Wireless communication network security intelligent monitoring system based on machine learning

Hongkun Liu 1, Nianci Wang 2,* and Sirong Liang 3

1 School of Information Science and Engineering, University of Jinan, Jinan, China;
2 Department of Electrical Engineering and Information Technology, Shandong University of Science and Technology, Jinan, China;
3 School of Communication and Information Engineering, Xi’an University of Posts & Telecommunications, Xi’an, China.

*Corresponding author e-mail: 201803203320@sdust.edu.cn

Abstract. Aiming at the problems of traditional wireless communication network security vulnerability monitoring systems such as low monitoring accuracy and time-consuming, a machine learning-based intelligent monitoring system for wireless communication network security vulnerabilities is proposed. In the hardware design of the monitoring system, based on the overall architecture of the wireless communication network and the data characteristics of the wireless communication network, it is divided into a vulnerability data collection module, a vulnerability data scanning module, and a network security vulnerability intelligent monitoring module. In the vulnerability data collection module, the wireless data collector is used to collect vulnerability data in the vulnerability database, and according to the attributes of the vulnerability data, the XSS vulnerability detection plug-in is connected to the vulnerability scanner to scan for wireless communication network vulnerabilities; When the communication network vulnerability data signal is traced, the system session operation of monitoring the vulnerability data. The software part introduces the neural network algorithm in the machine learning intelligent algorithm to process the hidden data in the security vulnerability data. The experimental results show that the wireless communication network security vulnerability intelligent monitoring system based on machine learning can effectively improve the system monitoring accuracy and the efficiency of wireless communication network security vulnerability monitoring.

Keywords: network security breach; machine learning; Wireless communication.

1. Introduction

With the rapid development of wireless network technology, major network operators regard the development of wireless communication network as an important development goal and continuously increase the investment in wireless network [1]. With the advent of 5G technology, wireless communication network has also achieved considerable development, but the resulting security issues have become the focus of research in this field. Wireless communication network security is related to the information security of society and even the country [2]. Among them, wireless communication
network security vulnerability has become the main problem that needs to be solved at present. Security vulnerability in communication network will produce a large number of vulnerability data, which is a series of data generated by security vulnerability in hardware, software, protocol or specific communication system. By analyzing leak-hole data, the causes of leak-hole formation can be obtained and the leak-hole can be repaired in time to ensure the security of wireless communication network. Therefore, how to improve the capability of autonomous defense and network security vulnerability monitoring of wireless communication network system has become a hot issue in this field [3]. For this reason, relevant researchers have done a lot of research on this.

Literature [4] proposed a vulnerability monitoring method based on dynamic stain analysis to identify the vulnerabilities of communication network nodes. This method collects network node vulnerabilities according to their properties by analyzing their properties. The adaptability function of vulnerability identification is used to identify the node vulnerabilities of communication network. This method can effectively identify the leaky holes in wireless network nodes, but the operation process of this method is complicated and the work efficiency is low. In reference [5], a vulnerability monitoring technology based on hardware virtualization is designed. Through the construction of the overall framework and the detailed design of hardware and software, vulnerability scanning tools are used to collect the vulnerability data in the system, and the collected vulnerability data is integrated and analyzed in detail. Machine learning technology is used to detect abnormal behavior intrusion in communication network. This method can effectively intercept abnormal intrusion by analyzing various abnormal behaviors in communication, but the vulnerability identification has the problem of low accuracy.

Based on the problems of the above methods, the design of an intelligent monitoring system for wireless communication network security vulnerabilities based on machine learning is proposed. The system introduces machine learning algorithms, and completes the design of an intelligent monitoring system for wireless communication network security vulnerabilities through the design of hardware and software. The experimental results show that the system can effectively monitor the security vulnerabilities of wireless communication networks, with high monitoring accuracy and high work efficiency.

2. System hardware design
Once the vulnerabilities appear, they will attack the entire network system, and vulnerabilities are also more common in wireless communication network systems [6]. The security vulnerabilities of the wireless communication network are the main reason that causes the communication network to be attacked and intruded [7]. The timely detection of security vulnerabilities in wireless communication networks is very important. The overall architecture of the wireless communication network is shown in Figure 1.

![Figure 1. The overall architecture of the wireless communication network](image1)

Wireless communication network in the actual network deployment, the PTK-5500 controller is set in the provincial core network to manage the wireless communication network platform and ensure the security of the wireless communication network.
The original wireless communication network security vulnerability monitoring system mainly uses ICMP Echo and Broadcast ICMP scanning technology to scan wireless communication network vulnerabilities. The operation process of the system is to send requests to the wireless communication network and wait for the host to respond to the monitoring, and the internal structure of the monitoring system is complex. The long response delay is not conducive to the timely monitoring of wireless communication network vulnerabilities. The hardware of the improved system includes three modules: vulnerability data acquisition module, vulnerability data scanning module and wireless network security vulnerability intelligent monitoring module. The overall architecture of the system is shown in Figure 2.

![Figure 2. The overall framework of the monitoring system](image)

In Figure 2, vulnerability data is captured directly and t-MPLS high-speed data transmission technology is adopted to transmit data acquired through collection, scanning and monitoring. Machine learning technology is used to improve the overall efficiency of vulnerability monitoring, and machine learning is used to scan vulnerabilities at high speed to achieve efficient vulnerability monitoring. The improved monitoring system is more sensitive to the response of vulnerability monitoring and reduces the development cost of the system.

2.1. Vulnerability data collection module
In security vulnerability data acquisition module, the wireless communication network security vulnerability data acquisition, loopholes for wireless data belong to sex, analysis the relation between the data, data integration uncertain security leak hole, and into the corresponding data collection, choose wireless data collector integrated security hole data acquisition [8]. The data collection process of wireless communication network security vulnerability is shown in Figure 3.

![Figure 3. Data collection process of wireless communication network security vulnerabilities](image)

The power interface of the data collector is DC12V direct plug-in type, and the network cable is connected through the RJ45 network port, and the data from the transmitter can be forwarded to the server, which is convenient and simple to operate [9].

2.2. Vulnerability data scanning module
The system is equipped with a vulnerability scanner for the smooth operation of wireless communication network nodes. The vulnerability scanner interface classifies and scans the data of wireless communication network nodes, and gathers different data nodes into the same data set to ensure the security of vulnerability data scanning process. XSS vulnerability detection plug-in [10] is set in the
scanner, through which wireless communication network security vulnerabilities are scanned. The structure diagram of XSS vulnerability detection plug-in is shown in Figure 4.

![Figure 4. Internal structure diagram of XSS vulnerability detection plug-in](image)

2.3. Wireless communication network security vulnerability intelligent monitoring module
When tracking the wireless communication network vulnerability data signal, monitor the system session operation of the vulnerability data, analyze the communication network security vulnerability information according to different customer standards, mark the system vulnerability data, select a reasonable matching mode, and reorganize the communication network IP fragmentation, Improve the performance of the high-level protocol system, reduce the complexity of spatial data search, use this as the basis of vulnerability data monitoring, select data information that does not match the system, and combine them to form a complete vulnerability data set.

3. System software design
In order to strengthen the software part of the monitoring system, this paper introduces a machine learning algorithm, which is combined with the intelligent monitoring system software to realize the intelligent monitoring of wireless communication network security vulnerabilities.

Assuming that most of the data sequence to be tested in the wireless communication network is normal wireless communication network data, the security vulnerability data becomes the target of system monitoring. The normal data in the wireless communication network is processed through the optimal evaluation function $F: x \rightarrow y$, then there is $x_i \in X$, $y_i \in Y$, and the optimal evaluation function can be expressed as:

$$F^* = x + \frac{\omega}{n} \sum_{i=1}^{n} \phi(F(c_i))$$

In the formula, $\phi$ represents the loss function, $\omega$ represents the harmonic parameter of the security vulnerability data, and $F(c_i)$ represents the optimization rule.

In the process of wireless communication network security vulnerability monitoring, the optimal evaluation function is used to process normal data in the communication network. However, there are still abnormal data that are deeply camouflaged, so further processing of these data is required. Introduce the neural network algorithm, filter it, and build a three-layer neural network algorithm model, including input layer, output layer and rule layer. If the wireless communication network data is obscured, the output of each communication network node is:

$$\xi_i^1(c_i) = v(c_i), i = 1, 2, 3 \cdots n$$

$$\xi_i^2(c_i) = v(c_i), i = 1, 2, 3 \cdots n$$

$$\xi_i^3(c_i) = v(c_i), i = 1, 2, 3 \cdots n$$
The above three equations represent the communication network data output of the three-layer neural network. Calculate the fuzzy output value in each level:

\[ \tilde{x}_i^4 = \psi_i f_i (rc_1 + rc_2 + \cdots + rc_n), i = 1, 2, 3 \cdots n \]

In the formula, \( \psi \) represents the intensity of fuzzy processing, and \( r \) represents the momentum factor of wireless communication network data.

4. Experimental analysis

4.1. Experimental environment and parameter settings

The experiment was carried out on Matlab platform, operating system was Windows 10, E52678V3 processor.

The contents of the experiment parameters are set as shown in Table 1.

| parameter                  | Value                  |
|----------------------------|------------------------|
| CPU/GHz                    | 3.4                    |
| Router                     | Attack the router      |
| Server memory/GB           | 8                      |
| IP Data status             | normal                 |
| Running memory             | 4                      |
| Vulnerability data/items   | 100                    |
| Normal data/item           | 100                    |

Table 1. Experimental parameters

4.2. Analysis of experimental results

4.2.1. Time-consuming analysis of monitoring vulnerabilities. In order to verify the effectiveness of the method in this paper, experiments compare the time consumption of the method in this paper, the method in literature [4] and the method in literature [5] in wireless communication network security breach monitoring. The shorter the time, the higher the efficiency of this method. The experimental results are shown in Figure 7.

![Figure 5](image.png)

Figure 5. Comparison of time-consuming vulnerability monitoring by different methods

By analyzing Figure 6, it can be seen that under the same parameter conditions, the time-consuming of vulnerability monitoring in this paper is low. When 200 pieces of vulnerability data are monitored, the monitoring time of this method is about 1.4s, that of literature [4] is about 6.3s, and that of literature [5] is about 4.5s. Among them, the methods of literature [4] and literature [5] fuse the suspected vulnerability data, analyze the nature of the obtained data, and recollect these data during wireless communication network vulnerability monitoring. The operation process is complex and the system
response time is long. When the system monitors, it purposefully obtains the wireless communication network data, which can directly and effectively confirm and capture the vulnerability data in the wireless communication network, and the response delay is short. It is verified that the method has high efficiency and certain feasibility.

4.2.2. Accuracy analysis of monitoring vulnerabilities. In order to further verify the effectiveness of the system in this paper, the experiment compared the accuracy of the three methods when monitoring 200 pieces of wireless communication data, and the accuracy of detecting the leaked data. The experimental results are shown in Table 2.

| Monitoring data/item | Method of the article (%) | Literature [4] (%) | Literature [5] (%) |
|----------------------|---------------------------|--------------------|--------------------|
| 50                   | 97                        | 92                 | 90                 |
| 100                  | 95                        | 85                 | 82                 |
| 150                  | 92                        | 80                 | 76                 |
| 200                  | 90                        | 78                 | 70                 |

By analyzing the data in Table 2, it can be seen that with the continuous increase of monitoring data, the monitoring accuracy of the three methods presents a declining trend. Where, when the monitoring data is 100, the accuracy of vulnerability data monitored by the method in this paper is 95%, that of the method in literature [4] is 85%, and that of the method in literature [5] is 82%. When the monitoring data is 200, the accuracy of the method in this paper is 90%, the accuracy of the method in literature [4] is 78%, and that of the method in literature [5] is 70%. Although the monitoring accuracy shows a decreasing trend, the accuracy of the vulnerability data monitored by the proposed method is above 90%, which is higher than that of the other two methods, verifying the reliability of the proposed method.

5. Conclusion

Based on the traditional wireless communication network security vulnerability monitoring system, this paper proposes a wireless communication network security vulnerability intelligent monitoring system based on machine learning. Through the improvement of system hardware module functions, combined with machine learning intelligent algorithms, analysis of wireless communication network security vulnerability data attributes, etc., the design of an intelligent monitoring system for wireless communication network security vulnerabilities has been completed. The experimental results show that the accuracy of monitoring security vulnerabilities in wireless communication networks using this method is above 90%, and the work efficiency is high, which has certain practical significance in this field.

References

[1] Zhuang haiyan. Wireless communication network security risk prediction based on big data analysis technology [J]. Microelectronics and computer, 2019, 36(08): 97-100.
[2] Zhong Jinglong, Lü Liping. Multi-space key distribution algorithm for sensor network security [J]. Journal of Electronic Measurement and Instrument, 2019, 33(4): 125-132.
[3] Zhang Xiao. Research on active defense technology of ship communication network [J]. Ship Science and Technology, 2018, 40(24): 115-117.
[4] Li Jie, Yu Yan, Wu Jiashun. DOMXSS vulnerability detection algorithm based on dynamic stain analysis [J]. Journal of Computer Applications, 2016, 36(5): 1246-1249.
[5] Zhao Yuehua, Deng Yuanhao. Research and Implementation of Kernel Race Vulnerability Monitoring Technology Based on Hardware Virtualization [J]. Software Guide, 2015, 14(5): 161-164.
[6] Zuo Pengfei, Hua Yu, Xie Xinfeng, et al. Security encryption method for deep learning accelerator [J]. Computer Research and Development, 2019, 56(6): 1161-1169
[7] Zhang Bin, Guanghui, Chen Xi. Security architecture of wireless Mesh network based on smart contract [J]. Computer Engineering, 2019, 45(11): 16-23, 31

[8] Liu Meng, Wang Xiaoping, Ma Yuehui. Design of data acquisition system for railway subgrade settlement based on LoRa [J]. Journal of Geodesy and Geodynamics, 2019, 39(9): 987-990

[9] Qin Tianzhu, Zhang Weigang, Qu Shaocheng. Multi-channel data collector based on Modbus protocol [J]. Electronic Measurement Technology, 2017, 40(11): 175-178.

[10] Li Weifeng. Platform-based XSS attack mitigation technology [J]. Computer Programming Skills and Maintenance, 2017, 15(5): 92-94.