Efficient Detection of False Data Injection Attacks on AC State Estimation in Smart Grids

James Ranjith Kumar R. and Biplab Sikdar
Department of Electrical and Computer Engineering
National University of Singapore
Email: jamesranjithkumar@u.nus.edu, bsikdar@nus.edu.sg

***Abstract*—This paper proposes a simple non-iterative technique for detecting false data injection attacks on alternating current (AC) state estimators. The proposed method uses the nodal power injections and line power flows from the supervisory control and data acquisition (SCADA) system and voltage magnitudes and angles from phasor measurement units (PMUs) to the detect the false data injection attack. As the proposed method is independent of the state estimation outputs and does not depend on any other energy management system (EMS) functionality, it can be used to test the quality of the data even before the execution of the state estimation algorithm. The proposed method has been tested in the IEEE 118 bus system where false data with a magnitude ranging from 1% to 10 % is injected in four pairs of line power flows and one voltage measurement. It has been demonstrated that the proposed method can detect such attacks even when the attack magnitude is as small as 1%, which is not able to be deducted by conventional bad data detection techniques.**

***Index Terms*—Cyber-security, Smart Grid, SCADA, False Data Injection Attack, AC State Estimation, Bad Data Detection**

I. Introduction

Supervisory Control and Data Acquisition systems have historically been used by electric utilities to facilitate the monitoring, operation and control of power system networks. In addition to this SCADA system, various new components like Phasor Measurement Units, smart meters, and intelligent relays have recently started to be added to the grid. This evolving electricity grid with sensors, information and communication networks along with distributed controllers has been termed as a "Smart Grid". Smart grids can accommodate distributed generation, renewable integration, electric vehicles and other new technologies. Though this new evolution of the grid had brought various benefits for the utility and the end user, it had made the grid vulnerable to cyber threats. Consequently, research on cybersecurity of electric grids has received increasing attention in the recent past as it is a critical infrastructure and failure of power system network will lead to tremendous consequences [1].

The Energy Management System is the key component of an electric grid that carries out the computations required for monitoring, operation and control of the power system network. If the EMS is compromised by the attackers, then the decisions taken by the outputs provided by EMS may be erroneous and can lead to a disastrous consequences. An attacker can compromise the EMS in three ways: by attacking the sensors that measure the parameters of the grid, by infiltrating into the communication network that is used in the grid, or by directly attacking the EMS in the load dispatch center. In all these three attack scenarios, the attacker may disrupt the original information that is measured in the grid and replace it with a corrupted value which can harm the power system operation and control. These attacks are broadly classified as false data injection attacks. In addition to directly disrupting the grid's operation, any suspicion of such attacks can also negatively impact the operators. Even if there is any doubt in the minds of the operators that such an attack has occurred, it brings an element of disbelief on all the measurements that have been reported and eventually it will affect the observability. Thus it is critical to develop efficient and accurate techniques that can detect false data injection attacks on power grids.

As false data injection attacks artificially modify the measured values, the resulting values may not have the natural distribution of error. Hence such attacks may not be detected by existing methods that are used to detect the random errors in measurement values. False data injection attacks are also complex because the attacker may execute the attack in a coordinated fashion in order to make it difficult to detect. Many papers in existing literature have focused on studying the impact of such false data injection attacks in power system state estimation and developing methodologies for detecting such attacks. One of the pioneering works in this area is presented in [2] which shows that conventional methods which use the analysis of residuals for detecting bad data will not able to detect the attack if the attacker possesses the information of the power system network. The authors of [3] showed that the non linear representation of power balance equations (which is well known as AC state estimation) is quite robust against false data injection attacks as compared to the direct current (DC) state estimation (which uses certain assumptions to simplify the non linearity). Bi and Zhang proposed a method which uses the topological information to detect cyber attacks on DC state estimation [4]. Ashok et. al. have proposed an algorithm to detect false data injection attacks where other applications of EMS like economic dispatch and load flow are being involved

This research is supported by the National Research Foundation, Prime Minister's Office, Singapore under its Corporate Laboratory@University Scheme, National University of Singapore, and Singapore Telecommunications Ltd.

978-1-5386-0683-4/17/$31.00 © 2017 IEEE

for the detection process [5]. In [6], the data from the PMUs are used to estimate the line parameters which are compared against the actual values in order to identify whether the data is corrupted by the attacker or not. A majority of the false data detection techniques available in the literature are focused on DC state estimation and such techniques may not be applicable for AC state estimation. So an attempt has been made in this paper for the detection of false data injection attacks on AC state estimators which are also computationally efficient to be practical in online environments.

In this paper, a simple non iterative method has been developed for detecting false data injection attacks on a power system network. The principle behind the proposed method is that each of the values in the state variable should satisfy the governing equations not only for its respective node but also for all the nodes. In simple terms, the proposed method is based on verifying whether the measured values satisfy the governing equations with a reasonable tolerance. This proposed method is tested on the IEEE 118 bus system where the attack is carried out in such a manner that it can bypass the traditional bad data detection technique. It has been demonstrated that the proposed method is able to detect false data injection attacks whose magnitudes is as small as 1%.

This rest of the paper is organized as follows. In Section II, the threat model and our assumptions regarding the false data injection attacks has been presented. Section III details the proposed technique for detecting false data injection attacks and Section IV presents the simulation results to evaluate the performance of the proposed method, obtained using the IEEE 118 bus system. Finally, Section V provides the conclusion of this paper.

II. Background

This section reviews background material that are relevant to the proposed method for data injection attack detection, starting with the methodology for power system state estimation and bad data detection. This section also presents the threat model of false data injection attack.

A. State Estimation and Bad Data Detection

In a power system network, the nodal power injections, line power flows and voltage magnitudes are measured and transmitted by Remote Terminal Units (RTU) over the SCADA network and it is delivered to the EMS. PMUs will also send the measured magnitudes and angles of voltage to the EMS system. As the measurements have noise and in general all nodes do not have a PMU, it required to estimate the voltage magnitudes and angles using the measured quantities by means of a state estimator which is available in the EMS system. As the power balance equations are non linear, the Gauss-Newton method is typically used for estimating the system states and this method is termed as AC State estimation.

Let z be the m dimensional vector that contains all the measured values and $f(x)$ be the nonlinear function that maps the state variables x to the quantities that are measured. In power system state estimation, x represents the magnitudes and angles of node voltages and its dimensional size n is less than that of the measurements. In other words, $n < m$ in order to make it an over-determined system. As the measurements have noise, the mapping of the state variables to the measured values can be written as

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

where e is the noise that is added to the true quantity. This mapping is nothing but the set of power balance equations and it is non linear in nature. Hence the process of estimating the states is usually iterative. At the i^{th} iteration, the state correction vector is written as

$$\Delta x^i = \left(H^T(x^i)R^{-1}H(x^i)\right) \backslash H^T(x^i)R^{-1}\left(z - f(x^i)\right) \tag{2}$$

where $H(x^i)$ is the Jacobian matrix for the function $f(x^i)$ and R is the measurement covariance matrix. Using the state correction vector, the values of the state variables for the next iteration can be updated as

$$x^{i+1} = x^i + \Delta x^i. \tag{3}$$

This iteration process is repeated until the values of the state variables converge to a reasonable tolerance limit. In this power system model, by assuming that the voltage magnitudes are close to rated value and the difference of voltage angles in a line are extremely small, the equations may be linearized and can be solved fairly simply but with a trade-off in terms of the accuracy. Such a technique is popularly known as DC state estimation.

After convergence of the AC state estimation algorithm, bad data detection techniques [7] are used to detect the presence of any incorrect data. For this process, residuals are calculated as

$$r = \|z - f(x)\|_2 . \tag{4}$$

A threshold value τ is obtained from the error distribution (which is assumed to be known) and using the theory of χ^2 testing. Using the threshold value and the residual, the condition $r < \tau$ is verified. If this condition is not satisfied, it will trigger the EMS with an indication that bad data is present in the measurement.

B. Threat Model

As AC state estimation is a iterative technique, it requires a initial value for the states that are to be estimated. Consider that the initial value of state $\widehat{x}$ is close to the actual solution. Then the mapping function can be written in a linear form as

$$z = \widehat{H}\widehat{x} + e. \tag{5}$$

The expression above holds because AC state estimation is an iterative process and it will be approximately linear at the last iteration before convergence. In [2], it has been shown that if the attacker has the knowledge of the $\widehat{H}$ matrix, then the attacker can inject false data in the state variables without being detected by the conventional bad data processing technique. Let $z_a = z + \widehat{H}c$ be the measurement vector that is modified by the attacker so that the state vector can be modified as $\widehat{x}_a = \widehat{x} + c$. As shown in [2], the residue value with this modified measurement vector will be the same as the original vector which can be written as

$$\left\|z_a - \widehat{H}\widehat{x}_a\right\|_2 = \left\|z - \widehat{H}\widehat{x}\right\|_2 . \tag{6}$$

As the $\widehat{H}$ matrix is constant in DC state estimation, with this kind attack, it is possible to inject an attack vector of any magnitude without triggering the bad data detection technique. However, as the values in the H matrix changes in every iteration in AC state estimation, this kind of attack will be able to bypass the bad data detection algorithm only when the magnitude of the attack vector is considerably small.

For developing the false data detection technique, it is assumed that the attacker has the access to the network information which in turn can be used to find $\widehat{H}$. Also, we assume that the attacker is able to modify the measurements to any desired value z_a.

III. False Data Detection Mechanism

In this section, we present the proposed method for detecting false data injection attacks. The proposed method is based on the intuition that the equations governing the power flow should hold across the network. Thus the proposed method computes the values of voltages (both magnitudes and angles) at each node using the given values of nodal power injections, line power flows and voltage magnitudes. It then compares the computed values with the measured given values in order to detect any data modification. This section covers the methodology for handling the measurements of nodal power injections and line power flows, along with the voltage magnitude measurements.

A. Handling Nodal Power Injections

Consider that the values of nodal power injections (both real and reactive) and voltage magnitudes are available for all the nodes in a n bus system. Let $\widetilde{S}$ and $\widetilde{V}$ be the vectors of complex power injections and complex voltages at all the nodes respectively. Let $\widetilde{Y}$ be the bus admittance matrix of the given power system network. Assume that node 1 serves as the reference bus where the voltage angle is 0. The notation * indicates the complex conjugate operation. The notation $\mathrm{diag}(x)$ indicates a function that converts the vector x into a diagonal matrix with all the diagonal elements formed from x. The power balance equation for this nodal injections can be written in complex form as

$$S = \mathrm{diag}(\widetilde{V})\,(\widetilde{Y}\widetilde{V})^* \tag{7}$$

where

$$\widetilde{S} = \begin{bmatrix} S_1 & S_2 & \dots & S_n \end{bmatrix}^T \tag{8}$$

$$\widetilde{V} = \begin{bmatrix} V_1 & V_2 & \dots & V_n \end{bmatrix}^T \tag{9}$$

$$\widetilde{Y} = \begin{bmatrix} Y_{11} & Y_{12} & \dots & Y_{1n} \\ Y_{21} & Y_{22} & \dots & Y_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ Y_{n1} & Y_{n2} & \dots & Y_{nn} \end{bmatrix} . \tag{10}$$

By simple algebraic manipulations, (7) can be written as

$$YV + Y_1V_1 = \mathrm{diag}(\widetilde{V}^*)^{-1}\widetilde{S}^* \tag{11}$$

$$= \mathrm{diag}\left(\begin{bmatrix} 0 \\ V^* \end{bmatrix}\right)^{-1} S^* + V_1^{-1}\widetilde{S}_1 \tag{12}$$

where

$$S = \begin{bmatrix} 0 & S_2 & \dots & S_n \end{bmatrix}^T \tag{13}$$

$$\widetilde{S}_1 = \begin{bmatrix} S_1 & 0 & \dots & 0 \end{bmatrix}^T \tag{14}$$

$$V = \begin{bmatrix} V_2 & \dots & V_n \end{bmatrix}^T \tag{15}$$

$$Y_1 = \begin{bmatrix} Y_{11} & Y_{21} & \dots & Y_{n1} \end{bmatrix}^T \tag{16}$$

$$Y = \begin{bmatrix} Y_{12} & \dots & Y_{1n} \\ Y_{22} & \dots & Y_{2n} \\ \vdots & \ddots & \vdots \\ Y_{n2} & \dots & Y_{nn} \end{bmatrix} . \tag{17}$$

Finally (12) can be written in standard linear form as

$$\left(\mathrm{diag}\left(\frac{S^*}{|V|^2}\right) - Y\right) V = (Y_1 - \frac{1}{|V_1|^2}\widetilde{S}_1^*)V_1 \tag{18}$$

$$V = (A^TA)^{-1}A^Tb \tag{19}$$

where

$$A = \mathrm{diag}\left(\frac{S^*}{|V|^2}\right) - Y \tag{20}$$

$$b = (Y_1 - \frac{1}{|V_1|^2}\widetilde{S}_1^*)V_1 \tag{21}$$

$$\mathrm{diag}\left(\frac{S^*}{|V|^2}\right) = \begin{bmatrix} 0 & 0 & 0 \\ \frac{S_2^*}{|V_2|^2} & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & \frac{S_n^*}{|V_n|^2} \end{bmatrix} . \tag{22}$$

It can be seen that (19) is a function which gives complex voltage values (both magnitudes and angles) as output by taking nodal power injections and voltage magnitudes as input. So if the data is not corrupted, the absolute value of the solution of (19) should be equal to the voltage magnitudes which provided as the input. Hence in order to satisfy this condition, the attacker needs to modify all the values of nodal power injections and voltage magnitudes in all the nodes which is difficult to achieve in practice. It can be easily seen that the Y matrix stays constant for the given topology and only the diagonal terms of the matrix A will change for the measurements of nodal power injections and voltage magnitudes over the time-line. So by using results from matrix theory [8, Page 166], the inversion of matrix A can be obtained with very low computational effort for every change in its diagonal elements. Hence a detection method based on this approach can be easily incorporated in online environment.

B. Handling Line Power Flows

Let F_{ij} be the complex line power flow in the line that connect nodes i and j with line impedance z_{ij}. Let y_{ij} be the inverse of the line impedance z_{ij}. The power balance equation of the line power flow F_{ij} can be then written as

$$F_{ij} = V_i \left(\left(V_i - V_j \right) y_{ij} \right)^* . \tag{23}$$

By simple algebraic manipulations, (23) can be written as

$$\begin{bmatrix} 0 \ldots y_{ij} - \dfrac{F_{ij}^*}{|V_1|^2} \ldots - y_{ij} \ldots 0 \end{bmatrix} \begin{bmatrix} \vdots \\ V_i \\ \vdots \\ V_j \\ \vdots \end{bmatrix} = 0 . \tag{24}$$

It can be seen that (24) can be easily appended in (18) for handling the line power flow measurements. Thus along with the measurements of nodal power injections and voltage magnitudes, the line power flows which are obtained from SCADA devices can be used for the verification of its untaintedness. This can be done by calculating the complex voltages by the proposed method and its magnitudes can be verified with the voltage magnitudes that are given as input. However as the measurements have some noise component, the calculated and the input magnitudes may not be equal and hence it is compared with a fixed threshold limit.

C. Proposed Algorithm

The proposed algorithm for detecting the false data injection attack is shown in Algorithm 1 where $S, F, |V|$ are the measurements of nodal power injections, line power flows and voltage magnitudes, respectively, and $\tau_{|V|}$ is the threshold limit between the calculated and the input voltage magnitudes. So when the output of this Algorithm a is 1, it signifies the presence of false data and vice versa.

Algorithm 1 Detection of False Data Injection

```
function DETECT($S, F, |V|$)
    Find the elements of $A$ and $b$ using $S, F, |V|$
    $V_c = (A^T A)^{-1} A^T b$
    if $\| |V_c| - |V| \|_\infty > \tau_{|V|}$ then
        $a = 1$
    else
        $a = 0$
    end if
    return $a$
end function
```

D. Practical Considerations

It is not always possible to obtain the measurements of nodal power injections, line power flows and voltage magnitudes from all the nodes. But if the system is observable, then the proposed method will provide a solution because the line power flows are used to compensate for unavailable nodal power injections and vice versa. The values of voltage magnitudes can be obtained from the measurements taken by SCADA devices or PMUs or even the output of the state estimator can be used. As the solution of (19) gives both magnitudes and angle values, it can be directly compared with the measurements taken by PMUs. It is to be noted that in the proposed method, the voltage magnitude at the reference bus V_1 is a input parameter but it is not at the output whereas the voltage magnitudes at other nodes are at both input and output. Even though V_1 is not computed, any modification from its true value will be reflected in the voltages computed at the other nodes.

IV. Results and Discussion

In order to demonstrate to effectiveness of the proposed algorithm, it has been tested on the IEEE 118 bus system.Since the AC state estimator program requires the measurements of voltage magnitudes and line flows, the power flow program is used to generate these values. From the power flow solution, 118 measurements of voltage magnitudes, 118 pairs of active and reactive power injections and 186 pairs of active and reactive power flows in each line were obtained. These values are provided as input to the AC state estimator. The AC state estimator and the proposed algorithm for false data detection have been coded in MATLAB environment. The tolerance limit for convergence for the AC state estimator is set as 10^{-4}. In the original measurements which are obtained from the power flow solution, the attack vectors are injected whose magnitudes are varied from 1% to 10%. These attacks are carried out such that they may bypass the bad data detection algorithm as given in [2]. The attack is carried out on the values of power flows in the lines that are connected to bus 110 and also on the power injection and voltage magnitude measurement taken at bus 110.

This analysis is carried out at fully loaded condition, 3/4th load condition and half loaded condition. As the residuals are used for verification of the measurements in the bad data detection technique, the residual of the solution provided by AC state estimator has been computed in each scenario for further analysis. These residuals are tabulated in Table I for each of the loaded conditions along with the maximum difference in the calculated and the input voltage magnitudes using the proposed method. From the results, we see that there is no appreciable difference in the residuals of the AC state estimator in the no attack case and when the attack magnitude is low. The determination of a threshold is difficult in such scenarios and thus traditional methods are unable to detect such attacks or have high false positives and negatives. In contrast, the proposed method shows clear difference between the no attack and attack cases, making it easy to select a threshold and accurately detect attacks with even very small magnitudes.

By choosing the attack vector as a linear combination of the columns of the Jacobian matrix, the residuals are supposed to be constant for any magnitude of attack. But the values of the residuals from the AC state estimator as given in Table I tend to reduce gradually if the attack magnitude goes beyond a certain limit. This is due to the iterative procedure of AC state estimation [3] and hence the Jacobian matrix tends to

TABLE I
COMPARISON OF PROPOSED METHOD WITH BAD DATA DETECTION TECHNIQUE

Attack Magnitude	**Full Load**		**3/4$^{\text{th}}$ Load**		**Half Load**	
	Residuals of AC State Estimator	$\lVert \lvert V_c\rvert - \lvert V\rvert \rVert_\infty$	**Residuals of AC State Estimator**	$\lVert \lvert V_c\rvert - \lvert V\rvert \rVert_\infty$	**Residuals of AC State Estimator**	$\lVert \lvert V_c\rvert - \lvert V\rvert \rVert_\infty$
No Attack	1.02E-03	1.10E-12	4.70E-04	1.51E-12	8.24E-04	3.27E-12
1	1.02E-03	1.11E-09	4.70E-04	4.65E-09	8.23E-04	4.58E-09
2	1.02E-03	2.27E-09	4.69E-04	9.47E-09	8.23E-04	9.34E-09
3	1.02E-03	3.48E-09	4.68E-04	1.45E-08	8.23E-04	1.43E-08
4	1.02E-03	4.74E-09	4.66E-04	1.97E-08	8.21E-04	1.94E-08
5	1.01E-03	6.06E-09	4.63E-04	2.51E-08	8.16E-04	2.47E-08
6	1.01E-03	7.43E-09	4.59E-04	3.08E-08	8.06E-04	3.03E-08
7	9.97E-04	8.87E-09	4.53E-04	3.67E-08	7.90E-04	3.61E-08
8	9.83E-04	1.03E-08	4.45E-04	4.28E-08	7.69E-04	4.21E-08
9	9.66E-04	1.18E-08	4.34E-04	4.92E-08	7.48E-04	4.84E-08
10	9.54E-04	1.31E-08	4.20E-04	5.58E-08	7.39E-04	5.49E-08

change in every iteration. Also the loading conditions did not significantly affect the values of residuals which are increasing in a gradual manner as the attack magnitude is increased. Hence it is difficult to fix a threshold which is robust against noise and the false positives they may induce. Also, if the threshold in the traditional method is chosen to be high in order to accommodate noise, it may not be possible to detect attacks with small magnitudes, leading to false negatives.

It is important to accurately detect false data injection attacks of small magnitudes because they may also cause significant damage to the power system operation. For example, if the power system network is operating under critical loaded conditions then if an attack takes place with a magnitude of around 5% on the line flows, then it may not cause suspicion to the operator and it may lead to load shedding. On the other hand, 5% of either increase or decrease in voltage will tend the operator to adjust the reactive power controls and transformer taps which may lead to instability in the system and also lead to tripping by the protection system.

By using the proposed method whose results are shown in Table I, the difference in voltage magnitudes in the proposed method has a significant jump from the order of 10^{-12} in a "No Attack" scenario to an order of 10^{-9} in a attack with a magnitude of 1%. Since there is a sharp shift, the threshold value can be chosen easily by heuristic methods even though the error distribution is not known. Thus even in a varying load situation, by fixing a threshold between 10^{-9} to 10^{-13}, the proposed method is able to detect false data injection attacks without producing any false positives or false negatives.

V. CONCLUSION

In this paper, we have developed a simple non-iterative technique for detecting false data injection attacks on AC state estimation. This method does not depend on any other functionalities of EMS software. Since it is non-iterative and only the diagonal terms of the matrix change with each set of data, it can be quickly solved and can be easily incorporated for online detection. The proposed method is implemented and tested on the IEEE 118 bus system. It has been shown that the proposed algorithm can detect the attack even if the attack magnitude is as low as 1%. While many of the existing schemes focus on DC state estimation, the proposed method works with AC state estimation and does not need the assumption that some set of measurements is secure.

REFERENCES

[1] T. Flick and J. Morehouse, *Securing the Smart Grid: Next Generation Power Grid Security*. Syngress Publishing, 2010.

[2] 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. 2011. [Online]. Available: http://doi.acm.org/10.1145/1952982.1952995

[3] G. Hug and J. A. Giampapa, "Vulnerability assessment of ac state estimation with respect to false data injection cyber-attacks," *IEEE Transactions on Smart Grid*, vol. 3, no. 3, pp. 1362–1370, Sept 2012.

[4] S. Bi and Y. J. Zhang, "Using covert topological information for defense against malicious attacks on dc state estimation," *IEEE Journal on Selected Areas in Communications*, vol. 32, no. 7, pp. 1471–1485, July 2014.

[5] A. Ashok, M. Govindarasu, and V. Ajjarapu, "Online detection of stealthy false data injection attacks in power system state estimation," *IEEE Transactions on Smart Grid*, vol. PP, no. 99, pp. 1–1, 2016.

[6] S. Pal, B. Sikdar, and J. Chow, "Classification and detection of pmu data manipulation attacks using transmission line parameters," *IEEE Transactions on Smart Grid*, vol. PP, no. 99, pp. 1–1, 2017.

[7] E. Handschin, F. C. Schweppe, J. Kohlas, and A. Fiechter, "Bad data analysis for power system state estimation," *IEEE Transactions on Power Apparatus and Systems*, vol. 94, no. 2, pp. 329–337, Mar 1975.

[8] G. L. Kusic, *Computer-aided Power Systems Analysis*. CRC Press, 2008.