Network Information Security Risk Assessment Based on Artificial Intelligence

Yaosheng Wang1,*

1Nanchang Vocational University, Nanchang, China, 330500

*Corresponding author e-mail: 38943770@qq.com

Abstract. With the development of society and the progress of human civilization, science and technology are more and more widely used in people's daily production and life, and artificial intelligence technology is also more and more widely used in this era. With the advent of the information age, the development of the network is faster and faster, and the popularization rate is higher and higher. The network information security problem has gradually become a hot issue of social concern question. With the increasingly open network environment, network attack tools become easier to obtain, more automated, more intelligent, which poses a huge challenge to information security protection. Therefore, in order to deal with the network information security problems in this information age, this paper studies the method of network information security risk assessment and analysis based on artificial intelligence, through in-depth study of network information security, simulate attacks on network information, so as to find the weakness of the current network information security system. In the research, a large number of network information security vulnerabilities are found by simulating the attack of network information, so as to repair the vulnerabilities one by one. Through the analysis, this paper studies the Content Filtering Gateway filtering system to filter out 94.8% of the virus and garbage, improve the network information security rate.

Keywords: Science and Technology, Artificial Intelligence, Network Attack Tools, Network Security

1. Introduction

Artificial intelligence (AI) has further expanded the ability to interact with human body and mind. "Alpha dog" has defeated two world go champions Li Shishi and Ke Jie, setting off a new wave to promote the global Internet artificial intelligence[1-2] technology development. On May 23, 2016, the national development and Reform Commission, together with the Ministry of science and technology...
and the Ministry of industry and information technology, jointly formulated a three-year action plan to promote the "Internet" of artificial intelligence. The first meeting clearly proposed to establish artificial intelligence industry, services and standardized basic service system by 2018, realize the breakthrough of artificial intelligence core technology, and cultivate a number of international leading artificial intelligence core technology backbone enterprises. In the future, the application and market scale of artificial intelligence will reach 100 billion levels in 2020. On March 5, 2017, Premier Li Keqiang once again clearly mentioned in his report on the economic work of the State Council Government in the past three years that it is necessary to further accelerate the cultivation and vigorously develop strategic emerging industries, and comprehensively implement the overall development plan of national strategic key emerging industries including the cultivation of emerging industries such as artificial intelligence in the past three years. This is also the first time that "artificial intelligence" has been explicitly included in the work report of the State Council Government in the past three years.

With the globalization of the world economy and the rapid advancement and development of Internet information security technology [3-5], the importance and application of information security system in social and national economic and political, military and socio-economic management fields are becoming more and more extensive, and the whole country and society rely more and more on the security of information system. At present, the problem of information system security has developed into a major overall problem related to the political stability, social stability and the healthy and orderly development and operation of the national economy. Information security management is essentially based on risk management. At present, with the rapid development of information technology, the theory and method of information security management are undergoing significant changes. From a single technical means to comprehensive management of technology and management, from the management of part of the project management of the whole system, from the perfect standard of experience management to scientific management, there is a clear level of security. The object of risk assessment is from comprehensive evaluation to human factor evaluation, from current situation evaluation to trend evaluation, from static evaluation to dynamic evaluation, from manual evaluation to automatic evaluation, from qualitative evaluation, quantitative evaluation to the combination of qualitative and quantitative evaluation. Combining with the actual situation of information system, improve and innovate relevant scientific theories and methods to ensure the continuous improvement of information system risk assessment [6-8] and management.

This paper mainly studies the method of network information security [9-10] risk assessment based on artificial intelligence. Network information security has long been a hot issue in today's era. In the information age, network security has become a hot issue. The risk assessment of network information security is urgent. Therefore, in order to carry out the risk assessment of network information security more accurately and efficiently, this paper introduces the concept of artificial intelligence, through the simulation of attacking network information, so as to find out the current network information security vulnerabilities and repair them, so as to achieve the purpose of network information security prevention and control.

2. Network Information Security Risk Assessment Method

2.1. Risk assessment Modeling of Network Information Security based on rbf Neural Network
Radial basis function neural network is a three-layer static feedforward neural network. The input layer is directly connected with the hidden layer, and the hidden layer is weighted with the output layer (linear function connection). The transfer function of hidden layer element of RBF neural network is radial basis function (such as Gaussian function), which is symmetric about the center. RBF neural network is a typical forward neural network. Let the number of neurons in input layer, hidden layer and output layer be \( N, M, P \) the input information vector is as follows: 
\[
X = [x_1, x_2, \ldots, x_N] \]
the output information vector is as follows: 
\[
Y = [y_1, y_2, \ldots, y_P] \]

Then the input-output relationship of the \( i \) first neuron in the hidden layer is as follows:
\[
z_i = \exp(-\|X - c_i\|^2 / 2\sigma_i^2), i = 1, 2, \ldots, M
\]
(1)

The output layer implements the \( R_i(x) \) to \( Y \), the linear mapping of, namely:
\[
Y = \sum_{i=1}^{M} w_i R_i(x) = \sum_{i=1}^{M} w_i z_i = \sum_{i=1}^{M} w_i \exp(-\|X - c_i\|^2 / 2\sigma_i^2), j = 1, 2, \ldots, P
\]
(2)

The purpose of constructing and training a RBF neural network is to make it learn and then consider the risk assessment modeling. Therefore, it is generally considered that there is only one output node, that is, the evaluation value of risk level. This structure can be easily extended to the case of multiple output nodes. The vector value of network information security risk factor evaluation index after quantitative processing and consistency processing is taken as the input of neural network. Quantitative data is to quantify each index of network information security risk through fuzzy evaluation method to meet the input data requirements of RBF neural network.

2.2. Information System Risk Assessment Method

From the perspective of risk management, information security risk assessment is to systematically analyze the threats and loopholes faced by information systems, use scientific methods and means to assess the degree of harm and possible security accidents, and put forward targeted protection countermeasures and rectification measures to prevent and solve information security risks, or to control the risks at an acceptable level, To maximize the security of the system and information.

3. Experimental Background and Design

3.1. Experimental Background

In the process of Internet popularization, there is a large management gap in the supervision of network content, whether in technology or law. Therefore, a large number of disturbing and spam information spread on the network, such as pop-up windows, floating objects, and other forms of contact page advertising, harmful scripts embedded into the touch page and computer viruses and other malicious programs automatically download files from the background of the website, commonly known as "rogue software", as well as various invasive spam and other viral mails. These intrusive e-mail and spam information not only bring bad Internet habits and experience to the users
and consumers living on the network, but also have a significant negative impact on the quality of network communication. These negative effects, to a certain extent, not only affect the communication efficiency of the network, but also lead to a huge waste of network resources.

3.2. Experimental Design

The collected information can be accurate to every day's data through the content filtering gateway, but we need to investigate the overall impact of network communication interference and spam information, so we will not interfere with the more detailed time distribution of information investigation, only consider the distribution of interference in a few months and spam information, and filter traffic in the same unit, The Content Filtering Gateway filters 94.8% virus and garbage, which improves the network information security rate. The statistical results are shown in Table 1.

| agreement | Number of scans | Number of viruses | Quantity of garbage | Content filtering |
|-----------|----------------|------------------|---------------------|------------------|
| POP3      | 59635          | 265              | 15364               | 0                |
| SMTP      | 6589           | 156              | 42                  | 0                |
| HTTP      | 3564863        | 25364            | 0                   | 756398           |
| FTP       | 3354           | 60               | 0                   | 0                |
| IMAP      | 0              | 0                | 0                   | 0                |
| NETBIOS   | 0              | 0                | 0                   | 0                |
| MSN       | 0              | 0                | 0                   | 0                |

4. Discussion

4.1. Situation Analysis of Information Security

At present, the security situation of China's network and information system is still very grim, and the international political task of maintaining a country's network information security is still very arduous. All kinds of foreign and hostile forces have destroyed and infiltrated China's important networks and information systems, and subversive and subversive activities have never stopped completely and are constantly upgrading. With the support of foreign hostile forces, reactionary forces at home and abroad frequently attack and destroy important information systems. Domestic cyber-crime continues to rise sharply. Internet theft is serious. The spread of computer viruses and illegal network intrusion are very serious. Criminals use the security loopholes of some important information systems to commit crimes, causing serious losses to users and causing many social
problems. Information system security management is not in place, security measures are not in place, information system operation accidents occur from time to time.

Based on the investigation and statistics of the annual network information system security report released in recent years, the development trend of various network security incidents is analyzed. Statistics show that the average annual growth rate of network security incidents is extremely significant. In 2018, the number of webpage malicious code events increased by 2.2 times. In the first half of 2019, about 10 million malicious codes were captured, with a year-on-year increase of 59.3%. Within one year, the number of webpage tampering incidents increased significantly. The survey results are shown in Figure 1.

![Figure 1. Year statistics of the number of tampered pages in China](image)

The security vulnerability of information system software is still the main source of various security threats. Trojan horse programs embedded in system vulnerabilities pose a serious threat to Internet Security in China. In 2015-2019 years, the number of hosts in Chinese mainland was doubled. In 2018, the number of hosts implanted with Trojan horses increased by 1.92 times to 53215 in 2017, and increased to 1003265 in 2019. In the first half of 2019, only 543454 was detected, and the results are shown in Figure 2.

![Figure 2. Statistics of the number of Trojan hosts implanted in China](image)

According to the statistical results of Figure 1 and Figure 2, in recent years, the risk of network information security in China is higher and higher, the number of network information attacks is more and more frequent, and the growth rate of network attacks year by year is also faster and faster. From the situation of network information attacks over the years, the main ways of network information
attacks in China are Trojan virus, webpage tampering and malicious agent Code attack, which also provides a repair direction for the current network information security prevention and control.

4.2. Development Prospect of Network Information Security Protection

The theory and technology of network security protection are summarized and refined from the practice of network security, and are used to guide the practice of network security protection. With the change of network security threat object and scope, the corresponding security protection theory and technology will also develop. This development trend is still around the scope of security risk and object identification, combined with specific time and environmental factors, forming a variety of complex network security situation. But in any case, all changes are inseparable. As long as we grasp the scope and object of risk identification and pay attention to the cross influence of time and environmental factors, we can summarize new safety protection theory and technology suitable for future needs.

Security assessment will develop from "security environment" to "security environment" and "security application capability". With the change of security situation, there are obvious deficiencies in solving security problems from the perspective of hardware and technology. In the network environment, network hardware, related software, network users, use rules or policies have become an overall system of mutual influence. Therefore, only from a single aspect to solve the security problem is bound to be unable to achieve well. Therefore, the implementation and evaluation of safety will focus on the construction of "security environment" and the cultivation of "security application ability". At the same time, the improvement of security policy and safety training will also be included in the important agenda of security protection. These seemingly "useful supplements" in the past will gradually rise to the same status as investment in hardware and software.

Since the birth of the network, there has been a security problem, its main purpose has been to show off technology and prank. But in recent years, this trend, which lasted for many years, has been completely broken. The utilitarianism purpose of network security threat has completely replaced technology show off and prank, which is reflected in all aspects of network security. The traditional virus damage system startup information almost no longer exists, and the number of virus infected files is sharply reduced. However, a large number of viruses with relatively single technology and single use are very popular. The boundaries between viruses and Trojan spyware are increasingly blurred. Their technology is nothing more than to realize the automatic loading of operating system boot process or application program execution process through various ways. Its main purpose is to collect user information, monitor user's addiction behavior, steal user's password and steal user's virtual property. Although the types of these threats vary greatly, they usually use technology to hide themselves by tampering with the entrance, hijacking the system functions. Therefore, the technology tends to be single basically.

The utilitarian development trend of this kind of security threat is reflected in the aspect of security countermeasures. It will guide the comprehensive development of security protection from simple safety protection technology research to the scientific, strengthened management and social engineering level of protection countermeasures. At present, host intrusion prevention system has appeared in technology, and Unified Threat Management has appeared to deal with these threats.
Generally speaking, utilitarianism of security threats leads to the diversified development of security protection theory and technology.

In short, the development of network technology and application will also promote the rolling development of network security theory and technical means. In the course of research, we must fully recognize this point, pay close attention to the dynamics in the field of network security at all times, critically absorb the latest ideological essence, and constantly explore new technologies and methods, so that our subjects will be constantly strengthened and perfected in the research process. Network information security still has a long way to go.

5. Conclusion

This paper mainly studies the network information security risk assessment and analysis based on artificial intelligence. With the rapid development of network information in the world, people's production and life are full of the application of network information, and the network information has been attacked more and more. Therefore, network information security has quietly become a hot issue in this era. In order to better protect people's network information security, this paper adopts the network information security protection governance method based on artificial intelligence, through the simulation of various network information security attacks on computer users in China, so as to find the current network information security vulnerabilities, and provide development direction for the protection of network information security.

References

[1] Jeavons, Andrew. What Is Artificial Intelligence?[J]. Research World, 2017, 2017(65):75-75.

[2] Raza M Q , Khosravi A . A review on artificial intelligence based load demand forecasting techniques for smart grid and buildings[J]. Renewable and Sustainable Energy Reviews, 2015, 50(oct.):1352-1372.

[3] Xiang Z , Magnini V P , Fesenmaier D R . Information technology and consumer behavior in travel and tourism: Insights from travel planning using the internet[J]. Journal of Retailing & Consumer Services, 2015, 22(jan.):244-249.

[4] Audirac, I. Information Technology and Urban Form[J]. Journal of Planning Literature, 2015, 17(2):212-226.

[5] Begovi B . Book Review: The Great Convergence: Information Technology and the New Globalization[J]. Panoeconomicus, 2017, 64(5):645-655.

[6] Aven T . Risk assessment and risk management: Review of recent advances on their foundation[J]. European Journal of Operational Research, 2016, 253(1):1-13.

[7] Martin J G A , Denis Réale. Temperament, risk assessment and habituation to novelty in eastern chipmunks, Tamias striatus[J]. Animal Behaviour, 2016, 75(1):309-318.

[8] Fraser-Mitchell J N . Modelling human behaviour within the fire risk assessment tool CRISP[J]. Fire & Materials, 2015, 23(6):349-355.
[9] Joshi C, Singh U K. Information security risks management framework – A step towards mitigating security risks in university network[J]. Journal of Information Security and Applications, 2017, 35(aug.):128-137.

[10] Carrapico H, Farrand B. 'Dialogue, partnership and empowerment for network and information security': the changing role of the private sector from objects of regulation to regulation shapers[J]. Crime Law & Social Change, 2017, 67(3):1-19.