Analysis of network security intelligent detection method in smart grid for power monitoring system

Shipeng Zhang1, 2, *, Wenzhe Zhang1, Zhiyuan Yang3, Huan Pei2

1South China University of Technology, Guangzhou, China
2China Energy Engineering Group Guangdong Electric Power Design Institute Co., Ltd., Guangzhou, China
3China Southern Power Grid Company Limited, Guangzhou, China

*Corresponding author: zhangshipeng@gedi.com.cn

Abstract. This paper presents an intelligent detection method for network security violations in power monitoring system. Among them, the cross-connection detection method based on device portrait obtains the association characteristics analysis between different network segment devices and systems, the host illegal extravasation trace detection method accurately extracts traces of suspicious extravasation behavior, and the weak password and high-risk service detection method detects the vulnerability of login interaction characteristics, finally, the effectiveness of the method is verified by an example. The technology proposed in this paper can improve the efficiency and accuracy of on-site illegal external investigation of power monitoring system, reduce the security risk introduced by on-site operation and maintenance, and avoid the grid intrusion or even power outage caused by network cross connection or virus.

1. Introduction

In recent years, the network security situation has become increasingly severe, and cyberspace has evolved into the main battlefield of international political struggle [1-5]. Network security is related to national sovereignty and has become a national strategy. It emphasizes that the key information infrastructure in the fields of energy and electricity may be attacked, which is the top priority of network security. In 2015, there was a large-scale blackout of Ukraine's power grid, in 2019, there were four large-scale blackouts in Venezuela, and the United States claimed to carry out cyber-attacks on Russia's and Iran's power grids, The above events show that the power grid security is related to national security and social stability. Power war against the production control system of power grid may occur, and network attack is the most likely means [6-8].

On the other hand, with the power grid companies speeding up the construction of ubiquitous power Internet of things, the company's network is more open and the terminal access is more extensive [9-11]. At present, the company has 343 new energy power plants, more than 400 intelligent substations and 16876 distribution network terminals, which are on the rise. The premise of more open network is that the power control area (core area, large power grid area and important customer area) is more solid. The continuous expansion of network boundary puts forward higher requirements and new challenges for the implementation of control area isolation and protection measures. The reference [12] proposed a new network security situation assessment method based on information fusion under multi-stage large-
scale network attack. In reference [13], a network security situation assessment method based on Improved D-S evidence theory is proposed, which reduces the influence of human factors on the weight of situation assessment. The reference [14] proposes a network security situation assessment method for multi-step attack. It focuses on the analysis of attack environment, identifies attackers by clustering the environment, and then analyzes the characteristics of each scene to identify the corresponding attack trajectory and attack stage, and quantifies the results to obtain the situation assessment results. The reference [15] proposed a network security situation assessment method based on Naive Bayes classifier, which fully considered the fusion of multi-source heterogeneous information and accurately showed the current network security situation as a whole.

This paper proposes an intelligent detection method for network security violations in power monitoring system, in which the cross connection detection method based on device portrait obtains the association characteristics between different network devices and systems, and the host violation trace detection method accurately extracts traces of suspicious extraneous behaviors. Weak password and high-risk service detection method detect the vulnerability of login interaction characteristics, and the effectiveness of the method is verified by an example.

2. Cross link detection method based on device portrait

In the power monitoring system, for the need of business and network redundancy, it is a normal operation for a control or acquisition device to connect to multiple internal LANs at the same time. However, if the equipment is connected to the internal control network, office network or even Internet at the same time due to design defects or human factors of operation and maintenance personnel, it is considered that cross connection has occurred. If the device is regarded as a person, multiple network connection information of the device is like multiple identity features, but a person's fingerprint is unique. Therefore, a device feature detection algorithm is proposed to depict the fingerprint characteristics of each device. Even if the network information of devices seen from different networks is different, it can accurately judge that they are the same device.

![Diagram](image.png)

**Figure 1.** Device fingerprint feature extraction process.

Figure 1 shows the process of device fingerprint extraction, which is generally divided into three stages: filtering stage, joint stage and enhancement stage. In the filtering stage, the mode residuals, i.e. noise residuals, can be obtained by the image difference before and after filtering:

\[
\hat{r} = I - F(I)
\] (1)
Where \( F(\cdot) \) represents the filtering process. Here, \( \hat{\rho} \) contains PRNU noise and other random noise that cannot be used for forensics.

After the first stage of filtering, in addition to PRNU noise, there is still a lot of random noise in the image, which cannot be used for image forensics. Therefore, it is necessary to combine the noise residuals extracted from \( L \) images taken by the same camera to obtain more reliable PRNU finger patterns. The most common way is to average the noise residuals to further remove other random noises in the process, and then obtain PRNU noise:

\[
\hat{K} = \frac{1}{L} \sum_{l=1}^{L} \hat{r}_l
\]  

(2)

Where, \( \hat{K} \) is the average of noise residuals?

In the enhancement phase, the common noise that cannot be used for forensics caused by CFA interpolation and JPEG compression will be further removed, so as to further enhance the PRNU noise, so that it can be better used for image source identification and image forgery detection. In this paper, a method is proposed to remove the non-unique artificial trace noise and image content noise caused by JPEG compression, CFA interpolation and sensor design from the frequency domain of noise residuals. This method is based on the assumption that the sensor noise is Gaussian white noise, so it has a smooth spectrum. Firstly, the noise residual is processed:

\[
P_{hl} = \frac{\hat{F}(\hat{r}_l)}{\hat{F}(\hat{r}_l)}, l=1,\ldots, L
\]  

(3)

Where; \( P_{hl} \) is the phase component of the noise residual of the first image. Then, all the phase components are combined for inverse Fourier transform to obtain the PRNU fingerprint \( R_p \):

\[
R_p = R_e\left[F^{-1}\left( \frac{\sum_{l=1}^{L} P_{hl}}{L} \right) \right]
\]  

(4)

Where \( R_e(\cdot) \) denotes the real part.

The detection technology developed based on this principle can be applied in dispatching master station, distribution master station, substation and power plant. Through the implementation of more than 100 kinds of industrial control common service detection technology, more than 10 kinds of fingerprint information of feature services are extracted, the fingerprint database of industrial control equipment is customized, and the device feature model is established combined with the open information of device port, The unique identification of equipment in power monitoring system is realized. Once the devices with the same or highly similar multi-dimensional characteristics are found in different network grids, it is very likely that there will be illegal cross area connection in the network.
Figure 2. Device fingerprint feature extraction process.

Figure 2 shows the process of illegal external connection detection based on device portrait. Specifically, after the detection device is connected to the local area network, the device data is collected, and the port opening of the device is obtained first. Under the premise of not passing through the firewall and switch ACL, the port opening of the same device in different networks should be the same. Therefore, open port is an important feature of device fingerprint. Next, according to the actual opening situation of the port service, we further obtain the service characteristics of SSL key, X11 in SSH and HTTPS services, the host name in NetBIOS services, and the service mapping information of RPC. After obtaining the data, different features are given different weights according to the uniqueness of the features, and the similarity calculation of the device fingerprint is completed after weighted summation.

Figure 3 shows the cross-area connection detection interface of the power monitoring system's illegal external connection rapid detection equipment. This technology breaks through the limitation of the existing network security detection equipment in the industry that only scans and analyzes a single network segment, deeply combines the network structure characteristics of the power monitoring system, and analyzes the correlation characteristics between different network segment devices and systems. Realize the accurate discovery of the high-risk hidden danger of cross region connection.
3. Detection method of host illegal external connection trace

The detection method of host illegal external trace plays an important role in the power monitoring system technical supervision, law enforcement inspection and event investigation and evidence collection. The technology integrates host security log, application log, registry and other basic data, deeply analyzes the traces of illegal extravasation, accurately extracts traces of suspicious extravasation behaviors such as remote login, brute force cracking, remote operation and maintenance software installation, USB access, network cable plug and drop records, and improves the efficiency and accuracy of detection and forensics.

3.1. Analysis of host login

This paper studies the characteristics of the main operating system (win7, win8, win10, redhat6, redhat5) in various logs, such as security log, system application log, etc. according to different event IDS, key information fields are extracted and analyzed to accurately judge the situation of remote login. Figure 4 shows the analysis interface of the equipment host login situation for the rapid detection of illegal external connection of the power monitoring system. The technology deeply combines with the network structure characteristics of the power monitoring system, and uses the correlation characteristics between the key information fields to realize the accurate discovery of the high-risk hidden danger of illegal external connection.

3.2. Analysis of host USB and network changes testing

It shows the detection results of USB plug-in and plug-in of the equipment host for the rapid detection of illegal external connection of the power monitoring system in figure 5, and Figure 6 shows the detection results of network changes of the equipment host for the rapid detection of illegal external connection of the power monitoring system. According to the corresponding key value of USB, we can judge all the USB media that have been inserted in the industrial control host, and list the serial number, manufacturer, the last plug time and other key information. According to the corresponding key value
of the network card, all the obtained IP addresses of the network card on the industrial control host can be found out, and whether the host has been connected to the external network can be judged accordingly, which can also provide the basis for the check of no ticket operation.

| path of backup file | C:\workspace\python\security-tools\udlc\udlc6 examples\usb and network card informations\windows7.reg | open | query |

| Vendor code | Product code | Manufacturer | Product name | Product serial number | Drive letter | Last plug-in time | Creation time |
|------------|-------------|--------------|--------------|------------------------|--------------|------------------|--------------|
| 6781       | 5591        | SanDisk_Corp | Ultra        | 4C5300012996...       |              | 2019/4/8 - 19:39 | 2019/8/1 - 17:06 |
| 6782       | 5591        | SanDisk_Corp | Ultra        | 4C5310001296...       |              | 2019/4/8 - 19:39 | 2019/8/1 - 17:06 |
| 6900       | 1000        | Silicon_Motion | Flash Drive | 06060606060601       |              | 2019/8/1 - 17:00 |              |
| 6900       | 1000        | Silicon_Motion | Flash Drive | 68060606060602       |              | 2019/8/1 - 17:00 |              |
| 6951       | 1643        | Kingston_Tech | DataTraveler3 | 0011C0EC3C47... |              | 2019/7/10 - 16:23 | 2019/8/1 - 17:06 |
| 60c2       | ab24        | Seagate_RSS_L | Backup_Area_P | NA213001M |              | 2019/7/24 - 22:30 | 2019/8/1 - 17:06 |
| 60c2       | ab24        | Seagate_RSS_L | Backup_Area_P | NA213001H |              | 2019/8/1 - 17:06 |              |
| 60ca       | 0129        | RealtekSemicon | RT5125Card_A | 80100203136300 |              | 2019/8/1 - 17:06 |              |

Network card change record (check all the IP addresses obtained by the network card to determine whether there is any outreach)

| IP address | Subnet mask | Gateway | DNS (issued by DHC) | DNS (system) |
|------------|-------------|---------|----------------------|--------------|
| 192.168.75.1 | 255.255.255.0 | 192.168.75.254 | 192.168.75.254 | 192.168.75.254 |
| 192.168.109.129 | 255.255.255.0 | 192.168.109.120 | 192.168.109.120 | 192.168.109.120 |
| 192.168.111.172 | 255.255.255.0 | 192.168.111.170 | 192.168.111.170 | 192.168.111.170 |
| 192.168.222.117 | 255.255.255.0 | 192.168.222.116 | 192.168.222.116 | 192.168.222.116 |
| 0.0.0.0 | 255.255.255.0 | 192.168.111.1 | 192.168.111.1 | 192.168.111.1 |
| 192.168.111.1 | 255.255.255.0 | 192.168.111.1 | 192.168.111.1 | 192.168.111.1 |

Figure 5. Power monitoring system violation and external connection rapid detection equipment host USB plug-in status detection.

Figure 6. Power monitoring system violation and external connection rapid detection equipment host network change detection.

3.3. Analysis of remote software testing
It shows the remote software detection interface of the equipment host for the rapid detection of illegal external connection of the power monitoring system in figure 7. The main purpose of illegal external connection is to carry out remote operation and maintenance, and the remote operation and maintenance generally uses remote control software such as remote desktop. The detection equipment accurately matches the used third-party remote-control software by reading the registry information, this indicates the possibility that the detected host has been operated and maintained remotely.
Figure 7. The remote software detection of the host computer of the power monitoring system violation and external rapid detection equipment.

The host security analysis function supports local online detection and offline centralized analysis. Local online detection can start the detection program by inserting the detection U disk into the tested host, and complete the detection on the tested host without installation and good confidentiality. The offline centralized analysis mode requires the inspectors to export the logs and configuration files that need to be analyzed and analyze them in the tool set. This mode can be used for rapid batch file analysis.

4. Detection method of weak password and high-risk service

Figure 8 shows the high-risk service detection interface of the power monitoring system's illegal external rapid detection equipment. The weak password and high-risk service problems of the industrial control equipment and the host are easy to cause them to be controlled remotely or spread a large area of virus. By combining the security and business depth, and working with the protection, automation, distribution network, power supply and other specialties of the Electric Power Research Institute, the paper studies the functions of the industrial control equipment in the service opening, protocol, network management and other aspects. The weak password and high-risk services of key industrial control services can be detected.

```plaintext

| IP   | Port | Protocol | Status | Service | Port Characteristics |
|------|------|----------|--------|---------|----------------------|
| 172.16.41.32 | 119 | tcp      | open   | mssql-server | sqlserver vulnerability |
| 172.16.41.32 | 115 | tcp      | open   | msrpc    | invalid              |
| 172.16.41.32 | 119 | tcp      | open   | netbios  | known                |
| 172.16.41.32 | 49152 | tcp | open | unknown  |                     |
| 172.16.41.32 | 49152 | tcp | open | unknown  |                     |

```
Figure 8. High-risk service detection of power monitoring system violations and outreach rapid detection equipment.

5. Conclusions
In this paper, an intelligent detection method of network security violations in power monitoring system is proposed, in which the cross-connection detection method based on device portrait is used to obtain the correlation characteristics of different network devices and systems, and realize the accurate detection of the high-risk hidden danger of cross area connection. The detection method of host illegal outreach traces accurately extracts traces of suspicious outreach behaviors, and improves the efficiency and accuracy of detection and forensics. The weak password and high-risk service detection method can detect the vulnerability of login interaction characteristics, and can detect the weak password and high-risk service of key services. The technology proposed in this paper can improve the efficiency and accuracy of on-site illegal external investigation of power monitoring system, reduce the security risk introduced by on-site operation and maintenance, and avoid the grid intrusion or even power outage caused by network cross connection or virus transmission, which has good social benefits

References
[1] Khyavi H M, Rahimi M. Conceptual Model for security in next generation network[J].2016 30th International Conference on Advanced Information Networking and Applications Workshops ,2016,591-595.
[2] Mahmoud L, Praveen R. Network security evaluation using deep neural network [J]. 2020 15th International Conference for Internet Technology and Secured Transactions (ICITST),2020.
[3] Vigneswaran K R, Vinayakumar R, Soman P K .Poomachandran P, Evaluating shallow and deep neural networks for network intrusion detection systems in cyber security[J].2018 9th International Conference on Computing Communication and Networking Technologies (ICCCNT),2018,1-6.
[4] Kwon D, Kim H, Kim J, Such C S,Kim J K.A survey of deep learning-based network anomaly detection[J].Cluster Computing, 2017,1-13.
[5] Miller J D, Zhen X,Kesidis G.Adversarial learning targeting deep neural network classification: a comprehensive review of defenses against attacks [J].Proceedings of the IEEE,2020,108(3), 402-433.
[6] HashimA,Medani R, Attia A T.Defences Against web application attacks and detecting phishing links using machine learning[J]. 2020 International Conference on Computer, Control, Electrical, and Electronics Engineering (ICCCCEE),2020.
[7] Banerjee U, Chandrakasan P A.A low-power elliptic curve pairing crypto-processor for secure embedded blockchain and functional encryption[J]. 2021 IEEE Custom Integrated Circuits Conference (CICC),2020.
[8] Marshal R,Gobinath K, Rao V V.Proactive measures to mitigate cyber security challenges in IoT based smart healthcare networks[J].2021 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS),2021.
[9] Palmer C,Jayson A, Brown E J.New methods in power Line carrier monitoring and analysis real-world examples and implications for protection system reliability[J].2021 74th Conference for Protective Relay Engineers (CPRE),2021,1-14.
[10] Zhang L X, Li Y,Qiu B J,Zhang J L,Liang W W.Design of communication power centralized remote monitoring system based on big data technology[J].2021 International Conference on Electronics, Circuits and Information Engineering (ECIE),2021,46-49.
[11] Divya V B,Latha N,Ashwinikumari P.IOT Enabled power monitoring and control of single phase induction motor[J].2021 International Conference on Emerging Smart Computing and Informatics (ESCI),2021,670-673.
[12] Hu L,Li H L,Wei Z H, Dong S Q, Zhang Z.Summary of research on IT network and industrial control network security assessment[J].2019 IEEE 3rd Information Technology, Networking,
Electronic and Automation Control Conference (ITNEC), 2019, 1203-1210.

[13] Lin Y W, Chen D Q, Peng Y. Information security risk assessment of power plant industrial control system based on D-S evidence theory [J]. Journal of East China University of Science and Technology: Natural Science Edition, 2014, 40(4): 500-505.

[14] Jin B H, Simon E Y, Dong S K, Khaled M D K. Stateless Security risk assessment for dynamic networks [J]. 2018 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN-W), 2018, 65-66.

[15] Yu Y, Wang J, Liu J Q, Han L, He X D, Lv S H. Multi-Dimension threat situation assessment based on network security attributes [J]. 2018 27th International Conference on Computer Communication and Networks (ICCCN), 2018.