market based power system," *Wall St. J.*, Apr. 8, 2009.

[4] A. Abur and A. G. Exposito, *Power System State Estimation: Theory and Implementation*. New York: Marcel Dekker, 2004.

[5] Y. Liu, M. K. Reiter, and P. Ning, "False data injection attacks against state estimation in electric power grids," in *Proc. 16th ACM Conf. Comput. Commun. Security*, Chicago, IL, USA, Nov. 2009.

[6] M. Esmalifalak, Z. Han, and L. Song, "Effect of stealthy bad data injection on network congestion in market based power system," in *Proc. IEEE Wireless Commun. Netw. Conf.*, Paris, France, Apr. 2012.

[7] L. Xie, Y. Mo, and B. Sinopoli, "False data injection attacks in electricity markets," in *Proc. IEEE Int. Conf. Smart Grid Commun.*, Gaithersburg, MD, USA, Oct. 2010.

[8] Z. Zhang, S. Gong, A. Dimitrovski, and H. Li, "Time synchronization attack in smart grid: Impact and analysis," *IEEE Trans. Smart Grid*, vol. 4, no. 1, pp. 87–98, Mar. 2013.

[9] Y. Yuan, Z. Li, and K. Ren, "Modeling load redistribution attacks in power system," *IEEE Trans. Smart Grid*, vol. 2, no. 2, pp. 382–390, Jun. 2011.

[10] Z. Zhang, M. Trinkle, A. Dimitrovski, and H. Li, "Combating time synchronization attack in smart grids: A cross layer defense mechanism," in *Proc. IEEE/ACM Int. Conf. Cyber Phys. Syst, (ICCPS)*, Philadelphia, PA, USA, Apr. 2013.

[11] H. Sandberg, A. Teixira, and K. H. Johansson, "On security indices for state estimators in power networks," in *Proc. 1st Workshop Secure Control Syst.*, Stockholm, Sweden, Apr. 2010.

[12] G. Dán and H. Sandberg, "Stealth attacks and protection schemes for state estimators in power systems," in *Proc. IEEE Int. Conf. Smart Grid Commun.*, Gaithersburg, MD, USA, Oct. 2010.

[13] M. Esmalifalak, G. Shi, Z. Han, and L. Song, "Bad data injection attack and defense in electricity market using game theory study," *IEEE Trans. Smart Grid, Special Issue on Cyber, Physical, and System Security for Smart Grid*, vol. 4, no. 1, pp. 160–169, Mar. 2013.

[14] O. Kousut, L. Jia, R. J. Thomas, and L. Tong, "Malicious data attacks on the smart grid," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 645–658, Dec. 2011.

[15] L. Liu, M. Esmalifalak, and Z. Han, "Detection of false data injection in power grid exploiting low rank and sparsity," in *Proc. IEEE Int. Conf. Commun.*, Budapest, Hungary, Jun. 2013.

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

[17] S. Cui, Z. Han, S. Kar, T. T. Kim, H. V. Poor, and A. Tajer, "Coordinated data-injection attack and detection in the smart grid: A detailed look at enriching detection solutions," *IEEE Signal Process. Mag.*, vol. 29, no. 5, pp. 106–115, Sep. 2012.

[18] Y. Zhao, A. Goldsmith, and H. V. Poor, "Fundamental limits of cyber-physical security in smart power grids," *IEEE Trans. Autom. Control, Special Issue on Control of Cyber-Physical System*.

[19] R. D. Zimmerman, C. E. Murillo-Snchez, and R. J. Thomas, "MATPOWER steady-state operations, planning and analysis tools for power systems research and education," *IEEE Trans. Power Syst.*, vol. 26, no. 1, pp. 12–19, Feb. 2011.

[20] J. J. Grainger and W. D. Stevenson, Jr, *Power System Analysis*. New York: McGraw-Hill, 1994, vol. 621.

[21] Z. Han, H. Li, and W. Yin, *Compressive Sensing for Wireless Communication*. Cambridge, U.K.: Cambridge Univ. Press, 2012.

[22] E. J. Cands and B. Recht, "Exact matrix completion via convex optimization," *Commun. ACM*, vol. 55, no. 6, pp. 111–119, Jun. 2009.

[23] E. Candès, X. Li, Y. Ma, and J. Wright, "Robust principal component analysis?," *J. ACM*, vol. 58, no. 3, pp. 1–37, May 2011.

[24] Z. Lin, M. Chen, L. Wu, and Y. Ma, "The augmented Lagrange multiplier method for exact recovery of corrupted low-rank matrices," UIUC, Tech. Rep. UILU-ENG-09-2215, 2009.

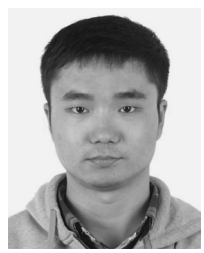
[25] D. P. Bertsekas, *Nonlinear Programming*. Belmont, MA, USA: Athena Scientific, 1999.

[26] J. Cai, E. Candès, and Z. Shen, "A singular value thresholding algorithm for matrix completion," *SIAM J. Optim.*, vol. 20, no. 4, pp. 1956–1982, Jan. 2010.

[27] D. P. Bertsekas, *Constrained Optimization and Lagrange Multiplier Method*. New York: Academic, 1982.

[28] Y. Shen, Z. Wen, and Y. Zhang, "Augmented Lagrangian alternating direction method for matrix separation based on low-rank factorization," Rice CAAM, Tech Report TR11-02.

[29] Z. Wen, W. Yin, and Y. Zhang, "Solving a low-rank factorization model for matrix completion by a nonlinear successive over-relaxation algorithm," Rice CAAM, Tech Rep. TR10-07.



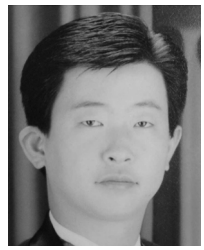
Lanchao Liu (S'11) received the B.S. degree in electrical engineering from Huazhong University of Science and Technology, China, in 2010. Now he is pursuing the Ph.D. degree at the University of Houston, TX, USA. His research interests are in the theoretical and algorithmic studies in signal processing and mathematical optimization, distributed and parallel computing algorithms, compressive sensing theory, statistical learning and inference, as well as their applications in communications, networks, smart grids, and hyperspectral imaging.

Mohammad Esmalifalak (S'12) received his M.S. degree in power system engineering from Shahrood University of Technology, Shahrood, Iran, in 2007 and the Ph.D. degree in electrical engineering from University of Houston, TX, USA, in 2013. From 2010 to 2013 he was Research Assistant in University of Houston. He is the author of the paper that won the best paper award in IEEE Wireless Communications and Networking Conference (WCNC 2012). His main research interests include application of data mining and machine learning in the operation and expansion of smart grids.

Qifeng Ding has a Ph.D. degree in electrical engineering from Texas A&M University, College Station, TX, USA, and a MBA degree from University of Houston, TX, USA. Currently he is a manager responsible for power system applications and development at CenterPoint Energy, Houston. He has been working in the power industry for more than fifteen years with experiences in power system modeling, power system operations software development, and cyber security management. He currently serves as the chair person for the EPRI grid operations task force. Dr. Ding also is a registered Professional Engineer in the state of Texas.

Valentine A. Emesih has B.S.E.E. and M.S.E.E. degrees from the University of Texas, Austin, TX, USA, Auburn University, Auburn, AL, USA, respectively

He is the Director of Control Systems Department for electric grid and market operations at CenterPoint Energy, Houston, TX, USA. He is responsible for various control systems used to securely monitor, manage and control advanced metering system meters, as well as electric distribution and transmission field devices. Prior to joining CenterPoint Energy, he held engineering, system development and project management positions for electric utility automation vendors Ferranti International Controls (now Ventyx ABB) and Johnson Controls (now ARINC Inc.). Mr. Emesih is a licensed professional engineer in Texas.



Zhu Han (S'01–M'04–SM'09–F'14) received the B.S. degree in electronic engineering from Tsinghua University, China, in 1997, and the M.S. and Ph.D. degrees in electrical engineering from the University of Maryland, College Park, MD, USA, in 1999 and 2003, respectively.

From 2000 to 2002, he was an R&D Engineer of JDSU, Germantown, MD, USA. From 2003 to 2006, he was a Research Associate at the University of Maryland. From 2006 to 2008, he was an Assistant Professor at Boise State University, ID, USA. Currently, he is an Assistant Professor in Electrical and Computer Engineering Department at the University of Houston, TX, USA. His research interests include wireless resource allocation and management, wireless communications and networking, game theory, wireless multimedia, security, and smart grid communication.

Dr. Han is an Associate Editor of IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS since 2010. Dr. Han is the winner of IEEE Fred W. Ellersick Prize 2011. Dr. Han is an NSF CAREER award recipient 2010. Dr. Han is a coauthor for papers that won several best paper awards in IEEE conferences.