Hindawi
Journal of Control Science and Engineering
Volume 2023, Article ID 9872131, 1 page
https://doi.org/10.1155/2023/9872131

Retraction

Retracted: Attack and Protection Technology of Intelligent Terminals for New Energy Internet Transmission, Transformation, and Distribution

Journal of Control Science and Engineering

Received 17 October 2023; Accepted 17 October 2023; Published 18 October 2023

This article has been retracted by Hindawi following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of one or more of the following indicators of systematic manipulation of the publication process:

(1) Discrepancies in scope
(2) Discrepancies in the description of the research reported
(3) Discrepancies between the availability of data and the research described
(4) Inappropriate citations
(5) Incoherent, meaningless and/or irrelevant content included in the article
(6) Peer-review manipulation

The presence of these indicators undermines our confidence in the integrity of the article's content and we cannot, therefore, vouch for its reliability. Please note that this notice is intended solely to alert readers that the content of this article is unreliable. We have not investigated whether authors were aware of or involved in the systematic manipulation of the publication process.

Wiley and Hindawi regrets that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our own Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

[1] S. Wang, M. Zhao, D. Liu, W. Su, and S. Zhang, "Attack and Protection Technology of Intelligent Terminals for New Energy Internet Transmission, Transformation, and Distribution," *Journal of Control Science and Engineering*, vol. 2022, Article ID 1620500, 9 pages, 2022.

Hindawi
Journal of Control Science and Engineering
Volume 2022, Article ID 1620500, 9 pages
https://doi.org/10.1155/2022/1620500

Research Article

Attack and Protection Technology of Intelligent Terminals for New Energy Internet Transmission, Transformation, and Distribution

Shengda Wang,[1] **Mingming Zhao**,[2] **Danni Liu**,[1] **Weijia Su**,[1] **and Song Zhang**[1]

[1]*JiLin Information & Telecommunication Company, State Grid Jilin Electric Power Corporation Ltd, Changchun, Jinlin 130000, China*
[2]*State Grid Cyber Security Technology (Beijing) Co., Ltd, Beijing 102211, China*

Correspondence should be addressed to Danni Liu; 202001000043@hceb.edu.cn

Received 31 May 2022; Revised 3 July 2022; Accepted 11 July 2022; Published 30 July 2022

Academic Editor: Jackrit Suthakorn

In order to improve the ability of the new energy Internet to defend against external attacks, the author proposes a dual Markov chain-based FDIA detection method suitable for the new energy Internet. Taking into account the FDIA principles and characteristics of the new energy Internet, and the fact that the new energy Internet contains a large amount of measurement data and changing operating states, the data to be detected is mapped to two different state spaces, and two different Markovs are generated. The detector of FDIA is generated according to the accuracy of energy Internet operation state estimated by the model. The correctness and effectiveness of the proposed detection method are verified by experimental cases. Experimental results show: The proposed FDIA detection method has excellent detection probability and less detection calculation, the detection probability can reach 98.60%, and the false alarm probability is only 1.35%, compared with the support vector machine method, the calculation amount is reduced by an order of magnitude. It is proven that the method can meet the application requirements of the new energy Internet.

1. Introduction

Energy Internet is a comprehensive application of advanced communication technology, power electronics technology, and intelligent management technology, connecting distributed renewable energy stations dominated by wind and solar energy, it is a complex system that realizes the interconnection and interaction of power network, natural gas network, transportation network, and information network. In the energy Internet, the energy transfer between various energy sources and the information exchange and communication of intelligent devices are realized by industrial control systems [1]. With the accelerated implementation of "Industry 4.0" and "Integration of Industrialization and Industrialization," industrial control equipment is more complex and diverse, and the risks of wireless application technology, industrial network viruses, and database management vulnerabilities will become more advanced and persistent threats (Advanced Persistent Threat, APT) into the industrial control system.

Data is the core asset of the Energy Internet, in the future, the data sources of the Energy Internet will cover all aspects of energy production, transmission, transaction, consumption, etc., showing the characteristics of extensive sources, large scale, and complex types [2]. The opening, interconnection, and sharing mechanism of the Energy Internet will lead to continuous malicious network attacks, these malicious network attacks take advantage of the coupling between the extensive cyber-physical systems in the Energy Internet, and produce a chain reaction of interactive communication, as a result, it will inevitably pose a great threat to the business system data in the production, transmission, transaction, and consumption of the energy Internet. Therefore, it is particularly important to study the data security of the energy Internet based on network attacks.

2. Literature Review

Jember et al. focus on the standardization of global smart grid support projects and innovative academic results in related areas, including generation, transmission, distribution, and microgrids, and including smart grid information management systems such as smart meter reading, real-time status monitoring, and data aggregation analysis modeling, as well as a detailed comprehensive analysis of advanced communication technologies, and pointed out that the smart grid information security threat defense will become a difficult problem that needs to be broken through in the future development of smart grid [3]. Dong proposed a specific framework for secure data aggregation using homomorphic encryption algorithms in a distributed energy environment, the user-end collection device uses homomorphic encryption to encrypt the collected user privacy-sensitive data, and edge nodes such as gateways in the Energy Internet can aggregate the data of users in the area without decryption, although this framework enables efficient data aggregation, it does not consider systems for real-time data collection [4]. In order to solve the problem of personal user privacy caused by frequent data collection, KHanna proposed a scheme for aggregating time series data, which supports high-frequency device data collection, and regularly uploads encrypted data to the aggregator to ensure the privacy of personal data [5]. Zhang proposed to develop a reputation-based trust management scheme for user devices and data centers in cloud systems. However, due to the more dynamic nature of the energy Internet system, device trust management is more complicated. The literature proposes an anonymous wireless LAN authentication protocol [6]. Specifically, replacing a person's real identity with a pseudonym, in order to prevent people from being tracked, however, this solution is not suitable for high-dynamic systems with real-time updates of devices. Zhu Before adding the gated recurrent unit structure to the fully connected layer of the convolutional neural network, a hybrid neural network was established to train the historical measurement data of the power grid. Similarly, the spatial and temporal characteristics of the data were extracted to realize the detection of false data. Detection of Injection Attack (FDIA) [7].

The author first analyzes the principle and characteristics of FDIA, and clarifies the construction method of FDIA; Then, an FDIA detection method for the new energy Internet based on dual Markov chains is proposed, which maps the huge measurement vector generated at each sampling moment to 2 distance spaces, and generates 2 Markov chain models to adapt to energy. The ever-changing state of the Internet, at the same time, the FDIA detector is generated according to the accuracy of the energy Internet operating state estimated by each model. Finally, a typical case is used to verify the proposed detection method, which further shows that the proposed FDIA detection method can meet the requirements of the new energy Internet for detection speed and detection accuracy.

3. Research Methods

3.1. Principles and Characteristics of FDIA. The new energy Internet is a large-scale power information physical system, and the errors of the information system are inseparable from the accidents of the physical system. Therefore, by analyzing the principle of FDIA acting on the new energy Internet, combined with the inherent bad data detection method of the power system, the concealment characteristics of FDIA are obtained, and the diversity characteristics of FDIA are obtained through the actual situation, ensure that the attack examples used in the study meet the requirements of practical applications [8].

The principle of FDIA acting on the new energy Internet is shown in Figure 1. When the false data vector attacks the information system of the new energy Internet, the measurement vector Z becomes $Z+a$, which causes the state estimation result $\hat{x}$ to generate a state error vector c, which in turn causes the scheduling model to generate an incorrect scheduling policy control variable u', eventually, the physical system runs in an abnormal state x'.

In practical situations, random disturbances of the measurement or telecontrol system will cause the measurement vector Z to produce bad data with random error characteristics. Bad data is not an attack, and the existing power system state estimation methods have passed $\mathbf{r}_W$ detection and $\mathbf{r}_N$ detection, realizing the detection of bad data [9]. The specific bad data detection methods are as follows.

Calculate the residual r_i of the ith measurement, the weighted residual r_{Wi} , the regularized residual r_{Ni}, and the calculation expressions are shown in equations (1)–(3), respectively.

$$r_i = z_i - h_i(\hat{x}), \tag{1}$$

$$r_{Wi} = \frac{r_i}{\sigma_i}, \tag{2}$$

$$r_{Ni} = \frac{r_i}{\sigma_{Ni}}. \tag{3}$$

Among them, z_i is the value of the ith measurement; σ_i is the standard deviation of the measurement error of the ith measurement; σ_{Ni} is the standard deviation of r_i; and $h_i(\hat{x})$ is the estimated value of the ith measurement, obtained by substituting $\hat{x}$ (the estimated value of voltage amplitude U and phase θ) into the measurement function $h(\theta, U)$. The specific measurement function $h(\theta, U)$ includes the branch active power measurement function $P_{ij}(\theta, U)$, the branch reactive power measurement function $Q_{ij}(\theta, U)$, the node injected active power measurement function $P_i(\theta, U)$, the node injected reactive power measurement function $Q_i(\theta, U)$, and the node voltage amplitude value. The measurement function U_i is shown in formula (4).

$$h(\theta, U) = \begin{bmatrix} P_{ij}(\theta, U) \\ Q_{ij}(\theta, U) \\ P_i(\theta, U) \\ Q_i(\theta, U) \\ U_i \end{bmatrix}. \tag{4}$$

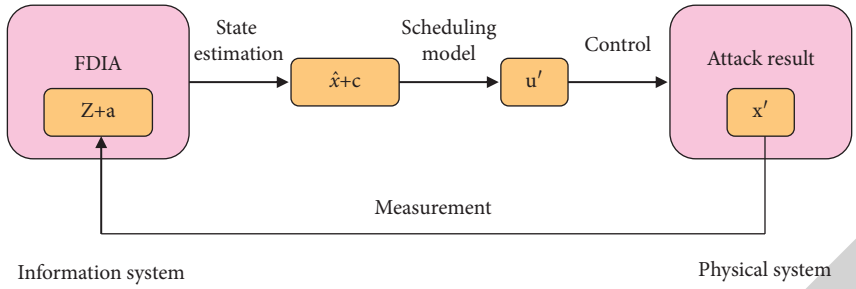

Figure 1: The schematic diagram of FDIA acting on the new energy Internet.

Equation (4) is a nonlinear equation system, the resistance component in the equation can be ignored in the transmission network, and it is approximated as a linear equation system. However, for distribution networks with lower voltage levels, the resistive component should not be ignored. Therefore, considering the application requirements of the new energy Internet, the author does not ignore the resistance component [10].

If the residual calculation result satisfies formula (5), it means that there is bad data in the measurement vector.

$$\begin{aligned} &\max\left\{\left|r_{wi}\right|\right\} > \delta_{tr1} \\ &\text{or } \max\left\{\left|r_{Ni}\right|\right\} > \delta_{tr2}. \end{aligned} \tag{5}$$

Among them, δ_{tr1} and δ_{tr2} are the thresholds for detecting r_w and r_N, respectively.

Stealth is an important feature of FDIA, which comes from the vulnerability of bad data detection methods. When there is no false data a and when false data a is included, the calculation expressions of the residuals are shown in equation (6) and equation (7) respectively.

$$r_1 = Z - h(\hat{x}), \tag{6}$$

$$r_2 = Z + a - h(\hat{x} + c). \tag{7}$$

Among them, r_1 and r_2 are the residual vectors when they do not contain and contain false data, respectively.

If the ideal attack vector a is constructed to satisfy equation (8), then $r_1 = r_2$, as a result, the bad data detection method based on residual calculation in the power system fails to detect false data. In other words, existing bad data detection methods are not suitable for FDIA detection [11].

$$a = h(\hat{x} + c) - h(\hat{x}). \tag{8}$$

Meanwhile, FDIA with cryptic features exhibits diverse features [12]. ①Incomplete attack capabilities lead to different false data with different degrees of sparsity. Let such an attack vector be $a\prime$, which is a vector with zero elements that can only achieve attacks on specific measurements. And the residual of the state estimation injected with $a\prime$ cannot trigger bad data detection, that is, the residual satisfies Equation (9). ② Different FDIAs have different degrees of influence on the measurement vector Z, resulting in different attack strengths of different FDIAs. The smaller the strength of the attack vector is, the smaller the change of the measurement vector Z is, attacks are hard to detect. The calculation expression of the attack strength P_a (unit is dB) adopted by the author is shown in formula (10).

$$\begin{aligned} &\max\left\{\left|r_{wi}\right|\right\} > \delta_{tr1}, \\ &\max\left\{\left|r_{Ni}\right|\right\} > \delta_{tr2}. \end{aligned} \tag{9}$$

$$P_a = 20\lg\frac{\sum_{i=1}^{m}\left|a_i'\right|/z_i}{m}. \tag{10}$$

Among them, a_i' is the element of $a\prime$; m is the number of measurement units.

To sum up, FDIA shows inherent concealment and diversity characteristics. In order to meet the requirements of practical applications, the detection method of FDIA should be able to detect various FDIAs.

3.2. FDIA Detection Method Suitable for New Energy Internet. According to the Markov chain, the operation state change model of the energy Internet is established, and the difference between the state change caused by FDIA and the normal state change law can be analyzed, and the detection of the energy Internet FDIA can be realized [13].

In order to improve the comprehensiveness of detection, so that the detection range of FDIA can cover FDIA with different sparsity and attack strength, and ensure that it is sensitive enough to weak attacks, the author uses two complementary Markov chains to model the operation state of the new energy Internet, and solves the problem that a single Markov chain model cannot effectively distinguish some FDIAs. Therefore, in order to avoid the false detection problem caused by the detection blind spot of a single Markov chain, the FDIA detection method should be generated based on the dual Markov chain model of the new energy Internet [14].

(1)The Markov Chain Model of the Operational State of the New Energy Internet.

The new energy Internet contains many measurement values with random variation characteristics, studying the state change process of each measurement separately will greatly reduce the computational efficiency. Energy Internet as a whole, and among them, the measurement values are mutually influenced. Therefore, the author studies the measurement vector Z at each sampling moment as a whole.

It can be seen from equations (4) and (8) that, as long as there is an attack vector, the measurement sub-vectors

(branch active power measurement P_{ij}, branch reactive power measurement Q_{ij}, node injected active power measurement P_i, node injected reactive power measurement Q_i, and node voltage amplitude measurement U_i) are subject to change. Therefore, to reduce the amount of data used for detection, this study selects the measurement sub-vectors P_{ij} and P_i to construct a vector Z_D, and uses the Markov chain to model the state change process of Z_D, and analyzes the state of Z_D and its transition law.

The state space, one-step transition matrix, and initial probability distribution vector are the three key elements for establishing the Markov chain model of the energy Internet, which together determine the properties of the Markov chain [15].

For the state space, by calculating the Euclidean distance d between Z_D and the specified reference vector Z_B, the similarity between the two is represented, and the evaluation standard of Z_D is unified; At the same time, considering that the energy Internet has a large amount of historical measurement data, the measurement vectors with close distance values are processed into the same state, and the distance values are further classified to generate a state space.

According to formula (11), the range of the distance value corresponding to the state in the state space is calculated.

$$[d_{\min} + (i-2)l, d_{\min} + il] \quad i = 1, 2, \ldots, N_S. \tag{11}$$

Among them, N_S is the number of states in the state space; l is the interval; $d_{\min}$ is the minimum value of the distance value d of all historical measurement data, and the calculation expression of d is shown in formula (12).

$$d = \sqrt{\sum_{n=1}^{N_z} \left(Z_{D,n} - Z_{B,n}\right)^2}. \tag{12}$$

Among them, $Z_{D,n}$ and $Z_{B,n}$ are the nth elements in Z_D and Z_B, respectively; N_z is the number of elements in Z_D.

For the one-step transition matrix, the distance of each historical measurement data and its corresponding state are calculated according to (11) and (12), and the one-step transition matrix P from state S_i to state S_j is obtained, as shown in formula (13).

$$P = \left[p_{S_i,S_j}\right], \tag{13}$$

$$p_{S_i,S_j} = \frac{N_{ij}}{N_i}. \tag{14}$$

Among them, N_{ij} is the number of samples transferred from state S_i to state S_j in one step; N_i is the number of samples in state S_i.

For the initial probability distribution vector, the sampling time before the time to be detected is taken as the initial time, and the state variable at this time is X_0, in the case of known historical data, its initial probability distribution vector $\pi(0)$ is known. The value of the element $\pi_{S_i}(0)$ in $\pi(0)$ is shown in formula (15).

$$\pi_{S_i}(0) = \begin{cases} 1 & X_0 = S_i, \\ 0 & \text{other.} \end{cases} \tag{15}$$

(2) FDIA detection method based on double Markov chain.

The key to FDIA detection of the new energy Internet lies in how to process the measurement changes caused by the attack vector into obvious changes in state values. However, the state change process of the new energy Internet is random and complex, which makes the single Markov chain established according to equations (11)–(15) insensitive to attack vectors with different sparsity and attack strengths, that is, the comprehensiveness of detection cannot be guaranteed, so that the detection probability is insufficient [16].

In order to make the operating state changes sufficiently sensitive to the diversity of FDIA, the authors choose two approximately complementary scenarios, using this as a benchmark scenario, a double Markov chain is generated. As a result, an FDIA detection method based on double Markov chains is constructed, and the structure is shown in Figure 2. The specific selection process of the two reference vectors Z_{B1} and Z_{B2} is shown in Figure 3. In Figure 3, P_{Lh} and Q_{Lh} are the historical active power and reactive power of the node load, respectively; $P_{Lh,\max}$ and $Q_{Lh,\max}$ are the maximum values of the historical active power and reactive power of the node load respectively; P_{DG} is the capacity of the distributed power supply; $P_{ij,1}$ and $P_{ij,2}$ are the branch active powers of scenario 1 and scenario 2, respectively; $P_{i,1}$ and $P_{i,2}$ inject active power into the nodes of Scenario 1 and Scenario 2, respectively.

Scenario 1 is the operating condition where the grid is fully loaded and the output power of the distributed power supply is 0, reflecting the situation of heavy load but no output of the distributed power supply; Scenario 2 is the operating condition where the grid is connected to half of the load and the distributed power supply is outputting full power, which reflects the situation of light load but the full output of the distributed power supply. By selecting a reference vector in two scenarios, it can be ensured that various false data will significantly change the operating state represented by the Markov chain model, reducing the probability of false detection [17].

For each Markov chain model in the dual model, the results can be obtained separately according to equations (11)–(15), historical data, and different reference values.

According to the generated double Markov chain model, the probability distribution vectors π_1 and π_2 of the operating state of the energy Internet at the time to be detected can be obtained, and then the expectation of the operating state at the time to be detected can be obtained, the running states S_1^E and S_2^E at the moment to be detected are estimated. The specific calculation expressions are shown in formulas (16)–(19).

$$\pi_1 = \pi_1(0)P_1, \tag{16}$$

$$\pi_2 = \pi_2(0)P_2, \tag{17}$$

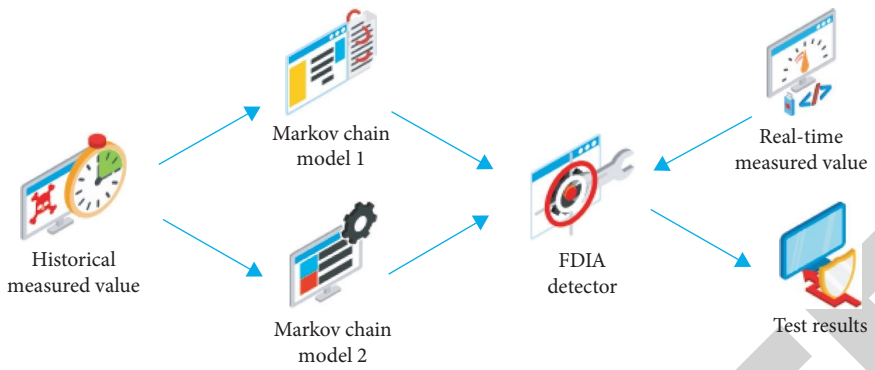

Figure 2: Structure of FDIA detection method based on double Markov chain.

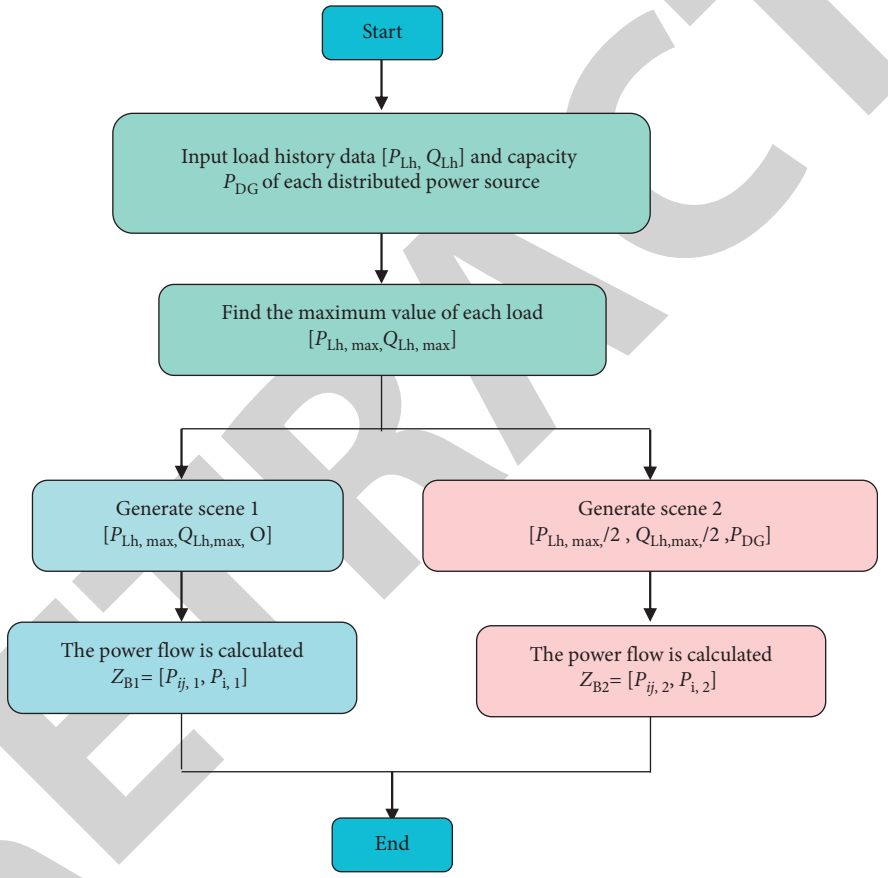

Figure 3: Flow chart of selection of reference vector.

$$S_1^E = \sum_{n=1}^{N_{S1}} \pi_{1,n} S_{1,n}, \tag{18}$$

$$S_2^E = \sum_{n=1}^{N_{S2}} \pi_{2,n} S_{2,n}. \tag{19}$$

Among them, P_1 and P_2 are the one-step transition matrices of the two Markov chains respectively; $\pi_1(0)$ and $\pi_2(0)$ are the initial probability distribution vectors of the two Markov chains respectively; N_{S1} and N_{S2} are the number of states of the two Markov chains respectively; $S_{1,n}$ and $S_{2,n}$ are the nth position in the state space of the two Markov chains respectively a status value; $\pi_{1,n}$ and $\pi_{2,n}$ are the nth elements of π_1 and π_2, respectively.

Two Markov chain models are used to estimate the historical data samples respectively, and the estimated values of the historical state are obtained as S_{ZB1}^E and S_{ZB2}^E, respectively. According to two different reference vectors, the actual values of the historical state are calculated as S_{ZB1}^E and S_{ZB2}^E, respectively, and the error values D_1 and D_2 between the actual state and the estimated state are calculated according to (20) and (21), respectively.

$$D_1 = S_{ZB1} - S_{ZB1}^E, \tag{20}$$

$$D_2 = S_{ZB2} - S_{ZB2}^E. \tag{21}$$

D_1 and D_2 reflect the accuracy of estimating known historical states using two different Markov chain models. The confidence interval is selected in the range of 95% to 99%, find D_1^* and D_2^* in D_1 and D_2 to satisfy (22) and (23) respectively, that is, the absolute values of 95%~99% of the elements in D_1 and D_2 are not greater than D_1^* and D_2^*, respectively. In this way, it can be considered that the estimated error intervals of the two Markov chains in the operating state of the Energy Internet are $[-D_1^*, D_1^*]$ and $[-D_2^*, D_2^*]D_2^*]$, respectively.

$$95\% \le p\left\{\left|D_{1,n}\right| \le D_1^*, \quad n = 1, 2, \ldots, N_h\right\} \le 99\%, \tag{22}$$

$$95\% \le p\left\{\left|D_{2,n}\right| \le D_2^*, \quad n = 1, 2, \ldots, N_h\right\} \le 99\%. \tag{23}$$

Among them, $p\{\cdot\}$ represents the probability of occurrence of an event $\{\cdot\}$; and N_h is the sampling number of historical data.

The accuracy of estimating the state of the data to be detected using the Markov chain model is the same as the accuracy of estimating the state of the historical data, and in order to ensure that the detector is sufficiently sensitive to the diversity of FDIA, generate a dual Markov chain energy Internet FDIA detector based on estimated error intervals $[-D_1^*, D_1^*]$ and $[-D_2^*, D_2^*]$, as shown in Equation (24).

$$\begin{cases} H_0: S_1^E - D_1^* < S_1^T < S_1^E + D_1^*, S_2^E - D_2^* < S_2^T < S_2^E + D_2^*, \\ H_1: S_1^T \le S_1^E - D_1^* \text{ or } S_1^T \ge S_1^E + D_1^* \text{ or } S_2^T \le S_2^E - D_2^* \text{ or } S_2^T \ge S_2^E + D_2^*. \end{cases} \tag{24}$$

Among them, H_0 is the assumption that the detection data is normal; H_1 is the assumption that the detection data is false data; S_1^T and S_2^T are the actual state values under the conditions of two different reference values at the time to be detected Z_D calculated according to formulas (11) and (12), respectively. If the actual state value satisfies the assumption H_1, it means that there is FDIA, that is, any Markov chain judges that the error between the actual state (S_1^T, S_2^T) of the vector to be detected and the estimated state (S_1^E, S_2^E) does not meet the normal estimation error interval of the Markov chain model, then it is considered that there is FDIA.

(3) FDIA detection process based on double Markov chain.

The author's proposed new energy Internet FDIA detection process based on a double Markov chain and its own characteristics can be seen, the FDIA detection method based on the double Markov chain is very suitable for the new energy Internet, the main reasons are as follows: ① Although the Markov chain uses a certain amount of historical data to complete the modeling of the operating state of the energy Internet, under the same amount of historical data, compared with the machine learning method based on historical data training, its computational complexity and performance are significantly reduced. The computational load is reduced obviously, and the performance is better. ② The one-step transition matrix in the Markov chain modeling process only needs to be generated once before detection, and after each detection, the new unattacked sample value is added to the historical database, and the one-step transition matrix is updated in real-time, the amount of computation is significantly smaller than the training model update of the machine learning method. ③ When the double Markov chain model is applied in practice, the parallel computing method can be adopted, and the application of double chain has little effect on the overall detection time [18].

4. Analysis of Results

The author adopts a standard 33-node distribution network model and adds typical random power sources and loads on the basis of the original network, the modified example structure is shown in Figure 4. In the figure, node 1 is the system power supply, node 9 is connected to an electric vehicle charging station, and node 17 and node 32 are, respectively, connected to a photovoltaic power supply with a capacity of 0.5 MW. Based on the measurement data collected by the power grid and a large number of fake data constructed, the author's example verifies the correctness and effectiveness of the proposed FDIA detection method.

4.1. Generation of Grid Measurement Data. The measurement data of the power grid is obtained from the measurement data of the load, photovoltaic power source, and electric vehicle charging station. Among them, the measurement data of load and photovoltaic power supply are constructed based on the changing trend of active power measurement data from August 22 to September 20, 2019 (30 days in total) based on the WESTERN region given by the website of PJM Company in the United States. Multiply the original load power and photovoltaic power supply power by the power per unit value at each moment, and the measurement data of each node load and photovoltaic power source sampled every 5 minutes is constructed [19].

The measurement data of the electric vehicle charging station is generated according to the load characteristics of the electric vehicle. In the case of knowing the number of electric vehicles, charging power, cruising range, the probability distribution function of charging start time, the probability distribution function of daily mileage, etc., generate load variation curves of EV charging stations sampled every 5 min. Among them, the number of simulated electric vehicles is 100, the charging power is 3.5 kW, and the cruising range is 300 km.

According to the load power, photovoltaic power generation power, and electric vehicle charging station load power sampled every 5 minutes, use the power flow calculation tool to calculate the power flow value of the power grid as the measurement data recorded by the electric meter, and add random errors that meet the normal data requirements to form 163, the measurement data of 30 d of measurement units (active and reactive power measurement of 32 branches,

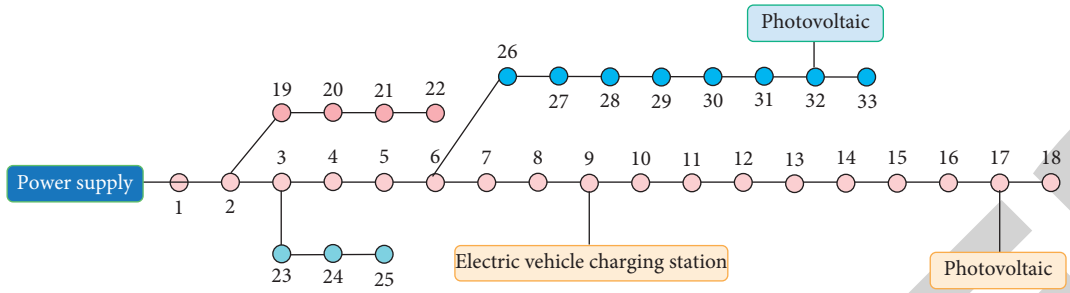

Figure 4: Topological structure of the 33-node distribution network after transformation.

active and reactive power measurement of 33 nodes, and voltage amplitude measurement of 33 nodes) [20].

4.2. Generation of Power Grid Attack Data. The loads and power sources in the new energy Internet are random, resulting in multiple state changes in a day. In order to verify the detection performance of the proposed detection method at different times, the calculation example in this section will be 03 : 00, 06 : 00, 09 : 00, 12 : 00, 15 : 00, 18 : 00, 21 : 00 on September 20., 24 : 00, these 8 moments are the injection moments of FDIA.

According to the characteristics of FDIA, a series of fake data are randomly constructed [21]. In order to cover as much as possible FDIA with different attack strengths and sparse degrees, randomly generate 8×6000 covert attack vector groups $a_1 - a_8$ for the above 8 times, the attack intensity range is [−30, 5] dB, and the zero elements of each attack vector satisfy the uniform distribution, and the specific zero elements at different times, the distribution is shown in Figure 5.

4.3. FDIA Detection. The detection method proposed by the author is used to detect the large amount of false data $a_1 - a_8$ generated in Section 4.2. In order to verify the detection performance advantage of the detection method proposed by the author, the Gaussian kernel function SVM with excellent performance is used to detect the same false data sample $a_1 - a_8$. Among them, SVM adopts the same historical measurement sample, 29 normal data samples, and 29 typical fake data samples are generated respectively for the above eight moments as training samples.

The detection probability of the FDIA detection method proposed by the author is better than that of the SVM method at each detection moment, and the lowest detection probability can reach 98.60% (12 : 00), which is significantly better than the highest detection probability of the SVM method of 76.92% (24 : 00). This is because the SVM method needs to use both normal data and fake data as training samples, and the fake data samples are difficult to cover as much as possible, and the fake data with different attack intensities and sparse degrees makes detection feature extraction difficult; The detection method proposed by the author only needs to model and analyze the state change law of normal data samples over time and does not need to consider false data samples, which reduces the impact of false data on the accuracy of the detection model.

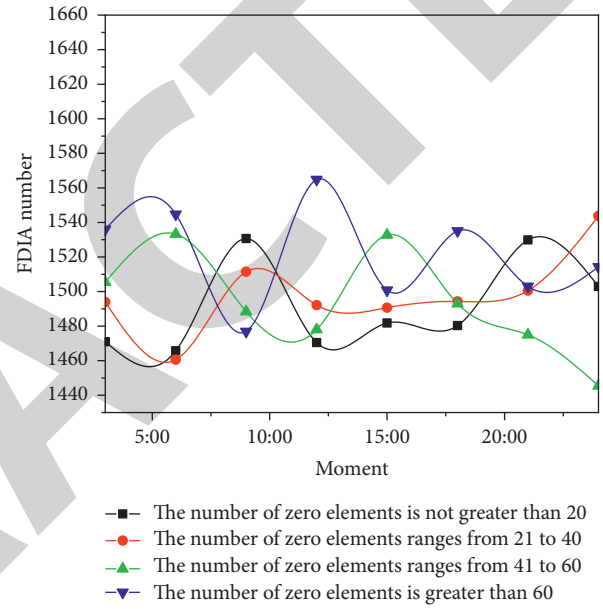

Figure 5: Distribution of zero elements of attack vector.

In order to verify the necessity and correctness of using the double Markov chain, the detection probability of the single Markov chain 1 and the single Markov chain 2 to the attack vector group $a_1 - a_8$ (the key information of detection is the same as that in Table 1) is calculated respectively, the results are all about 90%, it is less than the minimum detection probability of the double-stranded model of 98.60% (12 : 00), indicating that the double-stranded model will significantly improve the detection probability, which verifies the necessity and correctness of using the double-stranded model.

In order to verify the false alarm performance of the detection method proposed by the author, at 03 : 00, 06 : 00, 09 : 00, 12 : 00, 15 : 00, 18 : 00, 21 : 00, 24 : 00 on September 20, respectively, construct 500 normal data that meet the normal measurement error requirements at any time, and the detection method proposed by the author is used for detection, of which only 1.35% of the data is misjudged as false data, indicating that the detection method proposed by the author has very superior false alarm performance [22]. In order to verify the detection performance of the detection method proposed by the author with the change of attack intensity, the detection probability of the attack vector group $\mathbf{a}_1 - \mathbf{a}_8$ with the change of attack intensity is calculated, and the results are shown in Figure 6.

Table 1: Comparison of the calculation amount of the two detection methods.

Detection method	Multiplication calculation amount	Addition calculation amount
Author method	≥398	≥524
SVM method	≥3944	≥7482

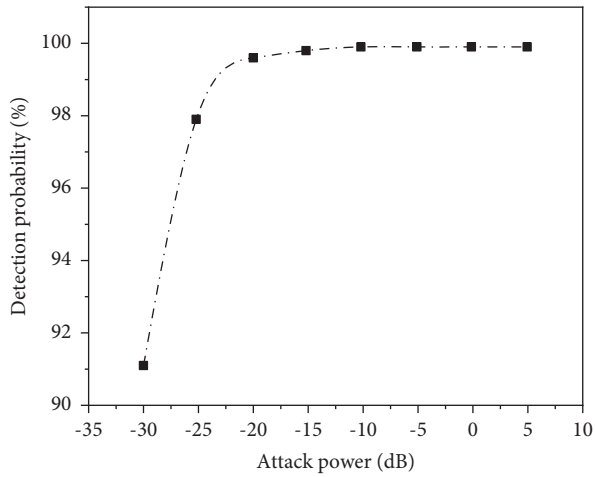

Figure 6: Variation curve of detection probability with attack intensity.

As can be seen from Figure 6, when the attack strength of FDIA is greater than -20 dB, the detection probability has reached 99.66% (close to 100%), and when the attack strength is very weak (-30 dB), the detection probability is also greater than 90%. It shows that the FDIA detection method proposed by the author is comprehensive, and further shows that the proposed detection method has very superior detection performance [23].

In order to verify the computational advantage of the detection method proposed by the author, the computational cost of the detection method proposed by the author and the SVM detection method in a single detection process are calculated respectively, the results are shown in Table 1.

It can be seen from Table 1, the detection calculation amount of the detection method proposed by the author is reduced by an order of magnitude compared with the SVM method. This is because the false data training samples added by the SVM method will increase the amount of detection calculation, and it is difficult to meet the requirements of detection speed and accuracy at the same time. The detection method proposed by the author does not need to consider false data samples, which effectively reduces the amount of detection calculation. The calculation results show that the proposed detection method has superior detection performance and less computation, the detection probability can reach 98.60%, and the false alarm probability is only 1.35% [24].

The results of the above examples verify the correctness and effectiveness of the FDIA detection method proposed by the author, and its superior detection probability, false alarm probability, and detection calculation amount fully meet the application requirements of the new energy Internet [25–27].

5. Conclusion

The FDIA detection method of the new energy Internet based on a double Markov chain is studied, and the following conclusions can be drawn based on the example simulation:

(1) Use the Markov chain to model the operation state of the new energy Internet, and generate the state space by the Euclidean distance between the measurement vector and the reference vector, which can well describe the correlation and difference between the measurement vectors, it avoids separate analysis of a large number of random measurement data, improves the detection performance, and reduces the amount of calculation;

(2) The dual Markov chain model selects two different operating scenarios as reference vectors, which can ensure that hidden and diverse attack vectors can cause significant changes in the state value of the new energy Internet Markov chain model, reducing the probability of false detection;

(3) The results of the calculation example show that the proposed detection method has superior detection performance and less computation, the detection probability can reach 98.60%, and the false alarm probability is only 1.35%, compared with SVM, the calculation amount is reduced by an order of magnitude, which fully meets the application requirements of the new energy Internet for FDIA detection accuracy and real-time performance.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This study was supported by Science and Technology Project of State Grid Jilin Electric Power Corporation Ltd. "Research on Safety Immunity Technology of Intelligent Power Distribution Integrated System" (NO.2021-58)

References

[1] S. Abdullah, M. N. Asghar, M. Ashraf, and N. Abbas, "An energy-efficient message scheduling algorithm with joint routing mechanism at network layer in internet of things environment," *Wireless Personal Communications*, vol. 111, no. 3, pp. 1821–1835, 2020.

[2] S. Höhne and V. Tiberius, "Powered by blockchain: forecasting blockchain use in the electricity market," *International Journal of Energy Sector Management*, vol. 14, no. 6, pp. 1221–1238, 2020.

[3] A. G. Jember, W. Xu, C. Pan, X. Zhao, and X. C. Ren, "Game and contract theory-based energy transaction management for internet of electric vehicle," *IEEE Access*, vol. 8, pp. 203478–203487, 2020.

[4] L. Dong, Q. Ni, W. Wu, C. Huang, T. Znati, and D. Z. Du, "A proactive reliable mechanism-based vehicular fog computing network," *IEEE Internet of Things Journal*, vol. 7, no. 12, pp. 11895–11907, 2020.

[5] A. Khanna and S. Kaur, "Internet of things (iot), applications and challenges: a comprehensive review," *Wireless Personal Communications*, vol. 114, no. 2, pp. 1687–1762, 2020.

[6] J. Zhang, G. Lu, H. Yu, Y. Wang, and C. Yang, "Effect of the uncertainty level of vehicle-position information on the stability and safety of the car-following process," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, pp. 1–15, 2020.

[7] Z. Zhu, Y. Chai, Z. Yang, and C. Huang, "Safety criteria based on barrier function under the framework of boundedness for some dynamic systems," *Science China Information Sciences*, vol. 65, no. 2, pp. 122203–122214, 2022.

[8] R. Dureja and K. Y. Rozier, "Formal framework for safety, security, and availability of aircraft communication networks," *Journal of Aerospace Information Systems*, vol. 17, no. 7, pp. 322–335, 2020.

[9] Z. Yan, Y. Wang, and J. Fan, "Research on safety subregion partition method and characterization for coal mine ventilation system," *Mathematical Problems in Engineering*, vol. 2021, no. 3, pp. 1–11, 2021.

[10] S. K. Dey and A. Ratnoo, "Unmanned aircraft systems conflict resolution using return-to-course maneuver," *Journal of Aerospace Information Systems*, vol. 17, no. 3, pp. 134–149, 2020.

[11] F. Rezaimehr and C. Dadkhah, "A survey of attack detection approaches in collaborative filtering recommender systems," *Artificial Intelligence Review*, vol. 54, no. 3, pp. 2011–2066, 2021.

[12] M. R. Habibi, H. R. Baghaee, F. Blaabjerg, and T. Dragicevic, "Secure mpc/ann-based false data injection attack detection and mitigation in dc microgrids," *IEEE Systems Journal*, vol. 16, no. 99, pp. 1–11, 2021.

[13] X. Zhang, X. Qiao, T. Liang, and K. An, "Secure performance analysis and pilot spoofing attack detection in cell-free massive mimo systems with finite-resolution adcs," *International Journal of Distributed Sensor Networks*, vol. 18, no. 1, 2022.

[14] P. Kumar, G. P. Gupta, and R. Tripathi, "An ensemble learning and fog-cloud architecture-driven cyber-attack detection framework for iomt networks," *Computer Communications*, vol. 166, pp. 110–124, 2021.

[15] M. Yang, H. Zhang, C. Peng, and Y. Wang, "A penalty-based adaptive secure estimation for power systems under false data injection attacks," *Information Sciences*, vol. 508, pp. 380–392, 2020.

[16] E. Jang, B. Wiese, P. Pilz, S. Fischer, and C. Schmidt-Hattenberger, "Geochemical modeling of co2 injection and gypsum precipitation at the ketzin co2 storage site," *Environmental Earth Sciences*, vol. 81, no. 10, pp. 286–18, 2022.

[17] A. Y. Lu and G. H. Yang, "False data injection attacks against state estimation in the presence of sensor failures," *Information Sciences*, vol. 508, pp. 92–104, 2020.

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

[19] D. N. Wategaonkar, S. V. Nagaraj, and T. R. Reshmi, "Multi-hop energy-efficient reliable cluster-based sectoring scheme using Markov chain model to improve qos parameters in a wsn," *Wireless Personal Communications*, vol. 119, pp. 393–421, 2021.

[20] X. Mei, C. Zeng, and G. Gong, "Predicting indoor particle dispersion under dynamic ventilation modes with high-order Markov chain model," *Building Simulation*, vol. 15, no. 7, pp. 1243–1258, 2022.

[21] B. Cai, L. Zhang, and Y. Shi, "Control synthesis of hidden semi-markov uncertain fuzzy systems via observations of hidden modes," *IEEE Transactions on Cybernetics*, vol. 50, no. 8, pp. 3709–3718, 2020.

[22] M. Bhutani, B. Lall, and A. Dixit, "Mac layer performance modelling for ieee 802.15.7 based on discrete-time Markov chain," *IET Communications*, vol. 15, no. 14, pp. 1883–1896, 2021.

[23] A. Sharma and R. Kumar, *Performance Comparison and Detailed Study of AODV, DSDV, DSR, TORA and OLSR Routing Protocols in Ad Hoc Networks*, in *Proceedings of the 2016 Fourth International Conference on Parallel, Distributed and Grid Computing (PDGC)*, Waknaghat, India, 2016.

[24] M. S. Pradeep Raj, P. Manimegalai, P. Ajay, and J. Amose, "Lipid data acquisition for devices treatment of coronary diseases health stuff on the internet of medical things," *Journal of Physics: Conference Series*, vol. 1937, no. 1, Article ID 012038, 2021.

[25] J. Liu, X. Liu, J. Chen, X. Li, and F. Zhong, "Plasma-catalytic oxidation of toluene on Fe_2O_3/sepiolite catalyst in DDBD reactor," *Journal of Physics D: Applied Physics*, vol. 54, no. 47, 2021.

[26] R. Huang, P. Yan, and X. Yang, "Knowledge map visualization of technology hotspots and development trends in China's textile manufacturing industry," *IET Collaborative Intelligent Manufacturing*, vol. 3, no. 3, pp. 243–251, 2021.

[27] L. Yan, K. Cengiz, and A. Sharma, "An improved image processing algorithm for automatic defect inspection in TFT-LCD TCON," *Nonlinear Engineering*, vol. 10, no. 1, pp. 293–303, 2021.