Design and Application of Security Monitoring System for Perception Terminal of Power Internet of Things

Hong Xu[1(✉)], Xin Sun[2], Jie-yao Ying[3], and Qing-li Niu[4]

[1] School of Software, Zhengzhou University, Zhengzhou 314500, China
xuhhhh06@outlook.com
[2] School of Electrical Engineering, Zhejiang University, Hangzhou 310000, China
[3] School of Software, Zhejiang University, Hangzhou 310000, China
[4] College of Information Engineering, Zhengzhou University of Science and Technology, Zhengzhou 450064, China

Abstract. The information acquired by the traditional power Internet of Things sensing terminal monitoring system is not comprehensive, which leads to the long time needed to monitor the terminal security vulnerabilities. In order to solve this problem, this paper designs a new security monitoring system of power IOT sensing terminal. On the basis of the traditional system hardware design, the overall architecture of the system is designed by fully considering the security function of the power IOT sensing terminal. Then, the data of sensing terminal is collected at the monitored object end, and the data display module is designed. Then, the specific monitoring module is designed from three aspects of monitoring process, power Internet of things sensing terminal application, client and server, so as to realize the security monitoring of power Internet of things sensing terminal. In the experimental part, we design the vulnerability of the power IOT sensing terminal and the possible attack actions under the vulnerability. The results show that compared with the traditional system, the system in this paper needs less time to monitor the vulnerability of the power IOT sensing terminal.

Keywords: Power Internet of things · Perception terminal · Security monitoring system · Data acquisition · Security vulnerability

1 Introduction

In order to fully and effectively implement the planning, design and management of power network, and realize the unified utilization of network information, the State Grid Corporation of China proposed the deployment arrangement for the comprehensive construction of ubiquitous power Internet of things [1]. The implementation of power Internet of things also puts forward new requirements for comprehensive perception of perception layer devices. Therefore, relevant experts design ubiquitous perception terminal installed on the user side on the basis of the original. However, the network communication between the Internet is usually protected by firewall and

S. Wang et al. (Eds.): IoTCare 2021, LNICST 414, pp. 373–385, 2022.
https://doi.org/10.1007/978-3-030-94185-7_25

intrusion detection system, and the monitoring inside the network is often forgotten, which is also the weak point of prevention [2]. Therefore, the current design of the power Internet of things perception terminal, there are non external way to infect the virus, from the internal deployment of the virus or Trojan horse to destroy the normal network communication, hacker attacks and other security risks.

In foreign countries, for IOT sensing terminal monitoring, equipment monitoring and fault diagnosis consultation and technology promotion are generally carried out through the network, and some information exchange formats and standards are formulated. Due to the rapid development of computer technology and communication technology, in recent years, China has begun to actively carry out this research [3]. Reference [4] divides the monitoring of Internet of things into two layers. The upper layer uses standard Ethernet, the lower layer uses s-485 protocol bus technology, plus servers and monitoring workstations to form a LAN monitoring system suitable for industrial field. Reference [5] a WWW browser is installed on the user terminal to obtain the online technical support and data exchange from the TSB of the remote service department through HTTP to complete the security monitoring of the Internet of things perception terminal. However, the information obtained by the traditional power Internet of things sensing terminal monitoring system is not comprehensive, which leads to a long time to monitor the terminal security vulnerabilities.

In view of the shortcomings of the traditional system, this study designed a new power Internet of Things sensing terminal security monitoring system. The design idea of the system is as follows:

(1) Considering the existing problems in the security of the sensing terminal of the electric Internet of Things and the status quo of the hardware design of the monitoring system, the hardware and software parts of the system are designed on the basis of clarifying the security functions of the sensing terminal.
(2) Design the data display module and monitoring module, and complete the security monitoring of the sensing terminal of the power Internet of Things from the perspectives of monitoring process, sensing terminal application, client and server.
(3) The design experiment proves that the system in this paper needs less time to perceive vulnerabilities.

2 Design of Security Monitoring System for Perception Terminal of Power Internet of Things

2.1 System Architecture Design

The security monitoring system of the power Internet of things perception terminal designed in this study mainly includes three modules: monitoring terminal software, monitoring data storage software and integrated display and control software. The functions of information monitoring, data storage and comprehensive display are processed respectively. The structure is shown in Fig. 1.

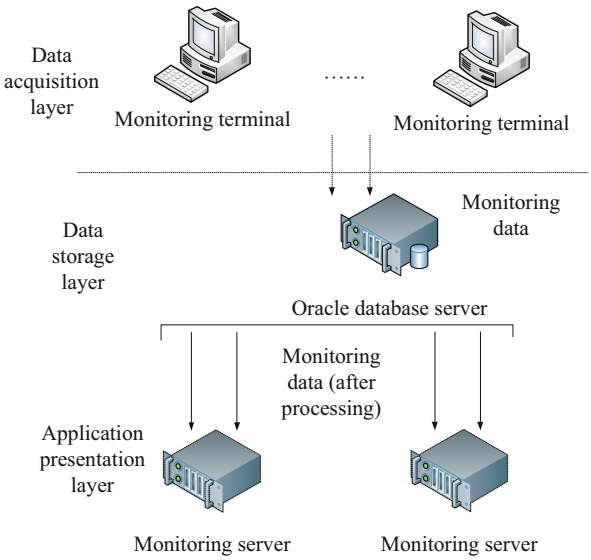

Fig. 1. Design of network monitoring system

As shown in Fig. 1, in the architecture of the monitoring system, the data acquisition layer monitoring terminal software mainly completes the monitoring data acquisition of the terminal and the data upload function after the data acquisition; the data storage layer completes the data storage, and the user can save the collected historical monitoring data and complete the data processing on this basis, which serves as the interface between the data acquisition layer and the application presentation layer In addition to the above two functions, the data storage layer completes the preliminary data analysis and processing in the data acquisition layer, and completes the secondary data analysis and processing through stored procedure programming, which greatly improves the data processing speed of the application presentation layer. Stored procedure programming is a database programming technology, It has the advantages of simplicity, security and high performance; the application presentation layer mainly completes the display of the data collected by the data collection layer, as well as the functions of data analysis, early warning and statistical report.

2.2 Collect the Data of the Sensing Terminal

The system achieves the acquisition of monitoring information by installing a terminal in the monitored object end, and then the monitoring terminal uploads the collected information to the monitoring server, so as to achieve the acquisition of information. Therefore, it is necessary to install the client in the monitoring terminal to fully control the monitoring terminal, and it will occupy a certain amount of monitoring terminal resources. The acquisition process is shown in Fig. 2.

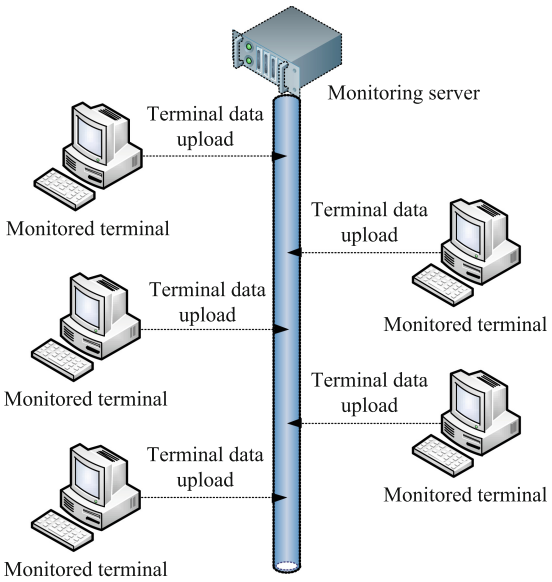

Fig. 2. Sensing terminal data acquisition

Because the monitoring terminal is installed with a client, when a monitoring terminal crashes or the network delays, it only leads to the disconnection of a single node and does not affect the monitoring server [6]. In addition, when the monitoring terminal changes (increases and decreases), additional operation of installing the monitoring terminal is needed. Secondly, the monitoring terminal needs to upload data to the monitoring server. When the monitoring server is installed with firewall, the access of the monitoring terminal will be limited.

2.3 Data Display Module

The data display module mainly completes the display of the data collected by the data acquisition layer, including three functions of monitoring data acquisition, monitoring data display and control monitoring terminal. Its structure is shown in Fig. 3.

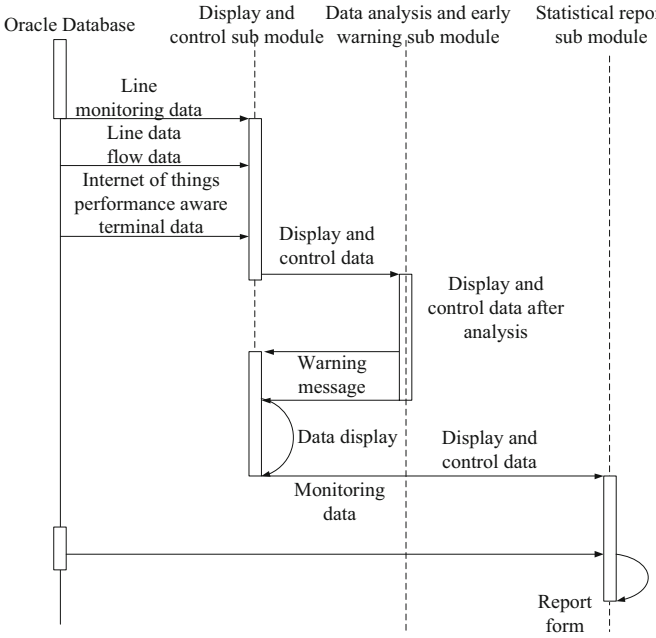

Fig. 3. Sequence diagram of data display software

In the software timing diagram of data display module shown in Fig. 3, the monitoring data acquisition is the interaction between display and control sub module through data interaction with Oracle database. The data including line monitoring data, line data flow data and equipment performance data, and data that have been analyzed and processed from the database storage process are obtained.

Monitoring data display is that after the display and control sub module obtains the monitoring data from Oracle database, it respectively realizes the line monitoring display, line data flow display and equipment performance display. The display and control sub module submits the obtained data to the data analysis and early warning sub module for data analysis, and carries out data early warning display according to the feedback results of the data analysis and early warning sub module.

After getting the monitoring data from Oracle database, the display and control sub module realizes the line monitoring display, line data flow display and equipment performance display respectively. The display and control sub module submits the obtained data to the data analysis and early warning sub module for data analysis, and carries out the data early warning display according to the feedback results of the data analysis and early warning sub module.

The control and monitoring terminal mainly includes monitoring terminal configuration modification and monitoring terminal stop, restart and resume control operations. The control and monitoring terminal completes the control of the monitoring terminal through the terminal link security confirmation.

2.4 Design of Monitoring Module of Monitoring System

System Monitoring Process

Data acquisition layer monitoring terminal software mainly completes the monitoring data acquisition and data upload function after data acquisition [7]. The data acquisition layer includes network lines, line data flow and network equipment related performance information. According to the functions to be realized, it is divided into five sub modules: system tray module, line monitoring sub module, line data flow monitoring sub module, equipment performance monitoring sub module and monitoring data storage module. Based on these five sub modules, the software module flow of terminal security monitoring system is designed, as shown in Fig. 4.

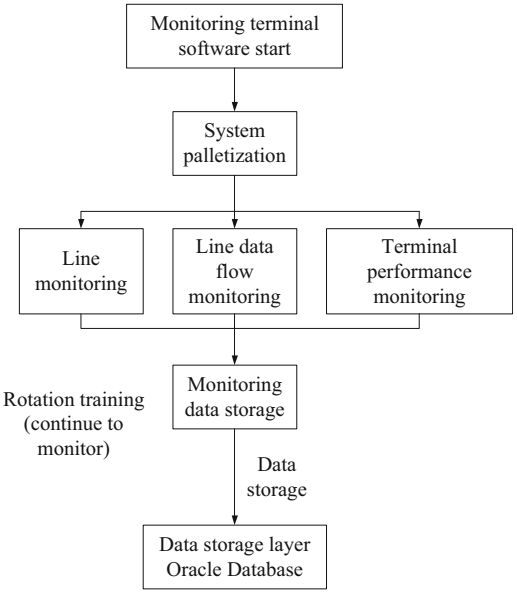

Fig. 4. Software module flow of terminal security monitoring system

As shown in Fig. 4, the software module flow of terminal safety monitoring system. After the system starts the system software, the software tray will be displayed in the system tray program at the bottom right of the system, which is used to identify the current monitoring terminal software in operation. Once the monitoring terminal program is abnormal, the system tray will disappear.

After the software tray of monitoring system is started, three monitoring threads will be started respectively: line monitoring thread, line data flow monitoring thread and device performance monitoring thread. In order to understand, this study is called sub module.

The software of monitoring system adopts three threads to realize the realization of the sub module of line monitoring, the sub module of line data flow monitoring and the performance monitoring module of equipment. The three threads perform the functions of these three sub modules respectively [8].

The three monitoring threads will simultaneously upload the acquired line monitoring data, line data flow monitoring data and device performance monitoring data to the data storage layer Oracle database through the monitoring data storage module.

Terminal Monitoring

Monitoring the power Internet of things perception terminal can be divided into two parts: the server and the client, respectively monitoring the power Internet of things perception terminal. The server is composed of security monitoring module, information display module, instant messaging module, integrated tool module and central database.

Security monitoring module includes: LAN scanning processing module, port summary processing module, filter analysis processing module, log processing module, firewall processing module, etc. The monitoring server dynamically analyzes all the incoming and outgoing IP addresses and ports in the LAN. According to the abnormal analysis of the ports and incoming and outgoing packets, the illegal operation can be judged. Summarize the ports by IP address to view the illegally used network processes. The abnormal IP address can be analyzed separately to determine the main object of illegal operation. Firewall can be used to block the port and address.

Information display module includes: screen capture processing module, client locking module, communication processing module, client management module, etc. It mainly monitors the client on a regular basis, and remotely captures the abnormal traffic. The client can directly view the screen. If illegal use is found, the message module will give a warning. If you don't pay attention to it, you can lock the client or remotely close the client.

Instant messaging module. It is mainly aimed at content and message capture in abnormal time, such as communication software.

The integration tool module includes: routing test and connectivity test. Using these tools to test the connectivity of local LAN and the function of remote network routing, the administrator can quickly find the cause of network failure.

Central database. It mainly stores and manages all kinds of data, and is the storage center of system monitoring data.

The client is composed of the message part and the request processing module sent by the local receiving server. Through the interaction between these menus, the integrity of the whole system can be guaranteed [9]. The client mainly includes the following parts:

Information capture part: mainly responsible for collecting the key system information (CPU, memory, process list, etc.) on the host.

Communication module: the main function is to receive instructions or messages sent by the server, make corresponding responses, such as lock/unlock, shutdown and other instructions, and realize encrypted communication with the server.

Hiding module: it is mainly responsible for the automatic loading of the client and the automatic hiding of the corresponding process.

Application Monitoring

When a computer starts an application, the operating system creates a process for the program. When the process is terminated, the application ends. Each process in Windows has its own address space, which contains the code and data of all executable modules or dynamically linked library modules. Only when the windows operating system creates a process for it and allocates the necessary resources, the program can run. For Windows environment, whether you double-click the application with the mouse or enter the command in the command line mode, the corresponding application creation is completed by the operating system process calling the windows API function. In this way, you can filter the corresponding application by monitoring the CreateProcess function. DLL has always been the foundation of Windows operating system. Functions in the windows API are included in the DLL. The three most important DLLs are Kernel32. DLL, User32. DLL and GDI 32. Dl. The use of DLL can save memory space very effectively. If multiple applications use a DLL together, the pages of the DLL will only be put into memory once, and all applications can share pages. And the resources in the DLL can be shared by all these applications. Because of these characteristics of DLL, we can monitor some API functions, and only DLL can inject into the address space of all processes.

HOOK API is an effective and simple way to monitor the application process. Hook is a mechanism for Windows to process messages. An application program can monitor some messages in a specified window by setting its subprogram, and the monitored window can be created by other processes [10].

Microsoft does not provide the relevant information of hook API, but from the characteristics of DLL and the functions provided by HOOK, it is not particularly difficult to implement hook API. In fact, the development of hook API technology has been very mature.

However, it should be noted that due to the problem of character set, there are two versions of a large part of Windows API functions: the version suitable for UNICODE and the version suitable for DBCS, which correspond to CreateProcessW of wide character set and CreateProcessA of double byte character set.

Since the operating system makes a large number of calls to system API that need to be monitored, in order to improve the response speed of the operating system, two methods are adopted to improve the efficiency of the operating system: the speed of accessing security policy files and the speed of matching rules.

During the policy check, if the normal file reading and writing method is adopted, the file needs to be opened and closed frequently, and the file is frequently read and written, which will reduce the efficiency of the operating system. Therefore, this system adopts the method of memory file mapping. Even if the application program accesses the file on the disk through the memory pointer, the process is to access the memory of the loaded file. When using memory-mapped files for I/O processing, the operating system performs data transfer pages. As for all internal pages, the virtual memory manager is responsible for management, because the virtual memory manager is a unified method It handles all disk I/O, so this optimization makes it capable of processing memory operations at the fastest speed.

Specifies the matching speed. The security policy rules are not arranged in disorder, but are classified according to the disk drive where the monitored object is located, and

arranged in alphabetical order. When the security policy is checked, what is known is the name of the monitored object, that is, the name of the file or folder, and the disk drive where the monitored object is located can be obtained according to the file name. The disk drive can be used to directly locate the scope of the strategy applicable to the monitored object according to the corresponding location index of the file, thereby greatly reducing the number of rule matching checks that need to be performed.

3 System Test

A comparative test is adopted to verify the effectiveness of the security monitoring system for the sensing terminal of the power Internet of Things designed in this paper. The perception terminal of the power Internet of Things in a certain area is taken as the experimental object. In order to enhance the contrast between the experimental results, the two traditional security monitoring systems were compared, and the time required to monitor the vulnerability of the sensing terminal of the power Internet of Things was taken as an indicator to verify the effectiveness of the different systems.

3.1 Experiment Preparation

Load the Rapid SCADA software, which can provide information to the power dispatcher, and run it on the Kali virtual machine on Windows Server 2020 system and several station-controlled virtual monitoring layers to complete the construction of the test platform.

On the perception terminal of the electric Internet of Things, the following three vulnerabilities are set:

1. In the case of unauthorized access, files that cannot be accessed are accessed, and file transmission occurs. The rhost vulnerability of the protocol, and the vulnerability is recorded as a_1;
2. Allow illegal users to send forged Modbus data packets, and the Modbus protocol authorization vulnerability appears, and the vulnerability is recorded as a_2;
3. Execution without permission Power Internet of Things scheduling command, a WinCC software vulnerability appears, and the vulnerability is recorded as a_3.

According to the three vulnerabilities set above, it is assumed that the power dispatching network may be subjected to the following attack actions:

1. Use vulnerability a_1 to obtain user rights and record it as a b_1 attack action;
2. Use vulnerability a_2 to deceive the network protocol and record it as a b_2 attack Action;
3. Use vulnerability a_3 to tamper with terminal data and record it as b_3 attack action.

On this basis, the perception terminal of the electric Internet of Things is set to three operating states, as follows:

1. Normal operating state;
2. Obtaining user authority state;

3. Manipulating the state of power dispatching network nodes.

In the above three states, the perception terminal information of the power Internet of Things was subjected to three attacks, and then the time required by the three system monitoring vulnerabilities was tested.

3.2 Experimental Result

The First Set of Experimental Results
The power Internet of Things sensing terminal is set to normal operation state, and then the security state of the power Internet of Things sensing terminal is monitored under different attack actions respectively, and the time required for the three system monitoring vulnerabilities is recorded. The experimental results are shown in Fig. 5.

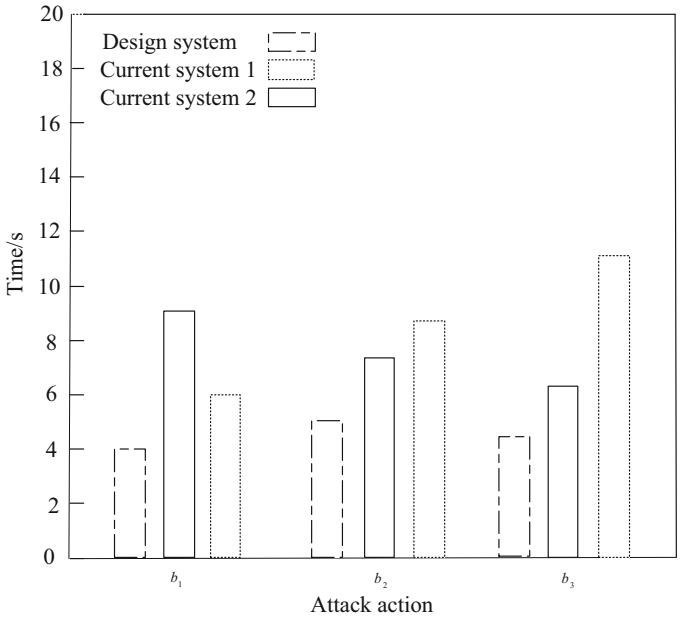

Fig. 5. The time required for different systems to monitor vulnerabilities under normal operating conditions

As can be seen from Fig. 5, under the b_1 attack action, it takes more time for system 1 to monitor the vulnerability than System 2. Under attack actions b_2 and b_3, it takes less time for system 1 to monitor the vulnerability than System 2. However, the monitoring time of these two systems is always longer than that of the system in this paper, which proves that the system in this paper is obviously superior to System 1 and System 2.

The Second Set of Experimental Results

The power Internet of Things sensing terminal is set to obtain the user's authority status, and then the security state of the power Internet of Things sensing terminal under different attack actions is monitored respectively, and the time required for the three system monitoring vulnerabilities is recorded. The experimental results are shown in Fig. 6.

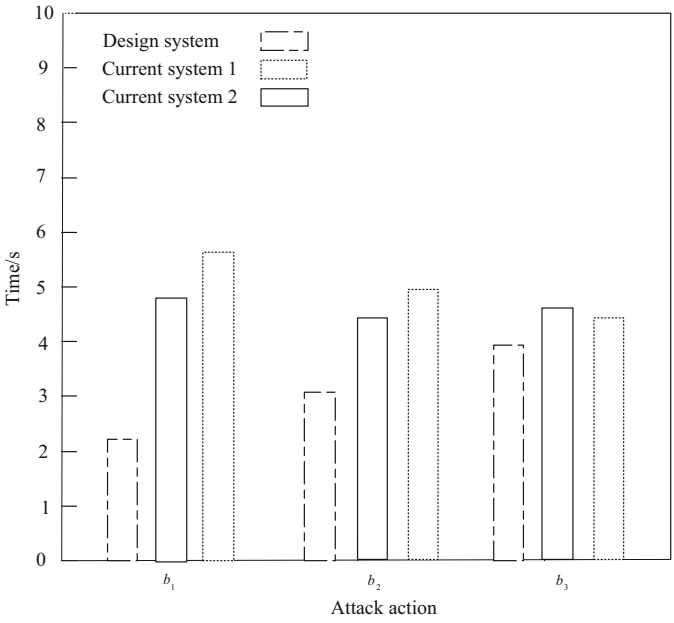

Fig. 6. Obtain the time required for monitoring vulnerabilities of different systems under the status of user permissions

As can be seen from Fig. 6, when the perception terminal of the power Internet of Things is in the state of obtaining user rights, the time required for monitoring vulnerabilities of the three systems is significantly reduced compared with that in the normal operation state. The average monitoring time of system 1 is 5 s, which is the longest. The average monitoring time of system 2 is 4.7 s, which is still relatively long. The average monitoring time of the system in this paper is 3.1 s, which is obviously more effective than that of System 1 and System 2.

The Third Set of Experimental Results

The power Internet of Things sensing terminal is set to manipulate the state of power dispatching network nodes, and then the security state of the power Internet of Things sensing terminal is respectively monitored under different attack actions, and the time required for the three system monitoring vulnerabilities is recorded. The experimental results are shown in Fig. 7.

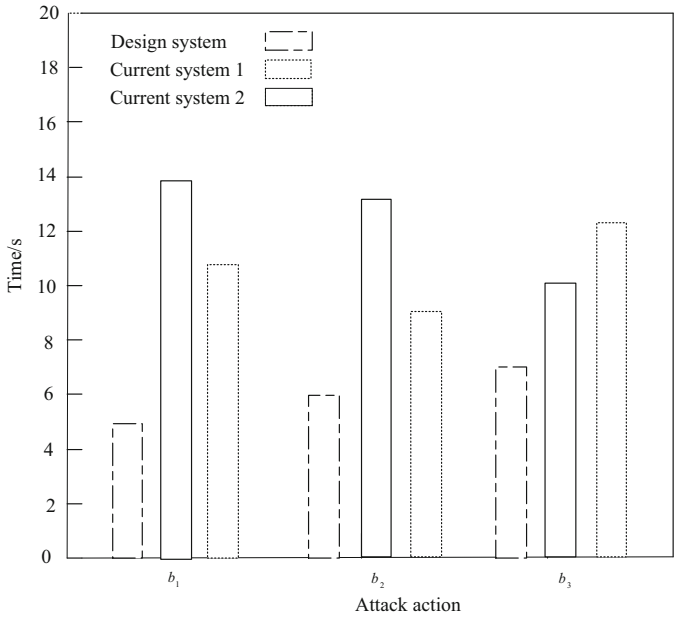

Fig. 7. The time required to restore stable operation of the network under the control of the state of the power dispatch network node

As can be seen from Fig. 7, when the sensing terminal of the power Internet of Things is in the state of manipulating the power Internet of Things nodes, the time required for monitoring vulnerabilities of the three systems is significantly increased compared with that in the normal operation state, indicating that the process of monitoring vulnerabilities is the most difficult at this time. In this state, the average monitoring time of system 2 is longer, up to 13 s. System 1 has the longest average monitoring time, up to 14 s. The maximum monitoring time of the system in this paper is 7.2 s, which proves that it is better than system 1 and system 2.

Causes of these results is that the system takes into account the problems existing in current electric power iot terminal security perception as well as the monitoring and control system hardware design present situation, in a clear perception terminal was designed on the basis of the safety function of system software and hardware parts, and the monitoring process, perception terminal application, the client and the server a few point of view, To complete the comprehensive and comprehensive security monitoring of the perception terminal of the electric Internet of Things, so as to reduce the time needed for its perception vulnerability.

4 Conclusion

In this study, a security monitoring system for the sensing terminal of the power Internet of Things is designed. Considering the existing problems in the security of the sensing terminal of the power Internet of Things and the status quo of the hardware design of the monitoring system, the hardware and software parts of the system are designed on the basis of clarifying the security functions of the sensing terminal. Then, the data display module and monitoring module are designed to complete the security monitoring of the sensing terminal of the power Internet of Things from the perspectives of monitoring process, sensing terminal application, client and server. This study also proved that the system needed less time to perceive vulnerabilities through comparative experimental results, thus proving the effectiveness of the system.

But the design of the security monitoring system, there are still some deficiencies. In the future research, it is also necessary to further study the weak links of the perception terminals of the electric Internet of Things and increase the practical functions of the monitoring system.

References

1. Lin, H., Luo, W.: Internet of things terminal monitoring based on network data analysis. Electron. Des. Eng. **28**(18), 101–105 (2020)
2. Huang, S., Zhang, X.: Design and implementation of monitoring system based on network terminal. Digital Technol. Appl. **37**(7), 94–95 (2019)
3. Lu, Q., Cui, W.: Security monitoring analysis technology of terminal layer in ubiquitous power IoT. Inf. Technol. (2), 121–125+134 (2020)
4. Xiao, A., Zhang, W., Zhao, D., et al.: Construction method of smart grid monitoring system based on IoTs. Inf. Technol. (12), 86–90+95 (2020)
5. Chen, J., Zhou, Z., Feng, W., et al.: Design of power monitoring system based on wireless network. Tech. Autom. Appl. **39**(4), 168–171 (2020)
6. Du, L.: Design of wireless temperature monitoring system for power cable. J. Beijing Polytech. Coll. **19**(1), 23–27 (2020)
7. Liu, S., Lu, M., Li, H., et al.: Prediction of gene expression patterns with generalized linear regression model. Front. Genet. **10**, 120 (2019)
8. Lei, Y.: Real-time monitoring system with wide spectrum and multiple parameters based on Internet of Things. Comput. Netw. **46**(6), 62–65 (2020)
9. Liu, S., Liu, D., Srivastava, G., Połap, D., Woźniak, M.: Overview and methods of correlation filter algorithms in object tracking. Complex Intell. Syst. **7**(4), 1895–1917 (2020). https://doi.org/10.1007/s40747-020-00161-4
10. Fu, W., Liu, S., Srivastava, G.: Optimization of big data scheduling in social networks. Entropy **21**(9), 902 (2019)