Letter

Detecting the One-Shot Dummy Attack on the Power Industrial Control Processes With an Unsupervised Data-Driven Approach

Zhenyong Zhang, Yan Qin, Jingpei Wang, Hui Li, and Ruilong Deng, *Senior Member, IEEE*

Dear Editor,

Dummy attack (DA), a deep stealthy but impactful data integrity attack on power industrial control processes, is recently recognized as hiding the corrupted measurements in normal measurements. In this letter, targeting a more practical case, we aim to detect the one-shot DA, with the purpose of revealing the DA once it is launched. Specifically, we first formulate an optimization problem to generate one-shot DAs. Then, an unsupervised data-driven approach based on a modified local outlier factor (MLOF) is proposed to detect them. To improve the detection performance, the measurements are preprocessed with the gamma transformation and the power patterns are extracted from historical data and integrated into the MLOF algorithm. Finally, extensive experiments are conducted to evaluate the performance of the proposed approach with real-world load data.

The industrial control processes of power systems are enabled by integrating advanced information and communication technology (ICT) into the physical infrastructures. However, the vulnerabilities exposed in ICT devices make power systems attractive to cyberattacks [1]. The false data injection attack (FDIA) [2] is one of the cyberattacks that aims to stealthily inflict the power system's control processes (e.g., state estimation, load frequency control, etc.). However, the bad data detection-bypassed FDIA is no longer stealthy if the detector evaluates the distances between the corrupted measurements and the near historical measurements. Thus, a deep stealthy attack, the DA is recently proposed to hide the corrupted measurements in historical measurements [3]. The DA is a variant of FDIA by enhancing the stealthiness against detectors using clustering methods.

As an emerging research topic, it is still an open issue to detect DAs effectively. The revisit of existing defense against traditional FDIAs [4] is beneficial to understanding DA. Among them, the measurement/state protection [5] is the most studied approach, which prevents the power system from being attacked by securing some critical measurements. But, the shortage of this approach is that only a few measurements can be trusted and the real-time operation might be affected if the data is protected with encryption. To provide a dynamic protection capability, the moving target defense approach [6] is recently put forward to thwart FDIAs by dynamically changing the network and physical parameters of power systems. But the active perturbation of system parameters might affect the safety and stability of the voltage, grid frequency, etc. To alleviate the impact of defensive approaches, the data-driven methods are promising alternatives to detect and identify FDIAs [7] and [8]. However, there are three challenges for the data-driven approaches to detect FDIAs. First, it is impossible to completely label the adversarial data for supervised approaches since the state space is uncountable. The same measurement might be contradictorily labeled since the modified measurements by FDIA sometimes are legal (i.e., satisfying the physics laws). Second, the assumption regarding specific distribution for a tested dataset, requested by some approaches, may not hold in practice, as different power systems are likely to yield different data distributions. Third, some complicated machine/deep learning methods have plenty of parameters that should be adjusted according to different power systems.

In this letter, our goal is to detect DAs with a data-driven approach to fill the gap. We pay a special emphasis on the one-shot DA. The one-shot setting is more reasonable because: from the attacker's perspective, he/she aims to destroy the system's control processes by using only one hit; while from the defender's perspective, it is the best to detect the attack at once after its execution. However, there are challenges to detecting the one-shot DA. First, prior knowledge about the one-shot attack is lacking, as it is rare during the system's operation. Second, since the DA is executed in a one-shot manner, it is almost impossible to monitor the long-term change of measurements since the system might have already crashed down. To address these issues, in this letter, we propose an unsupervised data-driven approach based on the local outlier factor (LOF) to detect one-shot DAs. According to our knowledge, it is the first work to propose an efficient algorithm to detect one-shot DAs. The main contributions are summarized as follows: 1) We present a formulation of the constrained one-shot DA; 2) The interval information and γ transformation method are adopted to enlarge the deviation of abnormal measurements; 3) A modified LOF algorithm is proposed to enable the efficient detection of one-shot DAs; 4) The performance of the proposed approach in terms of detecting one-shot DAs is evaluated with the real-world load data.

Problem formulation: Here, we consider a power transmission network that has a set $\mathcal{N}$ of buses and a set $\mathcal{L}$ of transmission lines. The DA is constructed to bypass the bad data detector and minimize the distance between the malicious and normal measurements. To compute a malicious measurement $\boldsymbol{z}'$ for DA, the following problem should be solved, which is:

$$\min_{\boldsymbol{z}'} \ \|\boldsymbol{z}'-\boldsymbol{z}_1\|+\|\boldsymbol{z}'-\boldsymbol{z}_2\|+\cdots+\|\boldsymbol{z}'-\boldsymbol{z}_r\| \tag{1}$$

$$\text{s.t.} \quad \mathbf{1}_{|N|}^T \Delta \boldsymbol{p}_d = 0 \tag{1a}$$

$$-\boldsymbol{\sigma}^T \boldsymbol{p}_d \le \Delta \boldsymbol{p}_d \le \boldsymbol{\sigma}^T \boldsymbol{p}_d, \ \ \sigma_i \in [0,1] \tag{1b}$$

$$\Delta f^l / f^l_{\max} > \delta^l, \quad \exists l \in \mathcal{L} \tag{1c}$$

$$\Delta \boldsymbol{f} = -\phi(\Delta \boldsymbol{p}_d) \tag{1d}$$

$$\boldsymbol{z}' = \boldsymbol{z} + [\Delta \boldsymbol{p}_d; \Delta \boldsymbol{f}] \tag{1e}$$

$$|\mathcal{N}_d| \le N_d^a < N_d \tag{1f}$$

where $\boldsymbol{z}_1, \boldsymbol{z}_2, \ldots, \boldsymbol{z}_r$ are r historical measurements, $\|\cdot\|$ denotes the norm operation (ℓ_2 norm is used here), $\boldsymbol{z}_i$ is the measurement collected at time instant i, $\mathbf{1}_{|N|}$ is an N-dimension vector with all elements equal to 1, $\Delta \boldsymbol{p}_d$ is a vector of maliciously injected loads of original loads $\boldsymbol{p}_d$, σ_i is the ith element of vector $\boldsymbol{\sigma}$, Δf^l is the injected error into the power flow measurement of branch l, $f^l_{\max}$ is the maximum tolerable power flow of branch l, δ^l is the overloading threshold of branch l, $\Delta \boldsymbol{f}$ is a vector of maliciously injected errors into power flows, $\phi(\cdot)$ represents the nonlinear relationship between power loads and power flows with the alternating current (AC) model, $\mathcal{N}_d$ is a set of loads that are corrupted by DA, N_d^a is the number of loads that can be corrupted, and N_d is the total number of

Corresponding author: Jingpei Wang.

Citation: Z. Y. Zhang, Y. Qin, J. P. Wang, H. Li, and R. L. Deng, "Detecting the one-shot dummy attack on the power industrial control processes with an unsupervised data-driven approach," *IEEE/CAA J. Autom. Sinica*, vol. 10, no. 2, pp. 550–553, Feb. 2023.

Z. Y. Zhang and H. Li are with the State Key Laboratory of Public Big Data and the College of Computer Science and Technology, Guizhou University, Guiyang 550025, China (e-mail: zyzhangnew@gmail.com; cse.HuiLi@gzu.edu.cn).

Y. Qin is with the School of Chemical and Biomedical Engineering, Nanyang Technological University, Singapore 639798, Singapore (e-mail: yan.qin@ntu.edu.cn).

J. P. Wang and R. L. Deng are with the State Key Laboratory of Industrial Control Technology and the College of Control Science and Engineering, Zhejiang University, Hangzhou 310027, China (e-mail: wjpbupt@163.com; dengruilong@zju.edu.cn).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/JAS.2023.123243

loads. The first constraint (1a) guarantees the stealthiness of DA. The second constraint (1b) limits the magnitudes of modified loads. The third constraint (1c) reflects the impact of DA on the power system. The fourth constraint (1d) is the stealthy constraint caused by physics laws. The fifth constraint (1e) gives the malicious measurement after DA. The last constraint (1f) limits the capability of the attacker to modify power loads. Due to the nonlinear and nonconvex properties caused by constraint (1d), we linearize it by using the Jacobian matrix: $\Delta \boldsymbol{f} = -\left[\frac{\partial \phi}{\partial \boldsymbol{p}_d}\right]\Delta \boldsymbol{p}_d$, where $\left[\frac{\partial \phi}{\partial \boldsymbol{p}_d}\right]$ denotes the Jacobian matrix by deriving $\phi(\Delta \boldsymbol{p}_d)$ with respect to $\boldsymbol{p}_d$. Thus, if the targeted loads are determined, the above problem becomes a convex optimization problem that is easy to solve.

The DA is proposed because traditional FDIAs can be easily detected using the clustering-based and principal component analysis (PCA)-based approaches [9], [10]. The malicious measurements of the DA are deeply hidden in normal measurements because the distances between them and normal ones are minimized. Besides, the DA can be executed in a one-shot manner and the power system is knocked down in a short time. Thus, the defender needs to detect the attack at the beginning when it starts. Therefore, in this letter, our goal is to detect one-shot DAs in an accurate and efficient way.

Main results: In the following, we propose an unsupervised data-driven approach to detect one-shot DAs based on the LOF, which has been widely used to detect outliers [11]. In this letter, the LOF is modified to make it compatible with the detection of one-shot DAs. Since a restricted neighborhood of each measurement point is taken into account, the proposed approach does not require any explicit or implicit notion of clusters.

Data preprocessing: First of all, the input measurements are preprocessed. The interval information is obtained by computing the difference between the current and previous measurements, which is $\Delta_i^j = |z_i^j - z_{i-1}^j|$, where z_i^j is the jth sensor's measurement at time i and $|\cdot|$ calculates the absolute value. We adopt the γ transformation to reshape the collected measurements to make them suitable for our context. For each Δ_i^j, the transformation is calculated as $d_i^j = s_i^j * (\Delta_i^j)^\gamma$, where s_i^j is the sign of $z_i^j - z_{i-1}^j$ and $\gamma > 0$ is the power factor. We introduce the sign factor s_i^j to capture the increasing and decreasing trends of power data. The transformation can map the small-range variation to a larger range, which can highlight the abnormal measurement (i.e., outlier) caused by the attack.

Local outlier detection: The pipelines of LOF are introduced as follows. First, the k-nearest-neighbors $R_k(\boldsymbol{d}_i)$ for each $\boldsymbol{d}_i = [d_i^1, d_i^2, \ldots]^T$ (formed by the preprocessed measurements) are searched based on a specified distance (e.g., the euclidean and cosine distance). Considering the high-dimension measurements, the cosine distance is adopted here, denoted by dist(·). The cosine distance has been widely used as a way to counteract Euclidean distance's problem with high dimensionality. Second, for each $\boldsymbol{d}_i$, the local reachability density (LRD) is computed according to the set of k neighbors $R_k(\boldsymbol{d}_i)$, which is $\mathrm{LRD}_k(\boldsymbol{d}_i) = 1/\left(\frac{\sum_{\tilde{\boldsymbol{d}} \in R_k(\boldsymbol{d}_i)} \mathrm{RD}_k(\boldsymbol{d}_i, \tilde{\boldsymbol{d}})}{|R_k(\boldsymbol{d}_i)|}\right)$, where $\mathrm{RD}_k(\boldsymbol{d}_i, \tilde{\boldsymbol{d}}) = \max(k\mathrm{dist}(\boldsymbol{d}_i), \mathrm{dist}(\boldsymbol{d}_i, \tilde{\boldsymbol{d}}))$ and $|R_k(\boldsymbol{d}_i)|$ is the cardinality of $R_k(\boldsymbol{d}_i)$. The k distance $k\mathrm{dist}(\boldsymbol{d}_i)$ is defined in [11]. Third, the LOF value for each $\boldsymbol{d}_i$ is calculated based on the LRD value, which is $\mathrm{LOF}_k(\boldsymbol{d}_i) = \sum_{\tilde{\boldsymbol{d}} \in R_k(\boldsymbol{d}_i)} \frac{\mathrm{LRD}_k(\tilde{\boldsymbol{d}})}{\mathrm{LRD}_k(\boldsymbol{d}_i)} / |R_k(\boldsymbol{d}_i)|$. A relatively large LOF value is obtained with $\boldsymbol{d}_i$ if the density of all its neighbors is higher than itself, representing a possible outlier (i.e., malicious measurement) is found.

However, there are challenges to directly applying the LOF algorithm to detect one-shot DAs. First, the collected measurements of power systems are in a form of the high-velocity data stream. Unlike the static dataset, the stream data might have different patterns during different periods. It is possible to mistake the adversarial data as normal although it is illegal in the current period. Second, the LOF algorithm is usually computational intensive since it works by analyzing the data in a global view. Its computational complexity increases with the size of the tested dataset. However, it is not acceptable to detect the one-shot DA for a long time since the power system changes very fast. Therefore, in this letter, we propose a MLOF algorithm to improve the efficiency of detecting one-shot DAs by utilizing the common power patterns extracted from historical measurements.

For example, the power patterns can be estimated according to load profiles and updated in an adaptive way. Here the power patterns are extracted from the real-world load data of New York State[1]. The load profiles on the date 20-01-2021 are plotted in Fig. 1. We can see that there are three patterns (dropping, climbing, steady) for the load change in a day. Although the amount of loads is changed with time, the load-change patterns remain the same for a certain period. Thus, the load-change patterns can be utilized to reduce the computational complexity of the LOF algorithm.

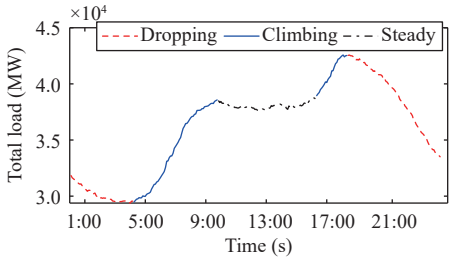

Fig. 1. Load-change patterns of the real-world load profiles.

By integrating the power patterns, the proposed MLOF works as follows. First, the normal measurements are divided into q data chunks ($C_1, C_2, \ldots, C_q$) according to q power patterns ($p_1, p_2, \ldots, p_q$) (e.g., dropping, climbing, and steady). Then, for each incoming measurement, the time period t ($t = 1, 2, \ldots, q$) that its belonging is first determined, then the k-nearest-neighbor search is performed only within the data chunk C_t. Based on the estimated k-nearest-neighbor, the LOF value is computed for all measurements in the data chunk C_t. If the incoming measurement has the largest LOF value, then it is recognized as a malicious measurement of the one-shot DA. The pseudo-code of MLOF can be found in Algorithm 1. Note that the q data chunks should be updated after a period of time since the power patterns might change due to the construction of new power facilities, the penetration of new energy resources, and etc.

The computational complexity of LOF can be formulated as $C_{\mathrm{LOF}} = O(f(n))$, where n is the size of the tested dataset, $f(n)$ is a monotonically increasing function, and $O(\cdot)$ calculates the computational complexity. As for MLOF, the computational complexity is $C_{\mathrm{MLOF}} = O(N)$, where N is a constant number, i.e., the size of the data chunk, which is independent of the increasing number of collected measurements.

Algorithm 1 The Modified Local Outlier Factor (MLOF) Algorithm

Input: $\{z_1, z_2, \ldots, z_n\}$: the dataset with n measurements;
z_o: the incoming measurement;
k: number of nearest neighbors;
Output: 0/1: being attacked by the one-shot DA (1) or not (0)
1 Preprocess the measurements $\{z_1, z_2, \ldots, z_n\}$ and z_o to $\{\boldsymbol{d}_1, \boldsymbol{d}_2, \ldots, \boldsymbol{d}_{n-1}\}$ and $\boldsymbol{d}_o$ based on the γ-transformation;
2 Group $\{\boldsymbol{d}_1, \boldsymbol{d}_2, \ldots, \boldsymbol{d}_{n-1}\}$ in q data chunks $C_1, \ldots, C_q$ based on the power patterns $p_1, \ldots, p_q$;
3 **if** $\boldsymbol{d}_o \in p_i$ **then**
4 $\tilde{C}_i = C_i \cup \boldsymbol{d}_o$;
5 **foreach** $\boldsymbol{d}_i \in \tilde{C}_i$ **do**
6 $R_k(\boldsymbol{d}_i) = \mathrm{findkNN}(\boldsymbol{d}_i, \tilde{C}_i)$);
//*find the k nearest neighbors
7 Compute $\mathrm{LOF}_k(\boldsymbol{d}_i)$;
8 **end**
9 **if** $LOF_k(\boldsymbol{d}_o)$ = the maximum LOF value in $\tilde{C}_i$ **then**
10 **return** 1;
11 **else**
12 **return** 0;
13 **end**
14 **end**

[1] NYISO load data. 2021, Available: https://www.nyiso.com/load-data

Experimental results: The performance of the proposed approach in terms of detecting one-shot DAs is evaluated with the IEEE 14-bus power system. To make the tested scenario more practical, the real-world load profiles of the New York State from 01-01-2021 to 31-03-2021 are incorporated to generate the attack data. The 11 loads from 11 main regions are used to act as loads of the IEEE 14-bus power system, while the measurements are created based on the load data. The one-shot DA is constructed by using the latest r measurements to solve the problem (1). To detect the one-shot DA, the historical measurements from the beginning to time i are used for LOF, COF [12], LDOF [13], NOF, DBSCAN, and iForest. The measurements on 20-01-2021 are used to extract the power patterns for MLOF. The evaluation metric "TP" means true positive and "FP" stands for false positive. As for LOF, COF, LDOF, NOF, DBSCAN, and iForest, the historical measurements $z_1, z_2, \ldots, z_{i-1}$ are normal, but the measurement z_i is attacked by the one-shot DA. The goal of LOF, COF, LDOF, NOF, DBSCAN, and iForest is to capture the abnormal measurement z_i with $z_1, z_2, \ldots, z_i$. As for MLOF, three data chunks C_1, C_2, and C_3, according to three power patterns (i.e., dropping, climbing, and steady), are extracted based on the measurements on 20-01-2021. The malicious measurement z_i is fed into C_1, C_2, or C_3 to test whether it is a malicious measurement or not. The parameter γ is set the same for all sensor measurements.

By default, the historical measurements for LOF, COF, LDOF, NOF, DBSCAN, and iForest are collected based on the loads from 01-01-2021 to 21-02-2021, while the historical measurements for MLOF are collected based on the loads on the date 20-01-2021. The malicious measurements are generated based on the measurements on 21-01-2021. The attack parameter r is 30. The transformation parameter γ is 1.1. All malicious measurements are constructed by solving the problem (1).

First, we compare the performance of MLOF and LOF in terms of detecting one-shot DAs with different k values. The experimental results are shown in Table 1. We find that the detection rate (i.e., TP rate) of one-shot DAs decreases when the k value increases with both MLOF and LOF. But the performance with MLOF is much better than that with LOF, which indicates that the LOF will treat the abnormal measurements as normal since it uses the historical measurements collected in a long term. On the other hand, the FP rates are below 5% with MLOF and below 1% with LOF, which shows that the LOF sacrifices the TP rate to reduce the FP rate.

Table 1. The TP and FP Rates of Detecting One-Shot DAs With MLOF, LOF, COF, and LDOF ($\gamma = 1.1$)

	MLOF		LOF		COF		LDOF	
k	TP	FP	TP	FP	TP	FP	TP	FP
10	89.30%	1.37%	56.85%	0.9%	73.50%	0.90%	74.70%	0.70%
20	82.75%	3.20%	42.71%	0.60%	48.60%	0.80%	64.60%	0.50%
30	74.46%	3.66%	31.53%	0.32%	29.30%	0.70%	55.80%	0.50%
40	71.36%	4.97%	23.44%	0.30%	17.20%	0.70%	48.40%	0.60%

We also evaluate the detection performance of one-shot DAs with the variants of LOF. COF is a variant of LOF to address the issue that the outlier has a similar neighborhood density as the normal data [12], while LDOF is extended from LOF to address the low-sensitive issue caused by the scattered real-world data [13]. The results are also presented in Table 1. It seems that the variants (i.e., COF and LDOF) of LOF have better performance in terms of detecting one-shot DAs than that of LOF but worse than that of MLOF. The results indicate that the power patterns are critical for detecting one-shot DAs.

Further, we also evaluate the performance of other algorithms beyond LOF to detect one-shot DAs. NOF is a variant of the K-nearest neighbor method by alleviating the difficulty to select an appropriate K value. DBSCAN is a common data clustering algorithm to detect outliers with data noise. Isolation forest (iForest) is a famous anomaly detection method to identify outliers from normal data points by measuring the distance between the data point and the rest data points. The TP rates of detecting one-shot DAs with the evaluated algorithms are presented in Table 2. We find that the TP rates with the NOF, DBSCAN, and iForest algorithms are lower than that with the variants of the LOF algorithm. In our opinion, this is because the evaluated algorithms are developed based on the distances between the outliers and normal data points, while the LOF algorithm is derived based on density estimation.

Table 2. The TP and FP Rates of Detecting One-Shot DAs With NOF, DBSCAN, and iForest ($\gamma = 1.1$)

NOF		DBSCAN		iForest	
TP	FP	TP	FP	TP	FP
72.90%	0.00%	62.80%	1.30%	18.80%	0.20%

Second, we compare the running time of LOF and MLOF with the same platform. The algorithms are computed in a core i7 laptop, which has a 1.10 GHz CPU and 16.0 GB memory. As shown in Fig. 2, the running time of LOF increases with the number of tested measurements, but that of the MLOF remains almost the same, which is always below 100 ms. The running time of the LOF algorithm reaches nearly 30 s when the tested measurements are collected for more than a month. The fitting curve for the running time of LOF is $rt = 2.061 \times 10^{-7} n^2 - 4.346n + 1.2247$, where rt is the running time of LOF and n is the number of tested measurements. The results show that it is hard to burden the intensive computations when there are too many tested measurements with LOF. Therefore, it is more efficient to use MLOF to detect one-shot DAs.

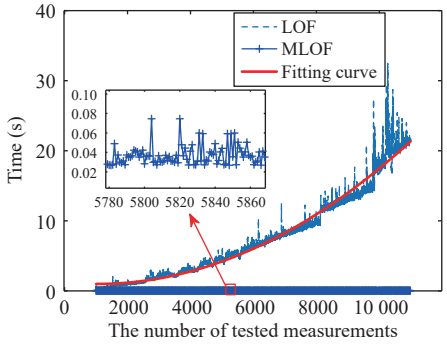

Fig. 2. The running time of LOF and MLOF algorithms.

Third, we evaluate the performance of MLOF when the input measurements are preprocessed with the γ transformation. The results are shown in Fig. 3. We find that the TP rate with the preprocessed measurements is much larger than those that are not preprocessed, while the FP rate is reversed. Therefore, the input measurements should be preprocessed with the γ transformation to improve the performance of MLOF in terms of detecting one-shot DAs. The experimental results also show that the MLOF algorithm has a good transferability to detect one-shot DAs since the performance does not degrade when the malicious measurements are constructed on the other dates (not on the date 20-01-2021).

Finally, we evaluate the performance of MLOF with different transformation parameters and the numbers of nearest neighbors. The results are shown in Fig. 4. We find that the TP rate is relatively larger when the γ value is between 0.5 and 1.1 and the k value is between 20 and 30, while the FP rate is relatively larger when γ is beyond 1.2 and the k value is beyond 35. From the results, the transformation parameter and the number of nearest neighbors of MLOF should be properly set to improve its performance of detecting one-shot DAs.

Acknowledgments: This work was supported in part by the Guizhou Provincial Science and Technology Projects (ZK[2022]

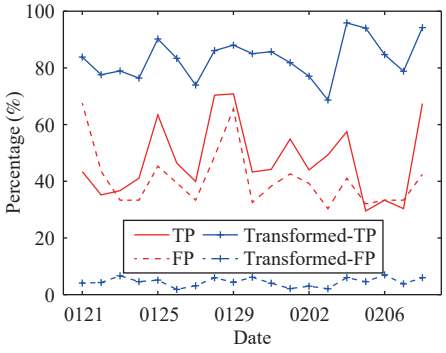

Fig. 3. The attack detection performance of MLOF with and without the γ transformation. The malicious measurements are constructed based on the load profiles on the dates 21-01-2021, 22-01-2021, …, 08-02-2021. "Transformed-TP" and "Transformed-FP" mean the TP and FP rates when the measurements are preprocessed with the γ-transformation.

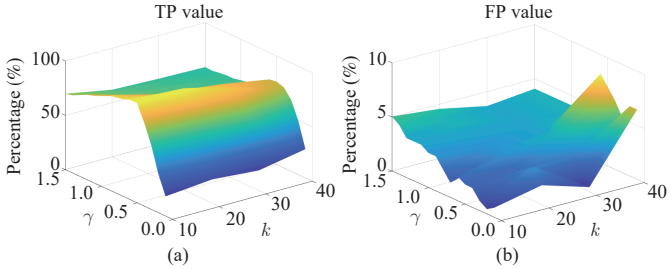

Fig. 4. The attack detection performance of MLOF with different γ and k values.

149), the Guizhou Provincial Research Project for Universities ([2022]104), the Special Foundation of Guizhou University ([2021]47), the GZU cultivation project of National Natural Science Foundation of China ([2020]80), Shanghai Engineering Research Center of Big Data Management, and the National Natural Science Foundation of China (62073285, 62061130220).

References

[1] W. Duo, M. Zhou, and A. Abusorrah, "A survey of cyber attacks on cyber physical systems: Recent advances and challenges," *IEEE/CAA J. Autom. Sinica*, vol. 9, no. 5, pp. 784–800, Apr. 2022.

[2] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Trans. Inform. Syst. Security*, vol. 14, no. 1, pp. 1–33, May 2011.

[3] 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.

[4] A. S. Musleh, G. Chen, and Z.-Y. Dong, "A survey on the detection algorithms for false data injection attacks in smart grids," *IEEE Trans. Smart Grid*, vol. 11, no. 3, pp. 2218–2234, May 2020.

[5] X. Liu, Z. Li, and Z. Li, "Optimal protection strategy against false data injection attacks in power systems," *IEEE Trans. Smart Grid*, vol. 8, no. 4, pp. 1802–1810, Jul. 2017.

[6] Z. Zhang, R. Deng，D. K. Yau, *et al.*, "Analysis of moving target defense against false data injection attacks on power grid," *IEEE Trans. Inform. Forens. Secur.*, vol. 15, no. 1, pp. 2320–2335, Feb. 2020.

[7] S. Peng, M. Sun, and Z. Zhang, "Application of machine learning in cyber security of cyber-physical power systems," *Automation Electric Power Syst.*, vol. 46, no. 9, pp. 200–215, Sept. 2022.

[8] J. Zhang, L. Pan, Q.-L. Han, C. Chen, S. Wen, and Y. Xiang, "Deep learning based attack detection for cyber-physical system cybersecurity: A survey," *IEEE/CAA J. Autom. Sinica*, vol. 9, no. 3, pp. 377–391, Mar. 2022.

[9] 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, Sept. 2015.

[10] A. S. Musleh, M. Debouza, H. M. Khalid, and A. Al-Durra, "Detection of false data injection attacks in smart grids: A real-time principle component analysis," in *Proc. 45th Annu. Conf. IEEE Ind. Electron. Soc.*, 2019, pp. 2958−2963.

[11] M. M. Breunig, H.-P. Kriegel, R. T. Ng, and J. Sander, "LOF: Identifying density-based local outliers," *ACM Sigmod Record*, vol. 29, no. 2, pp. 93–104, Jun. 2000.

[12] J. Tang, Z. Chen, A. W.Fu, and D. W. Cheung, "Enhancing effectiveness of outlier detections for low density patterns," in *Proc. Pacific-Asia Conf. Knowledge Discovery Data Mining*, 2002, pp. 535−548.

[13] K. Zhang, M. Hutter, and H. Jin, "A new local distance-based outlier detection approach for scattered real-world data," in *Proc. Pacific-Asia Conf. Knowledge Discovery Data Mining*, 2009, pp. 813−822.