Genetic Algorithm-Based Power System Information Security Risk Assessment Method

Fangneng Huang\(^1\)*, Mei Yong\(^1\), Zhou Jian\(^1\)

\(^1\)CSG Power Dispatching Control Center, Guangzhou, Guangdong, 510663 China

*Corresponding author e-mail: huangfn1@csg.cn

Abstract. With the innovation and application of new-generation information technologies such as cloud computing, Internet of Things, and mobile Internet, the importance of information security issues has become more prominent. As an important industry linking people's livelihood, the electric power industry will affect the safe operation of electric power once an information security incident occurs, and even lead to a large-scale blackout. Therefore, studying the information security risk assessment model of electric power enterprises has important theoretical value and practical significance. The purpose of this paper is to study the method of power system information security risk assessment based on genetic algorithm. This paper establishes a security risk quantification model, determines the operating parameters of the genetic algorithm in specific operations based on some literature cases, and compares the results in the literature with those in this paper. Based on a large number of investigations and interviews, this paper conducts research on information security risks, comprehensively considers the threats and vulnerabilities of the system, and analyzes the important impact of information security risks from the internal management, personnel, technology, and systems of electric power enterprises. Factors, the establishment of a power enterprise information security risk evaluation index system, this paper obtains data from actual system evaluation cases, uses multiplication, matrix method, and the genetic algorithm proposed in this paper to calculate the risk quantification model calculation results, and verifies the genetic algorithm the rationality and feasibility of combining with risk assessment, this method has practical application value. Experimental research shows that the risk value calculated by the genetic algorithm based on the risk quantification model proposed in this paper is more than 70% similar to the results calculated by the multiplication method and the matrix method, which proves that the model and calculation method established in this paper can be used. Applied to the specific evaluation implementation process.

Key words: Genetic Algorithm, Risk Assessment, Quantitative Model, Information Security
1. Introduction
With the obvious increase of power companies’ reliance on information systems and information technology, how to build a power company’s information system security system and how to evaluate the power company’s information system security has become an important topic for power companies’ information security [1-2]. The most basic and most important task of doing a good job in information security is to conduct a scientific and reasonable information security risk assessment [3-4]. Through information security risk assessment, it can be found early, dealt with in time, and effectively solve information security problems [5-6].

In the research of genetic algorithm-based power system information security risk assessment methods, many scholars have studied them and achieved good results [7-8]. For example, Bhuiyan MZA proposed sound laws and regulations that can effectively reduce information security risks, and a comparative study was made on the relationship between the level of perfection of laws and regulations and the level of corporate information security [9]. Weisi D adopted the fault tree model, deeply analyzed the information system, and truly evaluated the security performance of the information system [10].

This paper determines the fitness function, selection method, and various operating parameters of the genetic algorithm. Finally, a system example is used to verify the operability and effectiveness of the model, and multiple methods are used to compare the results to prove the availability of the method proposed in this paper. This paper uses specific evaluation examples to verify the operability and effectiveness of the information security risk assessment model based on genetic algorithms. The calculation results are compared with the calculation results of various risk value calculation methods commonly used in risk assessment.

2. Power System Information Security Risk Assessment Method Based on Genetic Algorithm

2.1. Information Security Risk Assessment Based on Genetic Algorithm
(1) Fitness function design
For the problem of solving the risk value, because the risk is the loss caused by the threat to use the vulnerability to the asset, the asset can be obtained from the risk assessment, and the fitness function can be designed as a description of the closeness of the individual calculated value to the actual estimated value.

\[
    \text{fitness} = |V_f - V_i|
\]

In this article, the smaller the fitness function value, the more likely an individual is to be selected, which means that when the \(V_f\) value calculated by the population individual is closer to the expert evaluation value \(V_i\), the individual will have a greater probability of being retained. In the new generation population.

(2) Selection and definition of genetic manipulation
1) Select operation
This article chooses the selection method: Roulette selection method. Assuming that the size of the population is \(m\) and the fitness of the \(i\)-th individual is \(f_i\), then the probability of the individual being selected can be obtained as follows:

\[
    P_i = f_i / \sum_{j=1}^{m} f_j
\]

It can be seen from the above formula that the selection probability reflects the proportion of the fitness of the selected individual in the total fitness of all individuals in the group. Individuals with greater fitness are more likely to be selected.

2) Crossover operation and mutation operation
Crossover operation and mutation operation work together to realize the process of genetic algorithm simulating biological evolution in nature, which is the process of generating new population individuals. Since this paper uses real-valued coding to encode feasible solutions, according to the principle, the discrete recombination method in real-valued recombination is selected for crossover...
operation, and real-valued mutation is selected for mutation operation.

2.2. Quantitative Model of Security Risk Assessment

(1) Asset value
In the evaluation, the value of the asset can be expressed by the absolute value, that is, the actual economic value of the asset, or the relative value, that is, the evaluation expert gives a value according to the importance of the asset in the system, and this value is used to express it. Asset value.

(2) Probability of threat
The meaning of probability is to describe the possibility of a random event. Generally, a real number between 0 and 1 is used to indicate the possibility of the event. The closer to 1, the more likely the event will occur; the closer to 0, the less likely the event will occur. Therefore, probability can be used to describe the possibility of a threat event. The greater the probability of a threat, the more likely it is to cause security losses to the system.

(3) The severity of vulnerability
Vulnerability exists objectively in the system, but its existence does not necessarily cause the loss of assets. Only when the vulnerability is threatened and exploited, will it cause damage to the asset. If the severity of the vulnerability is high, the extent to which it is exploited high.

(4) Effectiveness of safety measures
In the information system, the used security measures can effectively reduce the risk of the information system, but the security measures cannot completely prevent the risk from occurring. Defined here:

\[ Sm = 1 - \left( \frac{N_v}{N} \right) \]  \hspace{1cm} (3)

N_v represents the number of threats that actually caused losses to system assets, and N represents the total number of threats attacked by the system.

2.3. Construction Principles of Evaluation Index System

(1) The principle of comprehensiveness
The indicator system is an intuitive reflection of the information security risk status of an enterprise, and it should be more comprehensive and a hierarchical whole. Through reasonable index combing, construct an index system that can fully reflect the overall situation of the evaluation object. There is no absolute standard for how to divide the levels and indicators. It depends on the actual situation, as long as the evaluation goals can be expressed comprehensively and conveniently.

(2) Concise and scientific principles
Evaluation indicators must reflect the needs of evaluation targets, and set up a scientific and reasonable indicator system of appropriate size. The index level cannot be too much or too detailed, otherwise it will pay too much attention to the details in the evaluation process, and it cannot be too few or too rough, otherwise it will not fully reflect the evaluation object. In evaluating specific information security risks, we must make objective judgments based on actual conditions and should not look at one aspect unilaterally. The definition of the index must be clear, otherwise it will affect the results of the evaluation, or cause situations that cannot be evaluated.

(3) The principle of independence
The indicators to be set should be representative indicators, and the indicators should be independent of each other without overlapping information. In the establishment of the indicator system, attention should be paid to the overall goals, sub-objectives, and the integrity, independence and relevance of indicators. They are an indivisible whole and have their own independence.

(4) Principle of flexibility and operability
The ultimate goal of the evaluation index system is application. When constructing the index system, the flexibility of the index system should be considered. Add, delete or modify appropriately according to different requirements, and further concretize the indicators according to specific
conditions. In addition, the selected indicators should be as easy to measure as possible. For indicators that cannot be quantified, it is necessary to obtain data through expert scoring and other means.

3. Experimental Research on Power System Information Security Risk Assessment Method Based on Genetic Algorithm

3.1. Asset Identification
Information system assets not only refer to tangible and tangible items with actual economic value, but also refer to valuable information and resources related to the actual application of a system in the system organization. Assets are the protection goals in information security. Therefore, the value of assets in the assessed information system is usually not assigned by the actual economic value of the assets, but is determined by the conformity of a series of attributes such as confidentiality and integrity of the assets.

3.2. Vulnerability Identification and Assessment
In this paper, the vulnerability identification can be carried out from the technical level and the management level. The technical level needs to judge the security issues in all aspects of the seven-layer model of the information system. The management's recognition of vulnerability is divided into technical management and organizational management. As the name suggests, these two aspects are related to technology and management activities respectively.

3.3. Multiplication Method to Calculate System Risk Value
The multiplication method determines the relevant elements in a security incident by directly multiplying the values of two elements to express the value of another element. The principle of multiplication is:

\[ z = f(x, y) = x \otimes y \]  \hspace{1cm} (4)

If the function \( f \) is an increasing function, then the original operation of \( \otimes \) can be directly defined as multiplication, or it can be defined as multiplication and then modulo. It can be defined as:

\[ z = f(x, y) = x \times y \]  \hspace{1cm} (5)
\[ z = f(x, y) = \sqrt{x \times y} \]  \hspace{1cm} (6)
\[ z = f(x, y) = \left\lfloor \sqrt{x \times y} \right\rfloor \]  \hspace{1cm} (7)

Many definitions can also be selected as long as the above basic conditions are met. This article adopts the calculation method of formula (6) for the multiplication method.

4. Experimental Research and Analysis of Power System Information Security Risk Assessment Methods Based on Genetic Algorithm

4.1. Results Calculated Using Genetic Algorithms
Through the solution of genetic algorithm, the final results are shown in Table 1, where the representation of threat and vulnerability are replaced by corresponding numbers.

| Assets | Asset value | Threat frequency | Severity | Value at risk |
|--------|-------------|------------------|----------|---------------|
| Firewall | 4.25 | 3 | 4 | 9.53 |
| Switch  | 4.51 | 2 | 5 | 9.67 |

Table 1. Analysis of genetic algorithm calculation results
It can be seen from Figure 1 that when the genetic algorithm is used to calculate the evaluation model, assets affected by the same threat frequency and vulnerability severity may have different risk values, but these risk values are not much different. The reason is that when the genetic algorithm starts to run, it is necessary to randomly generate individuals with feasible solutions, that is, the initial value of $R_i$, $k$ is randomly generated within its value range during the calculation process, and various genetic operations are required during the genetic process. The operation process also randomly selects individuals to operate, so there will be some differences in the numerical calculation results of the same asset value, threat frequency and vulnerability severity, but this difference will not affect the final judgment of risk.

4.2. Multiplication Method to Calculate System Risk Value

In this paper, the genetic algorithm calculation method and the calculation result of the multiplication method are shown in Table 2. It can be analyzed from the table that the change trend of the risk value of the two methods for different assets is roughly the same.

| Numbering | Genetic algorithm | Multiplication |
|-----------|-------------------|----------------|
| 1         | 10.75             | 4.23           |
| 2         | 14.57             | 4.68           |
| 3         | 3.87              | 2.71           |
| 4         | 13.47             | 4.49           |
From Figure 2, it can be seen that the risk value calculated by the genetic algorithm based on the risk quantification model proposed in this paper is more than 70% similar to the result calculated by the multiplication method and the matrix method, and there is the same trend in changes. Multiplication and matrix methods are commonly used methods to determine the value of risk in risk assessment, so it can show that the models and calculation methods proposed in this article are reasonable and feasible, and prove that the models and calculation methods established in this article can be applied to specific assessments. Implementation process.

5. Conclusions
This article uses the data obtained from this article to set the operating parameters of the genetic algorithm used in this article, and calculates the model to verify the feasibility of the model and method in this article. In the process of using the genetic algorithm to simulate the model, the calculation efficiency is not measured. For analysis, the actual value is also used to express the risk calculation result, and the risk classification method when this method is used for evaluation is not studied. These will be gradually improved in further work.

References
[1] Sujatha R, Ramakrishnan M, Duraipandian N, et al. Optimal Adaptive Genetic Algorithm Based Hybrid Signcryption Algorithm for Information Security. Cmes Computer Modeling in Engineering & Sciences, 2015, 105(1):47-68.
[2] Jouini M, Rabai L B A. A Multi-Dimensional Mean Failure Cost Model to Enhance Security of Cloud Computing Systems. International Journal of Embedded and Real-Time Communication Systems, 2016, 7(2):1-14.
[3] Huang P, Xu T, Sun Y. A genetic algorithm based dynamic pricing for improving bi-directional interactions with reduced power imbalance. Energy and Buildings, 2019, 199(SEP.):275-286.
[4] Rachna Singh, Arvind Rajawat. Analytical Model for High–Level Area Estimation of FPGA Design. International Journal of Embedded and Real-Time Communication Systems, 2016, 7(2):1-14.
[5] Law Y W, Alpcan T, Palaniswami M. Security Games for Risk Minimization in Automatic Generation Control. IEEE Transactions on Power Systems, 2015, 30(1):223-232.
[6] Munteanu A B. Running the Risk IT – More Perception and Less Probabilities in Uncertain Systems. Information and Computer Security, 2017, 25(3):345-354.
[7] Ding T, Li C, Chen C, et al. Risk Assessment Based Long-Term Transmission System Hardening under Prior Probabilistic Information. IET Generation Transmission & Distribution, 2018, 13(1):108-115.

[8] Jouini M, Rabai L B A, Khedri R. A Multidimensional Approach towards a Quantitative Assessment of Security Threats. Procedia Computer Science, 2015, 52(1):507-514.

[9] Bhuiyan M Z A, Anders G J, Philhower J, et al. Review of static risk-based security assessment in power system. 2019, 4(3):233-239.

[10] Weisi D, Buhan Z, Hongfa D, et al. Risk-Based Probabilistic Voltage Stability Assessment in Uncertain Power System. Energies, 2017, 10(2):180.