An "End-Network-Cloud" Architecture Key Technology with Threat Perception and Collaborative Analysis

Jinxiong Zhao[1, a], Xun Zhang[1], Fan Yang[1], Zhiru Li [1], Yong Zhi[1], Qian Feng[2], Xiaoqin Zhu[1], Kang Qian[1]

1State Grid Gansu Electric Power Research Institute, Lanzhou 730070, China.
[2]State Grid Shanghai Electric Power Research Institute, Shanghai 200437, China.

[a]18352449382@163.com

Abstract. Network security has been included in the 13th five-year plan, and has been put to an unprecedented level of attention. In order to solve the breakdown at the substation end of the power grid, a solution is designed to combine the station end, the data transmission network end and the production control cloud end. First, establish a public cloud for storing and processing data; The data will then be uploaded to the public cloud in real time through the data transmission network: One is to judge abnormal data according to the data feature matching, and the other is to act as a data set for machine learning later. At last, real time data analysis is carried out on the power stations with the control cloud, and the problem is quickly judged. According to the report, the approach was designed to restore the losses of Gansu power grid up to 22.17 million.

Keywords: Network security, Substation end of the power grid, Production control cloud end, Data transmission network end.

1. Introduction

Network attack mainly refers to that an attacker breaks the three elements of information security and uses the potential vulnerabilities in confidentiality [1-6], integrity and availability to attack the network, which is reflected in the use and theft of system vulnerabilities [7-9], destruction of software and hardware data. For example, in 2003, the virus worm Slammer invaded the Davis-Besse nuclear power plant in Ohio, causing incalculable damage; In 2009, according to news reports, the virus worm Conficker caused the paralysis of several military warships and submarines; In 2010, the United States and Israel discovered Stuxnet [10], a computer worm that attacked Iran's Natanz uranium enrichment plant; In 2013, hackers used phishing software to steal details about U.S. intervention in the Syrian regime; In 2017, the extortion virus WannaCry swept the world [11]. Obviously, in recent years, cyber security incidents have been consistent, and even with the emergence of new technologies, more and more attacks will be exposed.

As an important part of the energy industry, the power grid has also become a favorite target of hackers in recent years. However, most of the current safety incidents in the power grid occur at the end of the substation or in the position related to the substation end. For example, in 2000, the abnormal shutdown of the control system in Sichuan’s Ertan hydraulic power plant caused the collapse of it’s power grid. In 2001, a logic bomb appeared in a power grid recording device; in 2003, a virus was found in the control system of The Three Gorges power transmission project. The fundamental reason is that the manufacturer of the transformer is miscellaneous and numerous. According to incomplete statistics, there are a total of 11 types and 2,836 sets of current transformer devices. Once a fault occurs at the end of a substation, it will cause great harm, slow reaction and less emergency measures.

In order to solve the above problems effectively, a "End-Network-Cloud" coordinated control solution, starting from the essence of the problem, was proposed by combining the substation end, the data transmission network end and the upper production control cloud. According to conservative estimates, the design reduces the total loss of Gansu power grid by about 22.17 million per year.

2. Basic Framework

The scale of Chinese information security industry is shown in FIG. 1. The government had the highest proportion, 25%. And the energy sector is behind telecom, finance and education by 10%, as shown in figure 1:

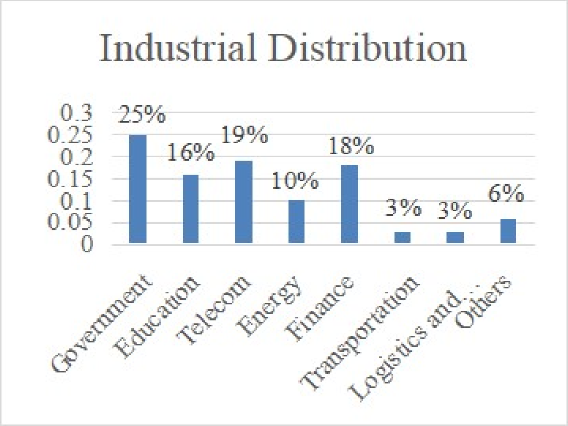

Fig. 1 Safety industry scale.

The horizontal coordinate in the Fig. 1 represents different industries, and the vertical coordinate represents the proportion of each industry in the security field. In order to prevent this kind of security event from happening in essence, the following defense structure system is designed:

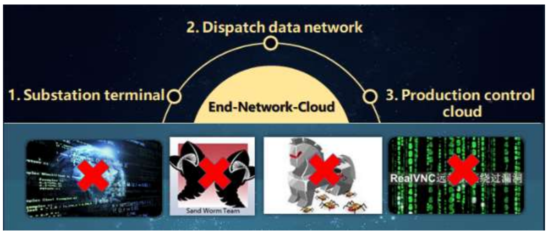

Fig. 2 Basic framework of End-Network-Cloud.

As mentioned above, this design idea closely combines the substation end, the dispatching data network end and the production control cloud to design an intelligent control system of the end network cloud. The sensor in the monitoring system of the substation end collects the data of each key par in real time, and then uploads it to the public cloud via the dispatching data network terminal to control the public production, effectively avoiding and reducing the potential accidents caused by physical security, operation safety, information security and network security of the secondary system. Thus, a secure and active defense system will be built for the next generation of smart grid. Fig. 3 shows the overall structure of "End-Network-Cloud". The first step is to collect data from the substation and upload it to the client of the industrial control system through different sensors. Then, Different types of switches are introduced at different exchange layers. Finally, all the collected data are successively transferred to the core layer switch through the sink layer switch. In the second step, all collected data is transferred to the public cloud of production control through data transmission as represented by cloud 1, cloud 2 and cloud 3 in the following figure.

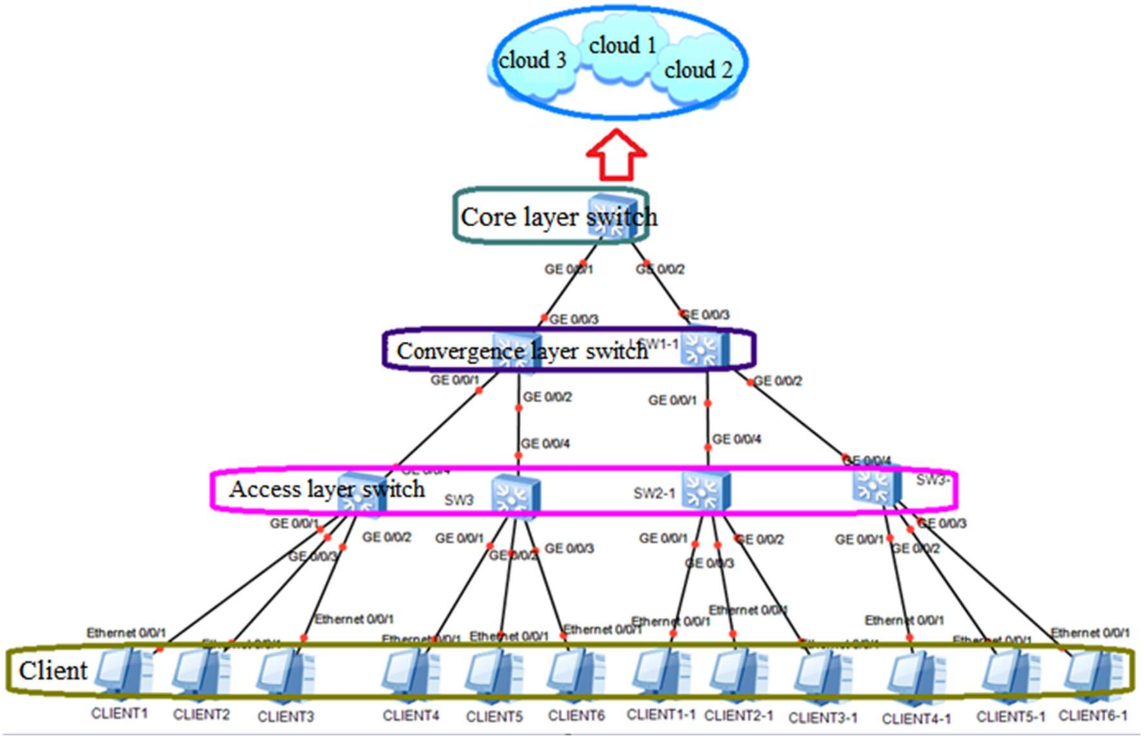

Fig. 3 Data transmission structure of End-Network-Cloud.

3. Cloud Design Principles

3.1. Intrusion detection/protection system component architecture.

One of the most important structures in the production control cloud is the intrusion detection and protection system component, which mainly consists of network detection engine, management control center, integrated information center and log analysis center. The role of the management control center is to monitor the activities of multiple network intrusion engines located locally or remotely and to provide unified data management. The management control center is often set up with main and substructure. Comprehensive information mainly provides detailed intrusion alarm information, such as intrusion IP address, attack characteristics, etc., providing online help to the response of the event; Log analysis center provides a variety of analysis methods, its function is to classify and extract historical alarm information, which can produce the management report that managers need. The structure is as follows:

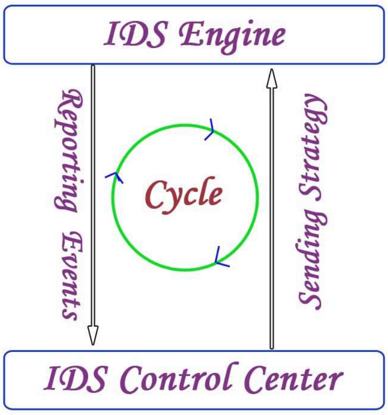

Fig. 4 Intrusion detection/protection system component architecture.

3.2. Intrusion detection/protection system functions.

The engine structure of the intrusion detection/protection system is as shown in Fig. 5. The main functions of the intrusion engine include reading uploaded data, data analysis and generation, event policy matching, event processing, etc. The detection engine is distributed in the network segment or installed on the host to be monitor the perform intrusion. The engine can monitor the data traffic in the network in real time and detect the attack according to the user's defined conditions. After the intrusion detection completed, the host engine issues an alarm to the control center, and then the manager will gives the location of intruder.

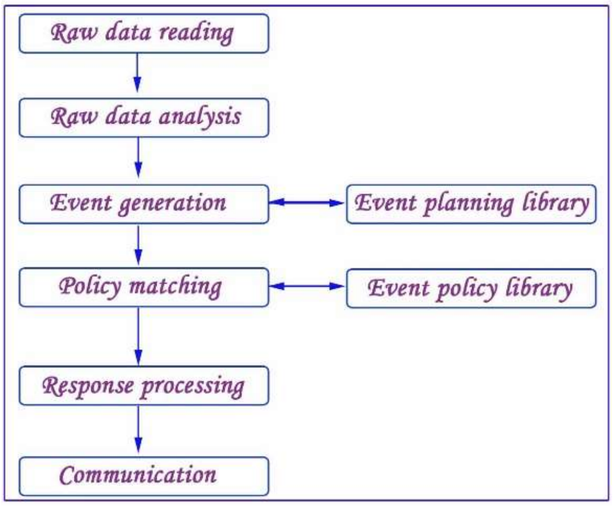

Fig. 5 Intrusion detection/protection system engine.

In line with different data sources at the substation end, the intrusion engine can be divided into two types: network model and host model. The intrusion engine has a powerful database of intrusion data feature sets to capture illegal intrusion behavior in real time. The main identification methods are as follows: to compare the difference between the mark set in TCP header and find the differences between the known correct and wrong mark union; Parsing DNS domain and checking the length of each domain; Tracking the number of consecutive times a command is issued, and detecting if it exceeds the preset upper limit. In the end, detailed illegal information can be presented and comprehensive reports can be generated by combining with the management system of the intrusion detection/protection control center, the working principle is as follows:

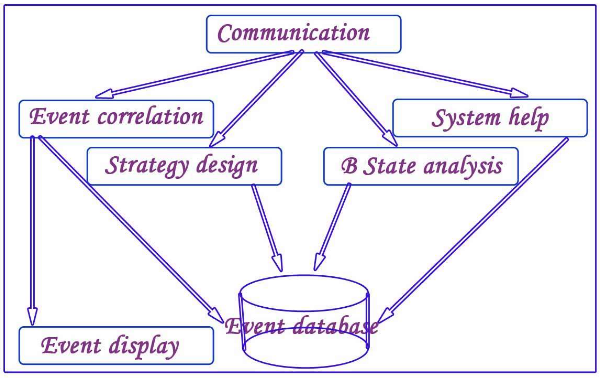

Fig. 6 Intrusion detection/protection control center principle.

4. Summary

We designs a solution which combines the substation end, data transmission network end and production control cloud to prevent most of the illegal intrusion in the substation terminals. The abnormal data can be detected by uploading different substation's data to production control cloud in real time through the data transmission network. Finally, the production control cloud is used to analyze the real-time data and the problem is located quickly. It turns out that the design does solve the problem of illegal intrusion at the substation end.

References

[1] Bryan H. Chong, Mario Ventresca, et al. Attacking Unexplored Networks-The Probe-and-Attack Problem. Complex Networks & Their Applications VI. Vol. 689 (2018), p. 692-703.

[2] Kerner, Sean Michael. Cyber-Security Reports Reveal Growing Concerns About Data Breach Risks. eWeek. (2018), p. 3.

[3] Angus Galloway, Graham W. Taylor, Medhat Moussa. Attacking Binarized Neural Networks. Statistics. 2017.

[4] Yosef Kornbluth, Gilad Barach, Mark Tuchman, Benjamin Kadish, Gabriel Cwilich, et al. Network Overload due to Massive Attacks. Physics. 2018.

[5] Gaogao Dong, Huifang Hao, Ruijin Du, Shuai Shao, H. Eugene. Stanley, et al. Localized attack on clustering networks. Physics. 2018.

[6] Bruno Requião da Cunha, Sebastián Gonçalves. Performance of attack strategies on modular networks. Journal of Complex Networks. Vol. 5 (2017) No. 6, p. 913-923.

[7] Katz, Eric. The DEA is Leaving Its Drug Seizures Vulnerable to Theft. Government Executive. (2016), p. 1.

[8] Yang Liu, Yuchen Zhou, Shiyan Hu. Combating Coordinated Pricing Cyberattack and Energy Theft in Smart Home Cyber-Physical Systems. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems. Vol. 37 (2018) No. 3, p. 573-586.

[9] PR Newswire. New Android Installer Highjacking Vulnerability Exposes Android Device Users to Data Theft and Malware. PR Newswire US. 2015.

[10] Zetter, Kim. Stuxnet. Wired. Vol. 21 (2013) No. 5, p. 139.

[11] Martin Guy, Ghafur Saira, Kinross James, Hankin Chris, et al. WannaCry-a year on. BMJ (Clinical research ed.). Vol. 361 (2018), p. 2381.