Cyber Attacks, Detection and Protection in Smart Grid State Estimation

Yi Zhou, *Student Member, IEEE* Zhixin Miao, *Senior Member, IEEE*

***Abstract*—This paper reviews the types of cyber attacks in state estimation as well as detection and protection schemes. Recent studies show that adversaries can not only generate attack vectors, which can bypass the conventional detector, but can also optimize the attack vector to compromise least number of sensors. We examined four types of attack in state estimation process. Then, we examined least effort false data injection attack on how to find the optimal attack vector. Based on the analysis, we implement χ^2 detector and Euclidean distance detector to detect attacks. We propose an effective way to protect power system sensors. The case studies are based on a 5-bus system and IEEE-14 bus system. It shows that least effort attack can make most significant deviation of state estimation by compromising least number of sensors. χ^2 detector can detect random data injection, bad data injection and DoS attack. However, false data injection can bypass conventional statistical detector, such as χ^2 detector. Euclidean distance detector can detect false data injection.**

***Index Terms*—Cyber attacks, power grid, state estimation**

I. Introduction

Power grid is a cyber-physical system (CPS) that consists of electrical equipments and communication systems. It supplies electric power through power transmission and distribution networks to large geographical areas. The Supervisory Control and Data Acquisition (SCADA) system in power system can collect power system measurements, monitor and control the power system. The control center can use these data to estimate state variables of the power grid so that the power system situation awareness and security will be enhanced. The sensors in power system measure three-phase instantaneous voltages, currents and their phasors. These data will be sent to the control center through a communication system. State estimation will be carried out in the control center. The estimates will be used to generate appropriate commands to control the system.

State estimation computes state variables in real-time based on meter measurements in the field. If the control center receives wrong measurements due to cyber attacks, wrong state estimation will be made. In turn, wrong decisions will be made, which might cause the system to collapse.

To achieve a high reliability and security level, the robustness of the communication system in the power grid should be improved [3], [4]. In this paper, we assume that the power system is running in steady state, and there is no load change or fault. We will use DC power flow model to represent the power system.

Most existing attacks are DoS attack, random data injection and bad data injection, since these three types of attack are easy to generate. These attacks can be detected by statistical detectors, such as χ^2 detector. However, if the adversary knows the configuration and information of the power system, he can technically generate false data attacks [5], which can bypass the χ^2 detector. The adversary can even find the most optimal attack vector to compromise least number of sensors.

For false data injection, Euclidean Distance detector [1] has been proposed to check the deviation at each estimation step. Based on the previous analysis, we propose an efficient method to protect least number of sensors and to detect most false data injection attacks based on the power system topology.

This paper is to 1) verify the effect of cyber attacks on hypothesis testing and indicate that false data injection cannot be detected by conventional hypothesis detection, 2) present least effort false data injection, 3) show that Euclidean Distance detector can detect false data injection, 4) prove how to most efficiently protect sensors to mitigate false data injection. The case study is based on a 5-bus system and IEEE-14 bus system.

This paper is arranged as follows. Section II explains Least Square Estimation (LSE) and Weighted Least Square (WLS) state estimation. Attack models are also presented. Section III introduces two types of detection, χ^2 detection and Euclidean Distance detection. A protection method is also presented in this section. Case studies and conclusion are presented in Section IV and Section V.

II. State Estimation and Conventional χ^2 Detection

This section will present LSE and WLS estimation in power systems. The mechanism of statistical detection is also explained. This detector can detect random data injection, bad data injection and DoS attacks.

A. State Estimation in Power Systems

Usually, a power flow model is a set of equations that indicate the running state of the power grid. The estimation process can be formulated as follows [2]:

$$z = h(x) + e, \tag{1}$$

where z is the measurement vector, x is the state vector, e is zero-mean variable vector that in Gaussian distribution and $h(\cdot)$ is a function. There are two types of estimation models: AC power flow model and DC power flow model.

AC power flow model is a set of equations that represents the relationship between voltage phasors and active/reactive power. This type of model is nonlinear model. $h(x)$ is a nonlinear vector function, since the active and reactive power can be derived by the following equations [2]:

Yi Zhou, Yi Zhou is with Dept. of Electrical Engineering, University of South Florida, Tampa FL 33620. Email: yizhou@usf.edu.

$$P_{ij} = \frac{V_i V_j}{X_{ij}} \sin(\theta_i - \theta_j), \tag{2}$$

$$Q_{ij} = \frac{V_i V_j}{X_{ij}} \cos(\theta_i - \theta_j) \tag{3}$$

where V_i is the i-th bus voltage magnitude and θ_i is the i-th bus phase angle. The power injection at bus i can be derived by [2]:

$$P_i = \sum_{j \in \aleph_i} P_{ij},$$
$$Q_i = \sum_{j \in \aleph_i} Q_{ij}, \tag{4}$$

where $\aleph_i$ refers to the adjacent buses to Bus i, P_{ij} is the active power flow from bus i to bus j, Q_{ij} is the reactive power flow from bus i to bus j, P_i is the active power injection at bus i, Q_i is the reactive power injection at bus i, X_{ij} is the reactance of branch between bus i and bus j, θ_i and θ_j are the voltages phase angles of buses i and bus j.

DC power flow model can approximate the AC power flow model. In this scenario, voltage magnitudes are assumed to be 1 per unit and angle difference of two connected buses are very close to each other. By doing so, all shunt elements, bus and branch and reactive power flow can be ignored in estimation process. So (4) can be linearized and rewritten by [2]:

$$P_{ij} = \frac{\theta_i - \theta_j}{X_{ij}} \tag{5}$$

$$P_i = \sum_{j \in \aleph_i} P_{ij}, \tag{6}$$

Measurements usually include the power flows P_{ij} and power injections P_i. The state variables include the phase angles θ_i.

$$z = Hx + e \tag{7}$$

where $z \in \mathbb{R}^m$ and $x \in \mathbb{R}^n$. The coefficients matrix $H \in \mathbb{R}^{m*n}$. In DC-model, $H^{m \times n}$ represents the relationship between the measurement vector and the state variable vector. H is a constant matrix. $e_i \in \mathbb{R}(i = 1, 2, 3...m)$ can be seen as zero-mean variables that in Gaussian distribution, which can be written as $e_i \sim (0, \Sigma)$.

1) Least Square Estimation (LSE): In LSE estimation procedure, the objective is to find $\hat{x}$ that minimize $J(x) = (z - Hx)^T (z - Hx)$.

2) Weighted LSE: In WLS estimation procedure, error variances need to be considered. The objective is to find $\hat{x}$ that minimizes $J(x) = (z - Hx)^T \Sigma^{-1} (z - Hx)$, where Σ^{-1} is a diagonal matrix with its element the reciprocals of the variances of meter errors. $\hat{x}$ can be found from the normal equation:

$$\hat{x} = (H^T \Sigma^{-1} H)^{-1} H^T \Sigma^{-1} z.$$

$J(x)$ is the cost function, which can be seen as the square of the norm 2 of the residual vector r ($r = z - H\hat{x}$, $J = r^T \Sigma^{-1} r$). It represents the estimation performance indication. Notice $(H^T \Sigma^{-1} H)$ could be singular if some measurements are assumed to be very accurate. In that case, we cannot use normal equation to find the estimate. Instead, QR decomposition method will be used to avoid conducting matrix inverse.

The original estimation model is first converted to

$$\underbrace{Wz}_{z'} = \underbrace{WH}_{H'} x + \underbrace{We}_{e'},$$

where $W^2 = \Sigma^{-1}$, $W^T = W$. We can find that the modified error from every meter has the same accuracy: $We \sim (0, I)$.

Consider $H' = QR$ ($Q \in \mathbb{R}^{m \times m}$ is an orthogonal matrix $Q^T Q = I$ and $R \in \mathbb{R}^{m \times n}$ is an upper triangular matrix), the estimate will be derived as:

$$\begin{aligned} \hat{x} &= (H'^T H')^{-1} H'^T z' \\ &= (R^T Q^T Q R)^{-1} R^T Q^T z' \\ &= (R^T R)^{-1} R^T Q^T z' \\ \\ &\Rightarrow R^T R \hat{x} = R^T Q^T z' \\ &\Rightarrow R\hat{x} = Q^T z' \end{aligned} \tag{8}$$

(8) indicates that matrix inverse is avoided. This paper uses CVX [6] toolbox in Matlab to implement state estimation, where QR decomposition based solving is automatically embeded. The CVX code shows as below:

```
function [X, J] = fun_LSE(Z, H);
cvx_begin %quiet
variable X(14,1)
minimize ((Z-H*X)'*(Z-H*X))
subject to
X(1) ==0;
cvx_end
J = ((Z-H*X)'*(Z-H*X));
return
```

In this code, X define as the state variables, J defineed as the system cost value. Z represents measurements vector that is measured from sensors embed in power grid. H is the Jacobian matrix of the power system. Because we set bus 1 as the reference bus, so the phase angle at bus 1 is 0° (degree).

B. Attack Models

Usually, the communication system in the power system may be subjected to the following attacks:

1) *Random Noise Injection*: The attack vector is a random noise attack.

2) *Bad Data Injection*: In these cases, the adversary injects non-designed data to the original measurements vector. The vector can be injected at any point in time and it could be a long term continuous attack or short term attack. Notice that, the mean value and covariance of random attack vector should be much larger than the normal noise. In this paper, we add a random attack vector or unchanged vector to the measurements to arbitrarily test its performance.

3) *DoS Attack*: The denial-of-service (DoS) attack is generated by jamming the communication channels, flooding packets in the network, and compromising devices to prevent data transfer, etc. by the adversary. The DoS attack could be on sensor data, control data, or both. In this paper, we model the DoS attack as the lack of available sensor data [1].

C. χ^2 Detection

In random data and bad data injection attack, because the attack vectors are not designed by the adversary, injected data may not be of the same dimension of z. In that case, the detector will trigger an alarm. If the system under DoS attack, the communication will be interrupted, which means the control center can not receive all the measurements data. If the range of bad injected data is same as the measurements vector z, the control center will use these polluted data to compute the wrong state variables. For these two type of attack, we can use χ^2 detector to test its cost function $J(x)$. Since $z \in \mathbb{R}^m$ and $x \in \mathbb{R}^n$, the freedom degree of $\|z-Hx\|$ is $m-n$. From χ^2 table, we can set a threshold τ for hypotheses test. If the cost function value larger than the threshold, the system is under attack.The threshold can easily be obtained from the χ^2-table. If $J(\hat{x}) > \tau$, we can say there is an attack vector added to the measurements vector [5]. The following figure shows χ^2 different probability density functions in different freedom degrees from 1 to 9.

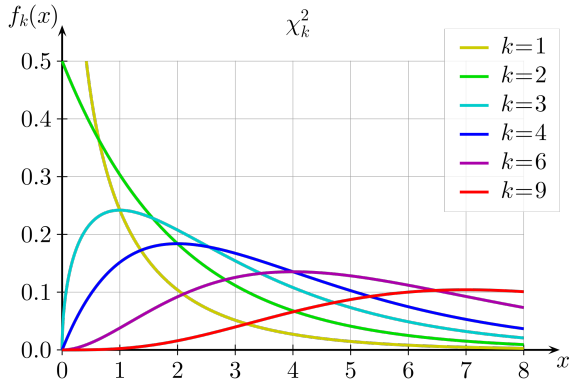


Fig. 1: χ^2 Probability Density Function [7]

III. False Data Injection Attack

If the adversary knows the configuration and information of the power system, he/she can design an attack vector to evade detection. The control center will get wrong state variables, and these wrong state variables can bypass conventional statistical detector. With previous knowledge, Hx is a linear vector function, which satisfy distributive property and associative property. If there is an attack that inject an attack vector a, the measurements vector becomes $z_a = z + a$. The control center will receive this manipulated vector and use it to process the estimation. To calculate the cost function that under attack, we define $\hat{x}_f = \hat{x} + c$, $\hat{x}$ as the original estimated state variables vector and c as the malicious error added to the original estimates. Then the following equation of new cost describes why false data injection can bypass χ^2 detector [2]:

$$\begin{aligned} \|z_a - H\hat{x}\|^2_{\Sigma^{-1}} &= \|z + a - H(\hat{x} + c)\|^2_{\Sigma^{-1}} \\ &= \|z - H\hat{x} + a - Hc\|^2_{\Sigma^{-1}} \\ &= \|z - H\hat{x}\|^2_{\Sigma^{-1}} \quad \text{when } a = Hc \end{aligned} \tag{9}$$

where $\|\cdot\|^2_{\Sigma^{-1}} = (\cdot)^T\Sigma^{-1}(\cdot)$.

This equation shows that the cost function will not change if there is a designed attack vector a that satisfy $a = Hc$ injected to the measurements vector. This type of attack will bypass the detector. If the adversary needs to change some state variables, he/she can compute the attack vector by using the H matrix.

A. Least Effort False Data Injection

Least effort false data injection [2] is a method to find the most optimal false data attack vector. In this paper, we assume there is 1 meter on each bus to measure its power injection and 2 meters on each branch to measure its power flow. These measurements are constitutes of the measurements vector z. The purpose of least effort attack is to find the sparest attack vector a with most zero elements and satisfies the vector function $a = Hc$. By doing so, the adversary can attack least number of sensors to get most deviation change of state variables. Referring to the previous knowledge, the adversary needs to know the topology and configuration of the power grid. (The adversary needs to find the sparsest attack vector to pollute the minimal sensors.) Since the system has n buses, considering that the adversary need to attack k state variables, $k \leq n$. The sparsest attack vector should satisfies the vector function $a = Hc$. Then the problem is to minimize the numbers of nonzero element in attack vector. This problem can be formulated as follows.

$$\begin{aligned} \min_{c} \quad & \|Hc\|_0 \\ s.t \quad & \|c\|_0 = k \end{aligned} \tag{10}$$

If there are k state variables that need to manipulate in an n-bus system, let $\Gamma = i_1, i_2, i_3 ... i_k$, be the adjacent sensors, $g\Gamma$ be the number of sensor measurements to be compromised, and $c_1 \neq c_2 \neq c_3 \neq ... c_k \neq 0$ are the number of nonzero elements [2]:

$$g\Gamma = k + 3\sum_{i=i_1}^{i_k} |Q_i| - \sum_{i=i_1}^{i_{k-1}} r_i - q \tag{11}$$

where the k is the state variables that need to be manipulated, Q_i is the adjacent buses which do not belong to Γ, r_i is the number of buses that are connected to bus i and $j (i \in \Gamma, j > i)$ together, and q is the number of buses that $|Q_i| = 0$ in Γ. Based on equation (10), the malicious measurement can bypass the χ^2 detector only if $a = Hc$. If the $c = (...c_{i1}...c_{i2}...c_{ik}...)^T$, $\Gamma = \{i_1, i_2, ..., i_k\}$, the attack vector a can be represented as :

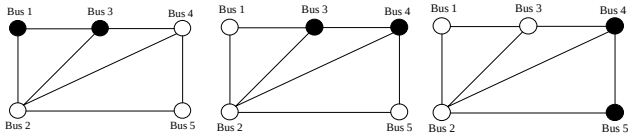
$$\underbrace{\begin{bmatrix} \vdots \\ a_{i1} \\ \vdots \\ a_{i_{g\Gamma}} \\ \vdots \end{bmatrix}}_{a} = \underbrace{\begin{bmatrix} H_{11} & \cdots & \cdots & H_{1n} \\ H_{11} & \cdots & \cdots & H_{2n} \\ \vdots & \ddots & \ddots & \vdots \\ H_{m1} & \cdots & \cdots & H_{mn} \end{bmatrix}}_{Jacobian Matrix} \underbrace{\begin{bmatrix} \vdots \\ c_{i1} \\ \vdots \\ c_{ik} \\ \vdots \end{bmatrix}}_{error} \tag{12}$$

Since H matrix is a $m \times n$ matrix and can be separated into two parts. First part is row 1 to n, this part defines the power injection at each bus. Second part is row $n+1$ to m, which

defines the power flow form bus i to bus j. We will use an example to explain the least effort false data injection.

B. Example

Here, we give a 5-bus system to demonstrate this theory. The topology of 5-bus system is shown below, black points show the state variables that are under attack:



(a) a (b) b (c) c

Fig. 2: Three scenarios of attacks.

In these scenarios, we set $k = 2$, which means that the adversary needs to change two state variables in x. In example a, if the adversary wants to change θ_1 and θ_3 ($\Gamma = \{\theta_1, \theta_3\}$), then the adjacent buses of Bus 1 are Bus 2 and Bus 3. However Bus 3 belongs to Γ, therefore $|Q_1| = 1$. Similarly $|Q_3| = 2$ (Bus 4 and Bus 2 are connected to Bus 3). There is only one bus connected to both Bus 1 and Bus 3, therefore $r_1 = 1$. The number of measurements he needs to change is $k + 3|Q_1| + 3|Q_3| - r_1 - 0 = 10$. Ten sensors need to be attacked to change θ_1 and θ_3. The sensors that need to have nonzero elements injected are at bus 1, bus 2, bus 3, bus 4, branch 1-2, branch 2-3 and branch 3-4. For help understanding, the following table shows some examples in the IEEE 5-bus system when $k = 1$ and $k = 2$.

TABLE I: Least Effort Attack Model for a Five-bus System

Γ \ z	Number	Sensors to be attacked
θ_2	13	Bus 1, 2, 3, 4, 5, Branch 1-2, 2-3, 2-4, 2-5
θ_4	10	Bus 2, 3, 4, 5, Branch 3-4, 2-4, 4-5
θ_5	7	Bus 2, 4, 5,Branch 2-5, 4-5
θ_1, θ_3	10	Bus 1, 2, 3, 4, Branch 1-2, 2-3, 3-4
θ_3, θ_4	12	Bus 1, 2, 3, 4, 5, Branch 1-3, 2-3, 2-4, 4-5

From these table, we know that, when $k = 1$, changing state variables of bus 5 is more optimal than changing state variables of bus 2 and 4, when $k = 2$, changing state variables of bus 1 and 3 is more optimal than changing state variables of bus 3 and 4.. If we list all combinations of Γ, we will get the most optimal attack vector that contains most zero elements.

IV. Attack Detection and Protection

Equation (10) shows that the χ^2-detector may not to detect the false data injection attack. Thus, we introduce the Euclidean Distance detector in the following section.

A. Euclidean Distance detector

χ^2 detector can detect random data injection, bad data injection or DoS attack, because with those data injection, the distribution of measurements vector will change significantly, the cost function will also change significantly. However, false data injection can not be detected by conventional statistical detector. The principle has been proved by equation (10).

For this type of manipulated data injection, it can be detected by using Euclidean distance detector. Euclidean can detect the distance deviation between measurements vector and estimated measurements vector, which can formulated by [1]:

$$d(p,q) = \sqrt{(p_1 - q_1)^2 + (p_2 - q_2)^2 + ... + (p_m - q_m)^2} \tag{13}$$

Where $p_i, i = (1, 2, ..., m)$ is the k step estimated measurements and $p_i, i = (1, 2, ..., m)$ is the $k - 1$ step estimated measurements. For each step, the estimator in control center will process measurements vector $p = z_{m_k}$ and give out the optimal state variables vector $\hat{x}$ to make the minimal residual between estimated measurements and original measurements. For each step, the detector will compare measurements vector z_{m_k} and $z_{m_{k-1}}$. Because measurements z are measured from wide area, it collect data from thousands sensors. Even if the adversary change measurements at each sensors marginally, the sum of thousands measurements will show great difference. If the $d(p,q)$ change suddenly, it means there is a injected vector. We also can set a hypotheses test that the threshold τ is based on history data. If the difference between the measurements and the estimated data is larger than τ, the detector will trigger an alarm, which means the measurements data is under attack. In this case, the threshold need to be choose carefully, because if the threshold is too large, some false data may bypass the detector, while if the threshold is too small, the misjudgment ratio of the detector will increase. The following figure shows the performance of the Euclidean Distance detector in the 5 bus system. At step 20, a false data vector is injected into the measurement. At step 50, this vector was taken away. We will see two spikes in Fig. 3: one at step 20 and the other at step 50, all due to the change of measurement vector.

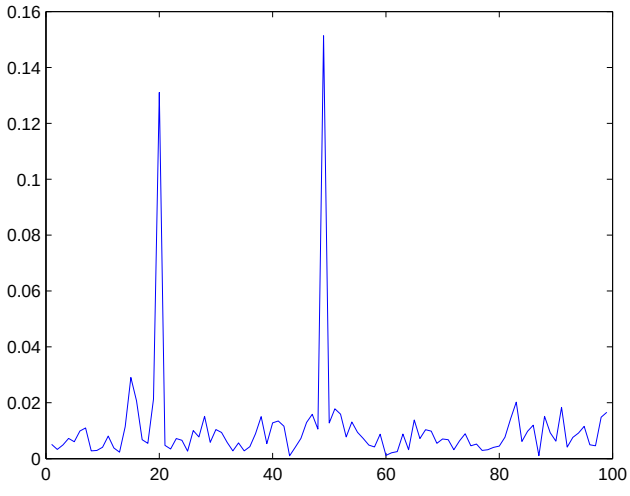


Fig. 3: Euclidean Distance Detection when false data injected at step 20 and end at step 50.

B. Protection

A power system is a large geographical area and contains thousands of sensors. Sensor protection cost a lot due to its large number. So we need to choose a small set of sensors for protection against false data injection.

As mentioned above, we assume there is 1 meter on each bus and 2 meters on each transmission line in DC model. It can be seen from equation (12), the largest factor to $g\Gamma$ is $3\sum_{i=i_1}^{i_k}|Q_i|$, which means that state variables at the buses that has more connections can not be choose as the optimal solution. Hence, for a given k, when Γ represents a set of buses with more connections to each other and connected to the least number of buses beyond Γ, the $g\Gamma$ will be smaller. So, the attack measurements elements need to choose the buses that are geographically close to each other [2].

We use IEEE 5 bus system to illustrate our protection strategy. In IEEE 5 bus system, bus 2 is connected to bus 1,3,4, and 5. If the adversary want to change the state variable of bus 2, he need to compromise the sensors of power injection P_1, P_2, P_3, P_4 and P_5, and power flows P_{12}, P_{21}, P_{23}, P_{23}, P_{32}, P_{24} and P_{42}. In other words, if the sensor on bus 2 is protected, the adversary has no chance to change state variables of bus 1,2,3,4, and 5. If we protect power flow meter on transmission line P_{12}, only the state variables of buses 1 and 2 are protected. Based on this analysis, we have a conclusion that the sensors on buses that has more geographical connection are more "important", the sensors that measure bus power injection are more "important". If we focus on protecting these sensors, the cost of protection will be more optimal.

V. Case Study

The study system is based on IEEE 5 bus system and IEEE 14 bus system. IEEE 5-bus system and 14-bus system parameters can be obtained from MATPOWER cases. The case study for 5-bus system is shown in Table II. The case study for the 14-bus system is shown in Table III. Since in DC power flow model, we ignore the power consumption on transmission line, power generation should equal to power demand. So, we add 0.134 $p.u.$ power at bus 5 to make total power generation equal to power demand.

We applied different attacks in these two systems. For random data injection, we inject an attack vector that follows Gaussian distribution, the mean value is about 50% of the measurements. For bad data injection, we inject unit vector to the measurements. For bad data with random data injection, we combined these two type of attack vector together. For false data injection, we added 0.1 to each state variables, and the attack vector can be computed based on H matrix. For DoS attack, we added some opposite numbers to the measurements to simulate that the control center can not receive some measurements. For IEEE 5 bus system, we assume the first 6 measurements are under DoS attack. For IEEE 14 bus system, we assume the first 7 measurements are under DoS attack.

The attack vector and cost function are listed in Table II and Table III. For IEEE 5-bus system, there are 5 state variables and 11 measurements. So, its freedom degree is $11-5=6$.

For IEEE 14-bus system, there are 14 state variables and 34 measurements, so its freedom degree is 20. Table IV shows percentage points of the χ^2 distribution, when freedom degree is 6 and 20. From the χ^2 distribution table and the data we get in case studies, we can see that random data injection, bad data injection and DoS attack change the cost function significantly, which means that these attack can not bypass the χ^2 detector. False data injection changes the cost function value marginally, so it can bypass χ^2 detector.

For false data injection, we use Euclidean distance detector to detect it. We set 100 steps for estimation process and apply false data injection attack beginning at step 20 and ending at step 50. The following figures shows that Euclidean distance detector detects the distance deviation changed at step 20 and step 50. If we set the threshold $\tau = 0.05$, the detector will trigger alarm at step 20.

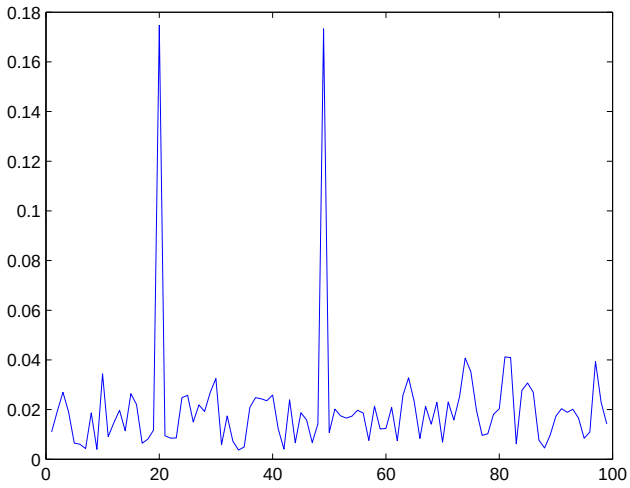


Fig. 4: Euclidean Distance Detection when false data injected at step 20 and end at step 50.

VI. Conclusion

There are three conclusions from this paper.

1) χ^2 detector can detect random data attack, bad data injection and DoS attack. However, false data injection attack can bypass it, because the attack vector is statistical optimized. The Euclidean distance detector can detect false data injection because with false data injection, the measurements vector will have distance deviation change. 2) To manipulate same number of state variables, least effort false data injection attack can compromise least sensors to escape detection. 3) The buses which have more geographical connections is more important. By protecting sensors on these buses, the system will be protected more effective.

References

[1] K. Manandhar, X. Cao, F. Hu, and Y. Liu, "Detection of faults and attacks including false data injection attack in smart grid using kalman filter," *IEEE Transactions on Control of Network Systems*, vol. 1, no. 4, pp. 370–379, Dec 2014.

TABLE II: IEEE 5-bus System Performance Under Attacks

Sensor number a_i / z_i \ Attack type		Random Data	Bad Data	Bad Data with Random Data	False Data	DoS Attack
1	0.4000	-0.5833	1	0.4167	$1.0e^{-14}$	-0.4000
2	-1.3000	-0.1181	1	0.8819	0.1776	1.3000
3	0.2349	0.9124	1	1.9124	0.1776	-0.2349
4	-4.0000	-0.7519	1	0.2481	0	4.0000
5	4.6651	-0.0585	1	0.9415	0	-4.6651
6	1.3585	0.7138	1	1.7138	0	-1.3585
7	1.5632	-0.9132	1	0.0868	0	0
8	-2.5217	0.3833	1	1.3833	0	0
9	0.0585	0.9580	1	1.9580	0	0
10	0.2934	-0.4335	1	0.5665	0	0
11	-2.1434	-0.7324	1	0.2676	0	0
$J(x)$	$1.1480e^{-13}$	4.5767	10.2457	13.6086	$1.1480e^{-13}$	9.8162

TABLE III: IEEE 14-bus System Performance Under Attacks

Sensor number a_i / z_i \ Attack		Random Data	Bad Data	Bad Data with Random Data	False Data	DoS Attack
1	2.3240	0.231	1	1.2307	$1.0e^{-15}$	-2.3240
2	0.1830	-0.247	1	0.7532	0.1110	-0.1830
3	-0.9420	0.754	1	1.7544	0.2220	0.9420
4	-0.4780	0.570	1	1.5697	0	0.4780
5	-0.2100	-0.070	1	0.9299	-0.4996	0.2100
6	-0.1120	0.628	1	1.6280	0.1110	0.1120
7	0	0.797	1	1.7969	-0.1110	0
8	0	-0.142	1	0.8585	0.1110	0
9	-0.2950	-0.331	1	0.6687	0	0
10	-0.0900	0.193	1	1.1933	-0.1110	0
11	-0.0350	0.804	1	1.8040	0	0
12	-0.0610	0.404	1	1.4041	0	0
13	-0.1350	-0.245	1	0.7549	0	0
14	-0.1490	0.470	1	1.4699	0	0
15	1.5606	0.908	1	1.9082	0	0
16	0.7634	0.086	1	1.0856	0	0
17	0.7143	0.080	1	1.0802	0	0
18	0.5812	-0.378	1	0.6222	0	0
19	0.4481	-0.858	1	0.1425	0	0
20	-0.2277	-0.636	1	0.3640	0	0
21	-0.5830	-0.814	1	0.1860	0	0
22	0.2913	-0.073	1	0.9270	0	0
23	0.1672	-0.981	1	0.0187	0	0
24	0.4185	0.830	1	1.8301	0	0
25	0.0617	0.285	1	1.2855	0	0
26	0.0752	-0.997	1	0.0028	0	0
27	0.1696	-0.939	1	0.0608	0	0
28	0.0000	-0.583	1	0.4169	0	0
29	0.2913	-0.090	1	0.9099	0	0
30	0.0633	-0.745	1	0.2545	0	0
31	0.1001	-0.983	1	0.0173	0	0
32	-0.0267	0.454	1	1.4542	0	0
33	0.0142	-0.292	1	0.7082	0	0
34	0.0489	0.561	1	1.5609	0	0
$J(x)$	$6.0330e^{-21}$	9.6654	24.624	35.4168	$6.0330e^{-21}$	2.5661

[2] Q. Yang, J. Yang, W. Yu, D. An, N. Zhang, and W. Zhao, "On false data-injection attacks against power system state estimation: Modeling and countermeasures," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 3, pp. 717–729, March 2014.

[3] A. Giani, E. Bitar, M. Garcia, M. McQueen, P. Khargonekar, and K. Poolla, "Smart grid data integrity attacks: characterizations and countermeasures x03c0;," in *Smart Grid Communications (SmartGridComm), 2011 IEEE International Conference on*, Oct 2011, pp. 232–237.

[4] J. Hao, R. J. Piechocki, D. Kaleshi, W. H. Chin, and Z. Fan, "Optimal malicious attack construction and robust detection in smart grid cyber security analysis," in *Smart Grid Communications (SmartGridComm), 2014 IEEE International Conference on*, Nov 2014, pp. 836–841.

[5] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Trans. Inf. Syst. Secur.*, vol. 14, no. 1, pp. 13:1–13:33, Jun. May 2011. [Online]. Available: http://doi.acm.org/10.1145/1952982.1952995

[6] I. CVX Research, "CVX: Matlab software for disciplined convex programming, version 2.0," http://cvxr.com/cvx, month = aug, year = 2012.

[7] Wikipedia, "Chi-squared distribution — wikipedia, the free encyclopedia," 2016, [Online; accessed 15-May-2016]. [Online]. Available: https://en.wikipedia.org/w/index.php?title=Chi-squared_distribution&oldid=719926527

[8] R. D. Zimmerman, C. E. Murillo-Sanchez, and R. J. Thomas, "Matpower: Steady-state operations, planning, and analysis tools for power systems research and education," *IEEE Transactions on Power Systems*, vol. 26, no. 1, pp. 12–19, Feb 2011.

df	$\chi^2_{.95}$	$\chi^2_{.90}$	$\chi^2_{.75}$	$\chi^2_{.50}$	$\chi^2_{.25}$	$\chi^2_{.10}$	$\chi^2_{.05}$	$\chi^2_{.01}$
6	1.635	2.204	3.455	5.348	7.84	10.64	12.59	16.81
20	10.851	12.443	15.452	19.337	28.83	28.41	31.41	37.57

TABLE IV: Percentage Points of the χ^2 Distribution