A High-Efficiency Security Monitoring Technology for New Energy Plant Station Network Border with Flow Characteristics Design

Jinxiong Zhao a, Jing Bai b, Zhiru Li, Xun Zhang, Xiaoqin Zhu, Runqing Bai

1 Grid Technology Center, State Grid Gansu Electric Power Research Institute, Lanzhou 730070, China.
2 Liu Yuanzi Primary School of Chedao, Qingyang 745717, China.

a18352449382@163.com, b786376280@qq.com

Abstract. With a straight-line growth of construction and network access in new energy plant stations, security threats of power stations also become more and more prominent [1-5]. For the safety inspection of new energy plant stations in Gansu province in 2016 and 2017 [6-9], 21 and 16 internet violations were detected, which brought huge security threats to the plant stations. At the same time, it also ringed alarm bells of safety protection for new energy plant station [10-11]. Therefore, we designed an efficient network boundary security monitoring technology to protect the stations.

Keywords: Network Security, New Energy Plant Stations, Security Threats.

1. Introduction
At present, the new energy plant station is mainly based on the safety protection scheme of power plant monitoring system (Guoneng safety [2015] No.36), which requires the establishment of information security protection system and safety reform. The document also stipulates that the safety protection of new energy plant station mainly includes the production control area and the management information area. The vertical encryption and authentication device for power is used between the production control area and the power dispatch data network.

Firewall, VLAN, intrusion detection, malicious code prevention and other comprehensive security protection are set up among the systems in the station domain, so as to realize security partition, horizontal isolation and special network, as well as vertical authentication and boundary protection with the power dispatch network. However, the requirement does not involve the communication security protection of the station control layer and the power generation unit acquisition terminal.

2. Flow Characteristics Design
2.1. Typical Attack Method.
Typical attack methods from the vertical network boundary of new energy plant stations are classified through investigation and extensive access to domestic and foreign materials and security cases, mainly including the following types:
(1) Traditional cyber-attacks. For example, DoS/DDoS attacks are of various types, including those based on TCP protocol, UDP, ICMP, and even application layer protocols such as HTTP and DNS. The purpose of these attacks is to paralyze key services in the network, resulting in the failure of network applications to operate normally. This kind of attack is characterized by large scale and easy to identify anomalies in macroscopic traffic statistics, but it is difficult to find single attack behavior in microscopic message content and application layer load.

(2) Stealth infiltration and scanning. This kind of attack firstly scans network structure, network node and network service. Secondly, by using known protocols and application vulnerabilities, remote control, APT Trojan implantation and other means are adopted to control part of the nodes and further complete scanning and attack penetration. Eventually, the network and critical nodes are taken over to achieve a variety of higher-level disruption activities. This kind of attack can be partially reflected in the macroscopic traffic characteristics, obvious anomalies can be found in the behavior characteristics of host level, and some key attack behaviors can also be found through deep message analysis.

(3) Hidden camouflage communication. One may encapsulate attack messages and secret messages in seemingly normal communication messages (such as camouflaging audio and video conferencing, disguising small ports below 1024, camouflaging DNS messages and encryption machines, etc.). This kind of attack is difficult to be identified by macroscopic traffic statistics, but can be found by detecting protocol standard conformity of communication message.

(4) Power control protocol application layer attack. For the vulnerability of application layer (such as industrial control protocol attack, cache overflow, code download, code injection, etc.), the attacker can send well-constructed application layer request or data load, and realize a series of attack purposes such as remote control, illegal operation of equipment (such as opening and closing gates), system paralysis and etc., that is obviously harmful. The identification method of this kind of attack is mostly implemented by deep packet content detection, but it is difficult to adapt to the variety of attack methods and find out the unknown application layer attack effectively.

Given the above attack characteristics, it’s necessary to design a technique of network boundary traffic modeling and abnormal network traffic analysis.

2.2. Network Traffic Analysis Techniques.

The main work includes two aspects. The first step is to study the protocols, so we studies the standard agreement of new energy station (such as SNMP, ICMP, ARP, Modbus, Modbus plus, IEC-61850 (DL/T 860), IEC-60870-5-104 (DL/T 634.5104), and IEC-61400-25 (GB/T 30966) of new energy wind power plant) or the private special communication agreement of plant station equipment (such as Siemens S7, Omron FINS, GE SRTP). The next step is to design the flow characteristic index, in other words, the design of traffic characteristic index is realized for standard protocol, network attack and its characteristics. In this paper, we adopt the method of traffic characteristic identification to design the traffic characteristic index of the application layer, realize the modeling of host, terminal and protocol behavior through the indicator set, attain the network feature expression and application layer anomaly detection through the data collection, and finally reach the target of identifying and warning application layer attack.

A 15-dimensional characteristic index is designed for traditional network attacks as follows:
Table 1. Network Characteristic Index

| Characteristic Index | Index Meaning                  |
|----------------------|--------------------------------|
| MPID                 | Number of measurement points   |
| BEGINTIME            | Statistics of start time        |
| SAVETIME             | Statistics of deadline          |
| IP                   | IP address                      |
| MAC                  | MAC address                     |
| BLOGUSER             | User account                    |
| IP_INBPS             | Inner average inflow            |
| IP_OUTBPS            | Outer average inflow            |
| TCP_INBPS            | Inner TCP average inflow        |
| TCP_OUTBPS           | Outer TCP average inflow        |
| UDP_INBPS            | Inner UDP average inflow        |
| UDP_OUTBPS           | Outer UDP average inflow        |
| TCP_FLOWS            | TCP session number              |
| TCP_PEERS            | TCP number of hosts             |
| UDP_FLOWS            | UDP session number              |

2.3. Method innovation.
Innovation is reflected in two aspects: Compensation for expertise in unknown application layer attack detection and a new unknown application layer attack detection technique. The Existing new energy station has a common fatal weakness, that is, the interaction of the communication protocols lack of important categories in the process of security mechanisms (terminal security authentication mechanism, the terminal identification mechanism, signaling and data encryption mechanism, denial and anti-counterfeit prevention mechanism, etc.), which makes the application layer attacked by hackers easily through standard protocols, such as fake nodes at random, tampering with the communication data, and even controlling equipment.

The application layer's attack identification through deep message detection (DPI) technology can only find part of the attack behavior (forging non-compliant message, caching overflow attack, etc.), but it can do little for impersonation and replay attack. Because the attack message and normal message are mixed, the content is almost indistinguishable. In particular, it is difficult to identify the attack messages from the content of the messages because of the various methods and types of carefully constructed along with attack messages.

Here, we adopt the application layer feature index extraction and anomaly detection method to identify the application layer attack online. And we design the characteristic index of the application layer according to the common application layer attack type and its performance (the new 15-dimension application layer index is designed at present).

3. Summary
A new unknown application layer attack detection technology is proposed by combining three technologies: application layer feature index design, the anomaly detection of application layer feature index, and the warning information database of application layer attack. These indicators and technologies are new technologies, methods and processes, which have not existed in previous fields.

Acknowledgements
This work was supported by the National Natural Science Foundation of China (61762058) and State Grid Science and Technology Projects (522722180007).

References
[1] Shaikh Shahriar Hassan, Soumik Das Bibon, Shohrab Hossain, Mohammed Atiquzzaman.
Security threats in Bluetooth technology. Computers & Security. Vol. 74 (2018), p. 308-322.

[2] Voznyuk Eugenia Vasylivna, Novak Oleksandr Yuriyovych, Samoilova Olga Igorivna. Nationalism as a threat to European security. Studia Humanitatis. Vol. 1 (2018).

[3] Military Technology. Global Threats and Regional Security. Military Technology. Vol. 42 (2018), p. 19.

[4] David Coyles. The security-threat-community. City. Vol. 21 (2017), p. 699-723.

[5] Alla Levina, Pavel Borisenko, Roman Mostovoy. SCA as mobile security threat. Proceedings of the XXth Conference of Open Innovations Association FRUCT. Vol. 776 (2017), p. 236-241.

[6] NGW's Gas Market Reconnaissance Group. Progress Energy is shutting down one of its older coal-fired power plants six years early as new electricity generating stations burning cleaner natural gas open. NGW's Gas Market Reconnaissance, 2011.

[7] WE Scott. Thermal plants will ease New Zealand's energy crisis. Huntly Power Station will first burn gas, then coal. Energy Int. p. 176.

[8] Dimitris Al. Katsaprakakis, Voumvoulakis Manolis. A hybrid power plant towards 100% energy autonomy for the island of Sifnos, Greece. Perspectives created from Energy Cooperatives. Energy, 2018.

[9] Bing J. Zhang, Qiao Q. Tang, Yue Zhao, Yu Q. Chen, Qing L. Chen. Multi-level energy integration between units, plants and sites for natural gas industrial parks. Renewable and Sustainable Energy Reviews. Vol. 88 (2018), p. 1-15.

[10] Daniel Doan. Protective Devices and Safety [Electrical Safety]. IEEE Industry Applications Magazine. Vol. 23 (2017), p. 5-6.

[11] D. Cohen, I. Erev. On safety, protection, and underweighting of rare events. Safety Science. Vol. 109 (2018), p. 377-381.