Threat Detection in Power Grid Based on Hierarchical Feature Cloud Computing Model

Jing Li¹, Jie Huang¹, Fen Liu²

¹State Grid Hubei Electric Power Co., Ltd, Hubei Wuhan, China, 430077
²Information & Communication Branch of Hubei EPC, Hubei Wuhan, China, 430077

*Corresponding author e-mail: gmq1988@126.com

Abstract. The extraction of subjective features such as the authority, purpose, and opportunity of power network operators has outstanding subjectivity. It is difficult to accurately quantify subjective features due to the subjective factors of operators, resulting in fuzzy subjective features. Traditional algorithms use subjective features to detect internal threats to the power grid. Once subjective factors interfere, they will cause the defects of fuzzy main features, leading to a decrease in the accuracy of threats to the internal power grid. This paper focuses on the detection of power grid internal threats based on a hierarchical feature cloud computing model. This paper proposes a power network internal threat detection method based on the hierarchical feature cloud mapping model; calculates the hierarchical mapping relationship based on the internal threat features to complete the internal threat detection of the power grid; experiments prove that the algorithm avoids subjective factors being affected by subject characteristics, and The ambiguity of features reduces the missed detection rate to below 15.3%.

Keywords: Power Characteristics, Insider Threats, Feature Clouds, Cloud Computing Models

1. Introduction
As the main energy source, electricity plays an irreplaceable role in industrial production and life. The safety of the power network is closely related to production and life. At this stage, the power network is well able to defend against external network attacks, but research on internal threat detection is still in its infancy. Threats within the power network are usually caused by the legitimate operators of power companies, and malicious operations on the power network will cause great damage to the power companies.

At present, in the process of daily production and management, enterprises give full play to the role of network information systems and improve operational efficiency. However, while increasing the work process, due to the variety of network information, threats to network information security continue to emerge [1-2]. At the current stage, during the development process of power grid companies, there are mainly the following threats: During the development process of power grid companies, the network and computer information systems appear to have a relatively medium scale,
covering almost all network sectors [3]. In order to meet the development needs of enterprises, it is necessary to realize the continuous expansion of computer network systems and set up a scientific network information system to cover all business departments in order to meet the development needs of power grid enterprises [4-5]. With the continuous expansion of computer network systems, we must increase the scientificity of the equipment to better make up the internal network subsystems of the enterprise and set the network structure scientifically. At the same time, the cross-cutting problems facing the network have solved the problem of network equipment redundancy. Therefore, the above-mentioned reason is the possibility that the network information security of power grid companies poses a huge threat; in the application process, various Viruses may invade network systems [6-7]. Once the virus invades, the performance of the mainframe of the power grid company will be significantly damaged, and important data and information of the company will also be damaged, which will bring irreparable losses to the company. And the normal operation of the computer system, various network devices such as switches and routers need to be configured [8-9]. During the construction process, in order to improve the security of the network system, it is necessary to take effective security measures. Avoiding the threat from network information systems [10].

Therefore, detecting threats in the power network is a major problem in the field of power security. Internal threat detection methods. At present, mainstream power networks. The algorithm for safely monitoring network actions is based on the internal threat detection methods of power networks. The minimum action chaining algorithm is based on the internal threat detection methods of power networks. 11-12. Among them, the most commonly used method for detecting threats inside the power network is based on target function algorithms. Due to the widespread application of threat detection methods in power networks, many scholars have paid attention.

2. Method

2.1 Threat Detection Inside the Power Network

Relevant theories of power network internal threat detection. The power network internal threat detection requires the extraction of the operator's authority, purpose, and opportunity characteristics. Based on the above characteristics, the threat degree of the operation behavior is predicted, and it is compared with the threat degree measurement standards to complete the internal power network. Threat detection.

Set the number of power network operators to n, the operator's authority characteristic parameter to $\alpha$, the objective characteristic parameter to be $\beta$, the opportunity characteristic parameter to be $x$, and the subject feature selection coefficient to be $\delta$. Using formula (1) can calculate the threat degree of internal network operation behavior parameter:

$$\gamma = \frac{\alpha |\beta^2 - x|}{\delta \sqrt{n^2 + 1}} + 1$$  \hspace{1cm} (1)

According to formula (1), the parameter of the threat degree of the internal operation behavior of the power network can be calculated, which is used to describe the degree to which the power network is subject to internal threats. Set the power network internal threat measurement standard to be $\omega$, and use formula (2) to perform power network internal threat detection:

$$\gamma = \frac{\alpha |\beta^2 - x|}{\delta \sqrt{n^2 + 1}} + 1$$  \hspace{1cm} (2)

According to formula (2), it can be known that if the threat degree parameter of the internal operation behavior of the power network is greater than the internal threat measurement criterion, it is judged that there is an internal threat in the power network; otherwise, it is judged that there is no internal threat in the power network.
Use formula (3) to calculate the rate of missed detection of threats inside the power network:

\[
\begin{align*}
\gamma > \omega & \quad \text{There are internal threats to the power grid} \\
\gamma \leq \omega & \quad \text{There is no internal threat to the power grid}
\end{align*}
\]

(3)

According to formula (3), the missed detection rate of threat detection inside the power network can be calculated, which is used to describe the degree of missed detection of threat detection inside the power network.

2.2 Defects of Power Network Internal Threat Detection Methods

According to formula (1), it can be known that if the subject feature selection coefficient is increased, the parameter of the threat degree of the operation behavior inside the power network will be reduced. According to formula (2), it can be known that the decrease in the threat degree parameter of the internal operation behavior of the power network will cause a missed detection phenomenon. According to formula (3), it can be known that the decrease of the threat degree parameter of the internal operation behavior of the power network will cause the increase of the missed detection rate of the power network internal threat.

This paper proposes a power network internal threat detection method based on a hierarchical mapping model. The characteristics of internal threats are extracted, and the mapping relationship of these characteristics is obtained through application. Establish an internal threat feature cloud model to realize internal threat detection in power networks. It avoids the defect that subject features are too blurred due to subjective factors, and improves the accuracy of threat detection within the power network.

3. Experiment

The detection principle is based on the conclusion that the normal behavior pattern of a program has a large degree of consistency, and anomalies usually only cause drastic changes in the behavior pattern within a local scope. When used here, the normal state transition vectors have stability. The state transition vectors obtained when the program runs normally should belong to the normal contour library. Once it is found that there are concentrated state transition vectors that are not in the normal contour library, it indicates that an abnormality has occurred.

The detection process can be described as:

(1) Take the collected system call sequence \( O \) as the sequence of observation events into the trained hidden Markov model, and use the Viterbi algorithm to obtain the optimal state transition sequence \( Q \) corresponding to \( 0 \).

(2) \( Q \) is divided by a sliding window to obtain the state transition vector set \( V \).

(3) Take a state transition vector from \( V \) and find a match in the normal contour library. If no match is found, go to step (4); if all the state transition vectors in \( V \) have been matched, the process ends.

(4) Increase the number of mismatched state transition vectors by 1 to calculate the mismatch rate of \( Q \). If the mismatch rate is greater than the preset threshold, it indicates that an abnormality has occurred; otherwise, go to step (3).

4. Discuss

4.1 Analysis of Threats Inside the Power Grid

The extraction of the subjective features of the power network operator's authority, purpose, opportunity, etc., and the influence of the subjective factors of the operator have excellent subjectivity and subjective features, so it is difficult to accurately quantify the results as fuzzy subjective features. In terms of power grid internal threat detection, traditional methods need to extract the main characteristics of power grid operators, predict the operation of the power grid, and finally complete
the power grid internal threat detection. Because the extraction of subject features is greatly affected by subjective factors and the subject features are not clear, the accuracy of threat detection in the power network is assumed to be reduced.

![Figure 1. Comparison of missed detection rates for different methods](image)

Therefore, due to the large subjective factor of the extracted features, it is impossible to avoid the defect that the features of the object are blurred. To verify the effectiveness of this white paper algorithm, experiments are needed. Establish a power network simulation environment, using conventional algorithms and this white paper algorithm to detect internal threats to the power network. Use simulation intrusion software to simulate each intrusion environment. In the environment, using the internal network of the power network, 10 valid experiments were selected for comparison. Figure 1 shows the calibration of the specific distribution of the results of threat detection inside each power network using the accuracy of the number and proportion of experimental samples as detection accuracy. The algorithm shows that the algorithm of this paper has a great advantage in the detection of internal threats to the power network under the condition that feature extraction is severely disturbed by subjective factors. By recording the relevant data of the experiment, Table 1 can be obtained.

| Table 1. Data Sheet for Threat Detection within Electric Power Networks |
|---------------------------------------------------------------|
| Internal threat detection data | Traditional algorithm | Algorithm |
| Testing time | 20s | 25s |
| Testing number | 20 | 20 |
| Number of internal threats | 45 | 63 |
| Number of internal threats detected | 38 | 57 |
| Miss rate | 15.56% | 9.5% |

As shown in Table 1, in the process of power network internal threat detection, by using the algorithm in this paper, we can find that the detection rate of power network internal threat detection is lower than the traditional algorithm.

4.2 Suggestions on Network Information Security Threats for Grid Enterprises

(1) The overall framework of a scientific construction system

In the process of constructing the overall system architecture of the network, grid companies can use new types of big data technologies to improve data analysis and processing capabilities, fully tap deep-seated services covered by data information, and comprehensively improve the level of risk warning and network security. The overall architecture mainly includes the data acquisition platform layer and management layer. During the system’s data collection process, it can effectively collect
all-round data of infrastructure operation and network information, and realize the effective transmission of the database. The platform can realize a series of methods such as synchronous data extraction and data conversion during the construction process. In the process of establishing an information system network early warning method or a risk early warning model, the efficiency of information collection can be achieved, and all-round calculation and analysis can be done well. At the management and application level, scientific classification of power resource information, real-time early warning of information network risks, and good auxiliary decision-making can improve the system's adaptive ability and ensure the normal operation of the power system.

(2) Channel security technology

At present, in the implementation process of ensuring channel safety technology, it is necessary to realize the transmission of communication channel data and improve the integrity and scientificity of information transmission in order to ensure the normal operation of the power grid system. For power grid companies, a comprehensive analysis of the access network is required. Considering that the main erection method is power overhead optical cables, a comprehensive analysis of power cables is performed at the physical level. It is necessary to ensure that the information has a certain degree of security to avoid corresponding human attacks. You can use the VPN virtual network to do channel encryption. This technology has low cost and simple operation, and can be used in the channel security improvement stage.

5. Conclusion

For the power grid, whether it is early planning or later safe operation, the ultimate goal is to provide services for economic development and ensure the smooth progress of people's production and life. This paper proposes an internal threat detection method for power networks based on a hierarchical feature cloud computing mapping model. Extract the characteristics of internal threats, calculate their mapping relationships, and build a cloud model of internal threat characteristics to enable detection of internal threats in power networks. Experimental results show that the algorithm improves the accuracy of threat detection in power networks.

References

[1] Bowen Du, Runhe Huang, Zhipu Xie. KID Model-Driven Things-Edge-Cloud Computing Paradigm for Traffic Data as a Service[J]. IEEE Network, 2018, 32(1):34-41.
[2] Chen, C, Chen, D, Yan, YN. Integration of numerical model and cloud computing[J]. Future Generation Computer Systems, 2018, 79(3):396-407.
[3] Hussin, Hnasayati, Salleh, Noor Afzan, Suahaimi, Mohd Adam. A Model to Assess the Impacts of Cloud Computing Use on SME Performance: A Resource-Based View[J]. Advanced Science Letters, 2018, 24(3):1800-1804.
[4] Ibrahim M, Mustafa I, M. Sadiq. A Group Decision-Making Method for Selecting Cloud Computing Service Model[J]. International Journal of Advanced Computer Science & Applications, 2018, 9(1):449-456.
[5] N. Senthamarai, M. Vijayalakshmi. Dynamic Resource Allocation Based on Energy Consumption Using Hyped-Up Voltage Frequency Scaling Model in Cloud Computing[J]. Journal of Computational and Theoretical Nanoscience, 2017, 14(4):1837-1843.
[6] Eric Bauer. Improving Operational Efficiency of Applications via Cloud Computing[J]. IEEE Cloud Computing, 2018, 5(1):12-19.
[7] Muhammad Shiraz, Abdullah Gani, Rashid Khokhar. A Distributed and Elastic Application Processing Model for Mobile Cloud Computing[J]. Wireless Personal Communications, 2017, 95(1):1-21.
[8] Zijian Cao, Jin Lin, Can Wan. Optimal Cloud Computing Resource Allocation for Demand Side Management in Smart Grid[J]. IEEE Transactions on Smart Grid, 2017, 8(4):1943-1955.
[9] Rodrigo N. Calheiros, Enayat Masoumi, Rajiv Ranjan. Workload Prediction Using ARIMA Model and Its Impact on Cloud Applications' QoS[J]. IEEE Transactions on Cloud Computing,
[10] Rui-Dong Wang, Xue-Shan Sun, Xin Yang. Cloud Computing and Extreme Learning Machine for a Distributed Energy Consumption Forecasting in Equipment-Manufacturing Enterprises[J]. Cybernetics & Information Technologies, 2017, 16(6):83-97.

[11] Hongming Cai, Yizhi Gu, Athanasios V. Vasilakos. Model-Driven Development Patterns for Mobile Services in Cloud of Things[J]. IEEE Transactions on Cloud Computing, 2018, 6(3):771-784.

[12] S. Bhama, G. R. Karpagam. Application of multivariate Gaussian model for discovery of healthcare services in cloud[J]. Cluster Computing, 2019, 22(6):1-8.