IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received May 26, 2020, accepted May 31, 2020, date of publication June 3, 2020, date of current version June 12, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2999585

Local False Data Injection Attack Theory Considering Isolation Physical-Protection in Power Systems

XUEQIAN FU, (Member, IEEE), GENGRUI CHEN, AND DECHANG YANG, (Member, IEEE)
College of Information and Electrical Engineering, China Agricultural University, Beijing 100083, China

Corresponding author: Xueqian Fu (fuxueqian@cau.edu.cn)

This work was supported by Chinese Universities Scientific Fund (2020RC029).

ABSTRACT Cyber security is a matter of the utmost importance in prosumer energy management systems and modern electric power transmission networks. Modern power system is a typical cyber physical system, which is formed by the deep integration of power network and information network. Cyber physical power system has the outstanding advantages of autonomy, reliability, flexibility and efficiency, which give hackers a chance to attack the power systems. Considering the energy distributions and local load redistributions, we propose a local AC false data injection attack model. Both the line power losses, and energy conservation are taken into account in establishing the local false data attack model. Because the state estimation in the actual power system allows some errors, we take the minimum residual in the region as the objective function. The effectiveness and feasibility of the proposed local false data attack theory are verified in the IEEE 57-bus test case. The simulation results show that the residual error of the injection vector obtained by this attack model is less than 30% compared with that in normal operation.

INDEX TERMS Cyber physical power system, false data injection attack, prosumer energy management, state estimation.

I. INTRODUCTION

There is a striking difference between the cyber physical power system and traditional power system. Cyber physical modeling and cyber security are of vital importance in prosumer energy management system. A significant concern is that multi-energy scheduling operation is a matter of the utmost importance for economy and renewable energy utilization in coupled electricity, heating and natural gas networks [1]. Research has been conducted in this field of integrated modelling and enhanced utilization of power-to-ammonia for high renewable penetrated multi-energy systems [2]. Noted that distributed renewable energy resources have a detrimental effect energy management in power systems [3]. To extract wind power time-series features, Wang *et al*. presented a deep prediction framework combining wavelet transform and deep convolutional neural network [4]. Wind speed time-series features can also be extracted using artificial intelligence, which has high effectiveness, efficiency and application [5], [6]. Artificial intelligence consists of feature learning, weight updater and multiple machine learning regressor [7].

So, it is obvious that before starting the cyber physical power system project, we still have many technical difficulties to overcome. In extreme cases, the solution to the problem of attack detection has been elusive.

With the penetration of modern information and communication technology in power systems, the information exchange between power network and information network is becoming more and more close. Due to the large-scale introduction of advanced information communication technology in the power systems, the automation and intelligence of the power system have been gradually improved, and a cyberattack has become a challenge to the safe operation. Research has been conducted in this field of enquiry.

In terms of cyber-physical system attack, false data injection (FDI) attack is always available in practice. An FDI attack can cause a blackout by evading detection by the bad data detection module in the supervisory control and data acquisition system [8]. A significant concern is that there is a tight link between physical consequences and a cyber-attack, which can induce sequential outages in power systems [9].

The associate editor coordinating the review of this manuscript and approving it for publication was Jiayong Li.

Zhao *et al*. presented an imperfect FDI attack model, which works well even for the direct current model-based power system nonlinear state estimation [10]. An attacker can not only launch an FDI attack at the physical system layer, but also block the wireless transmission channels between sensors and energy control centers [11]. Liu *et al*. modeled local FDI attacks, which made use of reduced network information and passed the examination of the state estimator [12]. Because false data may be treated as an outlier, Liu *et al*. designed false data attacks using dummy data, which can be hided among normal data [13]. The study in [14] emphasized that the outages of some lines can be masked via FDI attacks, which maximized the residual of lines. Yu *et al*. explored the failure probability issue of the false-data injection attack in electricity generation system, and designed stealthy attack and secure control strategies [15]. Because the missing information of power grid topology and transmission-line admittances have an adverse effect on attack damage degree, Yu *et al*. presented a blind FDI method for cyber-physical system attack using the principal component analysis without Jacobian matrix and state variables [16]. To overcome the attack shortcomings brought by limited information, Zhang *et al*. presented a multiple linear regression model to seduce the worst possible consequences [17]. In conclusion, scholars now generally agree that an attacker should mount FDI attacks on power systems using limited information rather than the complete knowledge about the power grid topology, transmission-line admittances in reality.

In terms of cyber-physical system attack detection, power system state estimation is always available in practically. Wang *et al*. presented a novel data analytical approach to mitigate FDI attacks by employing a margin setting algorithm, which yields good results in terms of attack detection accuracy [18]. Yu *et al*. presented a false data detection mechanism based on the combined wavelet transform and deep neural networks, which can detect operating condition deviations [19]. A deep learning-based intelligent mechanism was presented by He *et al*. to detect the behavior of FDI using the historical measurement data [20]. Yang *et al.* presented a novel data fusion algorithm to combat FDI and electronic countermeasure jamming attacks in networked radar systems [21]. Zhang *et al*. presented a data integrity attack detection method based on a grey relational analysis method, which evaluated the correlation between measurements and control variables [22]. Li *et al*. presented a proactive false data detection method, which can harness the distributed flexible alternating current transmission system devices, to detect the high-profile FDI attacks [23]. Because traditional weighted least square state estimation methods are invalid for FDI attacks on power systems, Gu *et al*. measured the distance between two probability distributions using Kullback-Leibler distance, whose deviation can help find the FDI attacks [24]. Manandhar *et al*. adopted the Kalman filter to estimate the variable range, which can help detect denial-of-service, random attack, and FDI attacks [25]. In conclusion, scholars now generally agree that optimal data attack can bypass the bad data detection (BDD), and new methods should be developed to defend against cyber attacks based on the variation deviations of variable interval or probability characteristics.

Because the defects of information communication system cannot be avoided, integrity attacks can be launched in different ways from many different device entrances. Data integrity attacks have the characteristics of low cost, long time and strong concealment. Although data integrity attack cannot directly affect the primary equipment in the power system, it may seriously damage the normal operation of the secondary equipment. When the communication network of the secondary system is maliciously attacked, it will do harm to the primary power system. The purposeful data integrity attack is enough to cause serious primary system oscillation and large-scale blackout. Data integrity attack is an urgent problem of a cyber physical power system.

The novel contributions of this paper can be summarized as follows. 1) We propose a novel, realistic and feasible FDI attack model. In practice, an attacker can't obtain the complete knowledge about the power grid topology, transmission-line admittances and power system operation information. The proposed attack model only needs to obtain the line parameters and measurement data in a certain area, as well as the terminal power data of the line connecting the boundary nodes in the grid. 2) The attack model considers the isolation physical-protection of the key nodes in actual power systems. We set up the measurement variables that cannot be tampered with and includes generator power output, zero injection node power.

The remainder of this paper is organized as follows. First, the traditional attack model and a new attack model are described. Second, an effective detection method is presented to solve the false data attack problems. Third, four cases are performed to verify the effectiveness of the proposed attack model and detection method.

II. ENGINEERING PRACTICE

There are some differences in communication mode and communication network defense between domestic and foreign information systems. Foreign power grid enterprises use microwave and carrier communication, and also use public network link to set up private network virtual private network for communication. Domestic power grid enterprises attach great importance to the security of power grid information system, and divide several security levels to ensure communication security. The power grid dispatching automation system is deployed in safety zone I, which uses optical fiber communication dispatching data private network for communication, and isolates with other safety zones through physical isolation devices, thus effectively ensuring the safety of the system. Data processing and calculation services of power grid metering automation system are deployed in safety zone III. The gateway data of power plants and substations are communicated by special dispatching data networks, and the measurement data of public transformer, special transformer and low-voltage side are communicated by general packet

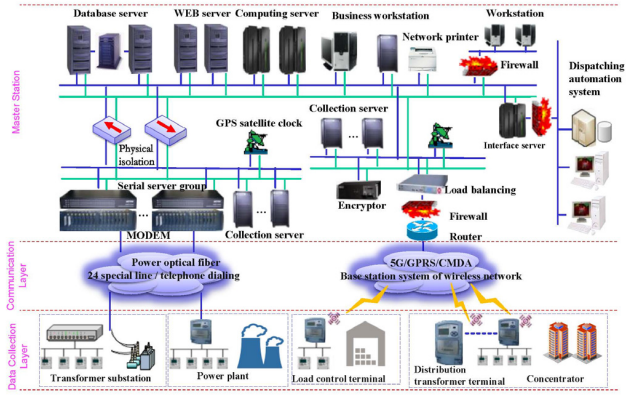


FIGURE 1. Communication architecture of power grid dispatching automation system and metering system.

radio service or mobile public network. The communication architecture of power grid dispatching automation system and metering system is shown in Fig.1.

The effective methods to prevent the cyberattack of power grid information physical system are: physical security, communication security and information security. In the aspect of physical security, it can improve the redundancy of the system by increasing the minimum number of meters in the right place, thus enhancing the immunity of the system to cyberattacks. In this case, the attacker needs to tamper with more measurement tables and increase the attack amplitude. At this time, the cost of cyberattacks in the physical system of power grid information will be increased a lot, and the probability of attack detection will be greatly increased. It is an important means to defend against cyberattacks by protecting vulnerable nodes of power communication networks. From the perspective of the attacker, local false data attack is more practical than data integrity attacks.

III. ATTACK MODEL

The state estimation of power system is the state estimation of real-time power flow. Considering measurement errors, the reliable state variables can be estimated using state estimation theories. It is realized by using the redundancy of the real-time measurement systems. State estimation can improve the accuracy of data, and eliminate the error information caused by random interference. State estimation is an important part of the power system energy management system, and the first threshold of cyberattack. Therefore, the attack model will consider the consistent state estimation.

A. TRADITIONAL ATTACK MODEL

Most of the existing attack models assumes that the attacker has known all the information of power system states, and attackers can determine the best attack vector. Data integrity attacks can disrupt the normal operation of the power grid and bypass the bad data detection mechanism. To bypass the detection mechanism of bad data, the attack vector should meet the following equation:

$$\min \left\| z - \boldsymbol{h}\left(\boldsymbol{x}^{\boldsymbol{a}}\right) \right\|_1 \tag{1}$$

subject to

$$P_i^a = \sum V_i^a V_j^a \left(G_{ij}\cos\theta_{ij}^a + B_{ij}\sin\theta_{ij}^a\right) \tag{2}$$

$$Q_i^a = \sum V_i^a V_j^a \left(G_{ij}\sin\theta_{ij}^a - B_{ij}\cos\theta_{ij}^a\right) \tag{3}$$

$$P_{ij}^a = \left(V_i^a\right)^2 g_{ij} - V_i^a V_j^a \left(g_{ij}\cos\theta_{ij}^a + b_{ij}\sin\theta_{ij}^a\right) \tag{4}$$

$$Q_{ij}^a = -\left(V_i^a\right)^2 \left(b_{ij}+y_c\right) - V_i^a V_j^a \left(g_{ij}\sin\theta_{ij}^a - b_{ij}\cos\theta_{ij}^a\right) \tag{5}$$

$$V_i^{\min} \le V_i^a \le V_i^{\max}, \quad i,j \in \Omega_A \tag{6}$$

$$\left|P_L^a - P_L^*\right| \le 0.5P_L^* \tag{7}$$

$$\left|Q_L^a - Q_L^*\right| \le 0.5Q_L^* \tag{8}$$

$$\sum P_L^a = \sum P_L^*, \quad \sum Q_L^a = \sum Q_L^*, L \in \Omega_{load} \tag{9}$$

$$V_G^a = V_G^*, \quad P_G^a = P_G^*, \ G \in \Omega_{gen} \tag{10}$$

$$P_n^a = 0, \quad Q_n^a = 0, \ n \in \Omega_0 \tag{11}$$

$$\sqrt{\left(P_{ijk}^a\right)^2 + \left(Q_{ijk}^a\right)^2} \ge S_k^{\max} k \in \Omega_{\mathrm{L}} \tag{12}$$

where $\boldsymbol{z}$ is the measured vector, x^a is the state vector under the attack, $\boldsymbol{h}(\boldsymbol{x}^{\mathbf{a}})$ is the estimated vector, P_i^a is the active power injection at the i^{th} node under the attack, Q_i^a is the reactive power injection at the i^{th} node under the attack, V_i^a is voltage amplitude at the i^{th} node under the attack, θ_{ij} is the phase angle difference between the i^{th} node and the j^{th} node under the attack, G_{ij} and B_{ij} are the real and imaginary parts of the elements in the row and column of the node admittance matrix, g_{ij} is the conductance of the i^{th} node to the j^{th} node, y_c is the ground susceptance between the i^{th} node and the j^{th} node, $\Delta P_{ij}^{\mathrm{a}}$ is the active loss between the i^{th} node and the j^{th} node under the attack, $\Delta Q_{ij}^{\mathrm{a}}$ is the reactive loss between the i^{th} node and the j^{th} node under the attack, P_i^* is the real active power injection at the i^{th} node, Q_i^* is the real reactive power injection at the i^{th} node, $S_k^{\max}$ represents the apparent power limits for the k^{th} branch, L represents the load number, n represents zero-injection node, a represents the false data, $*$ represents the real data, Ω_{L} is the set of lines, Ω_{load} is the set of load, Ω_{gen} is the set of generators, Ω_0 is the set of zero-injection buses. If the attacker has known all the information of the exact network topology, the attack vector can be established.

B. NOVEL ATTACK MODEL

A cyber defender can ensure that parts of the state variables cannot be tampered by enhancing patrol inspection or deploying redundant phasor measurement units. Load redistribution attack stands that the attacker can only attack the injected power and branch power flow, but not the the power station and zero injected node. The attack mode differences of this paper and [26] can be summarized as follows. 1) The traditional attack model assumes that the complete information can be obtained, but this is not realistic. Therefore, the proposed attack model is based on the local information. 2) The

traditional attack model assumed that the sum of power loads remains fixed, and the load redistribution is unchanged. The proposed attack model considers the sum of power loads and power losses remains fixed, which makes the attack more secretive. 3) To ensure that the attack can bypass the traditional residual test, voltage amplitudes and phase angles of the boundary nodes remain fixed in the proposed attack model.

$$\min \left\| \boldsymbol{z}^{\omega_A} - \boldsymbol{h}^{\omega_A}\left(\boldsymbol{x}^{\boldsymbol{a}}\right) \right\|_1 \tag{13}$$

subject to (2)-(6) and

$$\sum P_i^a + \sum \Delta P_{ij}^a = \sum P_i^* + \sum \Delta P_{ij}^* \tag{14}$$

$$\sum Q_i^a + \sum \Delta Q_{ij}^a = \sum Q_i^* + \sum \Delta Q_{ij}^*, \quad i,j \in \omega_A \tag{15}$$

$$\left|P_L^a - P_L^*\right| \le 0.5P_L^*, \quad L \in \omega_{load} \tag{16}$$

$$\left|Q_L^a - Q_L^*\right| \le 0.5Q_L^*, \quad L \in \omega_{load} \tag{17}$$

$$V_G^a = V_G^*, \quad G \in \omega_{gen} \tag{18}$$

$$P_G^a = P_G^*, \quad G \in \omega_{gen} \tag{19}$$

$$P_n^a = 0, Q_n^a = 0, \quad n \in \omega_0 \tag{20}$$

$$\sqrt{\left(P_{ijk}^a\right)^2 + \left(Q_{ijk}^a\right)^2} \ge S_k^{\max}, \quad k \in \omega_A \tag{21}$$

$$x_d^a = x_d^* \tag{22}$$

where ω_A is the set of the attacked nodes, ω_{load} is the set of power loads in the attack region, ω_{gen} is the set of generators in the attack region, ω_0 is the set of zero-injection nodes in the attack region, d represents the boundary node set, x_d is the initialize state array of boundary buses, ΔP_{ij}^* is the real active power between the i^{th} node and the j^{th} node, and ΔQ_{ij}^* is the real reactive power between the i^{th} node and the j^{th} node.

IV. DEFENSE MODEL

Compared with the state estimation method, the interval analysis method has lower calculation cost. Interval analysis method is a possibility method to describe the uncertainty rule of power system operation. A complete process has been established, as shown in Fig.2. The daily load curve is predicted using the data correlation rules, and the future load interval can be obtained. One can calculate the state variable intervals of the next period according to the load intervals of the next period. The attack should be detected by judging whether the state variables of power flow calculation are within the above ranges.

V. CASE STUDY AND DISCUSSIONS

We use a step-by-step validation method to demonstrate our example. The IEEE 57-bus test case is presented as the study object, as shown in Fig.3. Cyberattack and defense behaviors are simulated using MATLAB. YALMIP-master and IPOPT are used as mathematical model solvers. The machine performance will affect the simulation time. The simulations in this paper were performed at a Dell notebook, whose processor is an Intel(R) Core (TM) i7-9750HQ CPU @ 2.60 GHz, with 8 GB of available memory.

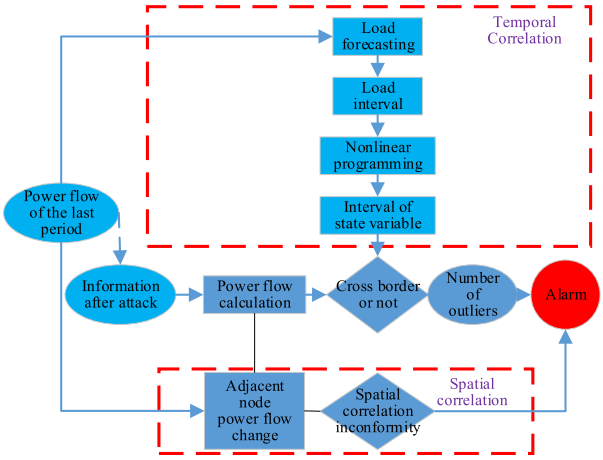


FIGURE 2. Cyberattack defense model structure.

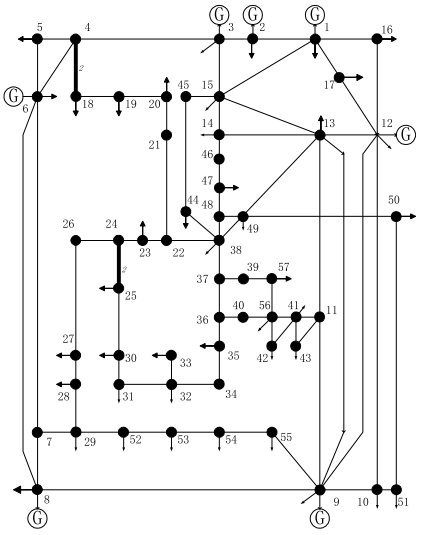


FIGURE 3. Network topology of IEEE 57-bus test case.

The attacker's goal is to overload transmission lines 39-57 and 56-57. The attack region contains PQ nodes 11, 35, 36, 37, 39, 40, 41, 42, 43, 56, 57. It is assumed that the attacker can obtain the following measurement information in the above region: voltage amplitude, node injection power, branch power. It is assumed that the attacker can obtain the following measurement information in the regional boundaries: the branch power into the above region. The attacker can tamper the following measurements: voltage amplitude, node injection power and branch power in the region. The attacker can't tamper the following measurements: voltage amplitudes of boundary nodes 11, 35, 37 and zero injection node injection power. The detection error setting parameters of interval estimation are as follows. The FDI attack model in [26] are presented to test the performance of the proposed method. The simulation differences of this paper and [26] can be summarized as follows. 1) This paper considers both the power losses and power loads, but [26] only consider the power loads. 2) This paper considers the measurement error constraints of boundary node voltage amplitudes, but

TABLE 1. Simulation conditions.

Case	Data	Loss	Error of voltage amplitude	Error of voltage phase	Average residual
1	local	with	0.0005 p.u.	0.18°	0.00066
2	local	without	0.0005 p.u.	0.18°	0.00064
3	integrity	with	0.0005 p.u.	0.18°	0.00914
4	integrity	without	0.0005 p.u.	0.18°	0.00374

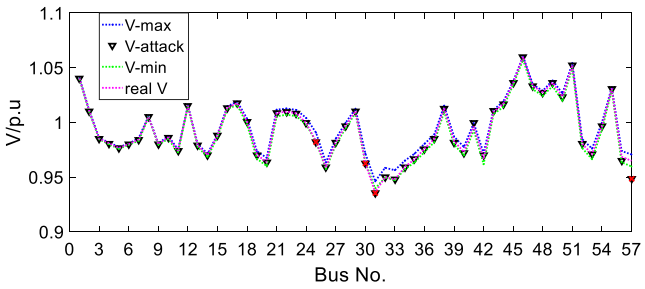


FIGURE 4. Case 1 amplitude results of cyberattack and defense.

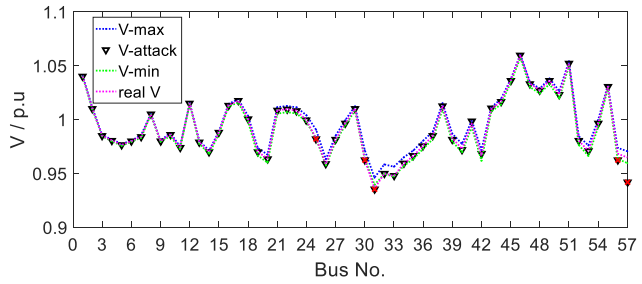


FIGURE 5. Case 2 amplitude results of cyberattack and defense.

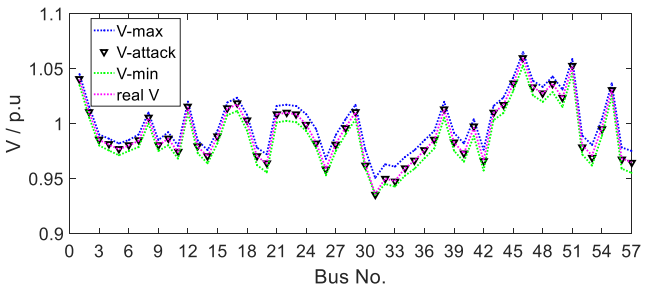


FIGURE 6. Case 3 amplitude results of cyberattack and defense.

the true values of the amplitudes and phase angles of the boundary node voltages are adopted in [26]. In this regard, the attack model in this paper is more in line with the actual project. Four cases are designed to prove the correctness of the proposed method, and the simulation conditions are shown in table 1.

We not only compare the impacts of power losses on cyberattack and detection, but also compare the impacts of global and local false data injection on cyberattack and detection, as show in Figs. 4, 5, 6, 7 and 8.

With respect to local FDI considering power losses, there are four detected nodes, whose voltage amplitudes are out

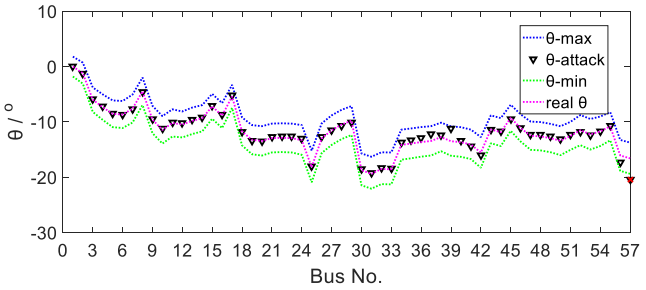


FIGURE 7. Case 3 angle results of cyberattack and defense.

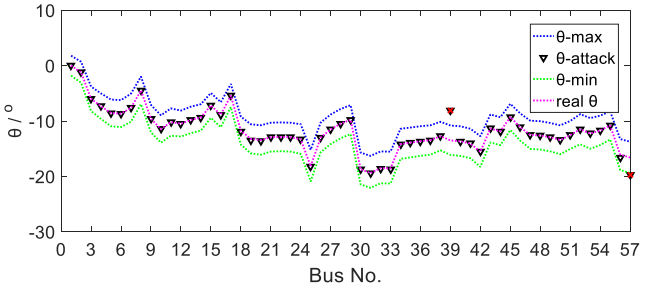


FIGURE 8. Case 4 angle results of cyberattack and defense.

of limits. With respect to local FDI without considering power losses, there are five detected nodes, whose voltage amplitudes are out of limits. The local FDI model with power loss is more secret than that without power losses. The reason is that interval estimation takes power losses into account, and it is easier to expose without power losses.

The attack of data integrity can obtain more information than FDI using local data, so the attack is more secretive than FDI using local data. When the attack of data integrity considers power losses, the traditional interval estimation can't detect the attack any more. The above simulation results just show that it is very important to realize physical protection for key nodes.

The detection of phase angle becomes a new method besides the detection of amplitude. From the simulation results, it can be seen that one abnormal point is detected for the FDI model considering power losses, and there are two points are detected for the FDI model without considering power losses. The importance of power losses in constructing attack model is illustrated and should address more concern. The essence of cyberattack is to destroy the power grid operation on the basis of satisfying the rules of data detection. The essence of cyberattack defense is to discover cyberattack by using more operation rules of power systems.

VI. CONCLUSION

The attack of cyber physical power system is a difficult problem that must be faced on the road of power grid informatization. There are few researches on local attack. Most of the works focus on the data integrity attack, which is inconsistent with the engineering practice. However, a local false data attack is the source of security risk. In this paper, local false data attack modeling and simulation are carried out. This

paper first analyzes the attack of load redistribution in detail, and demonstrates the feasibility in practice. The attack model includes power flow constraints, attack constraints of PV and PQ nodes, power injection constraints of contact nodes, and total power injection constraints. Then we test the detection effect of local false data attacks on state interval estimation detection, and the simulations verify the effectiveness of the proposed method. The local attack and detection methods of cyber physical power system need to be further studied and explored, and the security defense theory is very important for the safe operation of power grid.

REFERENCES

[1] D. Xu, Q. Wu, B. Zhou, C. Li, L. Bai, and S. Huang, "Distributed multi-energy operation of coupled electricity, heating and natural gas networks," *IEEE Trans. Sustain. Energy*, early access, Dec. 2020, doi: 10.1109/TSTE.2019.2961432.

[2] D. Xu, B. Zhou, Q. Wu, C. Y. Chung, C. Li, S. Huang, and S. Chen, "Integrated modelling and enhanced utilization of power-to-ammonia for high renewable penetrated multi-energy systems," *IEEE Trans. Power Syst.*, early access, Apr. 2020, doi: 10.1109/TPWRS.2020.2989533.

[3] V. V. S. N. Murty and A. Kumar, "Multi-objective energy management in microgrids with hybrid energy sources and battery energy storage systems," *Protection Control Mod. Power Syst.*, vol. 5, no. 1, pp. 1–20, Dec. 2020.

[4] H.-Z. Wang, G.-Q. Li, G.-B. Wang, J.-C. Peng, H. Jiang, and Y.-T. Liu, "Deep learning based ensemble approach for probabilistic wind power forecasting," *Appl. Energy*, vol. 188, pp. 56–70, Feb. 2017.

[5] H. Z. Wang, G. B. Wang, G. Q. Li, J. C. Peng, and Y. T. Liu, "Deep belief network based deterministic and probabilistic wind speed forecasting approach," *Appl. Energy*, vol. 182, pp. 80–93, Nov. 2016.

[6] H. Wang, Z. Lei, X. Zhang, B. Zhou, and J. Peng, "A review of deep learning for renewable energy forecasting," *Energy Convers. Manage.*, vol. 198, Oct. 2019, Art. no. 111799.

[7] H. Wang, Y. Liu, B. Zhou, C. Li, G. Cao, N. Voropai, and E. Barakhtenko, "Taxonomy research of artificial intelligence for deterministic solar power forecasting," *Energy Convers. Manage.*, vol. 214, Jun. 2020, Art. no. 112909.

[8] G. Liang, S. R. Weller, J. Zhao, F. Luo, and Z. Y. Dong, "The 2015 Ukraine blackout: Implications for false data injection attacks," *IEEE Trans. Power Syst.*, vol. 32, no. 4, pp. 3317–3318, Jul. 2017.

[9] L. Che, X. Liu, Z. Li, and Y. Wen, "False data injection attacks induced sequential outages in power systems," *IEEE Trans. Power Syst.*, vol. 34, no. 2, pp. 1513–1523, Mar. 2019.

[10] J. Zhao, G. Zhang, Z. Y. Dong, and K. P. Wong, "Forecasting-aided imperfect false data injection attacks against power system nonlinear state estimation," *IEEE Trans. Smart Grid*, vol. 7, no. 1, pp. 6–8, Jan. 2016.

[11] Y. Guan and X. Ge, "Distributed attack detection and secure estimation of networked cyber-physical systems against false data injection attacks and jamming attacks," *IEEE Trans. Signal Inf. Process. Netw.*, vol. 4, no. 1, pp. 48–59, Mar. 2018.

[12] X. Liu, Z. Bao, D. Lu, and Z. Li, "Modeling of local false data injection attacks with reduced network information," *IEEE Trans. Smart Grid*, vol. 6, no. 4, pp. 1686–1696, Jul. 2015.

[13] X. Liu, Y. Song, and Z. Li, "Dummy data attacks in power systems," *IEEE Trans. Smart Grid*, vol. 11, no. 2, pp. 1792–1795, Mar. 2020.

[14] X. Liu, Z. Li, X. Liu, and Z. Li, "Masking transmission line outages via false data injection attacks," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 7, pp. 1592–1602, Jul. 2016.

[15] L. Yu, X.-M. Sun, and T. Sui, "False-data injection attack in electricity generation system subject to actuator saturation: Analysis and design," *IEEE Trans. Syst., Man, Cybern. Syst.*, vol. 49, no. 8, pp. 1712–1719, Aug. 2019.

[16] Z.-H. Yu and W.-L. Chin, "Blind false data injection attack using PCA approximation method in smart grid," *IEEE Trans. Smart Grid*, vol. 6, no. 3, pp. 1219–1226, May 2015.

[17] J. Zhang, Z. Chu, L. Sankar, and O. Kosut, "Can attackers with limited information exploit historical data to mount successful false data injection attacks on power systems?" *IEEE Trans. Power Syst.*, vol. 33, no. 5, pp. 4775–4786, Sep. 2018.

[18] Y. Wang, M. M. Amin, J. Fu, and H. B. Moussa, "A novel data analytical approach for false data injection cyber-physical attack mitigation in smart grids," *IEEE Access*, vol. 5, pp. 26022–26033, 2017.

[19] J. J. Q. Yu, Y. Hou, and V. O. K. Li, "Online false data injection attack detection with wavelet transform and deep neural networks," *IEEE Trans. Ind. Informat.*, vol. 14, no. 7, pp. 3271–3280, Jul. 2018.

[20] Y. He, G. J. Mendis, and J. Wei, "Real-time detection of false data injection attacks in smart grid: A deep learning-based intelligent mechanism," *IEEE Trans. Smart Grid*, vol. 8, no. 5, pp. 2505–2516, Sep. 2017.

[21] C. Yang, L. Feng, H. Zhang, S. He, and Z. Shi, "A novel data fusion algorithm to combat false data injection attacks in networked radar systems," *IEEE Trans. Signal Inf. Process. over Netw.*, vol. 4, no. 1, pp. 125–136, Mar. 2018.

[22] Z. Zhang, Y. Wang, and L. Xie, "A novel data integrity attack detection algorithm based on improved grey relational analysis," *IEEE Access*, vol. 6, pp. 73423–73433, 2018.

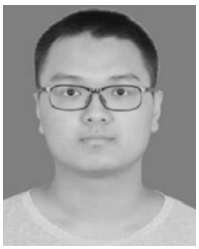
[23] B. Li, G. Xiao, R. Lu, R. Deng, and H. Bao, "On feasibility and limitations of detecting false data injection attacks on power grid state estimation using D-FACTS devices," *IEEE Trans. Ind. Informat.*, vol. 16, no. 2, pp. 854–864, Feb. 2020.

[24] G. Chaojun, P. Jirutitijaroen, and M. Motani, "Detecting false data injection attacks in AC state estimation," *IEEE Trans. Smart Grid*, vol. 6, no. 5, pp. 2476–2483, Sep. 2015, doi: 10.1109/TSG.2015.2388545.

[25] 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 Trans. Control Netw. Syst.*, vol. 1, no. 4, pp. 370–379, Dec. 2014.

[26] H. Wang, J. Ruan, G. Wang, B. Zhou, Y. Liu, X. Fu, and J. Peng, "Deep learning-based interval state estimation of AC smart grids against sparse cyber attacks," *IEEE Trans. Ind. Informat.*, vol. 14, no. 11, pp. 4766–4778, Nov. 2018.

XUEQIAN FU (Member, IEEE) received the B.S. and M.S. degrees from North China Electric Power University, in 2008 and 2011, respectively, and the Ph.D. degree from the South China University of Technology, in 2015. From 2011 to 2015, he was an Electrical Engineer with Guangzhou Power Supply Company Ltd. From 2015 to 2017, he was a Postdoctoral Researcher with Tsinghua University. He is currently an Associate Professor with China Agricultural University. His current research interests include energy management systems, automatic voltage control, energy Internet, and energy system integration.



GENGRUI CHEN was born in 1998. He is currently pursuing the B.S. degree with China Agricultural University, Beijing, China. His current research interests include false data injection attack detection model of the cyber-physical power systems, wireless communications systems, and cooperative networks.

DECHANG YANG (Member, IEEE) was born in 1983. He received the M.S. degree in electric engineering from China Agricultural University, Beijing, China, in 2008, and the Ph.D. degree in power system from TU Dortmund, in 2012. He is currently an Associate Professor with China Agricultural University. His research interests include active distribution network operation and control, integrated multi-energy system collaborative planning, economic dispatching, and optimal management.