Modelling and Countermeasures of False Data Injection Attacks Against State Estimation in Power Systems

Akintunde Samson Alayande[1], Nnamdi Nwulu[1] and Ayodeji Emmanuel Bakare[2]
[1]Department of Electrical/ Electronics Engineering Science, University of Johannesburg, South Africa
[2]Department of Electrical/ Electronics Engineering, University of Lagos, Nigeria
E-mail address: alayandeakintundesamson@gmail.com, nnwulu@uj.ca.za, bakare_ayodeji@yahoo.com

Abstract—**False Data Injection Attacks (FDIA) has been shown to be one of the serious security challenges combating power systems. This is becoming a grown concern to power utilities and has drawn the attention of power system researchers and Engineers in recent times. State estimation in power system operation and planning is therefore an important and an essential tool for monitoring and controlling the system to estimate the best state of the power system through meter measurements and power system topologies. This paper therefore presents the modeling and countermeasures for avoiding unnecessary total blackout within the system. The vulnerability of both the Transmission and the distribution power system to FDIA is also considered in this paper. The outcomes of this paper could serve as a basis for the development of necessary protective countermeasures against vulnerabilities within power system networks.**

***Index Terms*—Security, Internet of Things (IoT), False Data Injection Attacks (FDIA), Vulnerability, State estimation**

I. INTRODUCTION

Ensuring data integrity and security of any system is paramount for safe operation and protection of the system against manipulations. As the traditional grids are replaced with the smart grids, this poses a case of the power grid's vulnerability to cyber-attacks [1]. The smart grid as a national critical infrastructure is a system which integrates cyber and physical systems with constant communication between different parts of this system. It is therefore important to ensure data integrity and protect the system against manipulations. The application of Internet of Things (IoT) has made the communication link and the whole power system vulnerable to attacks. The power grids cannot be described as conventional cyber system but a cyber-physical system which is characterized by the communication or integration between cyber and physical systems [2]. The advancement brought by the smart grids can be lauded in the area of automation, grid monitoring and management, smart metering infrastructure and client side management. The resulting communication network of the power system has become more vulnerable to attacks and manipulations by intruders [2].

An important element of the smart grid is state estimation. The inputs of state estimation are confined to the P, Q injections at load buses and P, V values at voltage controlled-buses. State estimation is required for two reasons. First, the measurements from field devices such as Remote Terminal Units (RTUs) and sensors are thought to be noisy and contain some errors. Second, just in the case of load flow, the measurements contain some variables such as P, Q lines flows will be obtained which are not required for power flow calculations. Therefore, the best estimate of the operating state is obtained through state estimation and this estimate is subject to statistical analysis before it is accepted [3].

Power systems are constantly monitored and controlled by Energy Management Systems (EMS) or Supervisory Control and Data Acquisition (SCADA) Systems which require inputs from the state estimator to maintain the operating condition of the power system. The SCADA system collects measurements from field devices such as sensors in the network. The sensor measurements serve as input to the state estimator. The state estimator estimates the true state of the power system based on these measurements. The output of the state estimator are some voltage magnitudes and phase angles. Control actions and energy management systems are dependent on the output of the state estimator for safe operation of the power system. Therefore, state estimation uses data from meter measurements, calculates the best estimate of these measurements and the results are then used to control the grids. State estimation therefore plays an important role in power system monitoring and control [3] [4].

State estimation gives an estimate of the true state of the power system and most control action, studies and system operations depend on state estimation. Attacks against power system state estimation tends to endanger the power grids. Power system models can be AC or DC where the AC model considers both the real and reactive power and therefore equations for this model becomes nonlinear. For the

978-1-5386-7709-4/18/$31.00 ©2018 IEEE

simplified DC model, equations are linear and iterations are not required.

The susceptibility of the power grids to attacks is due to the architecture of the power grids as a cyber-physical system and the communication links have become more vulnerable to cyber-physical attacks. The introduction of advanced metering system infrastructure equipped with smart meters has played an important role in achieving the smart grid. However, as many inputs or outlets are available on the power grid, the more vulnerable the system becomes [4].

One of the attacks against power grid is the False Data Injection attack (FDIA). FDIA is a data integrity attack against state estimation in power systems where attackers compromise the sensor nodes. Mostly, attackers manipulate and mislead system operators into making inaccurate commands to cause power system blackout if not quickly detected and controlled [6]. The aftermath of FDIA is therefore major equipment failure and total power blackout. False data may be injected by compromising smart meter measurements, sensors or Remote Terminal Units (RTUs) or intruding the Supervisory communication [7] on the network.

Attackers can insert measurements which will not ordinarily be detected by the BDD [8]. Knowledge of the current configuration of the power system may lead to attacks not being detectable by current implementations of BDD as attackers look to inject data so closely related to the estimated states. Most BDD technique is based on the least weighted square method. Knowledge of the power system configuration will most definitely violate this approach. Many studies have suggested the protection of some strategically selected meter measurements to guard against FDIA [4], [9], [10]. Identifying a set of meter measurements such that the vectors necessary to inject FDIA by attackers is limited is a good practice. However, this method will not completely make the system immune to attacks and it is necessary that the measurements of the protected sensors be available at all times. For practical systems, the absolute protection of meters against attacks may not be achievable. Since SCADA devices and network topologies vary, it is therefore important to monitor systems properly to ascertain the most suitable FDIA implementations. As such, detection methods beyond these conventional methods needs to be formulated as the attacker can utilize measurements between the error ranges allowed by the least square method without being detected [6].

Ensuring data integrity and protection of the power grids is thus very important considering the importance of the power grids as a national critical infrastructure and the severe impact FDIA on the power system [5]. The automation that comes with the application of network computing leads to the vulnerability of power grids to cyber-attacks. Just like traditional cyber systems, the many outlets or connection links available on the system tend to increase its vulnerabilities [1]. False Data injection attacks (FDIA) against state estimation proves to be a way by which attackers compromise power system operation by injecting errors or false meter measurements to the power system. Most system parameters such as system stability and control depend on state estimation. Parameters of state estimation are required for making system based decision as regards physical system stability and control. FDIA can mislead system operators into making inaccurate decisions based on injected data. Recently, it has been demonstrated that False Data Injection (FDI) attacks could bypass bad data detection (BDD) in today's EMS/SCADA systems without being detected [2] [8] [11].

The remaining parts of the paper are organized as follows. Section II presents the literature review of relevant studies. Section III presents the mathematical formulations based on the DC power-flow as well as on AC power-flow models for state estimation. Section IV presents the state estimation analysis through power-flow measurement while section V concludes the study.

II. REVIEW OF RELEVANT LITERATURE

Several approaches for solving state estimation problem have been reported in the literature. For instance, in [12], the variation of the risk exposures with different FDIA implementations while also considering the performances of SCADA devices in different performance levels is presented. The work represents a techno-economic approach by examining different measurement protection schemes and introducing a quantitative metric (called Return of Investment) to evaluate the overall returns of the alternative MPSs. This method involves standardized assessment methods. However, it is a very cumbersome process taking into account many variables some of which include Risk exposure, Risk mitigation and Protection cost. A detailing the implementation of FDIA against various protective countermeasures is discussed in [13] and tabulated in [12]. A very important aspect in [12] is the use of Steiner Tree with a Heuristic Algorithm to obtain the quasi-optimal solutions. This was implemented on an IEEE 14 bus test system. The installation of power flow meters and power injection meters ensured system observability.

It is very important to note that FDIAs are not limited to power transmission systems. The extension to power distribution systems is very important. Unlike transmission systems, the estimated state of the distribution system is required by an attacker to launch an FDIA attack. The estimated state can be obtained mathematically from power flow or injection measurements. Although, attacks on power distribution systems, are not common it has been shown over the years that distribution systems are also vulnerable to attacks but greater sophistication is required to launch such attacks in comparison to the local FDI attack. In [14], the authors realized an FDI attack on power distribution system state estimations by approximating the system state based on power flow or injection measurements. It is worthy to note the ease with which the results of the approximated state were obtained. The new method proposed was found to more likely compromise the state estimation without being detected by the current Bad Data Detection in comparison with traditional attacks. This attack model showed more potency in corrupting the system state estimation and it is a

more realistic model as it reduces the need of obtaining the system state. The effect of FDIA on Load Frequency Control in power distribution systems can be devastating [15]. The role of the LFC is to maintain real power balance in the system. As real power demand changes, a frequency change occurs and this frequency error is amplified, mixed and sent to a turbine governor. The turbine governor then acts to restore the real power balance in the system by changing the turbine input. The data required for load frequency control is a function of state estimation.

Protection of meter measurements is also a method of preventing FDIA attacks from the grid operators' point of view. Protecting these sets of meter measurements and state variables is sufficient if there are no verifiable state variables. However, it is not feasible to protect all meter measurements.

In [16], the authors examined the potential of FDIA on causing power system blackouts. The elements of blackout considered are voltage violations, overloading and load shedding and also the comparison of the impact of the different configurations of the FDI attacks and the system response to various FDIA configurations through semi-definite programming. Since state estimation outputs are required by system operators to make some important decisions, manipulating sensor measurements by attackers can result in system operators making wrong decisions. The attackers require only a few sensor measurements in order to implement these attacks. These pose a new challenge as to the detection of bad data. Previous works have been based on the simplified DC model. An AC-based FDIA is possible and DC based FDIA could be detected by an AC-based BDD. The nonlinearity of power flow variables makes the AC based FDIA riskier and once constructed this new set of AC-based attacks are hard to detect. A basic assumption in launching an optimal attack using the AC model is that the attacker has access to the grid topology. Hence, as studies and research are being made from a cyber-security point of view, proper access controls should be put in place to ensure a proper network protection. The attacker can decide to fulfill the attack by targeting state estimations, falsifying voltage levels and ensuring maximum state deviations. Having said earlier that the detection of FDIA is more difficult when the AC model of the system is used compared to the DC model, considering the size of electric grids, the computation and complexity involved makes it a difficult process to achieve. It is also important that the detection of FDIA be performed in a timely manner to ensure prompt action is taken when an attack is detected. While most of the works on FDIA were not tested on large-scale power systems, the efficiency of such systems can be questioned. In the same vein, while considering the complexity and efforts required in analyzing some of these test systems and comparing the size of these systems with real power networks, the models proposed tend to be unrealistic. The possibility of cyber-attacks on power grids can be evaluated using the Markov chain for a cyber-physical model of the power system. This process can be sped up to achieve dynamic state estimations if implemented on (Graphics Processing Unit) GPUs [17]. In [18], an attack technique, which is based on the historical running states of the power system, is presented. The real time running state and the historical running states are checked for consistency and this forms the basis for the detection of FDIA [19]. A stealthiness corruption method is employed where the historical measurements from the database are used to replace the outputs of the state estimations. This is to prevent the stealthiness of FDIA from acting as the final outputs of state estimations. The historical states are then fed through a feedback loop to the state estimator. This repeated bad data detection helps to increase the accuracy of the state variables. The limitations of these method is that hacking of the communication link between the control center and power plant control room is not considered and FDIA can also be launched for the historical running state database which was not considered in [18].

Combined attacks on power systems tend to be riskier compared to the stealth FDI attacks. Such combined attacks can be executed in smaller indexes with limited resources. These attacks have lower detection probability. In [20], the authors compared the risks of combined attacks with FDI attacks.

III. MATHEMATICAL FORMULATIONS

A. BASED ON LINEAR DC STATE ESTIMATION MODEL

The voltages at the nodes and power angles are the state variables in a power system which is required for power system state analysis. However, the measurements from field devices contain measurements with large number variables such as P, Q line flows which are not required for power flow analysis. This shows the importance of state estimation in ridding the meter measurements of errors and redundant measurements [3]. The existence of enough measurements to realise state estimation after exceptional and gross errors have been removed makes the system observable. Otherwise, if many measurements have been removed due to error, state estimation cannot be achieved, then the system is said to be unobservable [21]. The conventional basis of state estimation is the Least Square Technique.

For a simplified and approximate DC model, the reactive power is ignored and the nodal voltages are kept constant. The state variables (voltages and power angles) are represented by the vector x. Denoting the state variables for an 'n'bus system as $'x'$. The vector can be expressed as [4] [22]

$$x = [\delta_2\ \delta_3 \ldots\ldots \delta_n\ V_1\ V_2\ V_3 \ldots\ldots V_n]^{\mathrm{T}} \qquad (1)$$

Where, δ_i represents the phase angles and v, the voltage magnitudes of the n-th bus. Assuming 'm' number of measurements were obtained, these measurements can be represented by,

$z = [z_1, \ldots., z_m]^{\mathrm{T}}$.

while considering the errors in the measurements and representing them by

hence, the relationship between the measure quantity z and the true value x can be related by;

$e = [e_1, e_2, \ldots\ldots, e_m]^T$

The measured quantity, true state and the errors can be represented by the equation;

$$z = h(x) + e \tag{2}$$

$$z = \begin{bmatrix} z_1 \\ z_2 \\ \vdots \\ z_m \end{bmatrix} = \begin{bmatrix} h_{1(x_1,x_2,\ldots,x_3)} \\ h_{2(x_1,x_2,\ldots,x_3)} \\ \vdots \\ h_{m(x_1,x_2,\ldots,x_3)} \end{bmatrix} + \begin{bmatrix} e_1 \\ e_2 \\ \vdots \\ e_m \end{bmatrix} = h(x) + e$$

$$\text{where, } h(x) = \begin{bmatrix} h_{1(x_1,x_2,\ldots,x_3)} \\ h_{2(x_1,x_2,\ldots,x_3)} \\ \vdots \\ h_{m(x_1,x_2,\ldots,x_3)} \end{bmatrix}, e = \begin{bmatrix} e_1 \\ e_2 \\ \vdots \\ e_m \end{bmatrix}, \text{ and, } x = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_m \end{bmatrix}$$

For an ideal case $e_1, e_2, e_3 and\ e_4$ which, represent the errors will be zero. The relationship between the errors can be expressed as

$$e = z - h(x) \tag{3}$$

By applying the weighted least-square (WLS) criterion, an estimate $\hat{x}$ of the state variable x is obtained and minimizes the performance index $J(\hat{x})$ that best fits the meter measurements, $J(\hat{x})$ is defined by

$$F(x) = (z - H(x))^T W(z - Hx) \tag{4}$$

where W is the weight matrix which is diagonal. To obtain the first order optimal condition, $F(x)$ is differentiated to obtain

$$\hat{x} = (H^T W H)^{-1} H^T W z \tag{5}$$

Sensor measurements are error prone and differ from calculated results which are free from errors. It is therefore required to estimate the true values of these measurements by eliminating the errors. Errors can be introduced into the measurements due to inadequacies of measurement devices, device failures or malicious actions. It is therefore important for power system operators to identify and correct bad data [12],[18],[23],[24]. There is an inbuilt scheme in most EMS for BDD. There exists a measurement residual and its Euclidean norm is compared against an acceptable threshold. These residual measurements represent the difference between the measured data and the true value of the measurement.

$$r = z - h(\hat{x}) \tag{6}$$

Bad measurements is assumed to exist if $||r|| > \tau$, where τ represent the pre-set threshold otherwise the measurement is accepted.

B. BASED ON AC STATE ESTIMATION MODEL

Unlike the DC model, in the ac power flow state estimation, power flows are nonlinearly dependent on the state variables and nonlinear equations are used for representation.

$$z = h(x) + e \tag{7}$$

where;

z represents the vector of measured values obtained from sensors (active and reactive power flows, power injections, voltage magnitudes and angles)

x represents the vector of state variables (voltage magnitudes and angles);

e vector of undesired measurement errors

h(x) vector function that relates measured values and state variables from the weighted least square method;

$$minF(x) = \left(z - h(x)\right)^T W(z - h(x)) \tag{8}$$

where W is the weighting metric. The elements in W correspond to the inverse of the accuracy of the measurements. The solution in this case requires iterations and the first order optimality condition is formulated as

$$\frac{dF(x)}{dx} | x = \hat{x} = -2J_h^T(\hat{x}) W\left(z - h(\hat{x})\right) = 0 \tag{9}$$

where J denotes the Jacobian matrix from the vector function $h(x)$ and $\hat{x}$ is the estimated state vector.

Assuming there are m meter measurements $z = [z_1, \ldots., z_m]^T$ and n state variables given by $x = [\delta_2\ \delta_3 \ldots\ldots \delta_n\ V_1\ V_2\ V_3 \ldots\ldots V_n]^T$. the resultant matrix H characterized by the mxn matrix. The matrix H is determined by the topology and line impedances of the power system [23], [25]. If the attacker has access to the matrix H of the power system, he can inject malicious measurements in order to compromise the meter measurements.

Considering two possible attack strategies where the attacker aims to find any attack vector that can result in a wrong estimate of state variables and the case of injecting a specific error into state variables.

Assuming the case of a malicious measurement denoted by z_a i.e $z_a = z + a$, where $a = [a_1, a_2, \ldots., a_m]^T$ is referred to as the attack vector. a is most likely to be identified by BDD if unstructured. However, in most recent attacks $a = Hc$ where $c = [c_1, c_2, \ldots., c_n]^T$ is an arbitrary nonzero vector can be undetected by BDD. These are referred to as FDIA. They may be referred to as unobservable attacks since their detection by current BDD schemes is not guaranteed and the operator cannot distinguish between the attack vectors and the state estimate vector.

$$\hat{x}_{bad} = (H^T W H)^{-1} H^T W z_a = (H^T W H)^{-1} H^T W (z + a) \tag{10}$$

$$\hat{x}_{bad} = (H^T W H)^{-1} H^T W z_a = (H^T W H)^{-1} H^T W (z + a) \tag{11}$$

Since $a = Hc$, formulating the 2-norm of the measurement residuals;

$$\left|\left|z_a - H\hat{x}_{bad}\right|z + a - H(\hat{x} + (H^T WH)^{-1}H^T Wa)\right|| \quad (12)$$

$$= ||z - H\hat{x} + (a - H((H^T WH)^{-1}H^T Wa)|| \quad (13)$$

$$= ||z - H\hat{x} + (Hc - H((H^T WH)^{-1}H^T WHc)|| \quad (14)$$

$$= \left|\left|z - H\hat{x} + (Hc - Hc)\right|\right| = ||z - H\hat{x}|| \leq \tau \quad (15)$$

Here it is demonstrated that the 2-norm of the measurement of Z_a is less than the preset threshold τ which means Z_a will be undetected by BDD. The injected error then becomes

$$\hat{x}_{bad} - \hat{x} = (H^T WH)^{-1}H^T Wa = c \quad (16)$$

Consider a balanced and symmetric distribution system using the single phase feeder shown in Fig. 1. . The total load consumed through a line between loads i and j is denoted by a complex variable I_{ij}, where the line impedance is denoted by Z_{ij}. I_{ij} denotes the current entering the line and the voltage at the node is denoted by v_i. The system can then be modelled as follows.

The Point of Common Coupling (PCC) delivering power to a set of nodes will be modelled as the reference or slack node. The nodes along the line except the reference node will be denoted by $N = \{1, \ldots, n\}$. The set of lines will be denoted by $L = \{1, \ldots, l\}$. The voltage at the reference node will be given as

$$V_0 = V_0 e^{J\theta_0} \quad (27)$$

The node is modelled as a PQ node where complex power injected. From the general power equation,

$$S_{ij} = V_i I^*_i \quad (18)$$

where I^*_i represents the complex conjugate of i_i. Applying this to the line, the complex flow along the line can be represented as

$$S_{ij} = V_i I^*_{ij} \quad (19)$$

Assuming that the shunt admittance on each node is negligible, the nodal current can be represented as

$$I_i = \sum_j^n I_{ij}$$

The line current can also be represented as;

$$I_{ij} = \sum_j^n I_k \quad (20)$$

where k represents the set of nodes $\{i, j\}$.

The relationship between the terminal voltages of the line terminals $\{i, j\}$ can be expressed as

$$V_j = V_i - z_{ij} I_{ij} \quad (21)$$

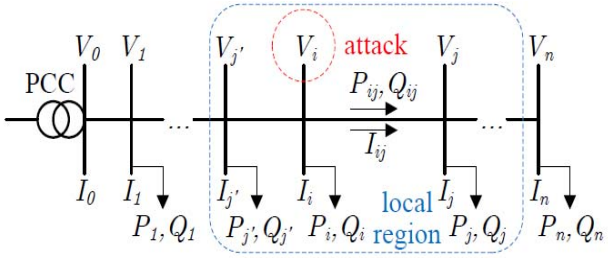

Fig. 1: A symmetrical and balanced distribution system

where z_{ij} represents the impedance of the line $\{i, j\}$.

The matrix h(x) which represents the measurement function can be written for meter measurements which are power flow in both directions (forward and reverse) (das power flow);

$$z = [P_L^{fwd}, Q_L^{fwd}, P_L^{rvs}, Q_L^{rvs}, P_N, Q_N, V_N] \quad (22)$$

where $P_{\mathcal{L}}^{fwd}, Q_{\mathcal{L}}^{fwd}, P_{\mathcal{L}}^{rvs} and\ Q_{\mathcal{L}}^{rvs}$ represent the power flow in both reverse and forward directions on all lines while $P_N, Q_N and\ V_N$ are the power flow injections and voltage magnitudes on all PQ nodes. The details of the measurement function $h(x)$ are given below

- if meter measurements are power-flow measurements P_{ij}, Q_{ij} on the line $\{i, j\}$, $h(x)$, then

$$z = [P_{\mathcal{L}}^{fwd}, Q_{\mathcal{L}}^{fwd}, P_{\mathcal{L}}^{rvs}, Q_{\mathcal{L}}^{rvs}, P_{\mathcal{N}}, Q_{\mathcal{N}}, V_{\mathcal{N}}] \quad (23)$$

where y_{ij} is the admittance of the line.

- For power injection measurements;

$$h_i^p(x) + jh_i^q(x) = v_i \sum_j y_{ij} (v_i - v_j)^* \quad (24)$$

- The voltage magnitude measurement can be expressed as

$$h_i^v(x) = v_i \quad (25)$$

IV. APPROXIMATE STATES ESTIMATION FROM POWER-FLOW MEASUREMENTS

Based on power flow measurements; defining the vectors $V_l, I_l and\ S_l$ as the voltage, current and complex power flows along the line;

$$S_L = (V_L) I_L \quad (26)$$

The relationship between the line voltages and currents can thus be given as

$$I_l = Y_{ij}(V_0 | V_N)^T \quad (37)$$

Partitioning the branch admittance matrix since the same partitioning can be achieved as the voltages; the line current gives;

$$I_l = (Y_{LO} | Y_{LN}) \begin{pmatrix} V_0 \\ V_N \end{pmatrix} \quad (28)$$

The nodal voltage can then be computed as

$$V_N = V_0 + Z_{NL} I_L \quad (29)$$

The assumptions in this approximation process are that the voltage magnitudes (in pu) of the nodes in distribution systems are close to each other with a range of 0.95 to 1.05. Also, the voltage phase angles are of very low values owing to the short power flows and short lines [26]. The current can therefore be approximated as

$$I_L \approx [diag(V_L^{-1})S_L]^* = (\frac{S_L}{V_0})^* \quad (30)$$

The voltages, V_N can now be approximated from the power flow measurements $S_L$as;

$$V_N \approx V_0 + Z_{NL}\left(\frac{S_L}{V_0}\right)^* = V_0 e^{j\theta}(1 + Z_{NL}S_L^*/V_0^2 \quad (31)$$

Equations shows that the system states V_N *and* θ_N can be approximated from the power flow measurements P_L *and* $Q_L$with V_0 *and* θ_0 taking as reference.

V. CONCLUSION

In this paper, the modeling and countermeasures for estimating the true states of power systems has been presented. The injection of false data into the measurements, which could be undetectable are studied and modelled. Various traditional techniques of preventing false data injection in modern power systems are reviewed. Voltage collapse, which is the main aftermath of FDIA on power networks, is briefly discussed. The mathematical formulations based on both AC and linear DC power-flow analyses are presented. The results of this paper could serve as a basis to the implementation of the models presented on a real time power system. It could also serves as an important signal to the system operators in proper monitoring and controlling of the system against bad data which could cause total system blackout.

REFERENCES

[1] G. Hug and J. A. Giampapa, Vulnerability Assessment of AC State Estimation With Respect to False Data Injection Cyber-Attack, vol. 3, IEEE Transactions on Smart Grid,, 2012.

[2] H. Karimipour and V. Dinavahi, Robust Massively Parallel Dynamic State Estimation of Power Systems Against Cyber_attack, IEEE, 2017.

[3] D. P. Kothari and I. J. Nagrath, Modern Power System Analysis, New Dehli: Tata McGraw Hill Education Private Limited, 2009, pp. 531-545.

[4] R. B. Bobba, K. M. Rogers, Q. Wang, H. Khurana, K. Nahrstedt and T. J. Overbye, Detecting False Data Injection Atacks on DC State Estimation.

[5] A. Anwar and A. N. Mahmood, Vulnerabilites of Smart Grid State Estimation against False Data Injection Attack, Renewable Energy Integration, Green Energy and Technology, Springer, 2014, pp. 411-428.

[6] M. Khalaf, A. Youssef and E. El-Saadany, Detection of False Data Injection in Automatic Generation Control Systems Using Kalman Filter, IEEE Electrical Power and Energy Conference (EPEC), 2017.

[7] Y. Yuan, Z. Li and K. Ren, Modeling Load Redistribution Attacks in Power Systems, IEEE Transactions on Smart Grid, 2011.

[8] Y. Liu, P. Ning and M. K. Reiter, False Data Injection Attacks Against State Estimations in Electric Power Grids, vol. 14, ACM Transactions on Information and System Security, 2011.

[9] T. T. Kim and H. V. Poor, Strategic Protection Against Data Injection Attacks on Power Grids, IEEE Transactions on Smart Grid, 2011.

[10] G. Liang, J. Zhao, F. Luo, S. R. Weller and Z. Dong, A Review of False Data Injection Attacks Against Modern Power Systems, IEEE Transaction on Smart Grids, 2015.

[11] A. Teixeira, S. Amin, H. Sandberg, K. H. Johansson and S. Sastry, Cyber Security Analysis of State Estimators in Electric Power Systems, Proc. of ACM Conf. on Dec. and Cont., 2010, pp. 5991-5998.

[12] J. Wang, D. Shi, J. Chen and X. Duan, Realistic Measurement Protection Schemes Against False Data Injection Attacks o State Estimators, IEEE, 2017.

[13] T. Lan, W. Wang and G. M. Huang, False Data Injection Attack in Smart Grid Topology Control: Vulnerability and Countermeasures, 2017: IEEE.

[14] R. Deng, P. Zhuang and H. Liang, False Data Injection Attacks Against State Estimation in Power Distribution Systems, IEEE Transaction on Smart Grid, 2018.

[15] D. D. Giustina, M. Pau, P. A. Pegoraro, F. Ponci and S. Sulis, Electrical Distribution System State Estimation: Measurement Issues and Challenges, IEEE Instrumentation & Measurement Magazine, 2014.

[16] J. Yan, Y. Tang, B. Tang, H. He and Y. (. Sun), Power Grid Resilience Against False Data Injection, Boston, MA, USA: IEEE, Power and Energy Society General Meeting (PESGM), 2016.

[17] H. Karimipour and V. Dinavalhi, On False Data injection Attack against Dynamic State Estimation on Smart Power Grids, 5th IEEE International Conference on Smart Energy Grid Engineerig, 2017.

[18] J. Zhu and X. Wei, Defending False Data Injection Attacks against Power System State Estimation: A Stealthiness Corruption-Oriented Method, IEEE, 2016.

[19] R. Xu, R. Wang, Z. Guan, L. Wu, J. Wu and X. Du, Achieving Efficient Detection against False Data Injection Attacks in Smart Grid, IEEE, 2017.

[20] K. Pan, A. Teixeira, M. Cvetkovic and P. Palensky, Cyber Risk Analysis of Combined Data Attacks Against Power System State Estimation, IEEE Transaction on Smart Grid, 2018.

[21] G. Hug and J. A. Giampapa, Vulnerability Assessment of AC State Estimation With Respect to False Data Injection Cyber-Attack, vol. 3, IEEE Transactions on Smart Grid, 2012.

[22] M. Jin, J. Lavaei and k. Johansson, A Semidefinite Programming Relaxation under False Data Injection Attacks against Power Grid AC State Estimation, Illinois, USA: Fifty-Fifth Annual Allerton Conference, 2017.

[23] R. Deng, G. Xiao and R. Lu, Defending Against False Data Injection Attacks on Power System State Estimation, vol. 13, IEEE Transaction on Industrial Informatics, 2017.

[24] O. Kosut, L. Jia, R. J. Thomas and L. Tong, Malicious Data Attacks on Smart Grid State Estimation: Attack Strategies and Countermeasures, IEEE, 2010.

[25] Y. Mo, T. H. kim, Brancik and D. Dickinson, Cyber-Physical Security of a Smart Grid Infrastructure, vol. 100, IEEE, 2012.

[26] M. E. Elkhatib, R. El-Shatshat and M. M. Salama, Novel coordinated Voltage Control For Smart Distribution Networks with DG, vol. 2, IEEE Transactions on Smart Grids, 2011, pp. 598-605.