New Scheme for Detecting False Data Injection Attacks in Power Systems

Guodong Liu 1, Hongli Guan 1, Ruiming Sheng 1, Daily Xian 2, Guoshu Liu 3, Chao Wu 1

1. Heze Power Supply Company of State Grid Shandong Electric Power Company, Heze 274000, Shandong Province
2. Institute of Smart Grid, Shandong University of Technology, Zibo 255000, Shandong Province
3. State Grid Shandong Electric Power Company Jiaozhou Power Supply Company, Qingdao 266300, Shandong Province

*Corresponding author e-mail: 331211152@qq.com

Abstract. Based on the low-rank nature of the matrix composed of grid measurement data and the sparse nature of the malicious attack matrix over a period of time, an inaccurate augmented Lagrangian multiplier method is used as a solution algorithm to construct a low-rank matrix recovery-based Fake data injection attack detection scheme. Based on the simulation results of the IEEE 57-bus standard test system, the relationship between the false alarm probability PFA and the threshold $\tau$, the relationship between the detection probability PD and the signal to attack ratio SAR, and the receiver characteristic curve (ROC) are analyzed in detail. Under the condition that the signal-to-noise ratio is 10dB and the false alarm probability is 5$, if the signal-to-attack ratio is less than 17dB, the detection probabilities of RPCA and PCA algorithms are 94% and 40%; if the signal-to-attack ratio is greater than 23dB, the detection probability of both Close to 0, it is no longer suitable for system monitoring. Compared to the PCA algorithm, the RPCA time performance is slightly worse, but it improves the detection probability and has a good detection effect when the signal-to-attack ratio is less than 17dB.

Keywords: Power Grid Information Security; Fake Data Injection Attacks; Low Rank Matrix Recovery; Detection Performance Analysis

Preface
Energy Internet takes the power system as the core, based on the Internet technology and new energy power generation technology, and integrates the power network and the information network into a complex multi-network flow system. The interdependence of the information network and the power network increases the operating risk of the power system [1]. If the information network is attacked, it may cause serious failure to the power network, causing a large-scale power outage or damage to important power equipment in the power system.
Modern power networks mainly use the SCADA system to realize the information exchange between the control center and remote terminal equipment (RTUS), and then provide a basis for decision-making for the control center. For cost considerations, smart meters generally do not add complex encryption technology, and communication. Increasingly, low-cost wireless communication networks and widely distributed public Internet will be used in the system, providing an entrance for malicious attacks. LIU Y first proposed the False Data Injection Attack scheme, Enabling attackers to tamper with the sensor measurement data and affect the state estimation results, while successfully avoiding existing bad data detection systems without increasing the risk of alarms. [4] analyzes the time correlation of the state quantity measurement matrix. And the limitation of attacker's ability will lead to the sparseness of the attack vector. It is proposed that the Robust Principal Component Analysis (RPCA) algorithm can be used to study the detection of false data injection attacks. Reference [5] uses the measurement of the state of the power grid for a continuous period of time. Time correlation, transform the problem of bad data detection into a matrix separation problem, and use principal component analysis (PCA) toThe flow is decomposed into normal subspace and abnormal subspace, so as to identify whether the measurement data has been tampered with. [6-8] detailed analysis of the attack strategy of the fake data injection attack and the potential harm of the attack. There is a lack of research on the detection performance of fake data injection attack detection schemes.

In order to analyze the performance of the fake data injection attack detection scheme in the power grid, based on the low rank of the grid state quantity measurement matrix and the sparseness of the attack vector, a fake data injection attack detection scheme based on the low rank matrix recovery technology was constructed, sar quantitatively characterizes the strength of the original data relative to the injection attack, and analyzes the detection performance of the scheme in detail.

1 system model

1.1 State estimation
The main purpose of power system state estimation is to estimate the current operating state of the power system based on various measurement information of the power system so that the control center can make timely decisions. The observation model can be expressed as

$$\mathbf{z} = \mathbf{h}(\mathbf{x}) + \mathbf{e} \quad (1)$$

Where: $h(\cdot)$ M-dimensional non-linear observation function representing the relationship between quantity measurement and state quantity, $e$ Zero mean measurement error vector.

For N-node power network, $n = 2N-1$ dimensional system state vector is $\mathbf{x} = (\mathbf{\theta}^T, \mathbf{V}^T)^T$, among them $\mathbf{V} = (\mathbf{V}_1^T \, \mathbf{V}_2^T \cdots \mathbf{V}_N^T)$ is the voltage magnitude vector, $\mathbf{\theta} = (\theta_2^T, \theta_3^T, \cdots, \theta_N^T)$ is the phase angle vector. The m-dimensional quantity measurement vector $\mathbf{z}$ Can be divided into two categories: $\mathbf{z}_p$, Composed of the active power flow measurement value $P_{ij}$ from bus i to j, and the injected active power measurement value $P_j$ at bus i; $\mathbf{z}_q$. It consists of the reactive power flow measurement value $Q_{ij}$ from bus bar i to j, and the injected reactive power measurement value $Q_j$ at bus bar i. This paper uses the first type of measurement, namely the active power flow measurement value $\mathbf{z}_p$.

$$\mathbf{e} = (e_1, e_2, \cdots, e_m)^T \text{is the zero mean measurement error vector, usually } m \gg n \text{ indicates high measurement redundancy. Here } e_i \text{ are independent Gaussian distribution variables, variance } \sigma_i^2 \text{ represents the relative uncertainty of the i-th quantity measurement. } e \sim \mathcal{N}(0, \mathbf{R}), \text{ among them } \mathbf{R} = \text{diag}(\sigma_1^2, \cdots, \sigma_m^2) \text{ is the covariance matrix.}$$

The state estimation problem is to find the optimal n-dimensional state variables of the observation model (1) $\hat{x}$ For DC systems, model (1) can be reduced to a linear model.
\[ z = Hx + e \]  \hspace{1cm} (2)

Among them, the observation matrix \( H = (h_{ij})_{m \times n} \).

Most current state estimators use weighted least squares estimation algorithms, and the estimated system state variable expressions are as follows

\[ \hat{x} = (H^TR^{-1}H^{-1})^{-1}H^TR^{-1}z \]  \hspace{1cm} (3)

However, malicious attack, noise, equipment failure, and sensor measurement performance of the attacker will have a greater impact on the state estimation results. In order to detect and identify bad data in the measurement, a hypothesis testing method based on measurement residuals came into being. Bad data identification can be achieved by comparing the magnitude of the L2 norm with the threshold \( \tau \) [3,5,6].

1.2 false data injection attack against state estimation

The tight combination of physical equipment and information equipment in the energy Internet makes the state estimator extremely vulnerable to network attacks. Therefore, intruders can tamper with the measurement data in the scada system through network attacks, making the measurement data received by the control center \( z_i \) contains malicious attack data, its model is

\[ z_i = z + a = h(x) + e + a \]  \hspace{1cm} (4)

Where: \( a = (a_1, a_2, \cdots, a_m)^T \) is the attack vector; \( Z = (z_1, z_2, \cdots, z_m)^T \) Measure the vector for the original quantity, \( a_i \) non-zero indicates that the attacker invaded the \( i \)-th sensor and measured the original quantity \( Z \). Replaced by a false quantity measurement \( z_i + a_i \).

LIU Y proposes a false data injection attack scheme: if and only if the attack vector \( a \) can be expressed as a linear combination of column vectors of \( h \) \( a = Hc \) is the linearization factor, and the measurement residual is not affected by the attack vector \( a \). Influence. \( \hat{x}_{ad} \) is the mean difference, and the L2 norm of the measurement residual after the attack is

\[ \| z_i - H\hat{x}_{ad} \| = \| z + a - H(\hat{x} + c) \| = \| z - H\hat{x} + (a - Hc) \| = \| z - H\hat{x} \| \]  \hspace{1cm} (5)

The attack scheme measures the amount of tampering \( Z \). At the same time, it does not change the measurement residuals, making traditional bad data detection methods invalid. In addition, if the attacker has a certain understanding of the network topology, he can modify the sensor measurement by entering the power system communication network through network intrusion, resulting in traditional bad data. The detection system is ineffective against new types of attacks. Therefore, it is necessary to rethink the fake data injection attack detection scheme.

2 detection scheme

In actual working conditions, the attacker's ability is limited. The attack is often limited to a specific location or a specific number of sensors or intermittently attacks the sensors, so the attack vector \( a \). In addition, the system state variables change slowly and the measurement vectors over a period of time have correlations, so this detection scheme is not to observe the measurement of the state of the power grid at an isolated moment, but to consider the measurement over a period of time.

The original quantity measurement vector at time \( k \) is \( z_k \), and the matrix composed of quantity measurements in time period \( t \) is \( Z = [z_1, z_2, \cdots, z_n] \in \mathbb{R}^{m \times t} \). The matrix of attack vectors in time period \( t \) is \( A = [a_1, a_2, \cdots, a_t] \in \mathbb{R}^{m \times t} \).

The quantity measurement matrix \( d \) containing malicious data can be expressed as:
\[ D = Z + A \] (6)

The column vector of the original quantity measurement matrix \( z \) is a continuous time grid state quantity measurement, which has high correlation, so \( z \) has low rank. The attacker's ability is limited, making the attack matrix a sparse on the rows and columns.

There is noise in the transmission process in actual working conditions, and its quantity measurement matrix \( d \) can be described as:

\[ D = Z + A + W \] (7)

Where \( W \) is a Gaussian noise matrix and its Frobenius norm \( \|W\|_F < \delta \).

The existence of the attack matrix \( a \) is detected from the actual measurement matrix \( d \), which is essentially a low-rank matrix recovery problem or a robust principal component analysis problem, so the low-rank matrix recovery algorithm needs to be analyzed.

2.1 Low rank matrix recovery algorithm

Low-rank matrix recovery (low-rank matrix recovery) is also called Robust Principal Component Analysis (RPCA). Reference [9] gives the definition of robust principal component analysis, that is, given a matrix \( D = Z + A \), where the original data matrix \( Z \) and the error matrix \( A \) are unknown, \( Z \) is known to have low rank and \( A \) is sparse, and \( Z \) is to be recovered.

By finding the lowest rank \( z \) that can produce the data matrix \( d \), and obey the constraints \( \|A\|_F \leq k \), can solve the above problem. Its Lagrange transform expression is

\[
\min_{Z,A} \text{rank}(Z) + \gamma \|A\|_F \\
\text{s.t.} \quad D = Z + A
\] (8)

Where: \( \text{rank} (Z) \) is the rank of the matrix \( Z \), \( \|A\|_F \) is the number of nonzero elements of matrix \( a \).

For a suitable compromise factor \( \gamma \), solving equation (8) can recover the original data matrix \( Z \) and the error matrix \( A \). However, due to the rank \( (Z) \) and \( \|A\|_F \) both are non-linear and non-convex combinatorial optimization functions, and it is very difficult to solve the above problems. In order to overcome the computational difficulties, the objective function is usually replaced with some convex functions and converted into corresponding convex optimization problems [10].

Function \( \text{rank} (Z) \) in the collection \( \{Z \in \mathbb{R}^{m \times n} | \|Z\|_{2,2} \leq 1 \} \) The convex envelope on is the kernel norm of \( z \) \( \|Z\| = \sum_{k=1}^{n} \sigma_k Z \) (i.e. the sum of all singular values of matrix \( z \)), \( \|A\|_F \). The convex envelope of (1,1) norm \( \|A\|_{1,1} = \sum_{i=1}^{m} \sum_{j=1}^{n} |A_{i,j}| \), Which eventually translates into the following convex optimization problem:

\[
\min_{Z,A} \|Z\|_F + \lambda \|A\|_{1,1} \\
\text{s.t.} \quad D = Z + A
\] (9)

In the formula: \( \lambda \) is the convexity coefficient, which is recommended in [11-12] \( \lambda \) for \( 1/\sqrt{\max (m, n)} \) \( (m \geq n) \).

The main methods for solving RPCA problems are iterative threshold method (IT), singular value threshold method (SVT), accelerated approximate gradient method (APG), accurate augmented Lagrangian multiplier method (EALM), and inexact augmented Lag Inexact Augmented Lagrange
Multipliers (IALM) and Alternate Direction Method (ADM). The IALM algorithm has the advantages of fast calculation speed and less storage space. Therefore, IALM was selected as the algorithm to solve the low-rank matrix recovery problem \cite{11-14}.

When using ialm for formula (9), write \(x = (z, a)\), \(\hat{f}(x) = \|Z\|_1 + \lambda_1 \|A\|_1\), \(h(x) = D - Z - A\), Then its augmented Lagrangian function is

\[
L(Z, A, Y, \mu) = \|Z\|_1 + \lambda_1 \|A\|_1 + \langle Y, D - A \rangle + \frac{\mu}{2} \|D - Z - A\|^2
\]

when \(Y = Y_k\), \(\mu = \mu_k\) Solve using alternate iteration method \(\min_{Z,A} L(Z, A, Y_k, \mu_k)\) \cite{11-12} approximate solution, the iterative update formula of \(a\) and \(z\) is

\[
Z_{k+1} = \arg \min_{A} L(Z_{k+1}, Y_k, \mu_k)
\]

\[
= D_{1/\mu_k} (\mu_k - A_{k+1} + Y_k / \mu_k)
\]

\[
2.2 \text{ Intrusion Detection Algorithm}
\]

Select the observation time length as \(K\), and note the data matrix \(D = Z + A + W\) observed during the period of \(t-K+1 \sim t\). The original data matrix \(Z\) is the active power flow value matrix of the power system, and \(W\) is the Gaussian noise matrix. \(A\) is the sparse attack matrix. The intrusion detection steps are:

1) Use the inaccurate augmented Lagrangian multiplier method to process the data matrix \(d\) to get an estimated attack matrix \(\hat{A}\).

2) Robust principal component analysis to calculate \(A\)-hat.

3) State judgment.

Consider the following binary assumptions:

\(H_0\): \(A (j, i) = 0\), which means that the attack at position \(j\) at time \(i\) is not detected;

\(H_1\): \(A (j, i) \neq 0\), which represents an attack at position \(j\) at time \(i\).

Due to the presence of noise, the recovered attack matrix \(\hat{A}\) It is not necessarily 0 at the location where there is no attack. In order to detect the abnormal value of the sensor measurement received by the control center, the absolute value of the attack at the position \(j\) at time \(i\) is estimated as a statistical judgment.

\[
T = \left|\hat{A}(j, i)\right|_H \otimes \tau
\]

When \(T\) is greater than the threshold \(\tau\) (\(\tau\) is determined by the false alarm probability), it is considered that an attack at position \(j\) at time \(i\) is detected. If an attack at any time and at any position is detected, an alarm is issued. The process is shown in Figure 1.
3 detection performance analysis

In order to perform performance analysis on the constructed detection scheme, artificial data is artificially constructed and injected into the active power flow data generated by the simulation for experiments.

The active power flow measurement value $P_{ij}$ from bus $i$ to $j$ is selected as the active power flow measurement $Z$. The active power flow data can be obtained by calculating power flow through MATPOWER. The IEEE57-bus standard test system file case57.m provided by MATPOWER is used as the simulation condition. (The reference capacity is 100MVA.) The IEEE57-bus standard test system has a total of 80 branches, so the number of measurement points is $m = 80$. The low-rank matrix recovery algorithm requires the original data matrix to have a low rank, that is, rank $(Z) \ll \min (m, K)$, so in this experiment, the observation time length $K = m = 80$ is selected, and the measurement matrix $Z$ is an $80 \times 80$ order matrix.

Use the real-time load data provided by PJM company on its website every 5 minutes on March 26, 2017 for normalization processing to generate a 24h standard load file, as shown in Figure 2. Assume that the IEEE57-bus standard test The load on each bus of the system changes according to the law of this standard load file, that is, the load of a bus at a certain moment is the bus load set in case57.m multiplied by the standard load factor at that moment. Calculated by MATPOWER Four of them represent the time-varying curve of the active power flow value on the branch line as shown in Figure 3, where: line1 is the branch line with the most active power flow fluctuations, line30 is the branch line with the least active power flow fluctuations, and line10 and line20 are active power flows. Typical branch between maximum and minimum fluctuations.
As can be seen from Figure 3, the measurement trend of the system state quantity is gentle. The rank \( Z \) of the active power flow value matrix calculated in the simulation test is \( 7 \ll \min (m, K) \), indicating that the active power flow value matrix of the power system meets the low Rank requirements.

While collecting the measurement data, use the method provided in [16] to construct fake data to conduct a malicious attack on a small part of the measurement data (the location and time of the attack are randomly selected). The attack matrix \( A \) is an \( m \times K \) sparse matrix, whose number of non-zero elements is \( k \), is randomly generated with a uniform position distribution, and the size is independent and uniformly distributed on \([0,100]\).

Define the Signal to Attack Ratio (SAR) as \( \text{SAR} = 10 \log_{10} \frac{\| Z \|_F}{\| A \|_F} \). The unit is dB, reflecting the strength of the original data relative to the injection attack.

However, noise is also mixed into the quantity measurement \( z \). In the simulation experiment, the noise matrix \( w \) is set to a Gaussian matrix generated by a random function. The signal-to-noise ratio is defined as \( \text{SNR} = 10 \log_{10} \frac{\| z \|_F}{\| w \|_F} \) in dB.

The detection probability \( p_D \) and false alarm probability \( p_{FA} \) are obtained by Monte Carlo experiments. The definitions of \( p_D \) and \( p_{FA} \) are

\[
P_D = \frac{N_{\text{Hit}}}{N_{\text{Hit}} + N_{\text{Miss}}} \quad P_{FA} = \frac{N_{\text{False}}}{N_{\text{False}} + N_{\text{Correct}}} \quad (14)
\]

In the formula: \( n_{\text{Hit}} \) is the number of times that a malicious attack was successfully detected at the correct location at the correct time; \( n_{\text{Miss}} \) is the number of times that there was an attack but no alarm;
\( n_{\text{False}} \) is the number of times that there was no attack but the alarm was reported; \( n_{\text{Correct}} \) is the number of correctly determined no attacks.

Next, analyze the detection performance of the detection scheme through the simulation test results, and compare the rcpa algorithm with the pca algorithm.

3.1 Relationship between false alarm probability \( P_{FA} \) and threshold \( \tau \)

![Figure 4](image4.png)

**Figure 4** Relationship between SNR = 10dB, false alarm probability \( P_{FA} \) of RPCA algorithm and threshold \( \tau \)

![Figure 5](image5.png)

**Figure 5** Relationship curve between PCA algorithm false alarm probability \( P_{FA} \) and threshold \( \tau \)

In order to analyze the relationship between the two algorithms, RPCA and PCA, and the threshold \( \tau \), a fixed signal-to-noise ratio SNR = 10dB was selected. The relationship between the false alarm probability \( P_{FA} \) and the threshold \( \tau \) under the two algorithms is shown in Figures 4 and 5. The calculation results show that regardless of the RPCA algorithm or the PCA algorithm, the false alarm probability \( P_{FA} \) decreases with the increase of the threshold \( \tau \). The RPCA algorithm threshold greater
than 0.009 can control the false alarm probability within 5%, and the PCA algorithm. The threshold needs to be adjusted above 0.313 to control the false alarm probability within 5%. Therefore, when the signal-to-noise ratio is the same, we want to control the false alarm rate to the same range. The threshold set by the RPCA algorithm should be less than the threshold set by the PCA algorithm.

3.2 Relation between detection probability $p_D$ and signal-to-attack ratio $SAR$

The signal-to-attack ratio $SAR$ reflects the strength of the original data relative to the injection attack, which in turn affects the detection probability $P_D$. In order to measure the relationship between the RPCA algorithm and the PCA algorithm and the signal-to-attack ratio $SAR$, a fixed signal-to-noise ratio $SNR = 10$dB, virtual alarm probability $P_{FA} = 5\%$, RPCA algorithm selection threshold $\tau_1 = 0.009$, PCA algorithm selection threshold $\tau_2 = 0.313$ (selected according to $P_{FA} - \tau$ curve), signal to attack ratio $SAR$ from 0 ~ 30dB change. Make $P_D$ - SAR curve as shown in Figure 6.

![Figure 6](image)

**Figure 6** Relationship between $SNR = 10$dB, $P_{FA} = 5\%$, detection probability $P_D$ and signal to attack ratio $SAR$

It can be seen from Figure 6 that the smaller the signal attack than the SAR, that is, the larger the injection attack relative to the original data, the higher the detection probability. Under the same attack intensity, the detection probability of the RPCA algorithm is higher than that of the PCA algorithm. When the signal-to-noise ratio is 10dB and the false alarm probability is 5%, if $SAR < 17$dB, the detection probability of RPCA algorithm can reach more than 94%, while the detection probability of RPCA algorithm is only 40%; if $SAR > 23$dB, RPCA and PCA algorithms detect The probability is close to 0%, and system monitoring will no longer apply.

3.3 roc curve

![Figure 7](image)

**Figure 7** roc curve of rpca algorithm and pca algorithm
Receiver Operating Characteristic (ROC) curves are used to describe the relationship between detection probability and false alarm probability, and then reflect the performance of the algorithm. To analyze the detection performance of RPCA algorithm and PCA algorithm, under the same experimental conditions (SNR = 10dB, SAR = 17dB), the ROC curves of the RPCA algorithm and PCA algorithm are shown in Figure 7. The results show the false alarm probability $P_{FA}$ When it is 0.02, the detection probability of the rpca algorithm can reach more than 95%, while the detection probability of the pca algorithm is only 47%. The same false alarm rate $P_{FA}$ Under the conditions, the detection probability of the RPCA algorithm is greater than the detection probability of the PCA algorithm, that is, the performance of the RPCA algorithm is better. From the time performance, the PCA algorithm runs once and the CPU takes 0.6s, while the RPCA algorithm runs once and the CPU takes 1.61. s, that is, the RPCA algorithm runs slower than the PCA algorithm. The improvement of the detection performance of the RPCA algorithm is at the expense of some time performance.

4 conclusion
Using the low rank of the grid state quantity measurement matrix and the sparseness of the attack vector, a grid false data injection attack detection scheme based on the low rank matrix recovery technology is constructed.

The signal-to-attack ratio SAR is used to quantitatively characterize the relative injection attack intensity of the original data, and the relationship between the detection probability PD and the signal-to-attack ratio SAR is analyzed. With a signal-to-noise ratio of 10dB and a false alarm probability of 5%, if SAR <17dB The detection probability of the RPCA algorithm can reach more than 94%, and the detection probability of the RPCA algorithm is only 40% .If SAR> 23dB, the detection probability of the RPCA and PCA algorithms is close to 0%, which is no longer suitable for system monitoring.

Analyzing the relationship between the false alarm probability PFA and the threshold τ, it is found that when the signal-to-noise ratio is the same and the false alarm rate is to be controlled in the same range, the threshold set by the RPCA algorithm is smaller than the threshold set by the PCA algorithm. The receiver characteristic (ROC) curve found that considering the detection probability, the RPCA algorithm is better than the PCA algorithm, and it has a good detection effect when SAR <17dB.

References
[1]. Tian Shiming, Luan Wenpeng, Zhang Dongxia, et al. Technology Forms and Key Technologies of Energy Internet [J]. Chinese Journal of Electrical Engineering, 2015, 35 (14): 3482-3494.
[2]. LIU J, XIAO Y, LI S, et al. Cyber Security and Privacy Issues in Smart Grids[J]. IEEE Communications Surveys and Tutorials, 2012, 14(4): 981-997.
[3]. LIU Y, NING P, REITER M K. False Data Injection Attacks against State Estimation in Electric Power Grids[C]//Proceedings of the 16th ACM Conference on Computer and Communications Security, 2009: 21-32.
[4]. LIU L, ESMALIFALAK M, DING Q, et al. Emesih, Zhu Han. Detecting False Data Injection Attacks on Power Grid by Sparse Optimization[J]. IEEE Transactions on Smart Grid, 2014, 5(2): 612-621.
[5]. VALENZUELA J, WANG J, BISSINGER N. Real-time intrusion detection in power system operations[J]. IEEE Transactions on Power Systems, 2013, 28(2): 1052-1062.
[6]. TEIXEIRA A, DAN G, SANDBERG H, et al. A cyber security study of a SCADA energy management system: Stealthy deception attacks on the state estimator[J]. arXiv preprint arXiv, 2010,1011-1018.
[7]. Yang Qingyu, Yang Jie, Ma Xunming. Research on Fake Data Injection Attacks in Power Systems [J]. Microelectronics & Computer, 2011, 28 (12): 175-179.
[8]. Liu Wan, Zhao Yuchen, Liu Yang, et al. Detection method of smart grid attack based on alarm
data fusion [j]. Journal of Shandong University (Science Edition), 2014,49 (9): 35-40.
[9]. WRIGHT J, PENG Y, MA Y, et al. Robust principal component analysis: Exact recovery of corrupted low-rank matrices by convex optimization[C]//Proceedings of Advances in Neural Information Processing Systems, 2009:2080-2088.
[10].KOSUT O, JIA L, THOMAS R J, et al. Malicious data attacks on smart grid state estimation: Attack strategies and countermeasures[C]//2010 First IEEE International Conference on Smart Grid Communications (SmartGridComm),2010:220-225.
[11].CANDES E J, LI Xiaodong, MA Yi, et al. Robust principal component analysis [J]. Journal of the ACM,2011,58 (3) : 1-37.
[12].SHI Jiarong, ZHENG Xiuyun, WEI Zongtian, et al. Overview of recovery algorithms for low rank matrix algorithms [j]. Application Research of Computers, 2013,30 (6): 161-1605.
[13].YUAN X, YANG J. Sparse and low-rank matrix decomposition via alternating direction methods[J]. Pacific Journal of Optimization, 2013, 9(1): 167-180.
[14].BOUWMANS T, ZAHZAH E H. Robust PCA via Principal Component Pursuit: A review for a comparative evaluation in video surveillance[J]. Computer Vision and Image Understanding, 2014, 122: 22-34.
[15].PJM Operational Data[EB/OL]. http: //www.pjm.com.
[16].ROCKAFELLAR R T. Convex analysis[M]. Princeton university press, 1997.