Scheduling Strategy Optimization and Security Protection Technology in Smart Distribution Network

Qing Ge1*, Ran Che1, Ruiyuan Fu1, Ling Zeng1, Chao Lu1

1State Grid Fuzhou Power Supply Company, Fuzhou, 350000, Fujian, China

*Corresponding author e-mail: geqing@hnsyu.edu.cn

Abstract. In the power system, distribution network is a very important link, and its operation quality and power supply reliability have a great impact on the whole social and economic development. Firstly, this paper analyzes the structure, function and characteristics of intelligent distribution network. Then it introduces the research status of optimization strategy based on genetic algorithm and its security protection technology, as well as the relevant basic theoretical knowledge. Then, aiming at the existing problems, the security protection system is designed for the power grid. Finally, through the performance test of the system, it is verified that the method is efficient and practical, and can effectively improve the security and stability of the power system, promote the further acceleration of China's sustainable construction process, improve the benefit level of power supply enterprises, and achieve the goal of social and economic development.

Key words: Intelligent Power Distribution, Dispatching Strategy, Security Protection, Protection Technology

1. Introduction

With the development of China's power system, the demand for power grid reliability is higher and higher. As an indispensable part of the national economic construction, the security and reliability of distribution network is an important symbol to measure the operation of a national power supply network. Therefore, it is particularly important to improve the operation quality and safety of distribution network [1-2].

Scholars have carried out relevant research on scheduling strategy optimization and security protection technology of intelligent distribution network. Some researchers respond to these challenges with efficient science and technology, and smart grid distribution strategy has attracted more and more attention of energy system researchers [3-4]. The essence of this method is to treat each grid component of the grid system as an agent, and each agent is required to interact with its adjacent agents. Each agent controls its behavior through the information it receives through local communication, so as to ensure that the whole system meets specific control objectives [5-6]. In the future power system, researchers discussed plug and play as an effective way to connect resources to the power grid. Similar to the computer system, plug and play in the power system means that the plug-in can be placed anywhere in the grid system without resetting the control. The plug and play interface includes a communication interface. Therefore, when the substation adds new equipment, it...
will automatically transmit data to the control center [7-8]. The above research lays a foundation for the optimization of dispatching strategy and the research of safety protection technology in smart distribution network.

Based on the analysis of the research status of security protection strategy in intelligent distribution network, this paper puts forward optimization methods for fault detection and diagnosis based on RFID technology, genetic algorithm and fuzzy theory. The simulation results show that these optimization methods can effectively reduce the number of misoperations and risk events, quickly reflect the probability of large-scale accidents in the power system, and improve the operation efficiency and reliability of the power grid. At the same time, it can also provide some reference value for relevant enterprises.

2. Discussion on Optimization of Dispatching Strategy and Safety Protection in Smart Distribution Network

2.1. Current Situation of Power Grid Safety Protection System

After years of development, the power grid security protection system has a considerable scope. There was only one SCADA system at the beginning. At present, in addition to SCADA system, protection systems such as power billing system (EBS), power market technical support system (emos), water distribution automation system, distribution network automation system and local substation safety measures are also added [9-10]. In recent years, with the upgrading of the system, the functions of each system have also been significantly improved. With the expansion of functions, the technical means of any safety protection system are evolving. The early security protection system used more proprietary technologies, such as data storage, use of file methods, file access, etc., which were also developed by the security protection system manufacturer [11-12]. When developing the system, each security protection system manufacturer rarely uses the commercial development platform and the underlying network defense. At the same time, only a few people use the security protection system and rarely communicate with the outside world. The disadvantage of this model is that the system function is weak, the openness is poor, and it is difficult to adapt to changes. However, such a system is quite secure, reducing contact with the outside world and reducing the possibility of being attacked. If the database is not used, there is no vulnerability caused by the database. With the progress of science and technology, this situation is gradually being broken. In order to meet the growing needs of users, the security protection system is developing in two directions: on the one hand, it learns from MIS system in technology and undertakes more and more business development platforms such as database, middleware and business development. Secondly, more and more users use system data, which increases the network between systems. Many systems are connected to MIS system and even Internet to provide web function and provide monitoring images, charts, reports, etc. for the majority of users.

At present, the degree of power grid automation has been significantly improved. Due to the wide application of communication and information technology in power system, the scope of Internet has been expanding. The information exchange between each distributed system and the terminal realizes the control, operation and management of the power supply system. A major problem of power grid system security: the reason is the error in communication information system and network monitoring system. A safe, reliable and stable power system is based on no problems, otherwise the power grid will not be stable, affect the society, production and living standards, and even cause social panic. Operational security, physical security and information security are three components of the security of communication information system and data monitoring system. Malicious attackers often use various small or microcomputers connected to the power grid to spread malware through the CNC smart grid to destroy the system. Like the security of computer network, high-performance information security must also face objective and subjective threats: the main reasons for the objective threats are the bad operation caused by the carelessness of employees and the bad practices of communication and information systems; Subjective threats come from active attacks from a variety
of sources, such as threats. Because the power grid puts forward high requirements for the reliability and real-time of information, central management has become an important feature of information communication in smart grid. The transmission network is connected with the distribution system distributed in the smart grid and provides a large part of electric energy to users through long-distance transportation. There are also distributed energy and high-pressure energy storage system. The information security of power grid will directly affect the physical and intelligent security control center, because it is through the control of power information that the communication network can effectively regulate the substation and modern transmission network. In order to ensure the information security of communication information system and network monitoring system, people should try to prevent people from forging, losing and deliberately damaging information property, so as to ensure the confidentiality, efficiency and speed of intelligent network communication. Do not destroy to prevent unauthorized third parties from identifying and stealing data. As the core technology in the security field, the existing cryptography theory can scientifically support the data security in the power grid. Cryptographic algorithms and protocols can solve the problems of virus protection, database security protection, access control, operating system protection and so on.

2.2. Power Dispatching Digital Certificate

The traditional postal routing system uses password strategy to identify employees, but once the password is leaked, account theft may occur. Moreover, with the development of network technology, hackers often do not need to visit the scene in person. As long as they use the remote account password, they can destroy it. At present, the network environment is complex, the level of information fusion is gradually improved, and information security has reached an unprecedented level. In view of the particularity of power system, digital certificate system has become a fundamental measure to ensure the security and reliability of energy information. Digital certificate system is applied to secure access of system and station data, transmission of energy monitoring information and application of big data analysis. The use of digital certificates for power distribution provides many technical advantages, which can be summarized in two aspects: security performance and scalability.

In terms of security performance, digital certificates have the following three advantages:

1. High security. If the password is compromised, the two factor authentication mode is also performed.

2. Completely isolated from external network. Due to the separation of internal and external networks, sending digital certificates is only used for internal networks, and the server issuing digital certificates is configured to work independently. The possibility of certificate theft is greatly reduced, so as to confirm that the personnel conducting data certificate authentication have sufficient reliability.

3. Unified certificate. The power grid system uniformly takes over the root certificate stipulated by the state. In terms of applicability, digital certificate has the following three advantages:

1. Support various algorithms at home and abroad. Whether the RSA algorithm provided abroad or the SM2 algorithm in China, the digital certificate is compatible and can be selected when establishing the certificate system.

2. The types of certificates are complete. The system can check the certificate data of personnel certificate, workplace certificate and special power grid protection device certificate.

3. The grid system has high adaptability and scalability. For special power supply security protection equipment and front-end encryption card equipment, they can meet the issuance requirements of power system certificate, and realize adaptive function expansion according to the update and upgrading of security protection equipment.

2.3. Problems in Power Grid Dispatching System

1. The distribution automation system previously used in the power grid does not adapt to the new situation of power grid development.

2. The system cannot implement unified management. When the system was just developed, due to the lack of foresight, various problems occurred in the current system, affecting the function of the
system. Now there are multiple operating systems in the system, which not only increases the load of the system, but also increases the burden of the system. The phenomena of protocol conflict and network conflict not only waste resources, but also make the communication between systems difficult.

(3) As each subsystem is developed by different manufacturers, it is difficult to organize and coordinate, and each manufacturer will have a "dispute" phenomenon, which will bring resistance to product maintenance and increase the maintenance cost of the system.

(4) With the increasing requirements of the state for power grid stability, if the system is no longer intelligent, it will not be able to meet our application needs.

2.4. Key Algorithms of Artificial Intelligence Technology

Basic PSO uses particles to represent potential solutions to problems. In the process of algorithm optimization, the corresponding fitness function value is obtained by using the particle position information in the objective function. This fitness function value can be used to measure the mass of particles. Each particle is related to its current speed, current position, the best position found in its own history, and the historical best position of the whole group to determine its current position.

The best position of particles in the optimization process is the individual particle flight experience, and the overall group optimization leads to the group flight experience. Particles can constantly change their flight speed and direction according to their own experience and their companions' experience, and constantly look for new positions to obtain the optimal solution in the solution space. The position s of particle i in the population can be expressed as: \( s_i = (s_{i1}, s_{i2}, ..., s_{in}) \), which is replaced in the objective solution function to obtain the value of the corresponding fitness function. The mass of particle i is determined by the value of the fitness function. The space velocity of particle V can be expressed as: \( v_i = (v_{i1}, v_{i2}, ..., v_{in}) \). When optimizing the algorithm, the particle updates its flight speed and position according to formula (1) and formula (2):

\[
\begin{align*}
    v_i(t+1) &= w \cdot v_i(t) + c_1 r_i \\
    s_{ij}(t+1) &= s_{ij}(t) + v_i(t+1)
\end{align*}
\]

Where: \( t \) represents the algebra of particle update iteration, \( v_j(t) \) is the flight speed of particle i in the j direction in the t iteration, and \( s_{ij} \) (1) is the component of the best individual position experienced by particle i in the j direction in the t iteration.

3. Experiment

3.1. Safety Protection Design Principles

This paper follows the following principles in terms of specific technical safety protection:

The safety protection force of the whole system should be based on the weakest limit of the whole system. Therefore, all control centers must comply with the security area plan and use the same security equipment at the border.

2) Simple and reliable principle;
3) Real time, continuous and safe integration principle;
4) Balance principle of demand, risk and cost;
5) The principle of combining practicality with progress;
6) The principle of unity of convenience and safety;
7) Overall protection principle and highlight key points;
8) The principle of superposition, division and strengthening the boundary;
9) The principle of overall planning and gradual progress;

3.2. Procedure Flow of Safety System

Figure 1 is the flow chart of the smart grid security protection system program.
4. Discussion

4.1. Performance Test and Analysis of Smart Grid Security Protection System

Table 1 shows the performance test data of the system.

| Number of runs | Response time (ms) | Amount of memory occupied (k) | Whether the early warning device is normal | Whether the receiving information is normal | Whether the message sent is normal |
|----------------|-------------------|-------------------------------|------------------------------------------|------------------------------------------|-----------------------------------|
| 1              | 52                | 2314                          | YES                                      | YES                                      | YES                               |
| 2              | 45                | 3012                          | YES                                      | YES                                      | YES                               |
| 3              | 53                | 2520                          | YES                                      | YES                                      | YES                               |
| 4              | 50                | 2630                          | YES                                      | YES                                      | YES                               |

Figure 1. Safety protection and early warning process

As can be seen from Figure 1, firstly, the security protection system will establish a database, bind users, and establish security early warning settings according to user needs. When a security threat is found, the system will immediately issue a warning, and the client will receive the early warning information. The protection system will not stop the alarm until the power grid receives the maintenance of relevant technicians.
As can be seen from Figure 2, the test results show that the response time of the safety protection system is fast, basically around 50ms. The amount of memory is small, and the early warning device and the module receiving and sending information can operate normally. This shows that the smart grid security protection system designed in this paper can effectively meet the protection requirements.

5. Conclusion
With the development of China's power system, the requirements for power grid reliability are higher and higher. Therefore, it is particularly important to improve the operation quality and safety of distribution network. Based on the analysis of the research status of security protection strategy in intelligent distribution network, this paper puts forward optimization methods for fault detection and diagnosis based on RFID technology, genetic algorithm and fuzzy theory. The simulation results show that these optimization methods can effectively reduce the number of misoperations and risk events, quickly reflect the probability of large-scale accidents in the power system, and improve the operation efficiency and reliability of the power grid. At the same time, it can also provide some reference value for relevant enterprises.

Reference
[1] Deng Z , Fu M , Zhang Q . A research of time slot optimization task scheduling strategy based on the hadoop[J]. Journal of Northwestern Polytechnical University, 2017, 35(1):32-37.
[2] Pan Chen, Teng Huan, Gong Yubin, et al. Research on optimal coordination scheduling strategy of micro grid in user side interactive mode [J]. Electrical measurement and instrumentation, 2019, 056 (005): 51-56
[3] Chen X , Li Z , Chen Y , et al. Performance Analysis and Uplink Scheduling for QoS-Aware NB-IoT Networks in Mobile Computing[J]. IEEE Access, 2019, 7:44404-44415.
[4] Ma Li, Wang Zongli, Liu Wei, et al. Research on multi layer optimization planning method for intelligent distribution network considering operational flexibility [J]. Power construction, 2018, 039 (006): 71-79
[5] Li P, Xiao J, Wang W. research on distribution of electronic environment around substations and optimization layout of on-line monitoring [J]. Meteorological and environmental research: English version, 2019, 010 (006): p.60-63
[6] Li J , Li H B , Zhang H T , et al. Research on the Effect of Cutter Position Points Distribution
Optimization on Surface Milling Accuracy[J]. Key Engineering Materials, 2018, 764:323-332.

[7] Shuai L, Zhicong Z, Xiaohui Y, et al. Research on a resource-constrained project scheduling problem in a hazardous environment and its staffing strategies based on PSO algorithm[J]. Systems Science & Control Engineering, 2018, 6(1):304-318.

[8] Liu n, Wang n, Shan n. research on Evaluation and optimization strategies of cultural ecosystem services of rural water spaces in Suzhou [J]. Landscape architecture frontier, 2021, 9 (2): 38-49

[9] Hongyan C, Xiaofei L, Tao Y, et al. Cloud Service Scheduling Algorithm Research and Optimization[J]. Security and Communication Networks, 2017, 2017:1-7.

[10] Shen X, Shahidehpour M, Zhu S, et al. Multi-stage Planning of Active Distribution Networks Considering the Co-optimization of Operation Strategies[J]. IEEE Transactions on Smart Grid, 2018, PP(2):1-1.

[11] Walter Gil-González, Montoya O D, Grisales-Norea L F, et al. Hybrid Optimization Strategy for Optimal Location and Sizing of DG in Distribution Networks[J]. Tecnura, 2020, 24(66):47-61.

[12] Zhao song. On the distribution characteristics and optimization strategy of public sports venues in Datong [J]. Sports science and technology, 2018, 039 (003): 84-85,87