Hindawi
Mathematical Problems in Engineering
Volume 2020, Article ID 4053825, 10 pages
https://doi.org/10.1155/2020/4053825

Research Article

Parameter Identification Method Based on Mixed-Integer Quadratic Programming and Edge Computing in Power Internet of Things

Jun Xiao,[1] You Situ,[1] Weideng Yuan,[1] and Xinyang Wang[2]

[1]*Power Dispatching and Control Center, Dongguan Power Supply Bureau of Guangdong Power Grid Co., Ltd., Dongguan, China*
[2]*China State Key Laboratory of Power Transmission Equipment & System Security and New Technology, Chongqing University, Chongqing, China*

Correspondence should be addressed to Xinyang Wang; 20141886@cqu.edu.cn

Received 24 July 2020; Revised 24 August 2020; Accepted 8 September 2020; Published 29 September 2020

Academic Editor: Yi-Zhang Jiang

With the rapid development of power Internet of Things, its scale is becoming larger and larger. Many advanced applications depend on the accuracy of network model and state estimation, and the accuracy of network model and state estimation largely depends on network parameter error. Therefore, a parameter identification and estimation method based on mixed-integer quadratic programming (MIQP) and edge computing is proposed. Firstly, a "cloud-tube-edge-end" architecture of power Internet of Things is proposed, and the edge computing layer collects terminal data and conducts data analysis, which greatly reduces the computing pressure of cloud center. In this architecture, the local state estimation is used to limit the branch with error data in a specific range to prevent the measurement errors in other ranges from affecting the local estimation process. Then, the parameter identification model is transformed into MIQP model, and a penalty factor is introduced into the optimization model to identify the parameter error and measurement error in the process of minimizing the objective function. Finally, data encryption, identity authentication, and other methods are used in edge computing to achieve network security protection, so as to avoid network attacks and information leakage in the process of data transmission. The proposed method is tested and analyzed in IEEE 14-bus test system. The results show that the proposed method can accurately determine and identify the error data in a certain probability in the actual operation of the power grid, which is convenient for the controller to find out the wrong data in time and determine the source of the error data, so as to set a reasonable data value.

1. Introduction

A major strategy for the construction of the power Internet of Things is proposed by the State Grid. Considering the characteristics of "large scale, high reliability, and strong security" in the current power grid, the accuracy and security of power Internet of Things advanced application system are bound to be higher and higher, and considering the current situation of power Internet of Things basic data application, it is necessary to study the practical parameter error detection, identification, and estimation methods and to develop a practical power Internet of Things power network parameter identification and data analysis system [1].

In the traditional identification method based on residual sensitivity analysis, it is difficult to distinguish the detected residual from the bad data in the measurement or the parameter error in the network [2, 3]. Reference [4] points out that the network parameter error and the measured bad data on the corresponding branch have similar effects on the final identification results from the point of view of parameter identification. Analysis methods based on residual sensitivity are generally based on the assumption that bad data in measurements have been identified and eliminated. On the basis of this hypothesis, [5] proposes a parameter estimation method based on specific measurement residuals, which corresponds the regularized measurement residuals to the related branch parameters. The too

large regularization measurement residuals indicate that the corresponding branch parameter information is suspicious [6]. Reference [7] proposes that a parameter identification method for global error drop index is proposed, the mathematical model of this method is derived theoretically, and the identification mode of several wrong parameters or bad data can be identified simultaneously by this method. In [8], a new parameter identification index, the regularized residual vector, and the identification index vector are proposed to identify the wrong measurements and parameters. Compared with the traditional residual sensitivity identification method, the parameter identification method based on augmented security estimation has obvious advantages. In [9], it is pointed out that the augmented security estimation identification method requires a high degree of measurement redundancy, and it is necessary to determine the suspicious parameter set in advance. In order to increase the redundancy of measurement and ensure the observability of parameters, [10] has adopted multisection measurement instead of single-section measurement in traditional augmented security estimation, the method of parameter identification based on multisection measurement has improved the redundancy of measurement, and the method of parameter identification based on multisection measurement has improved the redundancy of measurement in the traditional extended parameter identification. Reference [11] proposes a multicloud to multifog architecture and designs two kinds of service models by employing containers to improve the resource utilization of fog nodes and reduce the service delay. Experimental results show that our proposed method could reduce the service delay efficiently. However, the proposed method has not taken the data security into account in the data transformation. Aiming at the secure information sharing in the smart environment, [12] uses the identity-based signature to present an anonymous key agreement protocol for the Smart Grid infrastructure. This protocol enables the smart meters to get connected with utility control anonymously to avail of the services provided by them. Moreover, performance analysis is also observed to consolidate the reliability and efficiency of the proposed protocol. However, the algorithm cannot guarantee the security of user data in the edge computing environment while taking into account the accuracy of parameter identification. On the other hand, for most parameter identification methods, the wrong parameters usually need a complex operation to identify one by one. A regularized Lagrangian multiplier method for parameter identification is proposed in [13]. In this method, all parameters are assumed to have no errors and are treated as a series of equality constraints, so that the original parameter identification problem is equivalent to an optimization problem. Therefore, it is possible to identify bad data and parameter errors by regularized residuals and regularized Lagrangian multipliers. Based on the MIQP model and edge computing, a new method for optimal identification of power network parameters is designed in this paper. The main innovations are as follows:

(1) In order to realize the efficient management of massive line data, a "cloud-tube-edge-end" architecture of power Internet of Things is proposed. The edge computing layer collects terminal data and conducts data analysis, which greatly reduces the computing pressure of cloud center.

(2) Due to the overidentification problem in the existing parameter identification methods based on the overall error reduction standard, a parameter identification method based on MIQP model is designed, and a penalty factor is added to the optimization model to better distinguish the wrong parameters from the bad data, simplify the parameter identification process, and improve the identification accuracy.

(3) Because of the low-security configuration of the edge computing layer and the large number of terminal lines, it is easy to be attacked by network. Therefore, the proposed method provides security protection from four aspects: identity authentication and access control, network monitoring and intrusion detection, data encryption, and privacy protection, so as to ensure the data security in the system.

The rest of the paper is organized as follows: Section 2 mainly introduces the architecture of power Internet of Things. Section 3 analyzes the mathematical description of parameter identification and puts forward parameter identification model and local state estimation. On the basis of the previous chapters, Section 4 mainly introduces parameter identification using MIQP algorithm and security assessment based on edge computing. Finally, some examples of the algorithm are analyzed and the experimental results are given in Section 5.

2. The Architecture of Power Internet of Things

The power Internet of Things adopts the "cloud-tube-edge-end" architecture, as shown in Figure 1. Among them, "cloud," as the cloud master station platform of the power Internet of Things, realizes advanced applications such as asset management, dispatching automation, and energy analysis through big data analysis technology and artificial intelligence technology. As the data transmission channel between "end" and "edge" and "edge" and "cloud," "tube" provides differentiated communication requirements for various IP services of the power Internet of Things.

As the terminal equipment of the power Internet of Things, the "terminal" generally includes intelligent meters, branch box distribution network monitoring terminal, low-voltage fault indicator, and various types of sensor units. It undertakes the functions of monitoring, sensing, and collecting power Internet of Things and responds to the execution and protection functions of the "edge" layer of the power Internet of Things. Due to the large number of types of terminal equipment and the complexity of traditional manual access mode, the power Internet of Things should have plug and play and topology automatic maintenance functions.

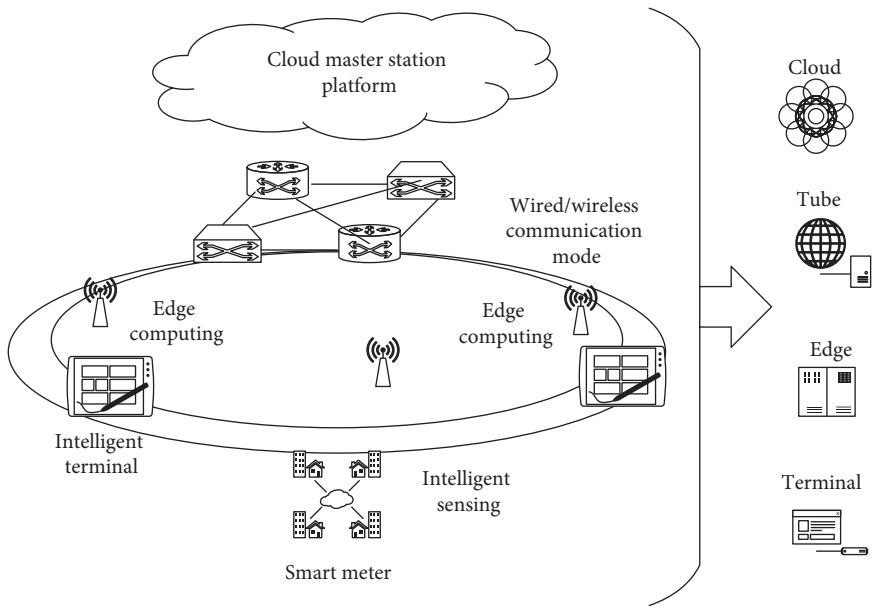

Figure 1: Architecture of power Internet of Things.

As the edge computing node of the power Internet of Things, "edge" connects the massive devices in the power system to realize real-time data perception, storage, and calculation. It can also be used as a bridge for data transmission to carry out data analysis and processing, alleviate the pressure of massive data upload to the cloud center, and ensure the real-time response processing of tasks. Under the control of cloud master station, edge computing nodes make decisions on the received tasks, choose to process locally or unload to other edge servers or cloud master stations, and change the networking and routing structure according to the amount of data, so as to realize the optimization of task processing. In addition, because the edge computing nodes are deployed near the power equipment, the battery power consumption of the terminal device connecting to the remote gateway is reduced, and the life cycle of the terminal device is prolonged.

In addition, with the gradual expansion of the application of the power Internet of Things, the real-time analysis of network parameters is very important to master the operation status of the power grid. And the related network security issues also need to be paid attention to. There are a large number of intelligent devices in power system, which is vulnerable to physical attacks when they are in an open physical environment. And in the edge computing mode, the security configuration of the edge node is relatively low, and the power data security is difficult to guarantee. Therefore, in the process of power grid parameter identification, it is necessary to carry out a certain security assessment to ensure the stable and reliable operation of the power system.

3. Mathematical Description of Parameter Identification

In the mathematical description of power system parameter identification, according to the actual parameter identification program, it is generally necessary to input the measured data and the data information of the system parameters, which is calculated by the static estimator model. Output system state estimates and identifies parameters and structure estimate [12]. The entire parameter identification process is shown in Figure 2.

For the measurement system, the measurement vector z is the m-dimensional vector, including the active power of the branch, the measurement of the reactive tidal flow, the active power of the node injection, the measurement of the reactive power, and the measurement of the voltage amplitude of the node. In the present power system, the measured data are mainly derived from the real-time data of supervisory control and data acquisition (SCADA) or wide area measurement system (WAMS), as well as the nontelemetry dataset by hand [14, 15]. There may be errors for each measurement, which can be described as follows:

$$Z = Z_0 + v_z, \tag{1}$$

where Z_0 is assumed to be the measurement real vector and v_z is the measurement error vector, assuming that v_z is a random vector with m-dimension obeying the mean value of 0 and variance of δ^2 normal distribution. For measurements that contain bad data, they are described as

$$Z = Z_0 + v_z + b, \tag{2}$$

where b is an exception error attached as bad data. For the power system, the mathematical description of parameter identification mainly includes network parameters and network wiring. For network parameter p, transformer parameters and line parameters are mainly considered in parameter identification: the former includes transformer ratio and reactance, and the latter includes line reactance and resistance.

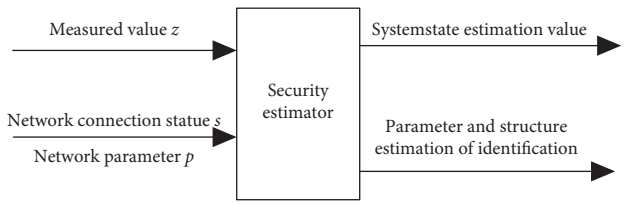

Figure 2: Security estimation input-output model.

3.1. Local State Estimation. The parameter identification is the node complex voltage, that is, voltage amplitude and voltage phase angle. The nodal complex voltage polar coordinates are expressed as shown in formula (3), where U is the amplitude of the voltage and the port is the voltage phase angle, and the rectangular coordinate form is shown in formula (4), in which e_i and jf_i are the real and imaginary parts of the complex voltage of the node, respectively:

$$\hat{U} = Ue^{j\theta}, \tag{3}$$

$$U = e_i + jf_i. \tag{4}$$

The measurement of the power system is usually the voltage amplitude of the node and the active power and reactive power injected into the node. In general power flow calculation, voltage measurement and node injection power measurement are known, and the measurement number is exactly equal to the number of states to be calculated [16, 17]. The types of measurement in parameter identification include the following three types [18]: node voltage amplitude, node injection power measurement, and branch first and end power values.

4. Parameter Identification and Security Estimation

The optimization method based on edge computing for power network branch error parameter identification is that the MIQP algorithm continuously iterates to optimize branch parameters and makes local estimation. Finally, the weighted sum of squares of local estimation residuals including suspicious branches is minimized.

4.1. Optimization Objectives. For the optimization problem described in this paper, the method of determining the objective function is as follows.

When some parameters of a branch are changed and the local partition of the branch is used for security estimation, the parameter error will make the objective function value of the security estimation larger to a certain extent. According to this characteristic, the objective function of the security estimation can be considered as the objective function of the optimization problem, and the branch parameters of the power network can be regarded as the variables to be optimized. The optimization model of the algorithm is as follows:

$$\min F = \sum_{i=1}^{N} r_w^2(x), \tag{5}$$

where N is the effective number of security estimations; x is the state quantity to be estimated, which is the node voltage amplitude and phase angle; r_w is the measurement residual value. Because the state variables need to be calculated by the security estimation and the security estimation is based on the actual parameters and measured data of the power network, the state variable x can be expressed as a hidden function with the actual parameters of the power network, so the expression is as follows:

$$x = f(g, b, y_c), \tag{6}$$

where g, b, y_c represents the wrong parameters of the power grid to be optimized, respectively.

In the actual optimization process, it will change with the number of iterations; while the power network parameters change, the state variables of local estimation will change and then affect the weighted measured residual value, namely, the objective function value. So when the objective function value in formula (5) is the smallest, the corresponding power network parameter value is the final optimization value of the parameter [19].

4.2. Parameter Identification Using MIQP Algorithm. Consider the power system measurement models as follows [20, 21]:

$$z = h(x, p_e) + \varepsilon, \tag{7}$$

where z is the measurement vector; x is the system state vector, including voltage amplitude and phase angle, so the network parameter error vector $h(x, p_e)$ is the nonlinear measurement equation of the relationship between the eigenvalue measurement and the system state and network parameter error; ε is the measurement error vector.

The measurement error can be divided into two parts [22, 23]:

$$\varepsilon = v_e + r, \tag{8}$$

where v_e is the error vector of suspicious measurement and the corresponding components of nonsuspicious measurement are all 0. r is the residual vector of measurement after eliminating the influence of dubious measurement. Substituting formula (8) into (7),

$$r = z - h(x, p_e) - v_e. \tag{9}$$

The following optimization model can be obtained by adding network parameter error and measurement error to weighted least squares security estimation problem and adding penalty factor to network parameter error and measurement error:

$$\begin{aligned}
\text{Minimize,}\quad & J(x, p_e, v_e, e_i, b_i) = r^T W r + P\left(\sum_{i\in S_p} e_i + \sum_{i\in S_m} b_i\right),\\
s.t.,\quad & r = z - h(x, p_e) - v_e,\\
& -Me_i \le p_{e,i} \le Me_i, \forall i \in S_p,\\
& -Mb_i \le v_{e,i} \le Mb_i, \forall i \in S_m,\\
& e_i \in \text{Binary}, b_i \in \text{Binary},
\end{aligned} \tag{10}$$

where W is the inverse matrix of the measurement error covariance matrix $\mathrm{cov}(r)$; P is an inverse matrix of the measurement error covariance matrix, which can be used as the weight matrix of measurement; P is a penalty factor of bad data and error parameters; M is a large enough positive value, which is generally chosen as 100; denotes the error of parameter i, is the i element of vector P_e; ve, I denotes the error of measurement i, is the i element of vector v_e, and the error of parameter I is the first element of vector v_e, and the error of parameter i is the first element of vector v_e; S_p is a suspicious parameter set; and s is a suspicious measure set.

By solving the above optimization model, the parameter identification of the power Internet of Things can be realized. The flowchart of parameter identification based on MIQP model is shown in Figure 3.

(1) To read the network model and measurement of the power system, firstly, the algorithm will read the network topology, network parameters, and measurement data for the actual power network.

(2) The edge computing is based on a single measurement section. The measurement error and parameter error are assumed to be 0, and the weighted least square method is used to calculate the security estimation. The initial vector r of the measurement residual and the Jacobian matrix H_x of the measurement can be obtained.

(3) Dubious measurements and parameter sets are selected, and dubious measurements and parameter sets are selected according to regularized Lagrangian multipliers or the total error drop index.

(4) The bad data and wrong parameters are identified by MIQP model, and the MIQP model is established based on the selected dubious measurement and parameter set. The MIQP model is solved by a branch cutting plane method or commercial optimization software, so as to determine the bad data and wrong parameters.

(5) The error measurement and error parameters are obtained by calculating the MIQP model, and the linear correction solution is given for the error measurement and error parameters:

$$p = p^0 + p_e. \tag{11}$$

(6) Finally, the algorithm needs to augment the security estimation of the identified error parameters.

4.3. Security Assessment Based on Edge Computing. In the edge computing layer of the power Internet of Things, a large number of line parameter data of terminal equipment are gathered, and the security configuration of the node itself is low, so it is vulnerable to network attacks, threatening the reliable operation of the power grid. In view of the security problem of edge computing in the power Internet of Things, corresponding defense measures need to be taken to ensure the security of the entire power system [24]. The security protection based on edge computing mainly includes identity authentication and access control, network monitoring and intrusion detection, data encryption, and privacy protection, as shown in Figure 4.

(1) Identity authentication and access control: during the data transmission of the power Internet of Things, each power terminal device and edge server should be given unique identity information. The terminal device sends a request to the cloud center by virtue of its identity information. The cloud center generates a public key and anonymous identity information for it according to the information of the terminal device and sends it to the edge device [25, 26]. The edge device decrypts and stores it locally with the private key. When the end device accesses the edge device, it sends a request to it, and the edge device authenticates it. Only after passing the authentication of identity information, it can access resources and perform other tasks [27].

(2) Network monitoring and intrusion detection: edge computing needs real-time detection of node risk, intelligent monitoring, and analysis of data transmission, so as to avoid security risks. The abnormal point detection algorithm based on statistics can be used to analyze the running state of the equipment in real time, identify the abnormal behavior in the network, and give early warning to the area that may be threatened by security.

(3) Data encryption: in the edge computing, the transmission content is encrypted based on attribute encryption. For power terminal equipment, if its attributes meet the access requirements of edge equipment, it is judged that the access can be allowed and the data information is decrypted.

(4) Privacy protection: in the power edge, the computing node can connect with the power edge devices through SSL sockets and select the target independently. Once the risk of information leakage is found, the computing node will send out an alarm message immediately. The edge device can adopt an encryption mechanism to establish the file management system of privacy data. When the user's privacy information needs to be called, the edge device sends a request to the user to obtain the call authority, and the user can update and improve or clear the sensitive data regularly.

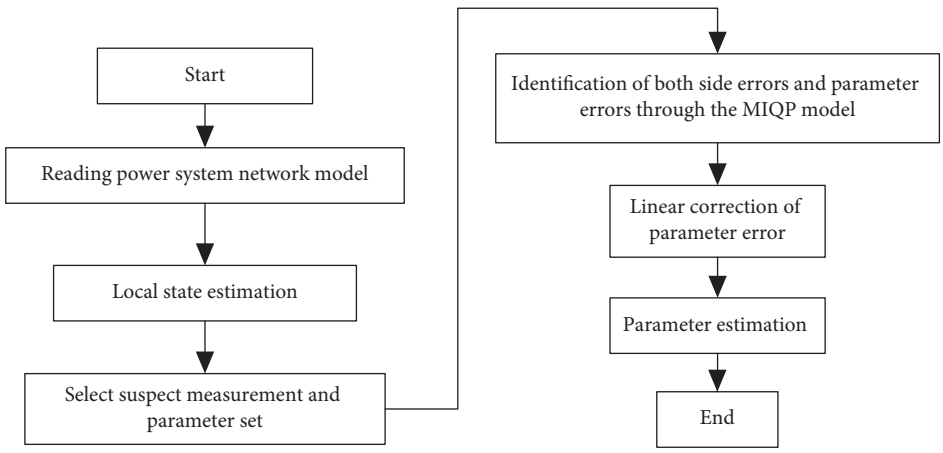

Figure 3: Flowchart of parameter identification based on MIQP model.

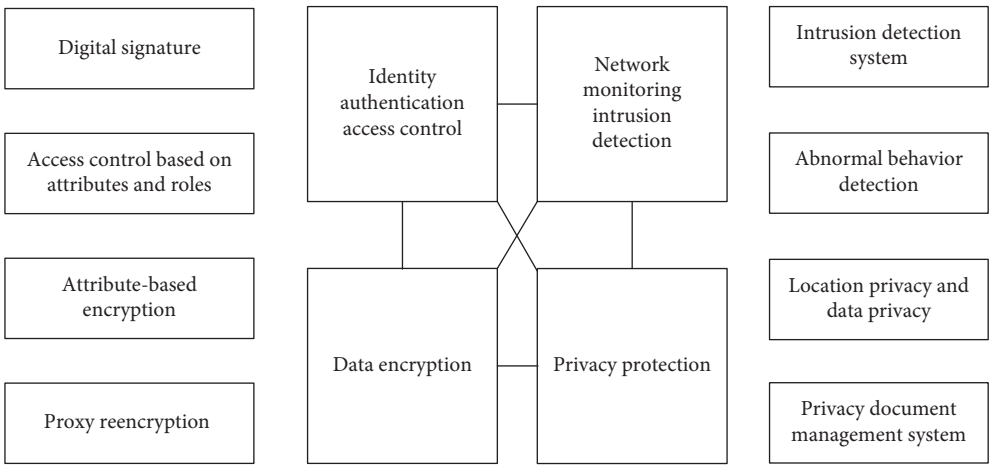

Figure 4: Security protection of edge computing layer.

5. Numerical Simulation and Result Analysis

5.1. Parameter Setting of Numerical Simulation. The parameter identification method of MIQP model is simulated and tested based on IEEE 14-node test system. The IEEE 14-node test system is shown in Figure 3. In the simulation test, the network parameter error is assumed to be reflected in the network branch reactance; the system adopts full measurement configuration; that is, all nodes are configured with voltage measurement, and both ends of the branch are equipped with active and reactive power measurements. In each example, no other deviation is introduced in the reactance of other branches or in the measurement of system analog quantity except for the assumed error.

5.2. Comparison and Analysis of Numerical Simulation Results. In the IEEE 14-node test system, the following three examples are tested based on the MIQP model parameter identification method, as shown in Figure 5.

5.2.1. Identification of Single Measurement Error or Parameter Error. This test example shows the simulation results of the identification of single measurement error or parameter error based on the MIQP model parameter identification method and the comparison with the simulation results of the total error drop index method. Table 1 shows a series of error identification results based on the MIQP model parameter identification method and the total error descent index method for a single bad data or error parameter. The parameters or measurement errors introduced in the example are 30% error of line reactance or ±5% error of single analog measurement, where x is branch reactance, P is branch active power measurement, and Q is branch reactive power measurement. The two methods have the same identification results on the identification of single bad data or wrong parameters.

When the error bias of a given assumption for a single measurement error or parameter error is assumed to be within ±50% of the error deviation of an error measurement or parameter, based on the MIQP model parameter identification method and the total error drop index method, the successful identification rate of all single measurement error and parameter error simulation examples is shown in Figure 6.

Table 1: Single error identification results with two methods.

Assumed bad data and wrong parameter branch	Total error drop indicator method		Parameter identification based on MIQP model
	Identification result	Maximum total error decline index	Identification result
X1-5	X1-5	580.790	X1-5
X2-3	X2-3	413.616	X2-3
P2-5	P2-5	35.738	P2-5
P2-4	P2-4	33.565	P2-4

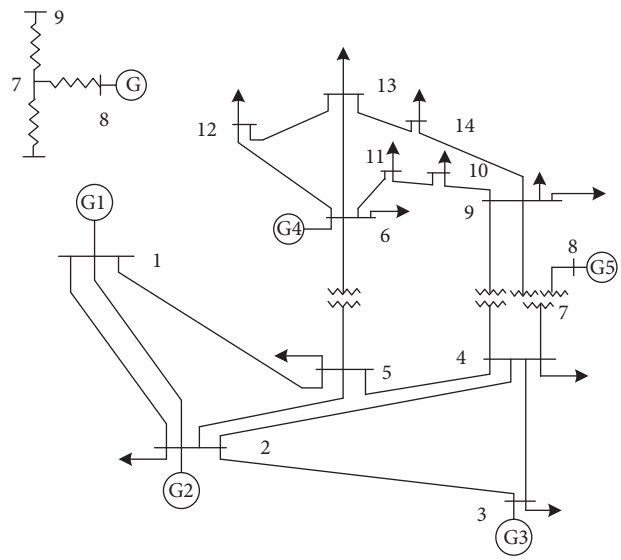

Figure 5: Diagram of IEEE 14-bus test system.

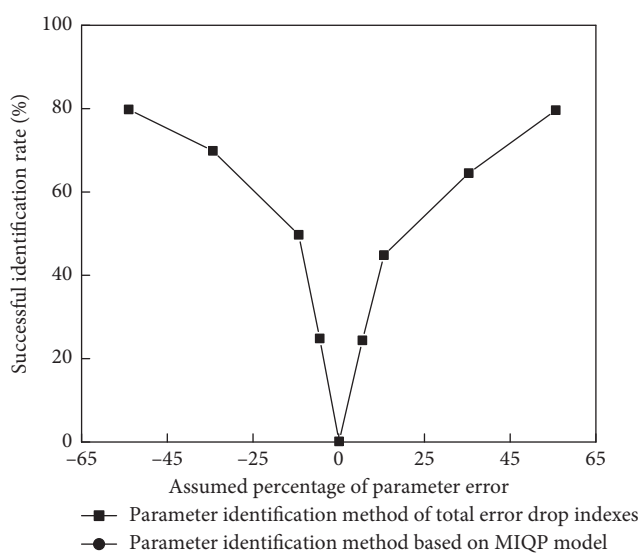

Figure 6: The framework of wireless vision sensor network.

In Figure 6, it is noted that as an increasing percentage error bias is introduced to the assumed error variables, based on the MIQP model parameter identification method and the total error drop index method, the successful identification rate of the single measurement error and the parameter error has been improved obviously. Under the condition of introducing the measurement error and parameter error of ±50%, the successful identification rate of both methods can reach 80%.

Table 2 shows a series of error identification results based on the MIQP model parameter identification method and the total error descent index method for two wrong

Table 2: Two parameter errors at neighbor branches identification results with two methods.

Assumed bad data and wrong parameter branch	Total error drop indicator method			Parameter identification based on MIQP model
	Iteration	Identification result	Maximum total error decline index	Identification result
X1-2	1	X1-5	132.434	X1-2
X1-5	2	X2-3	18.854	X1-5
X2-3	1	X4-5	336.403	X2-3
X2-4	2	X2-3	68.658	X2-4
	3	X2-4	84.561	
X4-7	1	X5-6	35.602	X4-7
X4-9	2	X4-7	6.163	X4-9

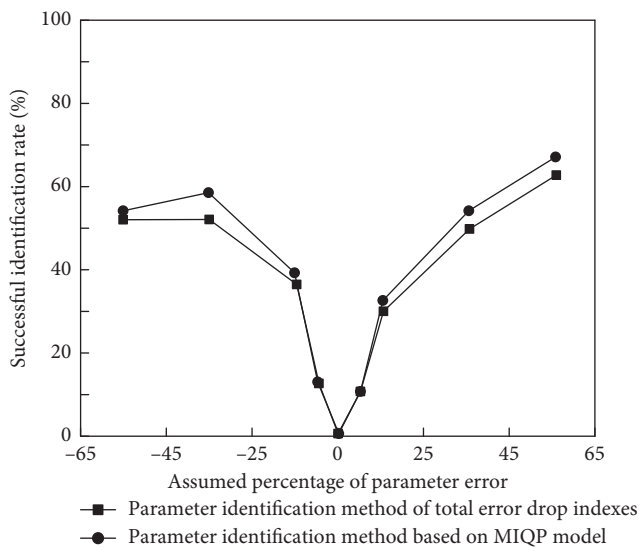

Figure 7: Successful identification rates for a single error with two methods.

Table 3: Results of one parameter and one related measurement error at the same branch.

Assumed bad data and wrong parameter branch	Total error drop indicator method			Parameter identification based on MIQP model
	Iteration	Identification result	Maximum total error decline index	Iteration
X1-2	3	X1-1	162.347	X1-1
P1-5	4	P1-2	18.263	P1-2
X2-4	4	X2-3	191.731	X2-3
P2-4	3	P2-4	20.594	P2-4

parameters of adjacent branches. The percentage error bias introduced by this example is 30% error introduced by line reactance.

When the error bias of the parameter is given and the error deviation of the wrong parameter is assumed to be in the range of ±50%, based on the MIQP model parameter identification method and the total error drop index method, the successful identification rate of two parameter error simulation examples for all adjacent branches is shown in Figure 7.

As shown in Table 3, both methods can accurately identify the parameter error and measurement error of the assumed same path. Moreover, the identification results based on the MIQP model parameter identification method and the total error descent index method are consistent, and both methods can simultaneously identify the parameter errors and the measurement errors of the same branch.

5.3. Comparison of Covert Data Integrity Assaults. The power monitoring system data integrity attack detection accuracy is

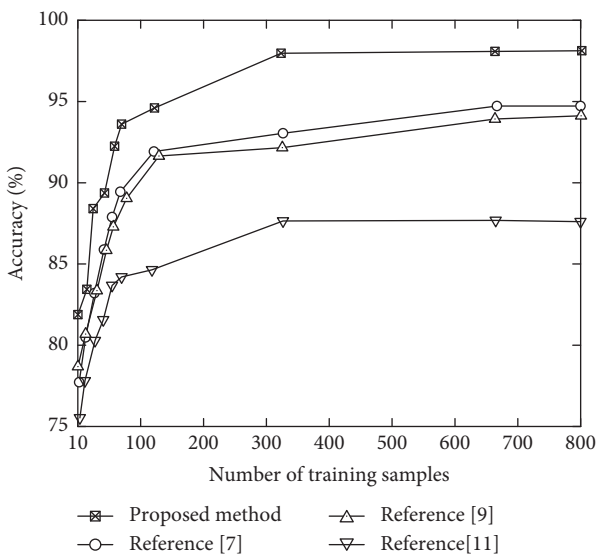

Figure 8: Comparison of covert data integrity assaults.

an important indicator to measure whether the grid data is abnormal or not [28]. The accuracy calculation formula is

$$\text{Accuracy} = \frac{\text{TP} + \text{TN}}{\text{Total Population}}. \tag{12}$$

Among them, a true positive (TP) is a point detected as a positive sample, and a true negative (TN) is a point detected as a negative sample.

In order to verify the performance of the proposed method, compared with the methods proposed in [7, 9, 11], the performance test results are shown in Figure 8.

It can be seen from Figure 8 that the proposed method is superior to other methods in ensuring data security and can achieve higher data anomaly detection accuracy with fewer training samples.

6. Conclusion

Considering the large scale of the power Internet of Things and the large number of measured data and basic parameters of power grid, a parameter identification method based on MIQP and edge computing is proposed. The local state estimation is carried out on the traditional state estimation method, and the estimated value is taken as the parameter input of MIQP model. In the optimization model, the penalty factor is introduced into the parameter error and measurement error, and the optimization objective of minimizing the error is solved to achieve the purpose of parameter identification. At the same time, in the edge computing, a variety of methods are used for security protection to ensure the reliable transmission of data. The algorithm model can not only effectively identify multiple parameter errors and measurement errors in the process of parameter identification but also effectively avoid over-identification in the overall error reduction index method, so that the algorithm has more ideal identification accuracy and network security protection.

However, although the proposed method can improve the efficiency of parameter identification to a great extent, the calculation of the model is more complicated when the power network is large, which leads to the decrease of identification efficiency. Therefore, improving the identification efficiency of the parameter identification method of MIQP model also needs to be studied and analyzed in the future.

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 work was supported by Science and Technology Project of Dongguan Power Supply Bureau of Guangdong Power Grid Co., Ltd. The project name is "Research on Power Grid Operation Situation Perception Based on the Online Real-Time Identification of Power Grid Equivalent Parameters" (no. GDKJXM20162533 (031900KK52160081)).

References

[1] A. C. Luna, N. L. Diaz, M. Graells, J. C. Vasquez, and J. M. Guerrero, "Mixed-integer-linear-programming-based energy management system for hybrid PV-wind-battery microgrids: Modeling, design, and experimental verification," *IEEE Transactions on Power Electronics*, vol. 32, no. 4, pp. 2769–2783, 2017.

[2] O. Gomozov, J. P. Trovao, X. Kestelyn, and M. R. Dubois, "Adaptive energy management system based on a real-time model predictive control with non-uniform sampling time for multiple energy storage electric vehicle," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 7, pp. 5520–5530, 2017.

[3] M. Wieczorek and M. Lewandowski, "A mathematical representation of an energy management strategy for hybrid energy storage system in electric vehicle and real time optimization using a genetic algorithm," *Applied Energy*, vol. 192, no. 7, pp. 222–233, 2019.

[4] L. Xiang, "Energy network dispatch optimization under emergency of local energy shortage with web tool for automatic large group decision-making," *Energy*, vol. 120, no. 9, pp. 740–750, 2017.

[5] Z. Shan, S. Liu, V. K. Sharma, and P. K. Varshney, "Optimal sensor collaboration for parameter tracking using energy harvesting sensors," *IEEE Transactions on Signal Processing*, vol. 66, no. 12, pp. 3339–3353, 2018.

[6] Y. Lin and A. Abur, "Robust security estimation against measurement and network parameter errors," *IEEE Transactions on Power Systems*, vol. 99, no. 2, pp. 57–70, 2019.

[7] A. Ashok, M. Govindarasu, and V. Ajjarapu, "Online detection of stealthy false data injection attacks in power system security estimation," *IEEE Transactions on Smart Grid*, vol. 9, no. 3, pp. 1636–1646, 2018.

[8] Y. Zhao, J. Liu, and L. Zhong, "Structural damage identification based on residual vectors and tree-seed algorithm,"

Acta Scientiarum Naturalium Universitatis Sunyatseni, vol. 56, no. 4, pp. 46–50, 2015.

[9] N. Nusrat, P. Lopatka, and M. R. Irving, "An overlapping zone-based security estimation method for distribution systems," *IEEE Transactions on Smart Grid*, vol. 6, no. 4, pp. 2126–2133, 2019.

[10] R. Deng, G. Xiao, and R. Lu, "Defending against false data injection attacks on power system security estimation," *IEEE Transactions on Industrial Informatics*, vol. 13, no. 1, pp. 198–207, 2017.

[11] M. Khalid, L. Xiong, C. S. Ashraf et al., "Pairing based anonymous and secure key agreement protocol for smart grid edge computing infrastructure," *Future Generation Computer Systems*, vol. 88, no. 4, pp. 491–500, 2018.

[12] J. Luo, L. Yin, J. Hu et al., "Container-based fog computing architecture and energy-balancing scheduling algorithm for energy IoT," *Future Generation Computer Systems*, vol. 97, no. 5, pp. 50–60, 2019.

[13] M. D. R. De Pinho and I. Shvartsman, "Lipschitz continuity of optimal control and Lagrange multipliers in a problem with mixed and pure state constraints," *Discrete & Continuous Dynamical Systems - Series A (DCDS-A)*, vol. 29, no. 2, pp. 505–522, 2018.

[14] K. S. Wong and M. H. Kim, "Emerging issues and challenges for cloud data at the edge," *International Journal of Web & Grid Services*, vol. 14, no. 2, pp. 123–145, 2018.

[15] Z. Sheng, S. Pfersich, A. Eldridge, J. Zhou, D. Tian, and V. C. M. Leung, "Wireless acoustic sensor networks and edge computing for rapid acoustic monitoring," *IEEE/CAA Journal of Automatica Sinica*, vol. 6, no. 1, pp. 64–74, 2019.

[16] X. Lai, H. Zhong, Q. Xia, and C. Kang, "Decentralized intraday generation scheduling for multiarea power systems via dynamic multiplier-based Lagrangian relaxation," *IEEE Transactions on Power Systems*, vol. 32, no. 1, pp. 454–463, 2017.

[17] C. Wang, Z. Wang, J. Wang, and D. Zhao, "Robust time-varying parameter identification for composite load modeling," *IEEE Transactions on Smart Grid*, vol. 10, no. 1, pp. 967–979, 2019.

[18] U. N. Okorafor and D. Kundur, "Security-aware routing and localization for a directional mission critical network," *IEEE Journal on Selected Areas in Communications*, vol. 28, no. 5, pp. 664–676, 2010.

[19] J. Chen, C. Liu, T. Wang, X. Wu, and H. Wang, "Influence of phasor measurement error on parameter identification for a synchronous generator," *Electric Power Components & Systems*, vol. 46, no. 11, pp. 1364–1374, 2018.

[20] Z. Zhang, B. Pan, M. Grediac, and W. Song, "Accuracy-enhanced constitutive parameter identification using virtual fields method and special stereo-digital image correlation," *Optics and Lasers in Engineering*, vol. 103, no. 5, pp. 55–64, 2018.

[21] J. Zhao, M. Netto, and L. Mili, "A robust iterated extended kalman filter for power system dynamic security estimation," *IEEE Transactions on Power Systems*, vol. 32, no. 4, pp. 3205–3216, 2017.

[22] R. Deng, G. Xiao, and R. Lu, "Defending against false data injection attacks on power system security estimation," *IEEE Transactions on Industrial Informatics*, vol. 13, no. 1, pp. 198–207, 2020.

[23] W. Jian, L. Zhu, Z. Xu, and X. Chen, "A variable selection method for soft sensor development through mixed integer quadratic programming," *Chemometrics & Intelligent Laboratory Systems*, vol. 167, no. 8, pp. 85–95, 2019.

[24] Y. Zhao and S. Liu, "Global optimization algorithm for mixed integer quadratically constrained quadratic program," *Journal of Computational & Applied Mathematics*, vol. 319, no. 6, pp. 159–169, 2017.

[25] Y. Wang, C. Lu, and X. Zhang, "Applicability comparison of different algorithms for ambient signal based load model parameter identification," *International Journal of Electrical Power & Energy Systems*, vol. 111, no. 17, pp. 382–389, 2019.

[26] Z. Wang, S. C. Fang, and F. D. Y. Gao, "Global extremal conditions for multi-integer quadratic programming," *Journal of Industrial & Management Optimization*, vol. 4, no. 2, pp. 213–225, 2017.

[27] C. Lyu, J. Song, J. Zheng et al., "In situ monitoring of lithium-ion battery degradation using an electrochemical model," *Applied Energy*, vol. 250, no. 1, pp. 685–696, 2019.

[28] F. Z. Ouaïl and M. E.-A. Chergui, "A branch-and-cut technique to solve multiobjective integer quadratic programming problems," *Annals of Operations Research*, vol. 267, no. 2, pp. 431–446, 2017.