*Electronics, Communications and Networks*
*A.J. Tallón-Ballesteros et al. (Eds.)*


*doi:10.3233/FAIA231209*

# Research on Network Security Access Based on Intelligent Active Defense

Yunxi FU[1], Zesan LIU, Ziting GAO and Wenjuan ZHANG
*State Grid Information and Communication Industry Group Co., Ltd., Beijing 100032, China*

**Abstract.** In recent years, with the construction of new power systems, the traditionally relatively closed power grid needs to be opened in an orderly way. The new power system forces more and more heterogeneous mass terminals to be exposed and deployed in the external network, and the power information system interacts frequently with the external system, increasing the attack surface, easy to be external mapping network key information, and increasing pressure of unknown attack. In order to realize the effective protection of network key information, reduce the risk of illegal detection and network attack, and provide technical support for the security protection of new power system. The first part of this paper is to solve the new attack threats faced by the power information system infrastructure by studying the network attack prevention and monitoring technology based on active intelligent defense. The second is to solve the increasingly serious problem of network scanning feature recognition by studying the defense strategies based on feature hiding and information confusion. In this way, the network security protection ability can be improved, and the construction of new power system can be strongly supported.

**Keywords.** Intelligent, active defense, feature hiding, information confusion

## 1. Introduction

As an important part of critical information infrastructure, power grid information infrastructure puts forward more stringent requirements for the security protection of network, data and business. In recent years, with the construction of new power systems, the traditional relatively closed power grid needs to be opened in an orderly way, forcing more and more heterogeneous massive terminals to be exposed and deployed to the external network. The power information system interacts with external systems frequently, and is easy to be mapped by the external network key information.

Illegal network scanning is a prelude to network attacks. How to make the network invisible and shield the external network mapping[1-5] has become a pain point in the industry to improve the security protection ability of the power information system[6-10], a critical infrastructure. The theoretical and technical system of network cloaking is still in the exploratory stage and imperfect. At the same time, the information system in the new power system is carried by backbone transmission, terminal access, local communication and other networks, and forms the power information communication infrastructure of cloud, pipe, edge and end[11]. Among them, the security protection

[1] Yunxi FU, Corresponding author, State Grid Information and Telecommunication Group Co., Ltd., Beijing, 100032, China;E-mail:yunxifu2018@163.com.

capability of the system side is relatively strong, but the edge side faces diversified integration characteristics such as heterogeneous access network integration. The level of security protection is not uniform. Therefore, in view of the continuous evolution of the new power system, exploring the application of network stealth technology in the power information system has become an important way to improve the security protection of the power information system, a key information technology facility, and is of great significance for promoting the security protection of the digital transformation of the power grid.

In summary, based on the existing network security protection architecture of power grid, this paper expands computing power from the side to the side, learns from the idea of "security definable, strategy configurable" endogenous flexible network security protection, breaks through the network dynamic stealth technology and the access key technology in the network stealth scene. It realizes the effective protection of network key information, reduces the risk of illegal detection and network attacks, improves the ability to resist unknown attacks, and provides technical support for the new power system security protection. Firstly, in the second section, we describe the technical difficulties of this research. Then, the third section introduces the technical route to solve these difficulties. Finally, the research content of this paper is summarized and the significance of this study is expounded at the end of the paper.

## 2. Technical Difficulties

Active stealth defense for power information system against illegal network scanning [12-17]. For the network anti-scanning method [18-20] and stealth deployment method, there is no authoritative and perfect technical scheme, especially the lack of systematic research on stealth strategy for power information communication network, and there may be problems such as large transformation cost and poor adaptability. Information hiding methods represented by zero-trust [21] technologies have static and deterministic characteristics, which cannot achieve effective defense when dealing with long-term and customized illegal network scanning methods. The hopping, transformation and redundancy defense mechanisms represented by network mimicry [22-25] and moving target defense [26-29] generally have problems such as high complexity and lack of detailed control strategies. Moreover, the existing defense mechanisms generally have the problem that access security is difficult to evaluate and access efficiency is difficult to guarantee in terms of service access.

## 3. Technical Route

### *3.1. Research on anti-lateral scanning technology based on virtual extensible LAN technology*

In this paper, we study the threat of internal illegal scanning and the requirement of feature hiding when power infrastructure is deployed in the cloud environment. This paper focuses on the lateral scanning threats of power infrastructure in multi-tenant environment, the boundary protection and feature hiding requirements of distributed system, and the dynamic stealth requirements of power information facilities in virtualized network environment and Software Defined Network(SDN) environment.

Based on the stealth requirements of power information facilities in the cloud and virtualization environment, the business segmentation method, network element dynamic deployment and control method of power information system in the cloud environment are studied, and the stealth deployment method and secure connection method based on virtual extensible local area network (VLAN) technology are studied. Vxlan-based anti-lateral scanning architecture can be described as Figure 1.

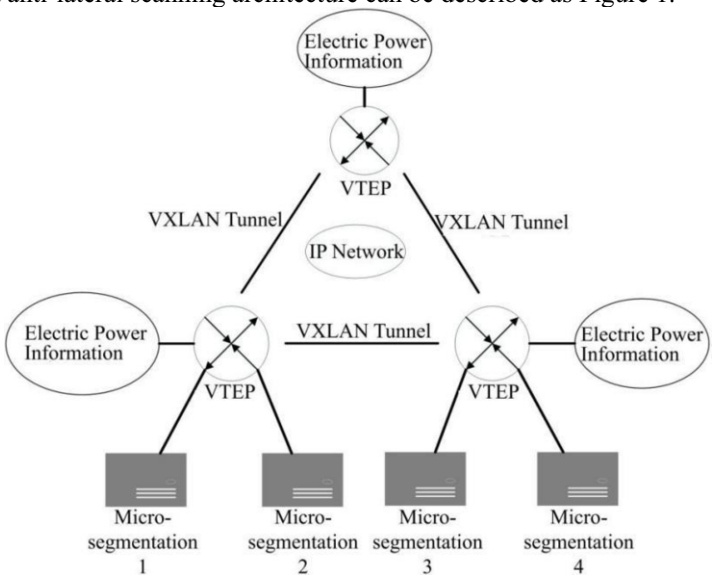


**Figure 1.** Vxlan-based anti-lateral scanning architecture

*3.2. Research on intelligent active defense technology based on network deception*

The illegal scanning defense methods based on artificial intelligence are investigated, and the application forms of artificial intelligence algorithms in active defense mechanisms are summarized. This paper studies the establishment of an intelligent active defense system for illegal scanning through artificial intelligence technologies such as reinforcement learning and generative adversarial networks. Through experiments and simulation, it intends to try to build a game mechanism between intelligent scanning algorithms, feature recognition algorithms and intelligent defense algorithms, and finally improve the intelligence level of stealth defense in power information systems.

This paper, research focuses on the combination of honeynet and other network deception technologies [30-32] with artificial intelligence to construct an intelligent active defense mechanism for illegal scanning, so as to improve the adaptability and feature recognition ability of traditional deception technologies. For the attacker, the task of the attacker is to obtain environmental information as much as possible in an unknown environment to achieve the purpose of the attack. The purpose of adaptive honeypot is to obtain as many characteristics of the attacker as possible by adopting the best response strategy. The essence of automated attack is a sequence of attack commands continuously executed by the attacker based on a fixed decision pattern. If an attack command is regarded as a state, the entire process of automated attack can be abstracted as a directed acyclic graph, and each state is an input attack command. Combined with the "confrontation" and "game" ideas in the generative adversarial network and mimic

honeypot, a mimic honeypot feature generation method based on generative adversarial network is studied. Through structure and parameter optimization training, new features of honeypot or service that are difficult to distinguish between true and false are generated, and the protection ability of intelligent defense system is further improved.

### *3.3. Study the continuous control method of typical power business in network stealth scenario*

The ideas of multi-factor authentication and continuous authentication are adopted, and the ideas of minimum authorization and dynamic authorization are adopted to establish the continuous authorization mechanism in the network stealth scenario. The access and authorization strategies in the network stealth scenario are designed, and the continuous monitoring scheme of the network behavior of the continuous business is established.

Firstly, in the face of similar attacks, the subject should adopt the principle of continuous authentication to control the power business. The principle of continuous authentication refers to the strategic decision point in the zero trust network architecture. The policy decision point component is responsible for the final decision of whether to grant access rights to subjects that need to access resources. The policy decision point will use the access policy and external input as input to the trust algorithm to grant, deny, or revoke access to the resource. The continuous authentication process is as Figure 2.

In the real-time monitoring of abnormal behavior, multiple indicators need to be monitored to make a comprehensive judgment, and abnormal behavior and risk level are evaluated according to the importance of the indicators and the collected values. Grey system theory, analytic hierarchy process, weight method, neural network method and so on are used in the evaluation process. The method of risk assessment mainly uses AHP and fuzzy theory. In the evaluation of methods and strategies, the risk value of many risk factors is difficult to obtain through an accurate statistics, this cannot be accurately quantified, the need to use fuzzy thinking, fuzzy mathematics can make an effective description of these fuzzy factors. Fuzzy comprehensive evaluation is the use of membership theory, that is, the theory of fuzzy mathematics, for complex, affected by multiple factors, hierarchical system problems, can make a better comprehensive evaluation, has good applicability, this evaluation method can be used in combination with the analytic hierarchy process.

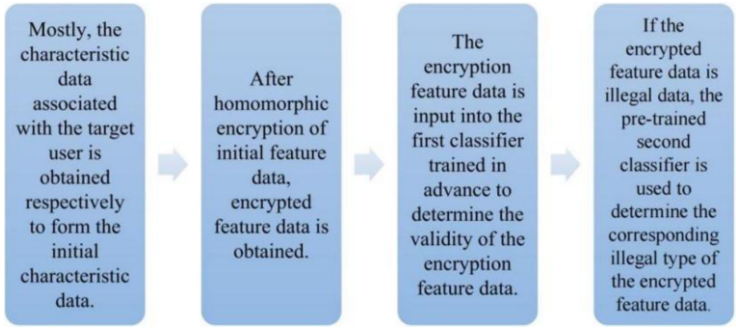


**Figure 2.** Business continuous certification process in smart grid scenario

## 4. Conclusion

Aiming at the problem of illegal access defense under the condition of network stealth, we designs a comprehensive stealth method for new power system information infrastructure according to the elastic network stealth technology architecture that supports software definition, constructs a defense mechanism against illegal scanning based on artificial intelligence and other technologies, and forms a network stealth capability construction scheme in the virtual extensible Local Area Network(LAN) environment. The dynamic secure access method and dynamic on-demand authorization method are proposed in the network stealth environment. While breaking through the dynamic network stealth technology, the service access in different network stealth scenarios is supported, and the illegal access defense system under the network stealth condition is built. This research can be applied to the development of information network and the enhancement of network stealth ability, which has huge social benefits.

## Acknowledgments

This work was supported by the National Key R&D Program of China (No2022YFB2403900), State Grid Corporation Headquarters Technology Project(5700-202341290A-1-1-ZN).

## References

[1] Huang W, Gu ZM, Guo J, et al. Research on power cyberspace surveying and penetration. Electric Power Information and Communication Technology, 2021, 19(12): 49-54.
[2] ZHOU Y, XU Q, LUO XY, et al. Research on definition and technological system of cyberspace surveying and mapping. Computer Science, 2018, 45(5):1-7.
[3] Liu H, Yao WJ, Sun C, Liu XD, Bao ZJ, Jia ZP, et al. Classification and application of cyberspace surveying and mapping system. Cyber Security and Data Governance, 2021, 40(10) :16 - 21.
[4] Zhao F, Luo XY, Liu FL,Research on cyberspace surveying and mapping technology. Chinese Journal of Network and Information Security, 2016, 2(9): 1-11.
[5] Guo L, Cao YN, Su MJ, Shang YM, Zhu YJ Zhang P, Zhou C. Cyberspace resources surveying and mapping: The concepts and technologies. Journal of Cyber Security, 2018, 3(4):1-14.
[6] Zu DF. Key Information infrastructure network security protection system. China Computer&Communication. 2018(13): 198-200.
[7] Du L, Tian HR. Accelerating the security protection of key information infrastructure in China. China Information Security, 2017(8): 37-38.
[8] Zuo XD. Overview of security supervision of key information infrastructure in foreign countries. China Information Security. 2016, 13(11): 52-53.
[9] Qiu YM, Ying H, Zhou L, et al. Research and practice on identification of power critical information infrastructure. Electric Power Information and Communication Technology, 2020, 18(11): 9-14.
[10] Gao Y, Lv X, Li Y, et al. A survey of research work on critical information infrastructure system security defense. Journal of Information Security Research. 2020,6(1): 14-24.
[11] Zhang BS, Pang SM. A security protection solution for MEC that synchronizes resources within clouds, edges, management and terminals. Information Security and Communications Privacy, 2020(S1): 44-48.
[12] Zou JH, Zhang Y. Research on network information security based on network security scanning. Computer & Network, 2013(24): 65-67.
[13] Chen YY. Research on network information security based on network security scanning. Network Security Technology & Application, 2021(12): 17-19.
[14] Tang Y, Zhou XJ. Research on network scan technology and security recovery tactics. Computer & Digital Engineering. 2008, 36(4): 90-93.

[15] Li J, Zhang GY, Gu S, et a. Implementation of port scan techniques and its application in network security. Application Research of Computers, 2004, (2): 101-105
[16] Hong H, Zhang YQ, Hu YP. Research on network security scanning technology. Computer Engineering, 2004, 30(10): 54-56.
[17] Liu J. Research on the concealment of computer network scanning technology. Computer Engineering and Design, 2005, 26(6: 1481-1485.
[18] Tong Q, Zhang Z, Wu JX. The Active defense technology based on the software/hardware diversity. Journal of Cyber Security, 2017, 2(1): 1-12.
[19] Li ZQ, Su S, Zeng XJ, et al. Active security protection against targeted attacks in power dispatching systems based on fictional deception traps. Automation of Electric Systems, 2016, 40(17): 106-112.
[20] Chen W. Research and application of active defense based on IoT honeypo. Network Security Technology and Application, 2021, 05: 13-14.
[21] Li SX, Zhou Z,Song QH, Xia Ling. Overview of zero trust architecture and related solutions. Computer Knowledge and Technology, 2023, 19(7): 85-87.
[22] Zhuang R, Deloach S A, Ou X. Towards a theory of moving target defense. ACM Workshop on Moving Target Defense. ACM, 2014: 31-40.
[23] Wu JX. Research on cyber mimic defense. Journal of Cyber Security, 2016, 1(4):1-10.
[24] Ma HL, Ren Q, Yi P. Modeling and quantitative evaluation of cyberspace mimic defense. ZTE Communication Technology, 2022, 28(6): 57-62.
[25] Wang YW, Wu JX, Guo YF, et al. Scientific workflow execution system based on mimic defense in the cloud environment. Frontiers of information technology & electronic engineering, 2018, 19(12): 1522-1536.
[26] Cai GL, Wang BS, WAng TZ, et al. Research and development of moving target defense technology. Journal of Computer Research and Development, 2016, 53(5): 968-987.
[27] Azab M, Hassan R, Eltoweissy M. ChameleonSoft: a moving target defense system. In: Dimitrios G, James J, eds. Proceedings of the 7th International Conference on Collaborative Computing: Networking, Applications and Worksharing. IEEE, 2011: 241~250.
[28] Penner T, Guirguis M. Combating the bandits in the cloud: A moving target defense approach. IEEE/ACM International Symposium on Cluster, Cloud, and Grid Computing. IEEE, 2017: 411-420.
[29] Fei S, Yu-Tong Z, Yu W, et al. Smart collaborative distribution for privacy enhancement in moving target defense. Information Sciences, 2018(479): 593-606.
[30] Li ZT, Xu XD. The analysis of dynamic honeypot and its design. Journal of Huazhong University of Science and Technology (Natural Science Edition), 2005, 33(2): 86-88.
[31] He HK. Application and research of honeypot technology in the field of network security. Security & Informatization, 2022(1): 128-133.
[32] Wang Y, Ai ZL, Zhang XG. Research and implementation of the network traceback technology based on honey-beacon and honeypot. Information Technology, 2018,03: 108-112.