Research on Network Security Automation and Orchestration Oriented to Electric Power Monitoring System

Xiaobo Ling[1], Longyun Qi[2], Man Li[3], and Jun Yan[2,4,5(✉)]

[1] State Grid Shanghai Municipal Electric Power Company, Shanghai 200122, China
[2] State Grid Electric Power Research Institute, Nanjing 210003, China
qilongyun@sgepri.sgcc.com.cn, yanjun_2021@163.com
[3] State Grid Shanghai Municipal Electric Power Company Songjiang Power Supply Company, Shanghai 201699, China
[4] Intelligent Manufacturing Department, Wuyi University, Jiangmen 529020, China
[5] School of Cyber Science and Engineering, Nanjing University of Science and Technology, Nanjing 210094, China

Abstract. Nowadays, an electric power monitoring system may cause great damage due to security incidents happened. Furthermore, traditional active defense technologies no longer guarantee the safety and reliability of an electric power monitoring system. Thus, it is urgent to develop a new security defense technology suitable for the electric power monitoring system, the new security defense technology can take precautions against the destructive attacks occurring in the electric power monitoring system. According to the analysis of the network security demands of the electric power monitoring system, we propose an active defense system framework based on security automation and orchestration technology (i.e., SAOT). The active defense system framework with multi-layer architecture and functional modules integrates modules such as the behavioral feature extraction of typical network security events, the security disposal strategy generation of typical network security events, and the automation orchestration of security disposal strategies. Furthermore, the SAOT active defense system framework simultaneously solves the aspects of the vulnerability and security problems in the electric power monitoring system. Finally, a case study is adopted to further describe and explain the SAOT active defense system framework. Results indicate that the SAOT active defense system framework can ensure the information security of the national power system in cyberspace.

Keywords: Network security · Security automation and orchestration technology · Electric power monitoring system · Active defense system

1 Introduction

Currently, computer, network and communication technologies are popular in modern power systems; furthermore, the electric power monitoring system is a piece of intelligent

M. R. Khosravi et al. (Eds.): CloudComp 2021, LNICST 430, pp. 195–206, 2022.
https://doi.org/10.1007/978-3-030-99191-3_15

equipment that monitors and controls the process of power production and supply based on computer and network technology, supported by communication and data networks. In fact, the electric power monitoring system makes sense to ensure the safe and stable operation of the modern power system [1]. Moreover, according to the neural network and control center of the whole power system, i.e., the electric power monitoring system, the countries and the governments can provide reliable electricity to industries efficiently and residents to enhance economic and social development in a further step.

However, computer, network and communication attacks against the electric power monitoring system have broken out frequently, and these computer, network and communication attacks have the characteristics of specialization, high hazard and high persistent threat [2, 3]. Thus, the security defense of the electric power monitoring system has already been emphasized at the national security level. Furthermore, as computer, network and communication security incidents may cause great damage to the electric power monitoring system, the power grid company needs to establish and improve a comprehensive security protection system of the electric power monitoring system continuously.

In the electric power monitoring system, the appropriate and rapid response to computer, network and communication attacks is crucial to minimize and avoid attack as it is hard to prevent all attack incidents before it comes out. To this end, it is now becoming significant to construct a quick and proper network security response in the electric power monitoring system. The network security response can minimize and avoid attacks to the electric power monitoring system caused by attack incidents; meanwhile, the network security response can reduce the possibility of data damage.

Drawing on mature security defense theories at home and abroad [4], and according to the analysis of the network security demands of the electric power monitoring system, we propose an active defense system framework based on the security automation and orchestration technology (i.e., SAOT). Furthermore, the SAOT active defense system framework consists of multi-layer architecture and functional modules. This framework mainly integrates modules such as the behavioral feature extraction of typical network security events, the security disposal strategy generation of typical network security events, and the automation orchestration of security disposal strategies. In fact, the active defense system framework simultaneously solves the aspects of the vulnerability and security problems in the electric power monitoring system to ensure the safe, stable, and economic operation of the modern power system and the electric power monitoring system; furthermore, the set of active defense system framework further ensures the information security of the national power system in cyberspace.

Contributions of this paper can be summarized as follows:

(1) To minimize and avoid attacks to the electric power monitoring system caused by computer, network and communication attack incidents, we propose an active defense system framework based on security automation and orchestration technology (i.e., SAOT). The SAOT active defense system framework can simultaneously address the vulnerability and security problems in the electric power monitoring system.
(2) The SAOT active defense system framework consists of multi-layer architecture and functional modules. This framework mainly integrates modules such as the

behavioral feature extraction of typical network security events, the security disposal strategy generation of typical network security events, and the automation orchestration of security disposal strategies.

(3) Finally, we employ a case study to further verify the effectiveness and feasibility of the SAOT active defense system framework. Meanwhile, the SAOT active defense system framework can ensure the safe, stable, and economic operation of the modern power system and the information security of the national power system in cyberspace.

The rest of this paper is organized as follows. Section 2 refers to related work. Section 3 presents the research motivation of the electric power monitoring system security defense. Section 4 presents an active defense system framework based on security automation and orchestration technology (i.e., SAOT). In Sect. 5, a case study verifies the effectiveness and feasibility of the SAOT active defense system framework. Finally, Sect. 6 summarizes the research content and future direction of the paper.

2 Related Work

2.1 Anomaly Detection

Anomaly detection is an active research topic and plays an important role in more and more fields. Currently, the role of anomaly detection in different scenarios has been explored and researched in many aspects [5]. For example, the work of [6] proposed a probability model of the mentioning behavior of a social network user, and the probability model detected the emergence of a new topic from the anomalies. For electric power data, Pang et al. [7] taken advantage of data mining correlation analysis, anomaly detection, hypothesis testing and sequence analysis methods in responding to the challenges faced by the information security protection system. Based on the deep learning algorithm, Hinami et al. [8] integrated a generic CNN model and anomaly detection based on environment to solve the problem of joint detection and recounting of abnormal events in videos; in practice, their first learned CNN with multiple visual tasks to separate object features and action attributes, and then recounted and detected anomalous activity by plugging the model into anomaly detectors. Furthermore, Luo et al. [9] were inspired by the capability of sparse coding-based anomaly detection, and presented a Temporally-coherent Sparse Coding (TSC) approach; the TSC approach mapped a temporally coherent sparse coding for stack RNN to enhance the reconstruction coefficient and executed identification based on reconstruction error. In fact, as smaller amounts of anomalous instances are combined with the dictionary, the TSC approach failed to detect similar types of anomalous activities. In addition, the log-based anomaly detection research was classified into two broad categories, i.e., online anomaly detection system and offline anomaly detection system [10]: for online anomaly detection system, as the events are recorded, the system performs anomaly detection in real-time; for offline anomaly detection system, the system is mainly used to debug or detect anomalies when they occur.

2.2 Active Defense

Traditional active defense methods mainly contain the fire-wall, honeypot techniques and so on. At present, academia and industry have made progress in active defense. For example, many defensive measures have been taken by the cybersecurity community to solve the adversarial intrusion problems in industrial control networks. Wang et al. [3] proposed an active defense system framework based on the analysis of the network security demands of the electric power monitoring system. The active defense system framework contained multiple modules (i.e., data collection, threat analysis and identification, active defense strategy library, etc.), and these modules were independent of each other. Furthermore, the security attacks of the industrial Internet have become more covert and diversified. Traditional active defense approaches only defended a single attack, so Sun et al. [11] showed a three-dimensional defense architecture depended on deception defense and active defense. The model can deal with the complex and diversified security protection requirements of the industrial Internet. In addition, Zhang et al. [12] presented an active DDoS defense model based on packet marking to address the problem of DDoS attacks. The model mainly contained two parts: the subsystem for tracking the attacks and the subsystem for filtering the attack flows. Meanwhile, the model used an authenticated packet marking scheme for IP trace-back to reconstruct the attack path efficiently. Ma et al. [13] proposed a malicious code intrusion active defense technology and the defense technology structure in solving the low defense efficiency and poor stability problems of the traditional LAN networks. Meanwhile, the system structure mainly contained three parts: executive layer, kernel layer and hardware layer, and the work-flow contained four parts, i.e., file display, file processing, file judgment and file compression.

In this section, we mainly show various existing anomaly detection and active defend methods. According to the above research analysis, we propose an active defense system framework based on security automation and orchestration technology (i.e., SAOT). SAOT can simultaneously solve the vulnerability and security problems in the electric power monitoring system. Next, we will describe the research motivation of the electric power monitoring system security defense in Sect. 3.

3 Research Motivation

In Fig. 1, the main structure of the electric power monitoring system is a multi-layer star network. Specifically, the electric power monitoring system adopts the double star structure between the backbone layer and the core layer; meanwhile, the upper point of the backbone layer and the core layer is regarded as the network node. As the network structure characteristics of the electric power monitoring system are multi-layer and distributed, the power monitoring system needs to realize self-defense within the node domain of the local level and cross-domain cooperation defense between different levels. In addition, existing security technologies have static superposition characteristics, and some existing defense methods have single and solidified characteristics. According to the above analysis, the existing security defense approaches fail to satisfy the demand of the electric power monitoring system with dynamic, active, and cross-domain defenses

under the background of new threats. Therefore, we will encounter and address some problems in the process of active defense, as follow:

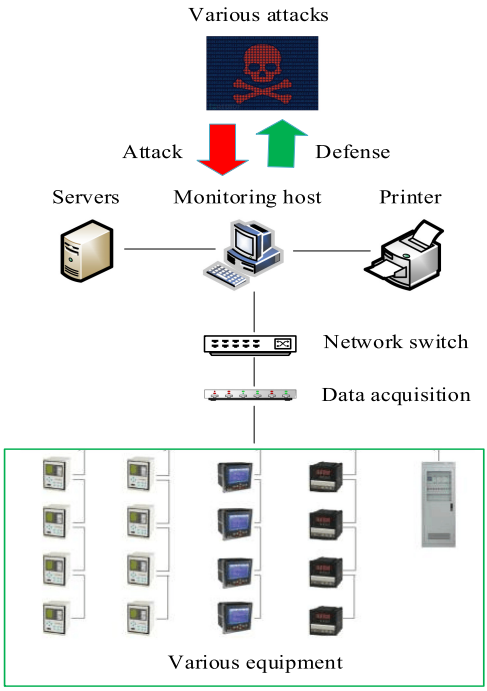

Fig. 1. An intuitive example of our research motivation.

(1) At present, all kinds of security facilities deployed on the electric power monitoring system mainly depend on the equipment's solidification strategy. Thus, the coordination among these security facilities is facing different safety defense objectives.
(2) Furthermore, various types of security operation information, equipment operation information and data log information data of these security facilities fail to collect, fuse, process and distribute rapidly, so the security facilities do not share security threat information among themselves in time and further increase the case of missing and misinformation of threat warning information.
(3) In the electric power monitoring system, the decentralized detection and response mechanisms need to be integrated to adaptively implement diverse security disposal strategies that support the master station layer, network layer, plant station layer, and various equipment (i.e., cross-network equipment, security equipment and host equipment). Thus, the electric power monitoring system can achieve the blocking and isolation of network security risks more reliably, accurately, and faster.

In short, according to the network structure of the electric power monitoring system and the existing security defense technologies, how to design a multi-level and cross-domain automation orchestration technology of security disposal strategies is the key and difficult point of this paper. Next, this paper proposes a new active defense system framework based on security automation and orchestration technology (i.e., SAOT), introduced in detail in Sect. 4.

4 An Active Defense System Framework Design

According to the above analysis, we propose an active defense system framework based on the security automation and orchestration technology (i.e., SAOT). As shown in Fig. 2, our active defense system framework follows a task sequence, and the task sequence mainly contains the following three activities: (1) the behavioral feature extraction of typical network security events, (2) the security disposal strategy generation of typical network security events, (3) and the automation orchestration of security disposal strategies.

4.1 The Behavioral Feature Extraction of Typical Network Security Events

As shown in Fig. 2, there are three diverse data source feature extraction technologies, i.e., data source feature extraction and analysis based on Agent acquisition, data source feature extraction and analysis based on network flow acquisition, and the behavioral feature extraction and analysis of ATT&CK attack.

Data Source Feature Extraction and Analysis Based on Agent Acquisition. The research of the data source feature extraction and analysis based on Agent acquisition focuses on log files collection, files integrity collection and command monitoring. For log files collection, the Agent log analysis module catches security issues such as system errors, configuration errors, intrusion attempts, and strategy conflicts by monitoring the log files on the server. As the built-in basic analysis rules of Agent can be issued uniformly through the network security management platform, we can identify the remote login of violent cracking, Web attack detection, database violent cracking, system abnormal errors, Web application anomalies and database error information. Furthermore, the Agent log analysis module has the self-adaptive ability, can automatically scan the log directory, and complete the automatic configuration.

For files integrity collection, the Agent files integrity monitoring module can monitor specific files, trigger logging when modifying these files and report to the network security management platform. In addition, the monitoring contents mainly include important Linux system files and Windows registry entries, executable programs, SSH keys and other custom attributes. The files and paths of the built-in Agent basic file integrity monitoring can be uniformly distributed through the network security management platform.

For command monitoring, the Agent command monitoring module can execute system commands, information queries, script predefined operations on the operating system, and then further realize process monitoring, port opening monitoring, network connection monitoring, resource performance monitoring, historical record monitoring, process monitoring, and other custom commands.

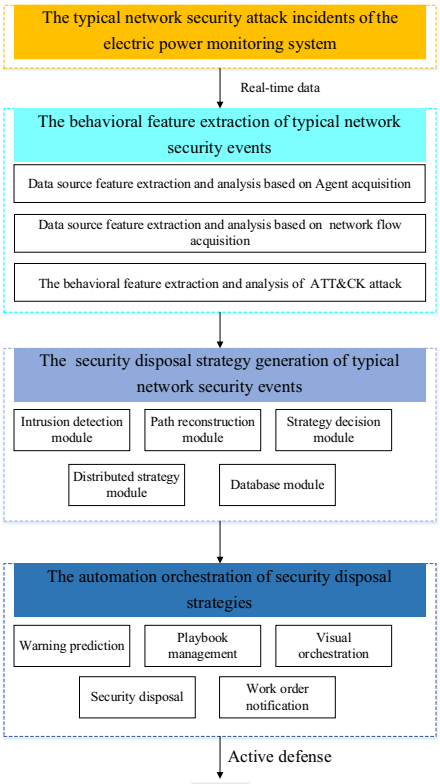

Fig. 2. An active defense system framework based on the security automation and orchestration technology.

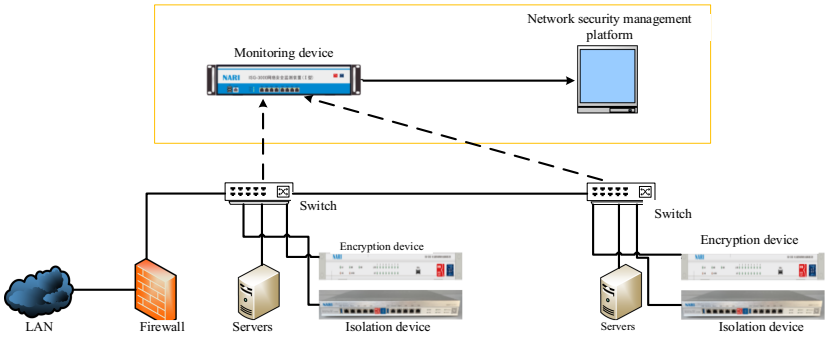

Fig. 3. An intuitive example of data source feature extraction and analysis based on network flow acquisition.

Data Source Feature Extraction and Analysis Based on Network Flow Acquisition. As shown in Fig. 3, the research of the data source feature extraction and analysis based on network flow acquisition concentrates on traffic storage, protocol analysis, and abnormal behavior collection.

For traffic storage, the traffic analysis module supports real-time collection and storage of 100M, Gigabit, and 10G network traffic, and has a certain length of flow data storage capacity and storage expansion capacity. Furthermore, the traffic analysis module can save various statistical data such as captured raw data packets, data streams, network sessions, and application logs in real-time. For protocol analysis, the protocol analysis module supports the recording of communication logs and connection information of common network protocols and industrial control protocols. For abnormal behavior collection, the abnormal behavior collection module detects and analyzes the network flow of the electric power monitoring system to detect abnormal information in the network in time and alarm. The classification of abnormal alarm includes worm, attack, Trojan, abnormal traffic, sensitive information, and so on. Furthermore, the parameter threshold detected by anomalies can be adjusted according to the electric power monitoring system's requirements, and the triggered anomaly information can be uploaded to the network security management platform.

The Behavioral Feature Extraction and Analysis of ATT&CK Attack. The research of the behavioral feature extraction and analysis of ATT&CK attack mainly contains two databases (i.e., threat intelligence database and ATT&CK model database) and four layers (i.e., data layer, analysis layer, recognition layer, and application layer).

In fact, the data layer mainly carries out data collection, normalization processing and data management of network events in the electric power monitoring system. The analysis layer includes two parts: feature analysis and correlation analysis. Furthermore, the analysis layer ascertains the APT attack clues, Trojan viruses, and violent password cracking from the algorithm model based on features. According to the APT attack clues obtained by the analysis layer, the recognition layer identifies and correlates the APT attack from the dimension of attack technology and attack tactics respectively, and finally generates the full picture of the APT attack from the perspective of the attacking team. The application layer mainly performs the visual presentation of the APT attack, the presentation of the global security situation, and the security early warning.

According to the above analysis, three diverse data source behavioral feature extraction technologies can realize the perception, discovery, and root tracing of network attack events in the electric power monitoring system.

4.2 The Security Disposal Strategy Generation of Typical Network Security Events

As shown in Fig. 2, the proposed security disposal strategy generation technology mainly includes five modules: intrusion detection module, path reconstruction module, strategy decision module, distributed strategy module and the database module. The whole security disposal strategy generation technology adopts the centralized control way, and the deployment process adopts the distributed implementation way.

As shown in Fig. 4, the intrusion detection module will respond timely when it detects the intrusion attack. At the same time, the intrusion alarm and attack data are transmitted to the path reconstruction module. Once receiving the intrusion alarm and attack data information, the path reconstruction module will analyze the attack event and reconstruct the path, and send the reconstructed attack path information (i.e., attack topology information) to the strategy decision module. After receiving the attack topology information, the strategy detection module starts to analyze the attack topology information and formulate the corresponding security strategy. After that, the prepared security strategy information is edited into strategy request information and sent to the distributed strategy module. Then, the distributed strategy module generates the corresponding security strategy rules and the deployment information. The distributed strategy module integrates the generated security strategy rules and deployment information, edits the strategy request response information, and sends it to the strategy decision module. At last, when the strategy request-reply is received from the distributed strategy module, the strategy decision module sends a strategy reply message to the intrusion detection module to complete the strategy generation process. Meanwhile, all generated entire strategies are stored in the database module.

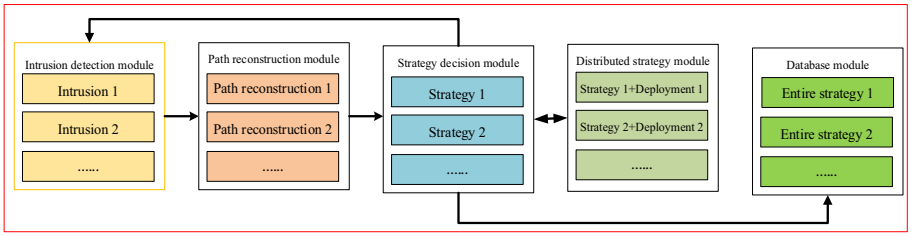

Fig. 4. The process of the security disposal strategy generation technology.

Based on the behavioral feature extraction of typical network security events, the response and generation of the security disposal strategy can be completed by evaluating the impact factors comprehensively such as event type, event frequency, response time, scope, and risk.

4.3 The Automation Orchestration of Security Disposal Strategies

As shown in Fig. 2 and Fig. 5, the proposed automation orchestration of security disposal strategies mainly includes five parts: warning prediction, playbook management, visual orchestration, security disposal, and work order notification. Additionally, the process of the automation orchestration of security disposal strategies can achieve the blocking and isolation of network security risks reliably, accurately, and faster.

The warning prediction is mainly made up of trigger conditions and response actions. In fact, the warning prediction is a continuous analysis and response to a group of related log events. Furthermore, the warning prediction can assign different Playbook scripts to different types of cases with the case processing function, and supervise the execution. For playbook management, Playbook is a “script” that records the security engineer’s

workflow. Common Playbooks include investigation and forensics, global blocking, host isolation, work order, email warning, etc. In fact, Playbook can be created and saved through visual orchestration and can be referenced by rules. Meanwhile, the Playbook is triggered when the conditions are met, and the response device is called to perform the response action.

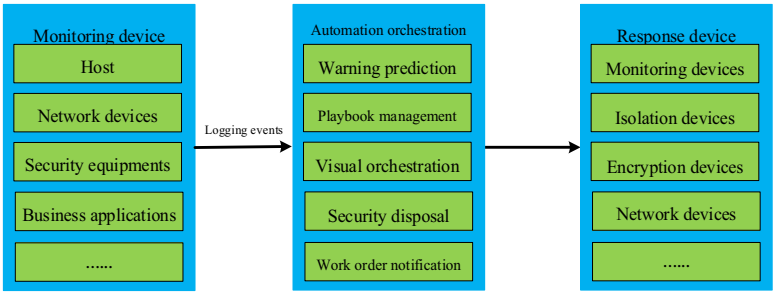

Fig. 5. The process of the automation orchestration of security disposal strategies.

The visual orchestration charges for generating strategies and Playbooks. The visual orchestration simplifies the security operational disposal process by the drag-and-drop way. In addition, the visual orchestration provides context for security disposal and reduces the complexity of security incident disposal. For security disposal, the automatic orchestration ban is generally implemented by devices performing response disposal actions, and Playbook calls different triggered devices to perform disposal action. For work order notification, the manager will carry out relevant security disposals after receiving the work orders.

5 A Case Study

In this section, a case study is discussed to demonstrate the process of the active defense system framework based on the security automation and orchestration technology (i.e., SAOT).

In Fig. 6, we use the data information provided by NARI Information & Communication Technology CO., LTD to implement the execution process of the SAOT method. First, we use three diverse data source feature extraction technologies (i.e., data source feature extraction and analysis based on Agent acquisition, data source feature extraction and analysis based on network flow acquisition, and the behavioral feature extraction and analysis of ATT&CK attack) to process existing data. Thus, the behavioral feature extraction of typical network security events approach can realize the perception, discovery, and root tracing of network attack events in the electric power monitoring system. Next, according to the behavioral feature extraction of typical network security events, the response and generation of the security disposal strategy can be completed by comprehensively evaluating the impact factors such as event type, event frequency, response time, scope, and risk. Finally, based on the behavioral feature extraction of typical network security events and the security disposal strategy generation, we take advantage

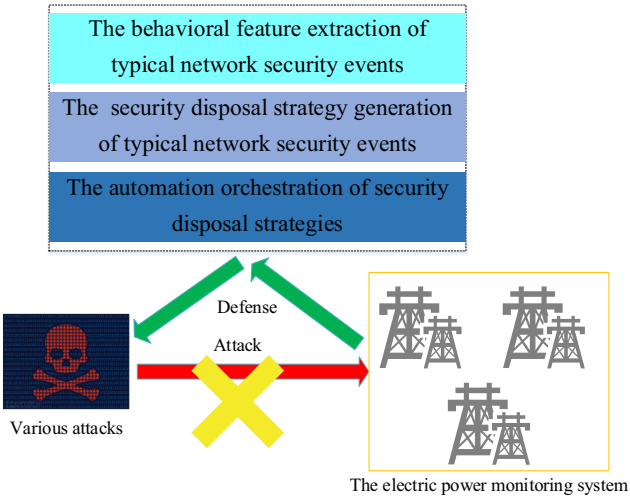

Fig. 6. A case study of the electric power monitoring system attack and defense.

of the automation orchestration mothed to adaptively implement and perform diverse security disposal strategies that support the master station layer, network layer, and plant station layer. Thus, the electric power monitoring system can achieve the blocking and isolation of network security risks more reliably, accurately, and faster.

6 Conclusion and Future Work

In this paper, we put forward a novel active defense system framework based on security automation and orchestration technology (i.e., SAOT). The SAOT mainly integrates modules such as the behavioral feature extraction of typical network security events, the security disposal strategy generation of typical network security events, and the automation orchestration of security disposal strategies. Furthermore, the SAOT simultaneously solves the vulnerability and security problems in the electric power monitoring system to ensure the safe, stable, and economic operation of the modern power system and the electric power monitoring system.

In the follow-up work, the real-world experiments are designed and performed to further validate the feasibility and effectiveness of the SAOT approach. Meanwhile, we will continue to verify the field test work of the security automation and orchestration technology suitable for the electric power monitoring system.

Acknowledgment. This work was supported in part by 2021 Science and Technology Project of State Grid Corporation: Research on Vulnerability Analysis and Threat Detection Key Technology of Power Monitoring System in Cyberspace. No. 5108-202117055A-0-0-00. The 4th project "Research on the Key Technology of Endogenous Security Switches" (2020YFB1804604) of the National Key R&D Program, the 2020 Industrial Internet Innovation and Development Project from Ministry of Industry and Information Technology of China, the Fundamental Research Fund for the Central Universities (30918012204, 30920041112).

References

1. Li, T., Su, S., Yang, H., Wen, F., Wang, D., Zhu, L.: Attacks and cyber security defense in cyber-physical power system. Autom. Electric Power Syst. **41**(22), 162–167 (2017)
2. Liu, N., Yu, X., Zhang, J.: Coordinated cyber-attack: inference and thinking of incident on Ukrainian power grid. Autom. Electric Power Syst. **40**(6), 144–147 (2016)
3. Wang, Z., Zhu, S., Huang, T., Zhu, J., Fang, H.: Research on network security active defense system oriented to electric power monitoring system. In: 2020 IEEE International Conference on Information Technology, Big Data and Artificial Intelligence (ICIBA), Chongqing, China, pp. 883–887. IEEE (2020)
4. Xu, R., Chen, J.: Collaborative defense architecture of cyberspace security. Commun. Technol. **49**(01), 92–96 (2016)
5. Qi, L., Zhang, X., Li, S., et al.: Spatial-temporal data-driven service recommendation with privacy-preservation. Inf. Sci. **515**, 91–102 (2020)
6. Takahashi, T., Tomioka, R., Yamanishi, K.: Discovering emerging topics in social streams via link anomaly detection. IEEE Trans. Knowl. Data Eng. **26**(1), 120–130 (2013)
7. Kim, H., Kim, I., Chung, T.-M.: Abnormal behavior detection technique based on big data. In: Park, J., Zomaya, A., Jeong, H.-Y., Obaidat, M. (eds.) Frontier and Innovation in Future Computing and Communications. LNEE, vol. 301, pp. 553–563. Springer, Dordrecht (2014). https://doi.org/10.1007/978-94-017-8798-7_66
8. Hinami, R., Mei, T., Satoh, S.: Joint detection and recounting of abnormal events by learning deep generic knowledge. In: 2017 IEEE International Conference on Computer Vision (ICCV), Venice, Italy, pp. 3639–3647. IEEE (2017)
9. Luo, W., Liu, W., Gao, S.: A revisit of sparse coding based anomaly detection in stacked RNN framework. In: 2017 IEEE International Conference on Computer Vision (ICCV), Venice, Italy, pp. 341–349. IEEE (2017)
10. Vannel, Z., Donghyun, K., Daehee, S., Ahyoung, L.: An unsupervised anomaly detection framework for detecting anomalies in real time through network system's log files analysis. High-Confidence Comput. **1**(2), 100030 (2021)
11. Sun, Y., Peng, X., Tian, Z., Guo, S.: A deception defense and active defense based three-dimensional defense architecture: DA-3DD design and implementation plan. In: 2019 15th International Conference on Mobile Ad-Hoc and Sensor Networks (MSN), Shenzhen, China, pp. 422–427. IEEE (2019)
12. Zhang, Y., Wan, Z., Wu, M.: An active DDoS defense model based on packet marking. In: 2009 Second International Workshop on Computer Science and Engineering, Qingdao, China, pp. 435–438. IEEE (2009)
13. Ma, L., Kang, Y.-J., Han, H.: Research on LAN network malicious code intrusion active defense technology. In: Gui, G., Yun, L. (eds.) ADHIP 2019. LNICSSITE, vol. 301, pp. 57–64. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-36402-1_6