Scalable Computing: Practice and Experience, ISSN 1895-1767, http://www.scpe.org
© 2024 SCPE. Volume 25, Issues 4, pp. 2614–2620, DOI 10.12694/scpe.v25i4.2913

CONSTRUCTION OF POWER SYSTEM NETWORK SECURITY DEFENSE BEHAVIOR DECISION-MAKING MODEL BASED ON ARTIFICIAL INTELLIGENCE TECHNOLOGY

FEILU HANG*, LINJIANG XIE†, ZHENHONG ZHANG‡, AND JIAN HU§

Abstract. According to the needs of power grid monitoring architecture and information security cooperation protection, this project builds a multi-level, deeply distributed active security cooperation defense mode. A complete implementation method is proposed from the perspective of model architecture and function mechanism. The optimal defense strategy based on grey correlation is studied according to the characteristics of cooperation between regions. In this way, the coordination between the equipment is realized to achieve multi-level protection from the host layer to the security equipment layer and then to the network layer. Multiple detection mechanisms are used to realize the comprehensive detection and integrated judgment of abnormal documents in the cloud environment. This provides maximum protection for cloud users. Experiments show that this method can effectively suppress the malicious attacks of malicious users and reduce the damage caused by viruses. In this way, both the cloud and the customer are protected.

Key words: Power system; Multi-level cooperative protection; Cooperative protection mode; Network security; Grey relational decision

1. Introduction. With the popularization of the computer, network, communication and other scientific and technological means, the modern power system has formed a complex system composed of a physical power supply and communication network. The power monitoring system is a commercial and intelligent device with computer and Internet technology as the core, which is the primary support for monitoring and controlling the production and supply of electric energy [1]. Power grid monitoring is critical to ensure the power supply's safety and stability. At present, information attacks on the power grid are frequent, showing the characteristics of specialization, high risk, internationalization, and strong continuity, which makes the security protection problem of the power grid monitoring system rise to a certain height. Relevant agencies have proposed the need for a common defense of "multiple vertical lines of defense." Some scholars intend to introduce the concept of cooperative defense into the system from the traditional information security perspective [2]. In theory, the cooperative defense model, system or mechanism is constructed to lay the foundation for the cooperative defense model and method. However, compared with the conventional information system, the security protection means of power grid monitoring is very different. General information security protection means cannot be well applied to the power grid [3]. The research on the security protection of power grid monitoring information at home and abroad mainly focuses on constructing a depth protection system suitable for the power grid, analyzing defense technology and the methods and means to deal with extreme accidents. However, the above research does not focus on the security protection architecture and application of multi-level collaborative information systems in power systems and also lacks comprehensive, detailed and efficient research on its collaborative mechanism and implementation [4]. Therefore, this project intends to study the safe and efficient network security cooperation protection mode and its implementation method to provide a theoretical basis and

*Information security operation and maintenance center of Information Center of Yunnan Power Grid Co., LTD., Kunming, Yunnan, China, 650000 (hangfeilu2021@163.com)
†Information security operation and maintenance center of Information Center of Yunnan Power Grid Co., LTD., Kunming, Yunnan, China, 650000
‡Network Security Management Center of Information Center of Yunnan Power Grid Co., LTD., Kunming, Yunnan, China, 650000
§Network Security Management Center of Information Center of Yunnan Power Grid Co., LTD., Kunming, Yunnan, China, 650000

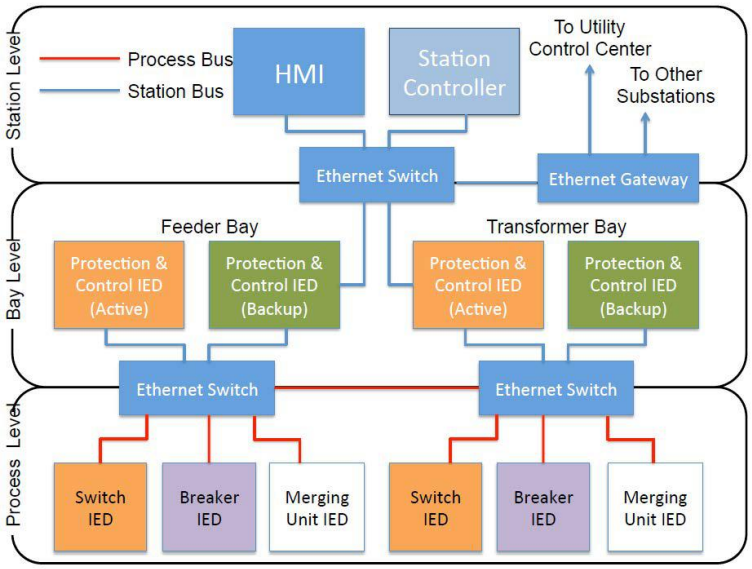

Fig. 2.1: *Architecture of electric power Active security defense system.*

technical support for improving network security accidents' response and control level in power grid security monitoring.

2. Active security defense model.

2.1. Active security defense architecture. The focus of secondary security protection of the power grid is to ensure the safety of the power grid. Defend against hackers, viruses and other attacks to ensure the availability and regular operation of the network [5]. This ensures the confidentiality and integrity of critical data stored and transmitted. Authenticates application systems and devices to prevent unauthorized access. Auditable and secure management of SPDnet and applications. This paper establishes a physical layer-based information security protection method (Figure 2.1 cited in IEEE Transactions on Industrial Informatics, 2017, 14(6): 2442-2451).

The structure of the active security defense system is as follows: 1) Horizontally, the basic level of legal management can be divided into laws and regulations, policies and regulations, security management and ethical guidelines. 2) Technical mechanism The Technical support layer can be divided into security communication protocol, network defense strategy, defense mechanism, and security service. 3) Multi-level protection includes preparatory protection, enhanced protection, detection of feedback, response to blocking, backup recovery, and summary improvement. You can configure the resources of various systems by configuring security protection policies, defense mechanisms, technologies, and services at different levels [6]. A more efficient in-depth defense strategy, mechanism and implementation method with independent intellectual property rights will be established from the three levels of border defense, network defense and management platform.

2.2. Deployment and implementation of power safety protection system. Many large power companies at home and abroad have encountered network security problems in the secondary system, which shows that it is difficult to achieve the safety of the power secondary system only by relying on conventional and passive protection means and only by effectively integrating and configuring it can its comprehensive performance be fully utilized [7]. New technologies such as defense-in-depth strategy mechanisms, unified threat management platforms, intelligent intrusion prevention systems, authentication and encryption and separation technology replace some of the inefficient security management and negative security detection technologies. The active defense strategy mechanism and active defense Security defense System described in this paper are used for practice (Figure 2.2 cited in Challenges in Power System Information Security). According to the

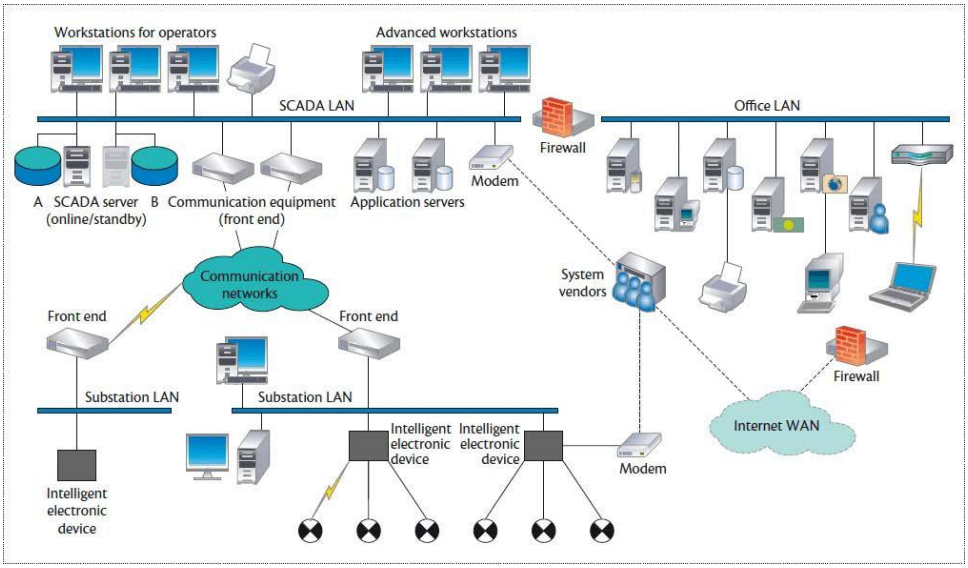

Fig. 2.2: *Architecture of active safety protection system for secondary power supply.*

layout of the active safety defense system of the power secondary system, the integration method is adopted to supplement each function module [8]. Then, the implementation and management of each security policy are unified to build a set of effective three-dimensional protection systems. As shown in Figure 2.2, a host-based intrusion prevention system is configured to monitor, defend against, and respond to abnormal behavior of the network and server. The monitoring and prevention of scheduling MIS and SPInet, DMIS internal access and DMIS access are emphasized. The network intrusion detection center can be managed, controlled, and unified. In combination with local server cluster response, cache support and synchronization of enterprise cloud computing servers, the client/server-side distribution is configured to the server side using function integration [9]. An access control mechanism based on the acceptable behavior of users is proposed to realize the comprehensive detection, protection and maintenance of users. At the same time, IPsec VPN technology establishes several VPNs with different logic based on CISCO routers.

3. Issuance of relevant decisions. Factors such as the impact degree, threat degree, reliability and timeliness of defense behavior, frequency and correlation degree of information security incidents are considered comprehensively. Construct a decision set, an assignment reference sequence, a correlation coefficient and a weight correlation degree [10]. The correlation between various factors and defense strategies in information security incidents is studied. For specific and consistent information security incidents, select relevant defensive measures and publish and implement them.

3.1. Decision Set. According to the specific information security accident, the relationship between each factor and protective measures is analyzed and established [11]. The data for Group n factors are listed in the following matrix. m is the number of defensive actions that can be taken.

$$(U_1', U_2', \cdots, U_n') = \begin{pmatrix} U_1'(1) & U_2'(1) & \cdots & U_n'(1) \\ U_1'(2) & U_2'(2) & & U_n'(2) \\ \vdots & \vdots & & \vdots \\ U_1'(m) & U_2'(m) & \cdots & U_n'(m) \end{pmatrix}$$

U_n is the set of m defense measures corresponding to the n impact shadow of a network security event. $U_n(m)$ is the m defense measure of the B impact factor of the event.

3.2. Assign a value to the decision set and determine the reference sequence. By assigning a value to the initial index of Class m possible protection measures corresponding to n factors in the above formula (3.1), the more significant the value, the greater the correlation. The optimal value of each influence factor is taken as the criterion to establish the corresponding reference sequence of various influence factors:

$$U_0' = (U_0'(1), U_0'(2), \cdots, U_0'(m))$$

U_0 is the reference sequence of a security risk index that occurs for a specific information system. Where $U_0'(m)$ is the expected security risk of Class m protective means.

3.3. Correlation coefficient. The binding factors of the corresponding elements of the decision group and the reference series are calculated separately from the equation (3.3), and the correlation factor matrix is formed:

$$L_i(t) = \frac{\min_i |U_0'(t) - U_i'(t)| + \gamma \times \max_i |U_0'(t) - U_i'(t)|}{|U_0'(t) - U_i'(t)| + \gamma \times \max_i |U_0'(t) - U_i'(t)|}$$

$$L_i(t) = \begin{pmatrix} L_1(1) & L_2(1) & \cdots & L_n(1) \\ L_1(2) & L_2(2) & \cdots & L_n(2) \\ \vdots & \vdots & & \vdots \\ L_1(m) & L_2(m) & \cdots & L_n(m) \end{pmatrix}$$

where $i = 1, 2, \cdots, n; t = 1, 2, \cdots, m; U_i(t)$ and $U_0(t)$ are the safety index t of each safety protection countermeasure under the i level factor of determining matrix and reference matrix [12]. The normalized minimum and maximum value are obtained by calculating each safety index's relative difference and each decision set's benchmark index. Finally, the matrix of correlation coefficients is obtained. γ is the analytic factor, $0 < \gamma < 1$. When the γ value is low, the larger the distance between the correlation coefficients, the larger the conclusion. In the calculation of the correlation degree of defense decision, the median value of γ is 0.5 to keep the deviation of the correlation coefficient consistent.

3.4. Weighted correlation degree. Through a comprehensive evaluation of the importance of various influencing factors in this information security accident. According to formula (3.5), the correlation system matrix calculates each factor's protection measure's security index and the average correlation coefficient between each factor. This reflects the correlation between various protective measures and the baseline sequence [13]. The correlation degree between the information security accident and various protection schemes is given.

$$p_i = \frac{1}{m} \sum_{t=1}^{m} \varphi_t \times L_i(t)$$

$i = 1, 2, \cdots, n; t = 1, 2, \cdots, n; \varphi_t$ is the weight of each factor in their respective influence. p_i' is the weighted mean of the i defense measure in this incident [14]. This paper takes the USB wireless card of a service device to access a specific network security problem as an example to analyze. Table 3.1 Uses the maximum relevancy evaluation algorithm to test this example and concludes that the correlation coefficient of the "network card disabled" processing method is significant.

4. Simulation experiment and result analysis.

4.1. Experimental simulation and description. The test environment comprises three servers, one router, and six clients. Using .NET to develop identity authentication authorization, behavior evidence standardization, document discovery mechanism, credibility evaluation and other modules [15]. The abnormal file was operated on a VMware virtual workstation, and the dynamic analysis was carried out. On a small-scale cloud storage platform, use Net Flow Tracker to monitor the status of each service in real-time. 1) Build customer trust $D = \{0.3, 0.6\}$. The user is then asked to authenticate. A small-scale cloud storage system $L = \{L_1, L_2, L_3\}$ can be divided into three layers. L_1 indicates a rejection of the service. L_2 means that only the file can be read. L_3 is for files that can be edited and downloaded. C between $[0, 0.3)$ is a customer with a

Table 3.1: *Examples of information security incident prevention strategies based on relevancy.*

USB wireless card access event	Business impact degree	Security level	Frequency of policy reliability occurrence	Duration	Correlation with other events	Correlation degree
Disable network card	104	104	626	0	104	96.81
The front switch port is powered off	94	104	83	83	94	82.53
Tunnel blocking	73	83	94	52	73	64.24
The primary route is blocked	42	52	104	10	42	52.05
Specific gravity distribution	21	21	16	21	36	-

poor credit rating and enjoys the business of grade L_1.C between $[0.3, 0.6]$ is a general honor customer. All its business is grade L_2. C between $[0.6, 1)$ are customers with higher credit, who enjoy L_3 type of service. Set the credibility level of the suspicious file to $T = \{0.4, 0.5\}$. Ci has good document credibility in the range $[0, 0.4)$.Ci has A trust level of unknown in the range [0.4, 0.5). Ci has a trust level of Trusted in the range $[0.5, 1]$. 2) In the interaction between users and cloud computing, BM constantly monitors users' behaviors and records them in the behavior database as user behaviors. The trust evaluation model evaluates users' credibility [16]. And give early warning to potential emergencies. The user's business level is given real-time early warning so that the user can dynamically adjust the business level according to their own needs.

4.2. Operation of confidence evaluation cases. The Performance Monitoring Center collected 12 types of evidence from users within 30 minutes. The average evidential value, $Q = \{Q_1, Q_2, Q_3, Q_4, Q_5, Q_6, Q_7, Q_8\}$

$$= \{0.62, 0.51, 0.88, 0.83, 0.74, 0.67, 0.73, 0.54\}$$

$L = \{L_1, L_2, L_3, L_4\} = \{0.33, 0.28, 0.15, 0.08\}$ is obtained by normalizing it. Determine the weights for performance and security features [17]. The following uses performance features as an example. Experience shows that IP packet response time, IP transmission rate, throughput rate and bandwidth occupancy can best reflect the performance characteristics of users. $[d(Q_1) = d(Q_4) = d(Q_6) = d(Q_7)] > [d(Q_2) = d(Q_8)] > [d(Q_3) = d(Q_5)]$. Build the initial judgment matrix:

Determine the weight of performance characteristics and safety characteristics [18]. The practice has proved that in the network, the response time of IP packets, IP data transmission rate, traffic and occupancy rate are the best indicators.

$$[d(Q_1) = d(Q_4) = d(Q_6) = d(Q_7)] > [d(Q_2) = d(Q_8)] > [d(Q_3) = d(Q_5)]$$

Generate a preliminary decision matrix:

$$EP = \begin{bmatrix} 0.5 & 1 & 1 & 0.5 & 1 & 0.5 & 0.5 & 1 \\ 0 & 0.5 & 1 & 0 & 1 & 0 & 0 & 0.5 \\ 0 & 0 & 0.5 & 0 & 0.5 & 0 & 0 & 0 \\ 0.5 & 1 & 1 & 0.5 & 1 & 0.5 & 0.5 & 1 \\ 0 & 0 & 0.5 & 0 & 0.5 & 0 & 0 & 0 \\ 0.5 & 1 & 1 & 0.5 & 1 & 0.5 & 0.5 & 1 \\ 0.5 & 1 & 1 & 0.5 & 1 & 0.5 & 0.5 & 1 \\ 0 & 0.5 & 1 & 0 & 1 & 0 & 0 & 0.5 \end{bmatrix}$$

Calculate $\varphi_{\underline{Q}}^T = \{0.161, 0.107, 0.071, 0.161, 0.071, 0.161, 0.161, 0.107\}^T$ weighted vector for evidence related to performance characteristics: A. The importance of evidence related to safety features is $[d(L_3) = d(L_2)] > d(L_1) > d(L_4)$ in pairwise comparison. And similarly, the weight vector is going to give us $\varphi_L^T = \{0.208, 0.333, 0.333, 0.125\}^T$. If the importance of the user's behavioral feature is $d(Q) < d(L)$, then the feature weight is $\varphi_g^T = \{0.25, 0.75\}^T$. The user behavior characteristic evaluation value $G = K \times \varphi^T = (0.656, 0.222)^T$ is obtained by formula (3.4). Find out the user behavior of the evaluation result $C = 0.67$. The user has a high reputation and can edit and download files in a small-scale cloud storage system. Figure 4.1 shows the overall level of trust change caused by the gradual increase of undesirable actions, such as illegal connections

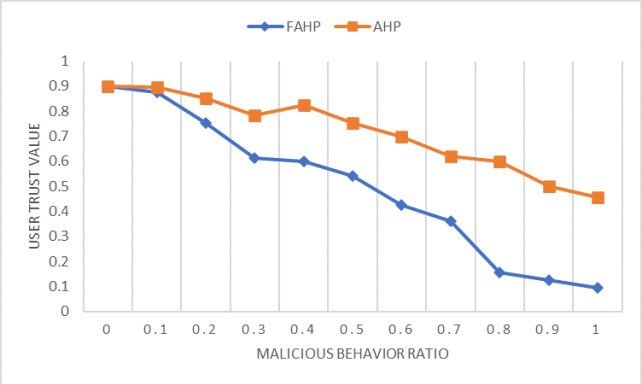

Fig. 4.1: *Changes in trust values of customer machines.*

and critical port scanning, when users interact with the cloud [19]. When there are a lot of malicious activities in the network, the trust value obtained by the fuzzy analytic hierarchy process (AHP) decreases faster than that by AHP and is closer to the cognitive law of human beings. This method can detect low credit users earlier and faster than the analytic hierarchy process and help verify the rights management system to upgrade the customer's business level in real-time, thus reducing the security risks in the cloud.

When constructing the decision matrix, the analysis should be carried out according to the specific situation of customers. Security features become more important if the user is in a non-security situation. Therefore, even if the same evidence is obtained for the same customer, its judgment matrix is different under different circumstances.

5. Conclusion. A multi-level safety protection system of power monitoring system has been established. This project plans to start from three levels: the host layer, security equipment layer and network layer. Security risks at different levels are classified and actively defended through self-defense and cross-domain cooperation. The experimental results show that the proposed method can adapt well to the security protection requirements of the current power grid monitoring system, enhance the security protection level of the power grid, and make the power grid change from the traditional passive defense to the active defense. The research work of this project has crucial academic significance and practical application prospects.

REFERENCES

[1] Hu, H., Liu, Y., Chen, C., Zhang, H., & Liu, Y. (2020). Optimal decision making approach for cyber security defense using evolutionary game. IEEE Transactions on Network and Service Management, 17(3), 1683-1700.
[2] Zhang, K., Zhang, J., Xu, P. D., Gao, T., & Gao, D. W. (2021). Explainable AI in deep reinforcement learning models for power system emergency control. IEEE Transactions on Computational Social Systems, 9(2), 419-427.
[3] Xiong, W., Legrand, E., Åberg, O., & Lagerström, R. (2022). Cyber security threat modeling based on the MITRE Enterprise ATT&CK Matrix. Software and Systems Modeling, 21(1), 157-177.
[4] Georgiadou, A., Mouzakitis, S., Bounas, K., & Askounis, D. (2022). A cyber-security culture framework for assessing organization readiness. Journal of Computer Information Systems, 62(3), 452-462.
[5] Zhang, D., Feng, G., Shi, Y., & Srinivasan, D. (2021). Physical safety and cyber security analysis of multi-agent systems: A survey of recent advances. IEEE/CAA Journal of Automatica Sinica, 8(2), 319-333.
[6] Sarker, I. H. (2023). Machine learning for intelligent data analysis and automation in cybersecurity: current and future prospects. Annals of Data Science, 10(6), 1473-1498.
[7] Maček, D., Magdalenić, I., & Redep, N. B. (2020). A systematic literature review on the application of multicriteria decision making methods for information security risk assessment. International Journal of Safety and Security Engineering, 10(2), 161-174.
[8] Abdallah, M., Naghizadeh, P., Hota, A. R., Cason, T., Bagchi, S., & Sundaram, S. (2020). Behavioral and game-theoretic security investments in interdependent systems modeled by attack graphs. IEEE Transactions on Control of Network Systems, 7(4), 1585-1596.
[9] Chen, X., Qu, G., Tang, Y., Low, S., & Li, N. (2022). Reinforcement learning for selective key applications in power systems: Recent advances and future challenges. IEEE Transactions on Smart Grid, 13(4), 2935-2958.

[10] Cao, R., Hao, L., Gao, Q., Deng, J., & Chen, J. (2020). Modeling and decision-making methods for a class of cyber–physical systems based on modified hybrid stochastic timed petri net. IEEE Systems Journal, 14(4), 4684-4693.
[11] Wu, T., Xue, W., Wang, H., Chung, C. Y., Wang, G., Peng, J., & Yang, Q. (2020). Extreme learning machine-based state reconstruction for automatic attack filtering in cyber physical power system. IEEE Transactions on Industrial Informatics, 17(3), 1892-1904.
[12] Ani, U. P. D., Watson, J. M., Green, B., Craggs, B., & Nurse, J. R. (2021). Design considerations for building credible security testbeds: Perspectives from industrial control system use cases. Journal of Cyber Security Technology, 5(2), 71-119.
[13] Ning, X., & Jiang, J. (2021). Design, analysis and implementation of a security assessment/enhancement platform for cyber-physical systems. IEEE Transactions on Industrial Informatics, 18(2), 1154-1164.
[14] Kim, D. W., Choi, J. Y., & Han, K. H. (2020). Risk management-based security evaluation model for telemedicine systems. BMC Medical informatics and decision making, 20(1), 1-14.
[15] Zhu, L., Li, Y., Yu, F. R., Ning, B., Tang, T., & Wang, X. (2020). Cross-layer defense methods for jamming-resistant CBTC systems. IEEE Transactions on Intelligent Transportation Systems, 22(11), 7266-7278.
[16] Sengupta, S., Chowdhary, A., Sabur, A., Alshamrani, A., Huang, D., & Kambhampati, S. (2020). A survey of moving target defenses for network security. IEEE Communications Surveys & Tutorials, 22(3), 1909-1941.
[17] Liu, Y., Gao, S., Shi, J., Wei, X., & Han, Z. (2020). Sequential-mining-based vulnerable branches identification for the transmission network under continuous load redistribution attacks. IEEE Transactions on Smart Grid, 11(6), 5151-5160.
[18] Olowononi, F. O., Rawat, D. B., & Liu, C. (2020). Resilient machine learning for networked cyber physical systems: A survey for machine learning security to securing machine learning for CPS. IEEE Communications Surveys & Tutorials, 23(1), 524-552.
[19] Sahu, A. K., Padhy, R. K., & Dhir, A. (2020). Envisioning the future of behavioral decision-making: A systematic literature review of behavioral reasoning theory. Australasian Marketing Journal, 28(4), 145-159.

Edited by: Zhigao Zheng
Special issue on: Graph Powered Big Aerospace Data Processing
Received: Nov 27, 2023
Accepted: Dec 15, 2023