İSTANBUL UNIVERSITY CERRAHPAŞA

ORIGINAL ARTICLE
Electrica 2023; 23(3): 466-474

Security Protection Technology Based on Power Communication Terminal Intelligent Equipment

Danni Liu[1], Mingming Zhao[2], Shengda Wang[1], Xiaofu Sun[1], Haoran Sun[1]

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

Cite this article as: D. Liu, M. Zhao, S. Wang, X. Sun and H. Sun, "Security protection technology based on power communication terminal intelligent equipment," *Electrica*, 23(3), 466-474, 2023.

ABSTRACT

The aim of this study was to study the security problems faced by an Radio Frequency Identification (RFID) system in the whole process management of intelligent power distribution system equipment. Based on information security risks, the defects are analyzed, and how to protect distributed energy stations from information security threats in the energy Internet environment is discussed. This paper analyzes the new business communication requirements of distribution communication network and the security risks. The results are as follows: in the classification accuracy experiment, the accuracy of all kinds of classification is obtained through three algorithms [DAG-SVM based on minimum coupling degree, DAG-SVM based on maximum separability, and double-decision hyperplane (DDH)]. Among them, the accuracy of the optimized DDH algorithm in this paper is 98.65%, which is the highest of the three, and the time is the shortest, saving about 40%. A security protocol is proposed which has good protection against several attacks. Deep neural network was used to mine the power terminal attack by means of feature engineering and data enhancement, and the network-level security monitoring of power terminals is realized. The feasibility of the proposed method is verified by building a physical simulation platform, and the experimental results show that the proposed strategy can improve the security of power terminals.
***Index Terms*—**Intelligent power distribution equipment, power distribution communication network, safety protection.

I. INTRODUCTION

The smart grid is the second generation of the power network which continues to develop in the course of intelligence and automation. Continuous improvements are made to the energy conversion rate, power usage rate, and energy supply quality. However, at the same time, for smart electricity, the Internet faces many new security challenges. The power terminal is essential to the smart grid because it manages the generation, monitoring, and controlling of electricity. Therefore, in the smart grid security, the most critical is to confirm the safety of power stations. The existing solutions are generally carried out by monitoring the flow of power terminals. But, such security measures can only identify attackers that have characteristic properties at the traffic layer. Considering this, a deep learning-based power terminal safety monitoring technology is proposed, which aims at power generation. The device and network levels of terminals provide all-round protection for power terminals.

With the development of computer technology, compared to traditional industrial control systems, information technology, big data technology, artificial intelligence technology, and industrial automation technology have shown better performance resulting in continuous intelligence of infrastructure. The widespread application of information technology in the field of industrial control poses new challenges to traditional industrial control systems.

The control system of the electric power industry is to support the production of power in various links such as distribution, transmission, variation, distribution, use, and dispatch. Operational control is an integral part of the country's critical infrastructure and not only covers power monitoring system (including dispatch, power plant, substation, and distribution automation system) but also involves the user side and distributed power supply. The electricity information collection and other systems in the open environment, once damaged, may affect the country's home and social security. With the widespread use of information technology and the establishment and evolution of domestic and international security frameworks, the security threats of industrial

Corresponding author:
Danni Liu

E-mail:
liudanni5@163.com

Received: July 10, 2022

Accepted: January 11, 2023

Publication Date: July 7, 2023

DOI: 10.5152/electr.2023.22119

control systems cannot be ignored. The security threat of industrial control system cannot be ignored. Many blackouts in the world are initiated by cyberattacks. The accident has rung the alarm bell for us. It is urgent to improve the safety performance of the power grid in all directions. In addition to common security issues in the power grid, network information security incidents have occurred in domestic and foreign power enterprises one after another. In addition, there are many cases in which the normal process of the power grid is disrupted through cyberattacks. The power outage accidents caused by cyberattacks have been on the rise in recent years.

Smart grid is a new modern power grid that integrates cutting-edge energy and power technology, information and communication technology, analysis and decision-making technology, automatic control technology, and advanced sensing and measurement technology. Power grid infrastructure is also heavily integrated [1]. With the wide application of various advanced technologies in power grid, smart grid has become the inevitable trend of the development and reform of power system in the world. It takes the power system including power generation, transmission, transformation, distribution, power consumption, and dispatching as the object; highly integrates the new technologies of power, information, and automation; and realizes the intelligent exchange of information. As a key platform and important means to support the creation of smart grid, communication scheme will always run through the six-application links and play a vital role [2]. Smart distribution grid is the last link in the operation of smart grid, and it is also a key link. Power distribution communication network is an important part of the distribution grid and the infrastructure for building a smart grid. The power distribution communication network connects terminal power users, various distribution equipment, and power consumption equipment. It is essential to ensuring the availability of a consistent supply of energy, enhancing the operation efficiency of the power grid, and providing high-quality services to users. Due to social development, historical origin, and other reasons, the development degree of distribution automation in China is significantly lower than that in developed countries, and there is still a certain gap with the international advanced level in power supply quality [3]. Relevant investigations show that more than 95% of power outages are caused by the failure of distribution network to solve in time, resulting in nearly half of the power loss. Therefore, in order to achieve the goal of building a "strong" smart grid, we must attach great importance to the construction of a distribution power grid, especially the construction of a distribution power communication network as the basic guarantee of a distribution power grid [4].

The primary distinction between the traditional energy information network and the energy Internet information communication, when viewed from the perspective of the energy Internet's composition and commercial scenarios, is found in the areas of business application mobilization and renewable energy automation data access. In recent years, specialists and academics domestically and abroad have paid more and more attention to the research of power distribution and consumption communication network, and some key technologies have also made significant achievements. However, at present, the research on intelligent power distribution communication network in various countries mainly focuses on the power distribution communication network architecture, Guqian network guarantee mechanism, access network optimization mode, and the application of new communication technology, and there is relatively little research on the service quality provided by the power distribution communication network for power distribution automation, dispatching telephone and other power distribution information services [5]. The traditional power distribution terminal equipment management adopts bar code technology, which has low identification efficiency and needs to be read manually in close distance. It is unable to identify multiple terminals at the same time, and the labels cannot be reused, resulting in imperfect equipment information detection, high storage management cost, and lack of effective online control for operation and maintenance. As one of the most promising technologies in the Internet of Things, RFID technology has the advantages of anti-electromagnetic interference, batch identification of multiple terminals, and long identification distance. It is very suitable for the whole process management of large quantities of terminal equipment. However, because RFID technology adopts wireless communication technology, it not only is fast and convenient for the whole process management of power distribution terminal equipment but also brings information security protection problems such as security authentication, identity trust, and data confidentiality [6, 7].

Therefore, it is urgent to formulate a security protection authentication scheme to ensure the information security of power distribution terminal equipment on the basis of studying the specific application of RFID in the whole process management of power distribution terminal equipment. In this way, the safety protection level of the power distribution and consumption communication network can be improved from the fundamental equipment level to ensure the safe and stable operation of the power distribution and consumption system, the safety and reliability of business data, and the safety of user's power consumption, as depicted in Fig. 1. Based on the above examination, this study presents the service quality evaluation algorithm suitable for power distribution communication network and the access control mechanism for intelligent power distribution equipment on the basis of analyzing the business requirements and network security risks of power distribution communication network. Thus, it provides an important basis for improving the service quality of the power distribution communication network, realizing the real-time monitoring of the status information of the power distribution terminal equipment, ensuring the normal

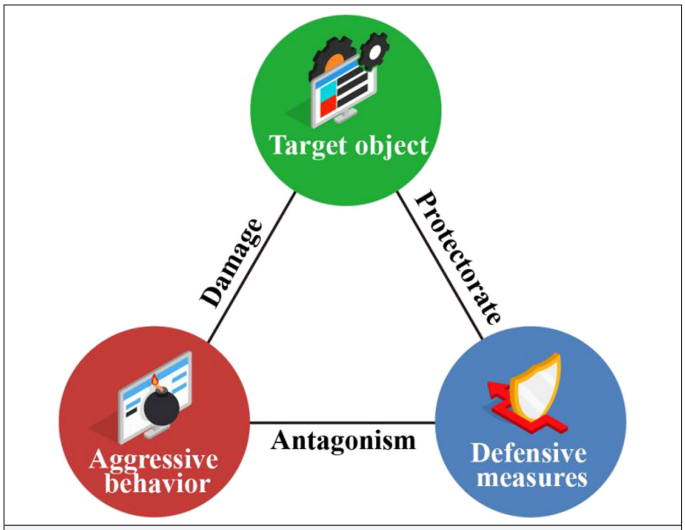


Fig. 1. Research and implementation of safety protection technology.

operation and rapid recovery after failure of power distribution terminal equipment, and ensuring the safe and stable operation of the power distribution system [8, 9].

II. LITERATURE REVIEW

In the smart grid's commercial system, there are numerous power terminal devices. For data acquisition in smart grid, the Set and Monitoring Control System (SCADA) is used to keep an eye on and manage the power terminal machinery in operation equipment telemetry, remote communication, remote control, and remote adjustment, namely "four remote." The remote terminal unit (RTU) and feedline terminal unit are essential parts of the SCADA system, among which the RTU is a characteristic embedded system, positioned in the substation equipment remote device. It is mostly accountable for assembling equipment electricity measure parameters and it communicates with the master station and responds to the master station's request. Many local and international academics are currently working on power terminal protection in order to enhance the safety performance of power terminals. The power station safety evaluation model is built, and the hardware security and network security of the power terminal are analyzed. According to international information security risk assessment regulations, the overall, system, application, and management security are evaluated. In the literature, evaluating the security of power terminals can guide us to provide more reasonable protection for power terminals with higher risk after evaluation, and allocate resources reasonably in the power grid to to improve the defense efficiency of power terminals.

Intelligent power distribution and consumption communication system is an important part of smart grid construction. It collects, processes, and monitors the information of power distribution equipment and user terminals in real time. The business provided involves the vital interests of power users. In order to ensure the security and integrity of information, advanced Internet of Things technology is required to monitor the status of power distribution and consumption terminal equipment in real time to ensure the high reliability of power distribution and consumption terminal equipment [10]. In addition, for the power consumption information acquisition system, the ultimate goal of the smart grid is to realize the two-way real-time interaction between users and the power grid. Users can view the real-time power consumption information through the smart meter so as to better plan their own power consumption, cooperate with the power company to optimize the allocation of power resources, and realize the high efficiency and energy saving of the power grid [11]. The combination of RFID tag and smart meter electric energy information acquisition and storage module can realize the synchronous acquisition of a large number of equipment information status and user power consumption information and provide data guarantee for the real-time interaction between users and power grid [12].

A. RFID System Security Authentication Protocol

Most of the authentication protocols in the RFID system are identity authentication protocols, which are used to test the legitimacy of

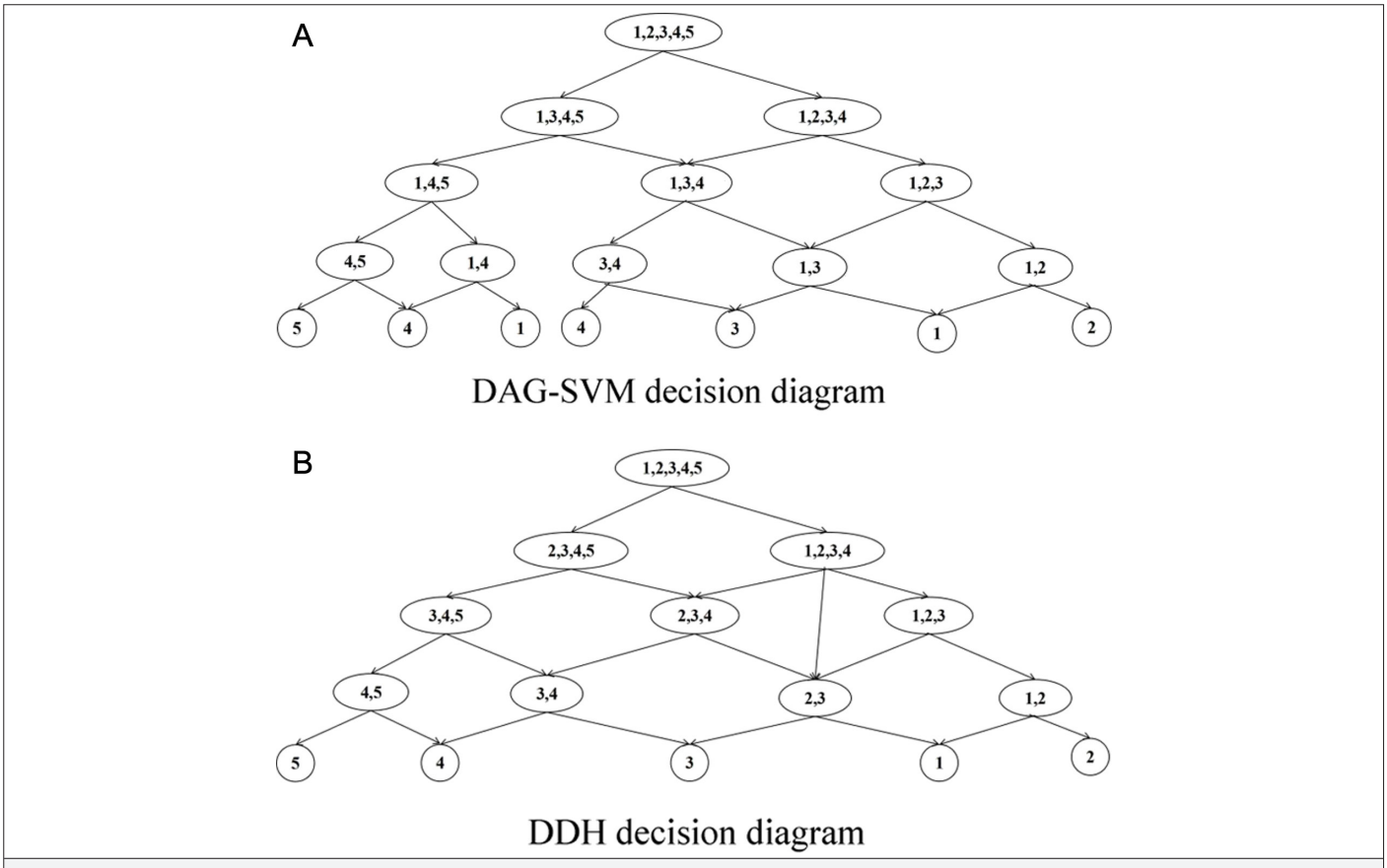


Fig. 2(a) and Fig. 2(b). Comparison between DAG-SVM and DDH decision diagram. (a) DAG-SVM decision diagram and (b) DDH decision diagram.

the identity of the two conversation entities. According to different authentication and RFID access control protocols [13], access control mainly solves the authentication of tags to readers, ensuring that only authorized and legal readers can read and modify tag information, so as to prevent the leakage of tag content; tag authentication is the process that the tag proves its legal identity to the background database or reader, that is, the reader authenticates the tag identity. Authentication key exchange protocol is generally the secret information established and shared by both parties (between the reader and a single tag) or multiple parties (between the reader and multiple tags). Symmetric encryption algorithm can be used in the protocol. The authentication between the reader and the tag is based on the two-way authentication protocol.

At present, the research on the RFID system security authentication protocol and related encryption algorithms at home and abroad has achieved fruitful results [14]. After analyzing the types of information security risks faced by RFID in power grid application, the existing security protection schemes are analyzed and compared from the aspects of anti-attack ability, protocol storage, and protocol communication times; in addition, using the random sequence stored in the tag to ensure the freshness of authentication information can effectively resist a variety of attacks, but the protocol cannot authenticate the identity of the reader and writer, and the security of the protocol is directly proportional to the length of the random sequence. It is not suitable for low-cost tags with limited storage capacity. Different messages in the protocol are also highly correlated, which is easy to cause information exposure. In order to resolve the discussed problem, researchers propose a security authentication protocol based on the synchronous update of random numbers. In the protocol, random numbers can not only be used for tag identity authentication but also be used as private keys to encrypt interactive messages, which increases the difficulty of message identification. However, the protocol is complex and is not suitable for low-cost passive tags [15].

A. RFID Security Authentication Protocol in Power Communication Network

Although the research results of security authentication protocols applied to the RFID system are rich at this stage, not all RFID security authentication protocols can be applied to the security protection requirements of power system due to the industry particularity of the power system itself. At this stage, the research on this aspect is also in its infancy, and most protocols only make some changes to the existing RFID security authentication algorithm, and the effect in practical application is still not ideal [16, 17].

There are still many instances of stations for distributing energy linked to the distribution network where automatic dispatching and monitoring of the connection to the grid has not been accomplished. There are still issues with automatic data exchange, and there are security threats associated with the grid's secure and stable operation. The security of mobile application information interaction is a major issue in the energy Internet information communication linked to business application mobilization. Information security is a critical concern related to the security of transaction funds and the operation of equipment. Examples include information searches, distributed power transactions, demand response, smart home control, and paying electricity bills via a mobile terminal.

TABLE I. EFFICIENCY AND ACCURACY OF THREE MULTICLASSIFICATION METHODS

	Classification Accuracy	Average Time Required for QoS Determination of a Single Service (ms)
DAG-SVM based on minimum coupling degree	98.41%	42.2784
DAG-SVM based on maximum separability	96.96%	42.0015
DDH ($t_2 = 0.75$)	98.64%	28.3124

III. RESEARCH METHODS

Side channel information refers to the operational information of various things related to the operating status of electronic devices, which is widely used for device status monitoring. In this paper, the side channel information of the terminal is analyzed and collected, and the equipment-level safety monitoring method of the power terminal is realized. In reference, information related to the operation content and running status of the equipment will be leaked in various ways.

The author proposed that we can realize the operation of the power equipment by analyzing the equipment bypass information. The author proposes utilizing the advantages of television, where the bypass signal of the device can determine the current display content of the television. In the field of security, a large number of scholars have also implemented a series of security monitoring technologies by exploring device bypass information. The author proposes a method for integrating hardware trojans in circuits using power equipment for side information detection, which has been experimentally verified to be effective in deteching hardware trojans in FPGA chips. Previous work has clarified that edge channel analysis can be used to analyze the interior of electronic devices. Meanwhile, side channel analysis has good characteristics of noninvasive and high robustness. Based on the requirement of power terminal security monitoring, we design the power terminal security based on side channel information. "Based on the requirement of power terminal security monitoring, we design the power terminal security based on side channel information. Full monitoring module, to achieve the power terminal equipment-level safety monitoring." should be"According to the requirements of power terminal security monitoring, we have designed a power terminal security monitoring module based on side channel information to achieve device level security monitoring of power terminals."

In order to solve the problems of lack of objectivity and low evaluation efficiency of traditional service quality QoS evaluation algorithms, this paper maps service QoS evaluation to service QoS level classification and proposes a real-time QoS evaluation method of power communication network service based on double-decision hyperplane (DDH) decision graph. This method extracts the characteristics of the service network layer to represent the service quality of the service, takes the existing service with known QoS level as the training sample of the classifier, and determines the formation of the decision graph by the construction order of the decision hyperplane [18]. In addition, the algorithm provides a new definition of the traditional inter class coupling and constructs DDH sequentially based on the principle of minimum inter class coupling at each layer of the decision graph to achieve incomplete classification of three QoS levels. Avoiding issues such as "error collapse" of low-level nodes, low adaptability of decision

TABLE II. SECURITY ANALYSIS OF RFID PROTOCOL

Program	Authentication	Retransmission Attack	Fake Attack	Tamper Attack	Blocking Attack	Permission Restrictions
The protocol proposed in this paper	Have	P	P	P	P	P
RFID authentication protocol based on key array	Have	P	P	P	O	O
RFID security protocol based on random sequence	Have R->T	P	T(P)R(O)	P	O	O

graphs, and fixed structure in traditional multi classification decision graphs [19].

A. Interclass Coupling

When constructing the decision hyperplane of each level of multi classification, it is necessary to adopt certain criteria to measure the distance between classes and separate the two classes with the best separability first, so as to reduce the classification error rate as much as possible. The separation degree between classes is usually used to ensure that the class interval at each decision node is as large as possible. The so-called degree of separation between classes is a measure of the degree of separability between classes. The greater the degree of separation, the easier it is to separate the two classes. The degree of separation between class i and class j is defined in (1):

$$s_{ij} = \frac{d_{ij}}{\sigma_i + \sigma_j} \tag{1}$$

where $d_{ij} = c_i - c_j$ represents the center distance between class i and class j, c_i and c_j are the sample centers of class i and class j, respectively, and i and j are the standard deviation of class i and class j, respectively. Class center distance reflects the distribution of samples between classes, and class variance reflects the distribution of samples within classes [20].

In order to solve the problems of low adaptability and fixed structure of decision graph, a new concept of coupling degree between classes is proposed in this paper. When calculating the distance between classes, the sample points near the class boundary are used as much as possible, and the other sample points are eliminated, so that the sample points used to construct hyperplane are consistent with the actual support vector to a great extent, so as to reduce the training time. Suppose that class i in the training set contains B training samples, $\boldsymbol{x}_i = \left\{x_i^1, x_i^2, x_i^3, \ldots, x_i^{M_i}\right\}$, and class j contains M_j training samples, $\boldsymbol{x}_j = \left\{x_j^1, x_j^2, x_j^3, \ldots, x_j^{M_j}\right\}$. The specific calculation method of coupling degree O_{ij} between classes is as follows (2):

TABLE III. COMPARISON OF EXPERIMENTAL OUTCOMES WITH STATE-OF-ART TECHNIQUES

Specification	Efficiency	Protection
Test outcomes	1 day	>92%
Previous outcomes	>15 days	<65%
Improvement	>100%	>55%

1. The sample centers of class i and class j are c_i and c_j, respectively; class center distance $d_{ij} = c_i - c_j$;
2. The distance $d_{ij}^m = x_i^m - c_j$, $1 \le m \le M_i$ between the sample m in class i and the center of class j, if $d_{ij}^m \ge d_{ij}$, eliminates the sample m in class I, $x_i = x_i - \left\{x_i^m\right\}$, and screen the samples in class j are also screend in the same way;
3. After screening (as mentioned in step 2), the number of class i samples is reduced to P_i and the number of class j samples is reduced to P_j. The average distance between P_i samples and P_j samples is calculated. The reciprocal of the average distance is defined as the coupling degree between classes. The smaller the value, the weaker the coupling degree between classes and the larger the absolute distance between classes, which is more conducive to the construction of the best hyperplane.

$$O_{ij} = \frac{P_i P_j}{\sum_{m=1}^{P_i}\sum_{n=1}^{P_j} x_i^m - x_j^n} \tag{2}$$

where $m = 1,2\ldots P_i$, $n = 1,2\ldots P_j$。

1) QoS level determination

For the service to be evaluated, its feature vector is x; then the QoS evaluation process of the service first uses the first layer SMV_{14} classification at the root node of the DDH decision graph. The distance from X to hyperplane $G(x) = 0$ can be expressed in (3):

$$d = \sum_{i=1}^{k} \alpha_i y_i K\left(x_i \cdot x\right) + b \tag{3}$$

d is defined as the decision distance, which can be positive or negative, which represents the current QoS level of the service. The specific judgment method is as follows:

1. If $d \le t_1$, it means that x belongs to non-4, that is, the service QoS belongs to one of 1, 2, and 3; then, the next step is to execute SMV_{13} on the left side of layer 2;
2. If $d \ge t_2$, it means that x belongs to non-1, that is, the service QoS belongs to one of 2, 3, and 4; then, the next step is to execute SMV_{24} on the right side of layer 2;
3. If t_1 d t_2, it means that x belongs to non-1 and non-4 categories, that is, the service QoS belongs to one of categories 2 and 3; then, the next step is to implement layer 3 SMV_{23};
4. In the new decision layer, repeat the process mentioned in 1, 2, and 3 until the lowest node determines the category of service QoS, and the level determination process ends.

B. Classification Decision

Based on the DAG-SVM with the maximum separability between classes, the decision hyperplane is constructed layer by layer to form a directed acyclic graph structure. As shown in Fig. 2(a), because the SVM is a binary classification, each service needs to make four QoS level decisions, the average number of decision hyperplanes to be traversed is large, the evaluation efficiency is relatively low, and the evaluation accuracy is not high; The DDH proposed in this paper constructs the decision hyperplane layer by layer according to the minimum coupling degree between classes. As shown in Fig. 2(b), due to the incomplete three classification of SVM, there is cross-layer direct division. Each service can determine the QoS level at most four times and at least two times. The average number of decision hyperplanes to be traversed is greatly reduced, which has high evaluation efficiency and accuracy.

Classification accuracy is an important index to measure the performance of classifier. In this paper, there are two definitions of classification accuracy under different circumstances. For the test business sample set, the classification accuracy is defined as:

Classification accuracy = number of correctly classified services/total number of tested services

The classification accuracy of a certain category in the test sample is defined as:

Classification accuracy = the number of test services correctly classified as class/the total number of class i services in the test sample

C. Application of RFID

RFID is a wireless communication technology, which can automatically identify equipment information and obtain relevant data in a non-contact way and realize the terminal state at any time. RFID electronic tag has the advantages of long service life, large storage capacity, anti-electromagnetic interference, easy embedding into equipment, multibatch identification, long identification distance, and so on. The introduction of RFID system in the management of power distribution equipment, writing the information of power distribution equipment into the RFID tag, and using RFID identifier supporting wireless data communication to manage power distribution equipment can greatly improve work efficiency, save labor cost, and avoid various errors in manual inventory so that power enterprises can more accurately grasp the stock, distribution, and maintenance of power distribution equipment, effectively improve the management level of various power distribution equipment, and reduce operation and management risks.

IV. RESULT ANALYSIS

There are four types of attacks against DTU: 1) attacks on the DTU distribution switch, (2) the information gathering assault, (3) the DTU monitoring route, and (4) the DTU overload attack all blow. The DTU distribution switch attack refers to the continuous on–off and on–off operation of the DTU control distribution switch which affects the stability of the power grid and at the same time reduces the service life of power switch. The information gathering effort refers to the significantly increased frequency of DTU collecting. The frequency of the detecting mechanism is not altered by the DTU information that is uploaded to the distribution automation's master station and substation. DTU monitoring routing attacks are a way to reduce monitoring. For example, this attack can reduce the initial eight monitoring channels to two, and significantly reduce the amount of data collected and communicated, thereby affecting power usage. The DTU overload attack increases the amount of computing in the DTU, making it impossible for legitimate services to get fast responses. This is similar to how a Disk Operating System (DoS) attack works.

A. Classification Accuracy

In the DDH decision graph method, the value of decision distance determines the proportion of directly dividing the third class across layers. The larger its absolute value is, the more samples will be divided directly across layers, resulting in the shortening of training time. However, if the value is too large, the first and second types of points will be mistaken for points that can be directly divided across layers, resulting in the decline of classification accuracy. For simplicity, in the case of the above samples, the classification time is short and the accuracy is high when it is found through multiple training. The accuracy rates of various types obtained by three algorithms (DAG-SVM based on minimum coupling degree, DAG-SVM based on maximum separability, and DDH) are shown in Fig. 3. The average time and total accuracy required for single service QoS level judgment are shown in Table I. The simulation results show that the DDH algorithm based on incomplete three classification is better than DAG-SVM in classification performance. This is because the number of SVM traversed by a large part of samples is less than 4, which greatly reduces the time required for decision. Moreover, due to the reduction of the number of SVM traversed and the appropriate selection of parameters 1 and *N*, the number of possible misclassification is reduced under the condition of ensuring the correct classification basis so that the overall classification performance is better improved.

B. Safety Simulation Experiment

In the intelligent power distribution system, RFID protocol vulnerabilities are generally divided into security vulnerabilities and privacy vulnerabilities. Security vulnerabilities mainly refer to those vulnerabilities that attackers can use to pass identity authentication or destroy the normal authentication of power distribution and consumption equipment. Privacy vulnerabilities mainly refers to authentication protocols that leak the privacy information of distribution

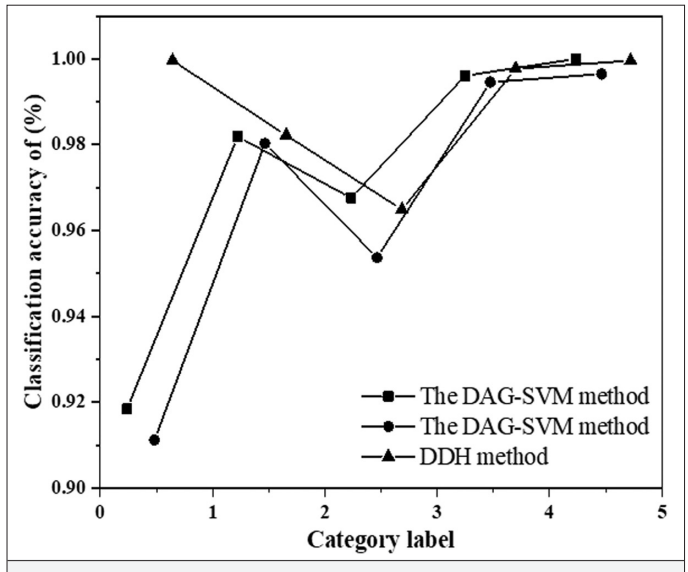


Fig. 3. Classification accuracy of three methods for each category.

equipment. Then, the attacker can obtain the device status information stored on the distribution equipment label from the communication content between the label and the identifier, thereby forging the device label to entering the system for planned attacks. The comparison between this protocol and other existing RFID security protocols in terms of identity authentication ability and resistance to various attacks is shown in Table II, where P and O, respectively, represent whether the protocol can resist such attacks or not. It can be seen from Table II that the security protocol proposed in this paper has good protection against various attacks. This paper proposes an equipment-level power terminal security protection method based on side channel. The side channel information of power terminals is collected, and Long Short-Term Memory (LSTM) neural network is used to connect the side channel timing information with power terminals. The working state is mapped to realize equipment-level safety monitoring of power terminals. This method has good accuracy, and it can realize the safety monitoring of power terminal as well. This paper proposes a deep learning-based network-level power terminal security protection method, which can be successfully implemented. Data mining and feature extraction are carried out on the communication packets of power terminals, and neural networks are generated based on adversarial methods. Data enhancement method is carried out to realize network-level security monitoring of power terminals.

This work establishes a side channel-based equipment-level security protection technique for the DTU security monitoring simulation platform. The experimental results demonstrate that this approach can precisely identify the DTU's aberrant status.

1. In terms of power terminal security monitoring methods, this study conducts channel acquisition and analysis of the power consumption of TN power terminal equipment, which can achieve non-invasive security monitoring of power terminals. In the practical applications of power terminals, there are also many other types of side channel information that we can monitor. Further, the accuracy of the equipment-level power terminal safety monitoring method is improved.
2. In terms of the equipment-level power terminal safety monitoring method, this paper realizes the work through the power terminal equipment. However, the intrinsic mathematical mechanism of this method needs to be further studied.
3. For power terminal safety monitoring method at the network level, we proceed through the power terminal data message. The safety monitoring of power terminals is made possible through data mining and feature extraction, and the model performs well. However, the safety monitoring model based on deep neural network will bring a lot of computation to the safety monitoring system. How to reduce these costs remains to be further studied.

Research into various information security protection and network attack technologies has steadily revealed a number of problems with the control system network, and the information security test in the actual control system environment will lead to specific destructions. Due to the special nature of some control and information systems, testing them in a real environment could cause the fundamental functions of those systems' control systems to become unavailable. The distributed energy station control system's security test should not interfere with the system's normal operation in order to prevent losses. Based on this technique, we are able to introduce data instances. Table III shows how the implementation of our new solution considerably improved process efficiency as well as security, and various data instances are introduced as a result of this strategy.

The following summarizes the present situation of the distributed energy in China utilizing natural gas as fuel: numerous distributed heating, electricity, and cooling projects using oil and gas as fuel are currently in use in Beijing, Shanghai, Guangzhou, and other cities around China. The economy, ecology, and society have all clearly benefited from these developments. The "developing energy industry development plan" has also gone through several adjustments and is now finished. The cumulative direct investment will increase by up to 5 trillion yuan throughout the planned period (2011–2020), according to Jiang Bing, director of planning and development at the National Energy Administration. The strategy gives legislative suggestions for the use of clean coal, smart grid, distributed energy, new energy for cars, and other technologies in the commercial sector, directly encouraging the investment boom in distributed energy in China.

V. CONCLUSION

Based on the analysis of the overall architecture and communication technology of intelligent distribution communication network, this paper analyzes and summarizes the current business requirements and new business communication requirements of distribution communication network and analyzes the security risks faced by intelligent distribution communication network from the application layer, network layer, and terminal equipment layer. Then, from the perspective of service quality evaluation and terminal equipment security in network security protection, this paper focuses on the service quality evaluation algorithm of power distribution communication network and the access control protocol algorithm of power distribution terminal. The service quality evaluation algorithm based on radar chart is proposed, which is oriented to the real-time QoS evaluation mechanism of mass DDH service and the access control protocol for distribution and consumption equipment. The specific work is as follows:

1. Aiming at the disadvantage that the traditional service QoS algorithm is difficult to extract the disadvantage index, it provides a basis for more reasonable reflection of the operation quality of the distribution grid service so as to better optimize the routing and improve the network structure and service topology;
2. The real-time QoS evaluation mechanism of power distribution network based on Distributed Denial of Service (DDoS) service quality is proposed to meet the requirements of power distribution network real-time communication;
3. Aiming at the specific application of the RFID system in the information security of intelligent power distribution system and the whole process management of equipment, an access control protocol for intelligent power distribution equipment is proposed to realize that the identifier has the authority to operate the equipment information. The distributed energy station information security analysis is the foundation of the energy under the Internet environment. The control system for distributed energy stations is examined in this research. The information security system's security danger is carefully examined, and the associated security measures are suggested. Specific safety measures should be applied to practice projects, which will serve as a direction indicator for future developments.

Peer-review: Externally peer-reviewed.

Author Contributions: Concept – D.L.; Design – M.Z.; Supervision – S.W.; Funding – X.S.; Materials – S.W.; Data Collection and/or Processing – M.Z.; Analysis and/or Interpretation – H.S.; Literature Review – D.L.; Writing – H.S.; Critical Review – X.S.

Declaration of Interests: The authors have no conflicts of interest to declare.

Funding: This work 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).

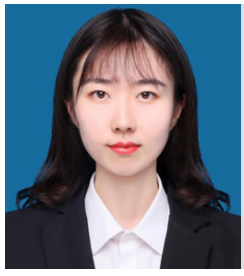
REFERENCES

1. R. V. Yohanandhan, R. M. Elavarasan, R. Pugazhendhi, M. Premkumar, L. Mihet-Popa, and V. Terzija, "A holistic review on cyber-physical power system (cpps) testbeds for secure and sustainable electric power grid – part – ii: classification, overview and assessment of cpps testbeds," *Inte. J. Elect, Power & Ener. Sys.*, vol. 136, p. 107718, 2022.
2. Y. Shao, Y. Wang, Y. Yang, and X. Wang, "Research on a secure communication protocol based on national secret sm2 algorithm," *J. Comput. Commun.*, vol. 10, no. 1, p. 42–56, 2022. [CrossRef]
3. Y. Ge, G. Liu, G. Zhao, H. Liu, and J. Sun, "Observer-based h ∞ load frequency control for networked power systems with limited communications and probabilistic cyber attacks," *Energies*, vol. 15, no. 12, 2022. [CrossRef]
4. A. Guisasola, A. Cortés, J. Cejudo, A. da Silva, M. Losada, and P. Bustamante, "Reliable and low-power communications system based on IR-UWB for offshore wind turbines," *Electronics*, vol. 11, no. 4, p. 570, 2022. [CrossRef]
5. A. Riaz, and V. K. Sharma, "Performance comparison for finfet nanoscale static and domino logic circuits," *Int. J. Nanosci.*, vol. 21, no. 2, 2022. [CrossRef]
6. F. Deng, P. Mattavelli, and X. Zhang, "A distributed current sharing strategy for islanded ac microgrids based on low-bandwidth communication," *Electr. Power Syst. Res.*, vol. 206, p. 107777, 2022. [CrossRef]
7. K. U. Binu, S. J. Mija, and E. P. Cheriyan, "Nonlinear analysis and estimation of the domain of attraction for a droop controlled microgrid system," *Electr. Power Syst. Res.*, vol. 204, p. 107712, 2022. [CrossRef]
8. D. Asardag, and K. Donders, "C'est quoi post-truth," *Int. Commun. Gaz.*, vol. 84, no. 2, pp. 136–156, 2022. [CrossRef]
9. X. Ren *et al.*, "Design of multi-information fusion based intelligent electrical fire detection system for green buildings," *Sustainability*, vol. 13, no. 6, p. 3405, 2021. [CrossRef]
10. P. Ajay., B. Nagaraj., and J. Jaya, "Bi-level energy optimization model in smart integrated engineering systems using WSN," *Energy Rep.*, vol. 8, pp. 2490–2495, 2022. [CrossRef]
11. X. Liu, Y. X. Su, S. L. Dong, W.-Y. Deng, and B. T. Zhao, "Experimental study on the selective catalytic reduction of NO with C3H6 over Co/Fe/Al2O3/cordierite catalysts," *Ranliao Huaxue Xuebao J. Fuel Chem. Technol.*, vol. 46, no. 6, pp. 743–753, 2018.
12. G. Veselov, A. Tselykh, A. Sharma, and R. Huang, "Applications of artificial intelligence in evolution of smart cities and societies," *Informatica*, vol. 45, no. 5, 2021. [CrossRef]
13. J. Gu, W. Wang, R. Yin, C. V. Truong, and B. P. Ganthia, "Complex circuit simulation and nonlinear characteristics analysis of GaN power switching device," *Nonlinear Eng.*, vol. 10, no. 1, pp. 555–562, 2021. [CrossRef]
14. M. Y. Liu *et al.*, "Investigation of stretchable strain sensor based on cnt/agnw applied in smart wearable devices," *Nanotechnology*, vol. 33, no. 25, p. 255501, 2022. [CrossRef]
15. K. Hamblin, "Sustainable social care: The potential of mainstream 'smart' technologies," *Sustainability*, vol. 14, no. 5, 2022. [CrossRef]
16. A. K. Dogra, and J. Kaur, "Moving towards smart transportation with machine learning and internet of things (iot): A review," *J. Smart Environ. Green Comput.*, vol. 2, no. 1, pp. 3–18, 2022. [CrossRef]
17. L. Peng *et al.*, "Ag/vo2/ag sandwich nylon film for smart thermal management and thermo-responsive electrical conductivity," *J. Ind. Text.*, vol. 51, no. 1_suppl, pp. 728S–748S, 2022. [CrossRef]
18. A. Mutshewa, K. Kadimo, and M. B. Kebaetse, "Understanding the role of the bring-your-own-device policy in medical education and healthcare delivery at the university of Botswana's faculty of medicine. *Inform. Learn. Sci.*," vol. 123, no. 3/4, pp. 199–213, 2022.
19. U. Tariq, T. A. Ahanger, A. Ibrahim, and Y. S. Bouteraa, "The industrial internet of things (iiot): An anomaly identification and countermeasure method," *J. Circuits Syst. Comput.*, vol. 31, no. 12, 2022. [CrossRef]
20. Z. Wang *et al.*, "A design method for an intelligent manufacturing and service system for rehabilitation assistive devices and special groups," *Adv. Eng. Inform.*, vol. 51, p. 101504, 2022. [CrossRef]

Danni Liu, female, the Han nationality, Changchun, Jilin, M.E. degree, research area: data communication and network security protection technology. She is now working in JiLin Information & Telecommunication Company, State Grid Jilin Electric Power Corporation Ltd.

Mingming Zhao, male, the Han nationality, M.E. degree, research area: network security attack and defense technology and industrial control security attack and defense technology. He is now working in State Grid Cyber Security Technology (Beijing) Co., Ltd.

Shengda Wang, male, Han nationality, B.S. degree, research direction: power communication equipment and network security protection technology. He is now working in JiLin Information & Telecommunication Company, State Grid Jilin Electric Power Corporation Ltd.



Xiaofu Sun, female, Han nationality, M.E. degree, research direction: data communication networks and network security protection technology. She is now working in the JiLin Information & Telecommunication Company, State Grid Jilin Electric Power Corporation Ltd.

Haoran Sun, male, the Han nationality, M.E. degree, research direction: power communication. He is now working in the JiLin Information & Telecommunication Company, State Grid Jilin Electric Power Corporation Ltd.