Wide and Recurrent Neural Networks for Detection of False Data Injection in Smart Grids

Yawei Wang[1], Donghui Chen[2], Cheng Zhang[1](✉), Xi Chen[3], Baogui Huang[4], and Xiuzhen Cheng[1]

[1] Department of Computer Science, The George Washington University, Washington DC, USA
{yawei,zhangchengcarl,cheng}@gwu.edu

[2] College of Information and Science Technology, Beijing Normal University, Beijing, People's Republic of China
dh_chen@mail.bnu.edu.cn

[3] GEIRI North America, San Jose, CA, USA
xi.chen@geirina.net

[4] School of Information Science and Engineering, Qufu Normal University, Rizhao, Shandong, People's Republic of China
hjbaogui@163.com

Abstract. A smart grid is a complex system using power transmission and distribution networks to connect electric power generators to consumers across a large geographical area. Due to their heavy dependencies on information and communication technologies, smart grid applications, such as state estimation, are vulnerable to various cyber-attacks. False data injection attacks (FDIA), considered as the most severe threats for state estimation, can bypass conventional bad data detection mechanisms and render a significant threat to smart grids. In this paper, we propose a novel FDIA detection mechanism based on a wide and recurrent neural networks (RNN) model to address the above concerns. Simulations over IEEE 39-bus system indicate that the proposed mechanism can achieve a satisfactory FDIA detection accuracy.

Keywords: Smart grid · False data injection · Deep learning

1 Introduction

As one of the most critical infrastructures of Internet of Things (IoT), smart grid, also called smart electrical/power grid, intelligent grid, or futuregrid, is designed for the next generation power system. Unlike the traditional electrical grids that send electrical power only in one direction, from a power plant to consumers, smart grid improves on the electricity network by using bi-direction flows of electricity and data that provides electrical uses, power interruptions, and instantaneous feedback on system-wide operations back to power plant and

E. S. Biagioni et al. (Eds.): WASA 2019, LNCS 11604, pp. 335–345, 2019.
https://doi.org/10.1007/978-3-030-23597-0_27

regional power grid operators. By utilizing advanced communication and data processing technologies, smart grids are capable of delivering power in more efficient ways and responding to wide-ranging conditions and events. However, the heavy dependence on communication technology and big data highlights the potential vulnerabilities of smart grids to various cyber attacks. Although many communication standards, official guidelines, regulatory laws have been published as countermeasures such as IEC 61850-90-5 and the NISTIR 7628 Guideline [7,11], cyber attack issues still remain in smart grids.

False data injection attacks (FDIA), as a typical type of cyber attacks proposed by Liu *et al.* [20], has been recently identified as one of the most critical malicious behaviours against state estimation in smart grids. In such attacks, the goal of the attackers is to circumvent the conventional bad data detection system and either compromise the communication infrastructures [32] or attack the measurement devices through manipulating system variable measurements. Without effective and robust detection systems, attackers may stealthily launch FDIA multiple times and render a significant threat to smart grids [5].

Therefore, this paper investigates a novel deep learning approach to detect well-constructed FDIA that are not detectable by conventional bad data detection systems in smart grids. In particular, we proposed a wide and recurrent neural networks (RNN) model to learn the state variable measurement data and identify the FDIA. Our wide and RNN model consists of a wide component with a fully connected layer of neural networks and an RNN component with two LSTM layers. Essentially, the wide component can learn the global knowledge and the RNN component can capture the sequential correlations among state variable measurement data. This model integrates the advantages of the wide component and the RNN component resulting in a satisfactory performance in the detection of FDIA. The major research contributions of the paper can be summarized as follows:

- We propose a wide and RNN model to detect FDIA in smart grids. To the best of our knowledge, this paper is among the pioneer studies of using wide and RNN model in FDIA detection research.
- Our model combine the power of memorization of the global knowledge brought by the wide component and generalization of the new temporal knowledge brought by the RNN model.
- We assess the proposed FDIA detection mechanism with existing FDIA patterns on IEEE 39-bus power system test case. The simulation results demonstrate a satisfactory FDIA detection accuracy.

The rest of the paper is organized as follows: Sect. 2 presents an overview on related literature. Our system model is introduced in Sect. 3. Section 4 presents the wide and RNN model for FDIA detection. We then give the simulation settings and results in Sect. 5. Finally, we conclude the paper in Sect. 6.

2 Related Work

A wide range of research focus on the security challenges in smart grids. In this section, we briefly cover two research directions that are mostly related to our work. We first present the existing works for the construction of FDIA. Then, we provide an overview of FDIA detection mechanisms proposed in the literature.

2.1 FDIA in Smart Grids

FDIAs in smart grids were first introduced in 2009 [20] and expanded in [21]. Following these initial work, many researchers tried to investigate more realistic and effective attacks against the state estimation in smart grids. Kosut *et al.* [14] proposed two regimes of FDIA based on the number of meters that the adversaries can access. In [35], the authors introduced a special type of FDIA focusing on load redistribution (LR) and analyzed the damage to smart grid operation in different time steps with different prior attacking knowledge. An energy deceiving attack proposed by Lin *et al.* [17] was another type of FDIA that aims to affect the distributed energy routing process. Kim *et al.* [13] characterized the FDIA problem into a series of linear programs. Moreover, a comprehensive review of the state of the art FDIA methods against modern smart grid systems were presented by Liang *et al.* [15].

2.2 Detection Mechanisms Against FDIA

At the same time, much research effort has been devoted to devising mechanisms against FDIA using various techniques. Some researchers solved the FDIA detection problem by using different optimization methods. For instance, in [19], according to the sparsity of malicious attacks, the authors formulated the FDIA detection as a sparse matrix optimization problem and solved it by using nuclear norm minimization and low rank matrix factorization methods. Instead of the complex optimization computing, threshold-based comparisons were more commonly utilized to identify the FDIA. The authors of [23] employed the Kalman filter and the Euclidean detector with a selected threshold to detect FDIA in the IEEE 9-bus system. Similarly, by comparing a residual signals with a predefined threshold, a resilient attack detection estimator was proposed in [8] to detect the FDIA in a networked cyber-physical system. However, an increasing number of FDIA can bypass these threshold-based detectors. To combat this challenge, learning-based methods have been utilized to detect FDIA [26]. In [6], the authors proposed a FDIA detector by utilizing the principle component analysis and support vector machine (SVM). In [9], Conditional Deep Belief Network (CDBN) was proposed to reveal attack features, which was then exploited to detect the FDIA on real-time measurements. Motivated by the strengths of these learning-based methods, we propose a FDIA detection mechanism based on a novel wide and recurrent neural network (RNN) model in this paper.

3 System Model

FDIA is considered as one of the most severe malicious behaviours rendering a significant threat to the grid [5]. Well-constructed FDIA can effectively circumvent the conventional residual-based bad data detection mechanism in direct current (DC) state estimation. In this section, we briefly present the state estimation method that is widely employed in power utilities [34], the conventional residual-based bad data detection mechanism [4], and the general patterns of successful FDIA in smart grids.

3.1 State Estimation

State estimation was first proposed by Schweppe and Wilde in 1970 [29–31] as a weighted least-squares (WLS) problem. The goal of state estimation is to estimate the smart grid's operating conditions by using real-time data collected from the measurement units [27]. Typical measurements include bus voltage, active and reactive power injections at each bus, and complex power flows on branches. Based on the DC power flow model, we can construct the relationship between system states $\mathbf{x}$ and measurements $\mathbf{z}$ as a linear model as follows:

$$\mathbf{z} = \mathbf{H}\mathbf{x} + \mathbf{e}, \tag{1}$$

where $\mathbf{x} \in \mathbb{R}^D$ contains the voltage amplitude and voltage phase angle at the buses, $\mathbf{z} \in \mathbb{R}^N$ is the vector of measurements, $\mathbf{H} \in \mathbb{R}^{N \times D}$ is a Jacobian topological matrix that maps the system states to the measurements, $\mathbf{e}$ is the measurement error (additive noise) vector that is commonly modeled by the Gaussian distribution, i.e., $\mathcal{N} \sim (0_{N\times 1}, \mathbf{W}^{-1})$ where $\mathbf{W} \equiv diag\{\mathbb{R}^{-1}\}$ with diagonal elements proportional to variance of each measurement noise. State estimation aims to find an estimated state $\hat{\mathbf{x}}$ that fits the measurement $\mathbf{z}$ the best and minimizes the WLS error [27] defined as follows:

$$\hat{\mathbf{x}} = \arg_x \min(\mathbf{z} - \mathbf{H}\mathbf{x})^T \mathbf{W}(\mathbf{z} - \mathbf{H}\mathbf{x}). \tag{2}$$

In particular, (2) can be solved by using iterative approximation methods such as the Newton-Raphson method [2].

3.2 Conventional Bad Data Detection

In smart grid systems, in order to solve the problem of potential malicious attacks and the sampling error of measurement units, a residual-based bad data detection mechanism was employed to protect state estimations [24]. Given the measurements $\mathbf{z}$, the estimated state vector $\hat{\mathbf{x}}$ can be computed as follows:

$$\hat{\mathbf{x}} = (\mathbf{H}^T\mathbf{W}\mathbf{H})^{-1}\mathbf{H}^T\mathbf{W}\mathbf{z} = \mathbf{Y}\mathbf{z}, \tag{3}$$

where $\mathbf{Y} = \mathbf{H}(\mathbf{H}^T\mathbf{W}\mathbf{H})^{-1}\mathbf{H}^T\mathbf{W}$. Therefore, the residue vector $\mathbf{r} = \mathbf{z} - \hat{\mathbf{z}}$ with threshold γ being calculated using the difference between the observed measurements $\mathbf{z}$ and the measurements inferred by the estimated system state $\hat{\mathbf{z}} = \mathbf{H}\hat{\mathbf{x}}$

for DC power flow model. If $\|\mathbf{r}\|_2 > \gamma$, the estimated state is considered being compromised by bad data; otherwise, the estimated state is trustworthy. According to the threshold test proposed in [33], the value of γ is typically determined by the hypothesis test $Pr\{\|\mathbf{r}\|_2^2 >= \gamma^2\} = \alpha$, where α is the confidence level.

3.3 False Data Injection Attacks

FDIA have been recently identified as a critical malicious data attacks in a smart grid system [14,21,35]. The objective for performing FDIA is to mislead the system operator to treat a compromised state vector $\hat{\mathbf{x}}_{comp} = \hat{\mathbf{x}} + \mathbf{c}$ as the normal estimated system state, where $\mathbf{c} \in \mathbb{R}^n$ is a non-zero vector. To achieve this, the potential attackers aim to change the received measurements to $\mathbf{z_a} = \mathbf{z} + \mathbf{a}$ at the control center, where $\mathbf{a} \in \mathbb{R}^m$ is the injected attack vector which can be constructed as

$$\mathbf{a} = \mathbf{H}(\hat{\mathbf{x}} + \mathbf{c}) - \mathbf{H}\hat{\mathbf{x}}. \tag{4}$$

In order to bypass the bad data detector, the Euclidean norm of the residual $\mathbf{r_a}$ needs to keep unchanged

$$\begin{aligned} \|\mathbf{r_a}\|_2 &= \|\mathbf{z_a} - \mathbf{H}\hat{\mathbf{x}}\|_2 \\ &= \left\|\mathbf{z} + \mathbf{a} - \mathbf{H}(\hat{\mathbf{x}} + \mathbf{c})\right\|_2 \\ &= \|\mathbf{z} - \hat{\mathbf{z}}\|_2 \\ &= \|\mathbf{r}\|_2 \,, \end{aligned} \tag{5}$$

and the detailed injected attack vector construction is discussed in [28]. Therefore, the conventional residual-based bad data detection mechanism in DC state estimation might fail to detect FDIA that are well-constructed by adversaries who have prior knowledge of the gird including network topology $\mathbf{H}$ and estimated states $\hat{\mathbf{x}}$.

4 Proposed Wide and Recurrent Neural Networks for FDIA Detection

In the previous sections, we have shown that well-constructed FDIA can effectively bypass conventional bad data detection mechanisms and render a significant threat to smart grids. In this section, we propose a novel FDIA detection mechanism in DC power flow model based on the wide and deep learning framework [3].

In our approach, we feed the measurements $\mathbf{z}$ into the wide and RNN model consisting of the wide component and the RNN component. We explain them in details as follows.

4.1 Wide Component

The wide component is a fully connected layer of neural networks that is used to learn the global knowledge from the input data with a generalized linear model of the form $\mathbf{y} = \mathbf{w}^T\mathbf{x} + \mathbf{b}$, where y is the output; $\mathbf{x} = [x_1, x_2, ..., x_d]$ is the vector of d features; $\mathbf{w} = [w_1, w_2, ..., w_d]$ are the model parameters, and $\mathbf{b}$ is the bias. Motivated by the previous study [3,16], in the context of FDIA detection, we choose the wide component to learn the frequent co-occurrence of features by memorizing the estimated state estimation data $\hat{\mathbf{x}}$.

To be specific, every neuron in the wide component calculates the prediction score according to the following equation:

$$\mathbf{y}_j = \sum_{i=1}^{n} \mathbf{w}_{i,j}\hat{\mathbf{x}}_i + \mathbf{b}, \tag{6}$$

where $\mathbf{y_j}$ is the output in the jth neuron of the fully connected layer, n is the number of the input data $\hat{\mathbf{x}}$, $\mathbf{w}_{i,j}$ stands for the neuron weight between the ith input value and the jth neuron of the fully connected layer, and $\mathbf{b}$ is the bias. Within each neuron, the activation is given as follows:

$$a_j = f(\mathbf{y_j}) = \begin{cases} 0 & \text{if} \quad \mathbf{y}_j \leq 0 \\ \mathbf{y}_j & \text{otherwise.} \end{cases} \tag{7}$$

where a_j is the output of the activation calculation and $f(\cdot)$ stands for the rectifier linear units (ReLUs) which can effectively prevent overfitting. During the process of backpropagation, the neural network updates the neuron weights $\mathbf{w}_{i,j}$ iteratively based on the loss value sent back from the loss function.

4.2 RNN Component

In our approach, we set the RNN component as a many-to-one RNN model that makes use of sequential information $x_{(1)}, ..., x_{(t)}$ to predict the output. The mathematical model of the RNN is as follows:

$$\mathbf{h}_t = f(\mathbf{h}_{t-1}, \mathbf{x}_t), \tag{8}$$

where $\mathbf{h}_t$ and $\mathbf{h}_{t-1}$ represent the current and previous hidden states, respectively; f stands for a nonlinear function, and $\mathbf{x}_t$ refers to the feature observed at time step t. The constructed RNN mode is composed of two LSTM layers with five LSTM cells each. Each LSTM cell consists of three gates which are forget gate f_t, input layer i_t, and output gate o_t [10]. The information flow of LSTM cell is modeled as follows:

$$f_t = \sigma(W_f \cdot [h_{t-1}, x_t] + b_f), \tag{9}$$

$$i_t = \sigma(W_i \cdot [h_{t-1}, x_t] + b_i), \tag{10}$$

$$\tilde{C}_t = tanh(W_c \cdot [h_{t-1}, x_t] + b_c), \tag{11}$$

$$C_t = f_t \circ C_{t-1} + i_t \circ \tilde{C}_t, \tag{12}$$

$$o_t = \sigma(W_o[h_{t-1}, x_t] + b_0), \tag{13}$$

$$h_t = o_t \circ tanh(C_t), \tag{14}$$

where x_t is the input vector; h_{t-1} is the previous cell output; C_{t-1} is the previous cell memory; h_t is the current cell output; C_t is the current cell memory, $\sigma(\cdot)$ and $tanh(\cdot)$ stand for the sigmoid function and the hyperbolic tangent function respectively, and $\circ$ denotes the element-wise product; W_f, W_c, W_i and W_o represent the weight vectors for forget gate f, candidate c, input gate i, and output gate o, respectively.

After constructing the wide component and the RNN component, we combine them using a weighted sum of their output as hidden features and fed them to a logistic loss function for joint training and prediction. Motivated by the original approach of the wide and deep learning model [3,36], we use backpropagation to train our network. In particular, we set our prediction model as:

$$P(\mathbf{Y}=1|x) = \delta(\mathbf{W}[\mathbf{x}_{wide}, \mathbf{x}_{RNN}] + \mathbf{b}), \tag{15}$$

where $\mathbf{Y}$ is the binary label which represents that whether there is a FDIA or not in the input data; $\delta(\cdot)$ is the sigmoid function; $\mathbf{W}$ is the joint weights of the combined part of the network; $\mathbf{x}_{wide}$ and $\mathbf{x}_{RNN}$ stand for the features of the wide component and the RNN component, respectively, and $\mathbf{b}$ is the bias.

5 Case Study on IEEE 39-Bus System

In this section, we assess the performance of our proposed FDIA detection mechanism on IEEE 39-bus system, which is shown in Fig. 1, and compare results with those of other existing methods.

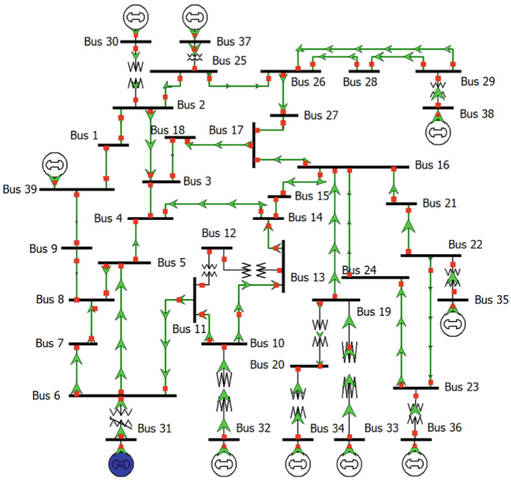

Fig. 1. IEEE 39-Bus system case [1]

5.1 Simulation Settings

The amount of data is critical to the results of neural networks. In this paper, we use DIgSILENT Power System Software [25] to conduct a simulation for generating 150,000 samples. Besides the above normal operational samples, we constructs another 50,000 FDIA samples based on the existing FDIA mechanism introduced in Sect. 3.3 that ensure they can bypass the conventional residual-based bad data detection. The configuration of the test system can be obtained from MATPOWER toolbox [37] including the network topology matrix **H**. For cross validation, according to the common practice [12], the total 200,000 samples are randomly divided into training data, validation data, and testing data by 6:2:2 ratio. All simulations are conducted on the computer with an Intel Core i7-9700K CPU, an Nvidia RTX 2080 Ti GPU, 64-GB RAM, and 1000 watt power supply. The proposed wide and RNN model is constructed and trained using Tensorflow.

5.2 FDIA Detection Performance Evaluation

In this paper, we use statistical performance matrix to evaluate the proposed FDIA detection mechanism and other existing works. We label a power flow measurement with FDIA as positive class and a normal measurement as negative class. As shown in Table 1, the four measurement instances that we used are defined as follows: True Positive (TP) is an outcome that correctly predicts the positive class, True Negative (TN) is an outcome that correctly predicts the negative class, False Positive (FP) is an outcome that incorrectly predicts the positive class, and False Negative (FN) is an outcome that incorrectly predicts the negative class.

Table 1. Definition of performance measurements

	Classified as FDIA	Classified as No attack
FDIA	TP	FN
No attack	FP	TN

We first calculate the prediction accuracy which is the proportion of correct results, either true positive or true negative, in a population for individual wide neural networks, individual recurrent neural networks, and the wide and RNN model we proposed. According to the simulation results in Table 2, the proposed wide and RNN mechanism can develop a satisfactory DC FDIA detection accuracy which is higher than those of the individual wide model and individual RNN model. Meanwhile, the FP rate and the FN rate of the wide and RNN model are lower than that of the individual ones.

Furthermore, for a complete comparison, we also present the simulation results of the three other DC FDIA detection mechanisms proposed in [6, 18, 22].

The individual detection accuracy of all the selected detection mechanisms is presented in Table 3. It can be observed that the proposed FDIA detection mechanism can remarkably outperform the previous work. In particular, the detection accuracy is improved from around 70% by [22] to more than 95%.

Table 2. FDIA detection performance of the proposed mechanism

		Wide	RNN	Wide and RNN
Training cases	TP+TN	75.31% (112,965)	92.68% (139,020)	95.39% (143,085)
	FP	14.65% (21,975)	4.85% (7275)	3.75% (5623)
	FN	12.98% (19,476)	4.49% (6735)	3.37% (5048)
Testing cases	TP+TN	75.13% (37,565)	92.58% (46,290)	95.23% (47,615)
	FP	14.78% (7390)	4.92% (2460)	3.78% (1892)
	FN	13.18% (6588)	4.53% (2265)	3.45% (1724)

Table 3. Comparisons of FDIA detection performance

Mechanism	Accuracy
Euclidean detector [22]	72.68%
Sparse Optimization [18]	86.79%
SVM-based [6]	90.06%
Proposed Wide and RNN	95.23%

6 Conclusion

In this paper, we propose a wide and RNN model to detect FDIA in smart grids. In particular, our wide and RNN model consists of the wide component and the RNN component, which takes advantage of memorization of the global knowledge of the input measurements and generalization of the temporal correlation between the measurements at successive time instants. We conduct extensive simulations on IEEE 39-bus system demonstrating the effectiveness and correctness of the proposed mechanism. For future research, we will consider making our FDIA detector adaptive to alternating current (AC) state estimation.

Acknowledgment. This work was partially supported by the US National Science Foundation under grant IIS-1741279, and the National Science Foundation of China under grants 61832012, 61771289, and 61672321.

References

1. Athay, T., Podmore, R., Virmani, S.: A practical method for the direct analysis of transient stability. IEEE Trans. Power Apparatus Syst. **2**, 573–584 (1979)
2. Bertaccini, A., Duduk, B., Paltrinieri, S., Contaldo, N.: Phytoplasmas and phytoplasma diseases: a severe threat to agriculture. Am. J. Plant Sci. **5**(12), 1763 (2014)
3. Cheng, H.T., et al.: Wide & deep learning for recommender systems. In: Proceedings of the 1st Workshop on Deep Learning for Recommender Systems, pp. 7–10. ACM (2016)
4. Deng, R., Xiao, G., Lu, R.: Defending against false data injection attacks on power system state estimation. IEEE Trans. Industr. Inf. **13**(1), 198–207 (2017)
5. Deng, R., Xiao, G., Lu, R., Liang, H., Vasilakos, A.V.: False data injection on state estimation in power systems-attacks, impacts, and defense: a survey. IEEE Trans. Industr. Inf. **13**(2), 411–423 (2017)
6. Esmalifalak, M., Liu, L., Nguyen, N., Zheng, R., Han, Z.: Detecting stealthy false data injection using machine learning in smart grid. IEEE Syst. J. **11**(3), 1644–1652 (2017)
7. Grid, N.S.: Introduction to NISTIR 7628 guidelines for smart grid cyber security. Guideline, September 2010
8. Guan, Y., Ge, X.: Distributed attack detection and secure estimation of networked cyber-physical systems against false data injection attacks and jamming attacks. IEEE Trans. Signal Inf. Process. Over Netw. **4**(1), 48–59 (2018)
9. He, Y., Mendis, G.J., Wei, J.: Real-time detection of false data injection attacks in smart grid: a deep learning-based intelligent mechanism. IEEE Trans. Smart Grid **8**(5), 2505–2516 (2017)
10. Hochreiter, S., Schmidhuber, J.: Long short-term memory. Neural Comput. **9**(8), 1735–1780 (1997)
11. Ikbal, A., Aftab, M.A., Hussain, S.S.: Performance comparison of IEC 61850–90-5 and IEEE C37. 118.2 based wide area PMU communication networks. J. Mod. Power Syst. Clean Energy **4**(3), 487–495 (2016)
12. James, J., Hill, D.J., Lam, A.Y., Gu, J., Li, V.O.: Intelligent time-adaptive transient stability assessment system. IEEE Trans. Power Syst. **33**(1), 1049–1058 (2018)
13. Kim, T.T., Poor, H.V.: Strategic protection against data injection attacks on power grids. IEEE Trans. Smart Grid **2**(2), 326–333 (2011)
14. Kosut, O., Jia, L., Thomas, R.J., Tong, L.: Malicious data attacks on the smart grid. IEEE Trans. Smart Grid **2**(4), 645–658 (2011)
15. Liang, G., Zhao, J., Luo, F., Weller, S.R., Dong, Z.Y.: A review of false data injection attacks against modern power systems. IEEE Trans. Smart Grid **8**(4), 1630–1638 (2017)
16. Liang, Y., Cai, Z., Yu, J., Han, Q., Li, Y.: Deep learning based inference of private information using embedded sensors in smart devices. IEEE Netw. **32**(4), 8–14 (2018)
17. Lin, J., Yu, W., Yang, X., Xu, G., Zhao, W.: On false data injection attacks against distributed energy routing in smart grid. In: Proceedings of the 2012 IEEE/ACM Third International Conference on Cyber-Physical Systems, pp. 183–192. IEEE Computer Society (2012)
18. Liu, L., Esmalifalak, M., Ding, Q., Emesih, V.A., Han, Z.: Detecting false data injection attacks on power grid by sparse optimization. IEEE Trans. Smart Grid **5**(2), 612–621 (2014). https://doi.org/10.1109/TSG.2013.2284438

19. Liu, L., Esmalifalak, M., Ding, Q., Emesih, V.A., Han, Z.: Detecting false data injection attacks on power grid by sparse optimization. IEEE Trans. Smart Grid **5**(2), 612–621 (2014)
20. Liu, Y., Ning, P., Reiter, M.K.: False data injection attacks against state estimation in electric power grids. In: Proceedings of the 16th ACM Conference on Computer and Communications Security, CCS 2009, pp. 21–32. ACM, New York, NY, USA (2009). https://doi.org/10.1145/1653662.1653666, http://doi.acm.org/10.1145/1653662.1653666
21. Liu, Y., Ning, P., Reiter, M.K.: False data injection attacks against state estimation in electric power grids. ACM Trans. Inf. Syst. Secur. (TISSEC) **14**(1), 13 (2011)
22. Manandhar, K., Cao, X., Hu, F., Liu, Y.: Detection of faults and attacks including false data injection attack in smart grid using Kalman filter. IEEE Trans. Control Netw. Syst. **1**(4), 370–379 (2014). https://doi.org/10.1109/TCNS.2014.2357531
23. Manandhar, K., Cao, X., Hu, F., Liu, Y.: Detection of faults and attacks including false data injection attack in smart grid using Kalman filter. IEEE Trans. Control Netw. Syst. **1**(4), 370–379 (2014)
24. Monticelli, A.: Electric power system state estimation. Proc. IEEE **88**(2), 262–282 (2000)
25. PowerFactory-DIgSILENT Germany (2017). https://www.digsilent.de/en/powerfactory.html
26. Ozay, M., Esnaola, I., Vural, F.T.Y., Kulkarni, S.R., Poor, H.V.: Machine learning methods for attack detection in the smart grid. IEEE Trans. Neural Netw. Learn. Syst. **27**(8), 1773–1786 (2016)
27. Phadke, A.G., Thorp, J.S., Karimi, K.: State estimlatjon with phasor measurements. IEEE Transactions on Power Systems **1**(1), 233–238 (1986)
28. Rahman, M.A., Mohsenian-Rad, H.: False data injection attacks against nonlinear state estimation in smart power grids. In: 2013 IEEE Power & Energy Society General Meeting, pp. 1–5. IEEE (2013)
29. Schweppe, F.C.: Power system static-state estimation, Part III: Implementation. IEEE Trans. Power Appar. Syst. **PAS–89**(1), 130–135 (1970)
30. Schweppe, F.C., Rom, D.B.: Power system static-state estimation, Part II: approximate model. IEEE Trans. Power Appar. Syst. **PAS–89**(1), 125–130 (1970)
31. Schweppe, F.C., Wildes, J.: Power system static-state estimation, Part I: exact model. IEEE Trans. Power Appar. Syst. **PAS–89**(1), 120–125 (1970)
32. Ten, C.W., Manimaran, G., Liu, C.C.: Cybersecurity for critical infrastructures: attack and defense modeling. IEEE Trans. Syst. Man Cybern.-Part A: Syst. Hum. **40**(4), 853–865 (2010)
33. Wu, F.F., Liu, W.E.: Detection of topology errors by state estimation (power systems). IEEE Trans. Power Syst. **4**(1), 176–183 (1989). https://doi.org/10.1109/59.32475
34. Wu, F.F.: Power system state estimation: a survey. Int. J. Electr. Power Energy Syst. **12**(2), 80–87 (1990)
35. Yuan, Y., Li, Z., Ren, K.: Modeling load redistribution attacks in power systems. IEEE Trans. Smart Grid **2**(2), 382–390 (2011)
36. Zheng, Z., Yang, Y., Niu, X., Dai, H.N., Zhou, Y.: Wide and deep convolutional neural networks for electricity-theft detection to secure smart grids. IEEE Trans. Industr. Inf. **14**(4), 1606–1615 (2018)
37. Zimmerman, R.D., Murillo-Sanchez, C.E.: Matpower 4.1 user's manual. Power Systems Engineering Research Center, Cornell University, Ithaca, NY (2011)