Retraction Notice

The Editor-in-Chief and the publisher have retracted this article, which was submitted as part of a guest-edited special section. An investigation uncovered evidence of systematic manipulation of the publication process, including compromised peer review. The Editor and publisher no longer have confidence in the results and conclusions of the article.

LS did not agree with the retraction. ZW, NC, and JC either did not respond directly or could not be reached.

Research on computer network security evaluation based on image recognition and neural network

Zilong Wang,[a] Lin Shi,[a,b,c,*] Ning Chen,[d] and Jie Chen[c]

[a]Nanjing University of Aeronautics and Astronautics, College of Economics and Management, Nanjing, China

[b]Southeast University, School of Cyber Science and Engineering, Nanjing, China

[c]Jiangsu Financial Information Management Center, Nanjing, China

[d]Jiangsu Water Conservancy Network Data Center, Nanjing, China

Abstract. In today's social development, the level of informatization has been greatly improved. Computer networks are now used in all aspects of society, especially with the popularity of mobile phones and computers. Basically, a mobile phone is a computer that stores all the information of a person, so it is indispensable for carrying out research on computer network security evaluation. The purpose of this article is to examine the growing state of information security threats in computer networks. Neural network technology, which is considered secure, has high flexibility, fast access to information, strong logic, and low failure. Toward creating a low-cost network topology, we used a low-cost network risk assessment method to assess the security of computer networks based on neural networks, and we evaluated existing risks that are appropriate for future computer security research. The results of the study show that neural networks using the Bayesian network method have a significant impact on network security. Considering the problems that can occur with information security risks, computer security systems based on neural networks have a 30% reduction in information error rate compared with traditional methods, and computer network systems based on neural networks have better learning performance to safeguard network security. Improving the security of information requires further research and evaluation of computer network security based on neural networks. © *2022 SPIE and IS&T* [DOI: 10.1117/1.JEI.32.1.011214]

Keywords: neural network; computer network; network security; evaluation research.

Paper 220477SS received May 6, 2022; accepted for publication Aug. 12, 2022; published online Sep. 15, 2022.

1 Introduction

Network security protects the hardware, software, and data in a network system from being damaged, altered, or leaked due to accidental or malicious reasons, allowing the system to operate continuously, reliably, and normally and preventing interruptions in network services. With the current developments of science and technology, information has become a critical component of society. The vigorous development of computer networks for handing information increasingly exposes more and more of our information to the hidden dangers caused by information leaks, which has been increasing. Therefore, the emphasis on information security also needs to be greater. As can be seen from current information security risks and some incidents, there are still many vulnerabilities in today's computer networks. Therefore, there remains a requirement to find a suitable solution that will address the huge information security risks. For individuals, improving network information security protects personal privacy and personal assets.

With the information leaks caused by individuals, the most common one is caused by clicking on unknown links and unknown devices, which are called logical security and physical security, respectively.[1] The back propagation (BP) nervous system is a multilayer network trained according to the error-backpropagation algorithm and is one of the most widely used

*Address all correspondence to Lin Shi, shiling717@nuaa.edu.cn

1017-9909/2022/$28.00 © 2022 SPIE and IS&T

models in the study of current nervous systems.[2] The principle of the BP neuropsychological study is to use a feedforward network with backscattering, without adjusting the level and weight of the network, thus reducing the sum of the square network errors.[3] There is no feedback link between individual neurons in the BP neurological model. The three-layered local structure consists of an obvious forward neural network with supporting layers.[4] A monolayer relay system is used to solve linear dissociative problems, whereas a multilayer relay system is used to solve nonlinear computer network problems.[5]

Xu et al.[6] indicated that the current computer network security problems mainly come from logical security and physical security, so it is necessary to strengthen the technical research in these two areas. Yang et al. also pointed out that, with the advancement of science and technology, it is necessary to prevent information security risks simultaneously.[7] Ma et al. found that network security problems not only are caused by improper operations but also include the accuracy of information entry and the timeliness of information processing; therefore, network security should focus on comprehensive improvement.[8] Shuo et al.[9] indicated that the current neural network technology is not mature enough for computer security, but the prospects are very good with the application of neural networks in computer network security able to address some of the shortcomings.[9] Xiao et al. indicated that the current application of neural networks should be based not only on the speed and accuracy of processing data but also on the learning type based on neural networks, so it can be useful for certain self-learning.[10]

Thus, this paper applies the Bayesian approach to the study of computer network security, i.e., understanding and analyzing the causes and reasons for network security problems and describing the basic methods for solving and continuing the study of computer networks. This paper first presents a systematic overview of the main contents and research objectives of the study. The second part is the theoretical foundation; it provides a comprehensive and systematic overview of logical security, physical security, and information security management in modern computer network security. In addition, it shows the degree of integration with current integration techniques such as Bayesian formulations and risk assessment models. The third part gives the research. In particular, neural network-based public factors and activities for computer network security, as well as the research conducted using Bayesian methods, are analyzed, and the experimental results are given. The fourth part summarizes the research results and give recommendation for the full application of Bayesian network risk analysis models and neural network strategies in computer network security.

2 Proposed Method

2.1 *Principle of Bayesian Detection of Network Security*

A Bayesian network is also called a belief network, or kernel network.[11] It is an acyclic graphical pattern describing the probabilistic relationships of the dependency among stochastic covariates and is the essential graph used in causal analysis.[12] It offers us a clear and succinct graphical model to illustrate interesting relationships between elements and allows for more clarity and easier understanding of intricate associations between elements.[13] The Bayesian network has many nodes and directed maps whose known target node's location can be determined by a given solution.[14] A Bayesian network links the introduction of pie charts to variables, so the logical relationships between variables can be easily represented. Bayesian networks have been proposed to solve general problems in the theory of possibilities. The following basic probability equation is often used in the search process.

The probability of the condition of $P(N|M)$ factor N depends on the presence of factor M, where M and N are two elements of E and $P(M) > 0$. Similarly, if $P(N) > 0$, then $P(M)|N)$ is called the probability of factor M conditionally if factor N occurs, where

$$P(N|M) = \frac{P(MN)}{P(M)}, \tag{1}$$

$$P(M|N) = \frac{P(MN)}{P(M)}. \tag{2}$$

From the above, we get

$$P(N/M) = P(M/N). \tag{3}$$

Once the Bayesian network model is built, the batch normalization (BN) knowledge can be explained. The reason is that, assuming the set of all variables to be $X = X1, X2, \ldots, Xn$, the set of variables in subset $E = e$ with respect to the set of variables in subset R has a probability distribution that is found by the equation:

$$p(R|E = e) = \frac{P(R, E = e)}{P(E = e)} = \lambda \Sigma_{X-(R \cup E)} P(X), \tag{4}$$

where there is a constant e and R could be any group of variables. More importantly, this is not merely a resource debate. In other words, if the probability of a particular cause, as well as the structure and variables of BN, is known, then the probability of the outcome is calculated by a Bayesian formula. The analytical argument of the results is logical, with the chances of an event being known and the opportunities caused by the event being discovered. An argument that combines the arguments of reason and analysis, i.e., when the chances of a particular incident and a specific cause are realized, then looks for other causes and aspects of the incident.

The computer security evaluation system mainly includes package logic security, physical security, and management security. These three aspects mainly include intrusion prevention, data encryption, anti-virus measures, digital signatures, software security, access control, system audit, data recovery and backup, equipment safety, fault tolerance redundancy, line safety, power supply safety, network room safety, electromagnetic leak prevention, emergency response mechanism, personnel safety training, safety management system, and safety organization system. In general, the reason for information leaks is the user clicking on an unknown link or using an unknown connection device, which are the aspects of logical security and physical security, respectively. These fuzzy methods can transform the uncertainty of factors into quantitative expressions; moreover, fuzzy mathematics is a study in reality, with many boundaries that are indistinguishable, and it can even apply an effective method to fuzzy things. Through it, people can correctly and objectively judge uncertain research subjects.

If $X = X1, X2, \ldots, Xn$ corresponds to the probability $P(Xi)$, $I = 1, 2\ldots$, the probability of a blurred incident is called the blurred event likelihood if the blurred episode is represented by the blurred set x. The calculation equation is

$$P(X) = \sum_{i=1}^{\varpi} U_X(x_i) P(x_i). \tag{5}$$

Assuming that the uncertain event y in y is known, the probability of occurrence of x in X is known as the uncertain probability of condition, and it is calculated as follows:

$$P(x, y) = \frac{P(xy)}{P(y)}, \quad P(y) > 0. \tag{6}$$

The equation for the total uncertainty probability, based on the definition of uncertainty conditional probability, is as follows:

$$P(A) = \sum_{i=1}^{\varpi} P(AB) P(B_i). \tag{7}$$

Simplifying the fuzzy total probability equation, we get

$$p(B|A) = \frac{P(B_i A)}{P(A)}, \tag{8}$$

$$P(B_i A) = P(AB_i) = P(A|B_i) P(B_i). \tag{9}$$

2.2 *Data Mining Technology and Related Algorithms*

The general definition of data mining refers to a process of extracting or analyzing and mining useful data from a large amount of data through various algorithms. It has specific prerequisites and constraints, and it is oriented to a specific domain, and it can deeply mine its hidden information. Data extraction, transformation, analysis, and related modeled data processing are used to analyze, extract, and output critical business information from the data for use in making business decisions. Data generation refers to the stage of computer file creation and exploration and the development of equipment for data information generation in the general sense, and it is the beginning of the life cycle of electronic files or source data. Simply put, data mining is a type of comprehensive data analysis method that is more in depth than other data analysis methods. Common data analysis and data selection equations for data mining are shown in Eqs. (10)–(13):

$$CRF_t(b) = \sum_{t=1}^{k} F(t_b - t_{b1}), \tag{10}$$

$$F(t) = \left(\frac{1}{\text{attenuation}}\right)^{\text{step}*t}, \tag{11}$$

$$C_j = \{t_i | f(x) = C_f \, 1 <= i <= n, 1 <= j <= n, \tag{12}$$

$$E(A) = \sum_{J=1}^{V} \frac{D_f}{D} \times \text{Info}(D_f). \tag{13}$$

Nowadays, the amount of information generated in the business field is increasing, with the business data containing useful information that may be crucial for business decisions. If data generation is just collecting the data, it has no meaning. Therefore, data mining can be further described as researching and analyzing a large amount of business data generated in accordance with the business goals set by the enterprise to reveal some regularities, which may be implicit, unknown, or possible. These rules can then be further modeled, so they can be better used for decision-making. Commonly used processing equations for analog processing are shown in Eqs. (14)–(16):

$$d_k = (y_k - c_k) \times c_k \times (1 - c_k) \;\; k = 1,2, \tag{14}$$

$$e_j = \left(\sum_{k=1}^{n} d_k v_j\right) \times h_j \times (1 - h_j) \;\; j = 1,2, \tag{15}$$

$$V_{jk}(N+1) = V_{jk}(N) + a_1 d_k(N) h_j. \tag{16}$$

2.3 *Image Recognition*

An image-based pattern recognition system usually consists of three parts, the first of which is the collection and acquisition of image data corresponding to the study and understanding of the subject under investigation, from which the data and information are extracted. the function of this step is to convert the target image into an electrical signal through electronic devices, such as cameras and scanners. The second part is the processing and preprocessing of the information, the function of which is to process, sort, and analyze the obtained electrical signals; to propose the essential features reflecting the characteristics of the target; and to extract and select that features that have a great influence on the results of the whole system identification and classification. The third part is the identification or classification process; the function of this part is to map the feature vector space of the previous part to the type space, which is equivalent to the process of making a conclusion from perceptual to rational understanding.[15] Figure 1 shows the original image and the image with noise.

In practical applications in which neural networks are used to achieve matching or recognition, the feature-based neural network recognition method has been widely adopted; it makes

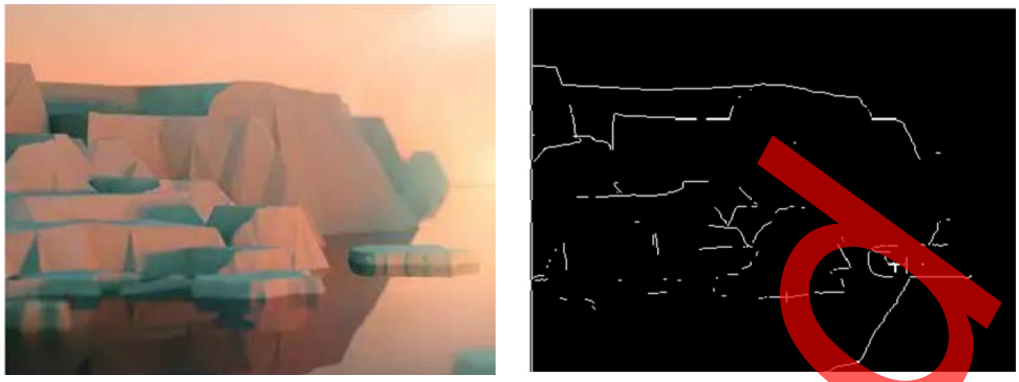

Fig. 1 Original image and noisy image.

Fig. 2 Filtered image and blurred weighted mean filter map.

full use of the human experience to acquire pattern features and uses the neural network as a feature clustering device to recognize the target image. These features include geometric features, statistical features, transformation features, and various fusion features. This method requires that the extracted features are accurate and reliable, reflecting the differences between images. The algorithm is usually based on the premise that the image being processed is not contaminated. All of these limitations make the algorithms less reliable, and most symptom extraction algorithms are very complex and computationally expensive, making it difficult to achieve real-time performance in real-world surveillance processes. Figure 2 shows the filtered image and the blurred weighted mean filter map.

The recognition method based on image pixel grayscale uses the simple processed raw image grayscale data as the neural network training data and directly uses the original image grayscale value as the input of the neural network. This approach has a large neural network, but the network has good anti-interference performance and a high recognition rate. This approach uses both global information and detailed information, i.e., it uses global information without neglecting detailed information, and it uses the neural network to automatically extract features. The method takes full advantage of the neural network's ability to process data in parallel, its ability to handle uncertain data, and its ability to tolerate errors., unlike feature-based recognition methods, which treat the neural network as a classifier. The algorithm in this paper filters the image as shown in Fig. 3. Image recognition is achieved by identifying and detecting objects or features in digital images or videos through computer cameras. It adopts a method of capturing, processing, examining, and understanding images.

3 Experiments

3.1 *Correlation of Experimental and Data Processing*

The experimental data come from the literature based on neural networks, and then it is compiled and analyzed with relevant data. Most of the experiments based on neural networks now use a BP

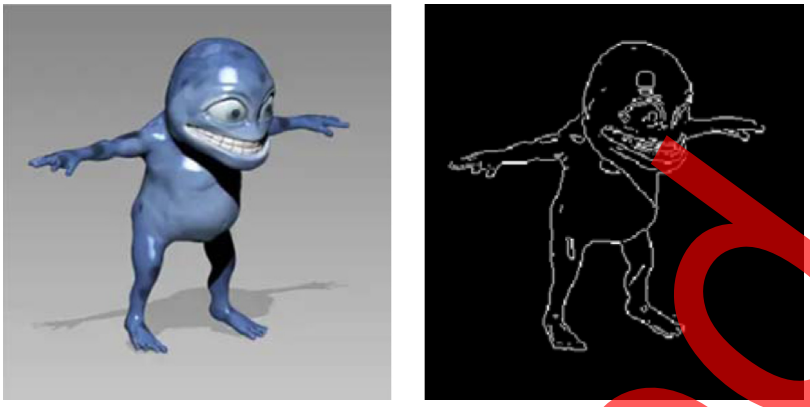

Fig. 3 Filtered image by proposed algorithm.

network as a reference, according to the relevant data obtained, and then use the output information of the computer to judge the obtained experimental data and processed it by a tool. The most widely used is the BP neural network model, which uses the steepest descent method for backpropagation, adjusts the relevant values, and minimizes the error. The design work of the output layer of BPNN is reflective of the results of the network security assessment. According to the evaluation design of the input layer, the number of nodes in the output layer is set to 2; then the output result of (1, 1) indicates that it is very safe, the output result of (1, 0) means basically safe, the output result of (0, 1) means unsafe, and the output result of (0, 0) means very unsafe.

After obtaining the network security information, the dangerous or intruding information is detected and analyzed from the original information, then the security of the network security information system is ensured, and finally the dangerous information is processed and prevented from affecting the original information in time. Comprehensive evaluation is the key to determining whether information is safe or whether it needs to be blocked. Therefore, a comprehensive analytical model is developed specifically for research on cyber security monitoring models. The purpose of developing a comprehensive analytical model is to establish a functional relationship between data analysis and data reliability, i.e., to use data obtained from different sources to determine the influence of different factors on a particular sector and to create a business model over time.

After receiving various network security information, the relevant information can be reasonably processed in accordance with the appropriate criteria. In addition, when defining a data collection model, it is necessary to determine the appropriate collection index. The upper and lower limits for determining whether the amount of accumulated data is abnormal are the collection index. There are two general ways of compiling statistics based on statistical models: the interval confidence method and the low probability method.

3.2 *Establishment of Data Algorithm and Bayesian Network Security Evaluation Model*

Based on the formation of the Bayesian network, membership transforms into a subset of indistinct related functions according to the opportunity status of each function.

An unconditional opportunity table was designed for each node. Finally, Ge Nine software was used to detect data leaks, and a security analysis model for computer networks was developed based on the Bayesian network. The Bayesian network can effectively use real-time data and sample data to define decision-making chains for immediate response to pollution, as well as to strengthen emergency capacity. Theoretically, it is important to plan for emergencies.

The set of fundamental factors is the set of key risk factors that lead to immediate data leaks, hence the design of the node proof system in a Bayesian network structure. Basic factors include intrusion prevention, data encryption, antiviral measures, digital signatures, software security, access control, system audit, data recovery and backup, equipment security, fault

Table 1 Determination of the risk level of information leaks.

Risk level	There is a problem	Risk evaluation
Primary risk	Logical security	>100
Secondary risk	Physical security	100 to 50
Tertiary risk	Management security	<50

tolerance redundancy, line security, power supply security, network room security, and electromagnetic protection factors such as leaks. Computer network security management systems mainly include the strategy and system, facility and personnel management, risk management, and environment and resource management, including cybersecurity incident management processes, cybersecurity planning guidance strategies and programs, and follow-up actions and information on the development of management process specifications, which strengthen the process control of network security incidents.

The evaluation system is used to analyze the existing data: it obtains the answer through data analysis from the detected data feedback and evaluates the quality of the relevant processing methods. Then based on the frequency of the problem, and it is divided into different levels. The details are shown in Table 1.

Once the contingent likelihood of having a condition for every knot in the Bayesian network is obtained, it is fed as "evidence" into the Ge Nine decision software, which then calculates the risk of a security breach. This is part of the Bayesian causal inference function. In addition to the causal inference function described above, Bayesian networks offer a diagnostic inference capability. Security risk evaluation aims to identify the factors that contribute to security risks and thus to target specific preventive measures. Computer networks are open, international, and free. Attacks on computer networks come from many sources, such as physical transmission line attacks, network communication protocol attacks, computer hardware, and software vulnerability attacks. Computer network security is facing international challenges. Not only can local network users attack computer networks, but hackers in other countries can also attack computer networks through the internet. Most computer networks have no technical restrictions on users, and users can freely obtain information and publish information. Moreover, most people do not pay much attention to their own potential information problems. As a result, problems such as clicking on unknown links and causing serious information leaks and property theft often occur. The impact of information leaks on society is great.

4 Discussion

4.1 *Risk Analysis of Information Security Risks*

The risk factors of information security leaks have different aspects and include logical security, physical security, and management security. To compare the risk factors, we analyze all current known factors contributing to information leaks and determine which factors have a greater impact and their proportion of total factors based on personnel and information leaks. An example of this is given in Table 2.

Table 2 Classification criteria for hazardous substance stockpiles.

Grade	Percentage of people affected	The size of the impact
Physical security	20%	Big influence
Logical security	70%	Great influence
Management security	10%	Less influence

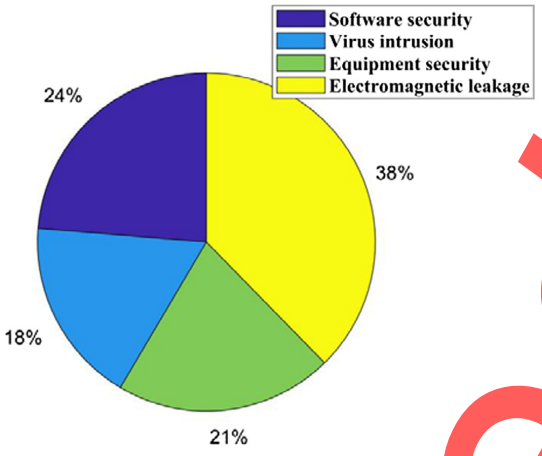

Fig. 4 Proportion of computer network security risks.

From the data in Table 2, it can be seen that, for the existing security risk factors, logical security issues are the largest part of known information security issues, accounting for 70%. In general, information leaked due to logical issues may cause more information to be leaked due to existing vulnerabilities. So current computer security networks should be upgraded for such problems, thereby reducing the occurrence of hidden information security problems.

In addition to judging the degree of information security risk from the causes of information leaks, it can also be judged by the percentage of information leaks and the impact of such leaks, including virus intrusion, software security, equipment security, and electromagnetic leaks. This has a greater impact on information security and specificity, as shown in Fig. 4.

As shown from the data in Fig. 4, direct virus intrusion accounts for only 5% of human information security issues, indicating that current computer network security is effective at preventing virus intrusion, but there is still some room for improvement. Among the risks, software security accounted for 40%, indicating that there are still certain problems in the prevention of risks to software security. This problem is also due to the addition of human factors. Some people have low security awareness and randomly install unknown software, which results in theft of information. Therefore, it is critical to strengthen not only security technology but also people's awareness of security protection.

An important item to measure risk is the accuracy and speed of processing information related to risk issues. If the computer network cannot quickly process a risk after a security problem occurs, the damage will continue to increase, and more privacy will be lost and more information will be obtained by others. The relationship between the speed of addressing processing problems and the risk of network security is directly proportional, as shown in Fig. 5.

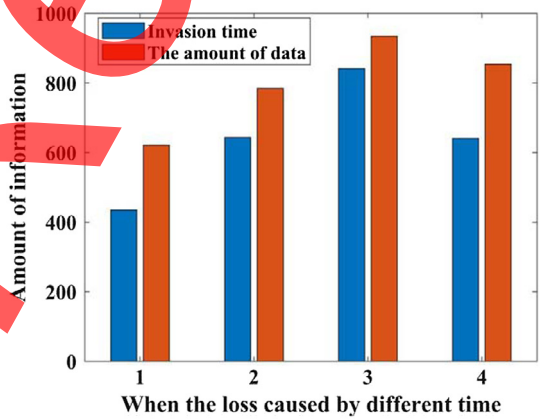

Fig. 5 Information processing speed versus information loss.

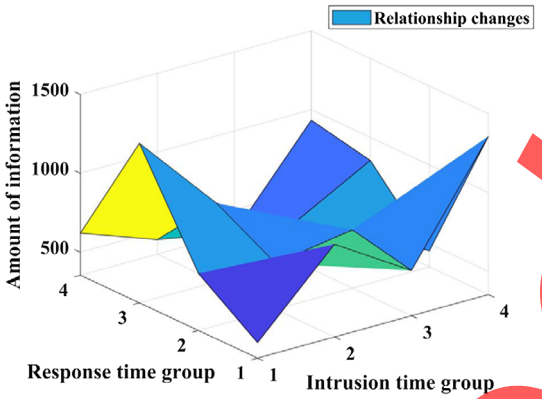

Fig. 6 Prevention of network security in advance.

After the network security is attacked, it takes a certain amount of time to steal information. It can be seen that the faster the processing speed is, the lower the network security risk is. By contrast, a slower speed will show an exponential increase in risk. From the beginning of the attack, 5 s of information loss directly became hundreds of thousands of information leaks. Therefore, faster processing speeds can deal with problems faster and thus better protect the security of a computer network.

According to pre-existing data, if there is a potential problem with network security, having related technologies to help software devices automatically enter protection mode will greatly reduce the problem of information leaks. An example is the Ali-pay payment function on TV programs; after the hacker attacked the user's device and obtained the user's information, they changed the user's payment password, but the software automatically entered a protection mode, so the hacker could not transfer the user's funds; the computer equipment stopped the loss in advance. The risk protection function and the speed of processing problems are also important for the protection of computer networks, as shown in Fig. 6.

It is shown in Fig. 6 that if the computer equipment can anticipate the risk of intrusion, when the problem occurs, it can be protected in advance; the risk can be relatively reduced by 80%, preventing the criminals from reaching the information. Neural network-based computing security has high self-learning efficiency and accuracy, which can greatly improve computer network information security.

4.2 *Analysis of Neural Network-Based Bayesian Network Computer Security Risk Evaluation Pattern*

Major drivers of data leaks come from the analysis of a Bayesian model of network risk evaluation, which can inform the methods of strengthening the security capabilities of a set of data networks. Another is the use of structured networks to combine data with hazard data to discuss security issues. Reasonable results can be used as a reference in a network incident investigation. The third is to strengthen the professional skills of technical personnel to improve network security issues, thereby promoting the development of network security. The role of the Bayesian risk assessment network is shown in Fig. 7.

Figure 7 shows that there are many reasons for computer network security risks, and if network security problems persist, the impact is even greater. Researching literature, case studies, consulting with experts, etc., we summarize the factors that influence information security issues. However, all aspects of the actual situation cannot be covered. On the other hand, instead of relying on large samples of data to calculate probabilities, combining adherent mathematics with Bayesian networks uses membership functions to calculate the probability of significant events to better represent cybersecurity issues. The computer increases this likelihood by 30% compared with standard methods, so there is more evidence for early warning, reference, and physical usefulness. This strongly confirms the validity of the Bayesian risk assessment model.

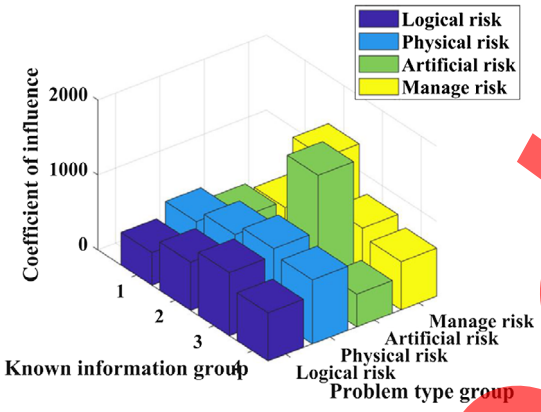

Fig. 7 Advantages of Bayesian risk assessment methods.

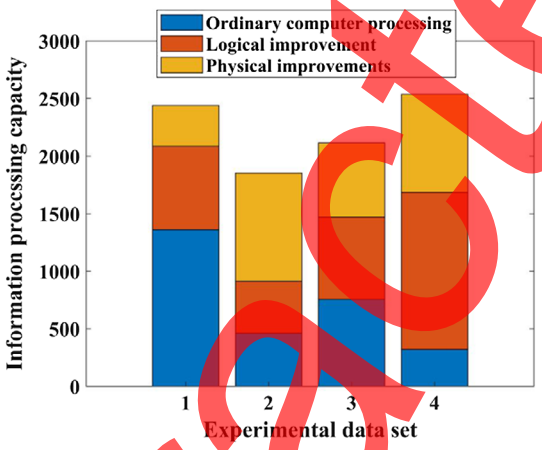

Fig. 8 Neural network improvement of the security of computer networks.

Computer networks, based on the principles of the nervous system, calculate the probability of a computer network security incident using the Bayesian method and then compare it with the probability of a normal computer network incident. The results are shown in Fig. 8.

Figure 8 shows that the use of fuzzy theory and Bayesian methods to evaluate network security risk issues to simulate computer network security problems using neural network-based computer security systems will result in higher security and autonomy. The ability to learn and anticipate risks in advance will enable more effective mitigation of computer network security problems. In terms of risk source factors, logical security has the greatest impact on computer network security; in terms of risks, physical security issues have the greatest impact on human losses.

5 Conclusions

(1) This paper assesses that, with economic development and the continuous upgrading of information technology, computer network security issues have become increasingly important and should not be underestimated. Once a network security problem occurs, people's privacy and other aspects of security will be threatened. In addition, people are now using electronic devices ubiquitously. Then, the misuse of this information by others will have a greater impact on individuals and society. Facing this increasingly important computer network security problem, the use of neural network-based computer network security methods through Bayesian method verification has become a focus of future research. Therefore, this paper uses the Bayesian method to study the problem of

computer network security, which is intended to deepen the understanding of emerging technologies and better apply it to real life.

(2) This article highlights the important role of the Bayesian risk assessment network. First, it identifies key aspects of information security issues that can provide clues to strengthening specific research on design and development of relevant capabilities. Second, it uses accuracy, speed, self-learning, and other processes of the nervous system to combine information with danger data to make inferences about the hidden dangers of computer networks. The results of the argument can be used as a reference in hazard investigations. Third, it provides references for development policies and technical issues related to network security issues and gives existing evidence of the ability of the Bayesian network to calculate emergency capacity and provide early warnings.

(3) This paper has conducted experiments on fuzzy Bayesian network security risk assessment models from the aspects of logical security, physical security, management security, and impact size. The results showed that logical security issues accounted for 70% of computer network security factors, physical security accounted for 20% of computer network security factors, and management security accounted for only 10%, but once the problem occurred, the impact would be even greater. We will focus on solving these problems based on the application of neural networks to computer network security issues in future work.

Acknowledgments

This research was supported by the National Social Science Foundation of China (Key Programs) (Grant No. 18AGL028). These no potential competing interests in our paper. All authors have seen the manuscript and approved it to submit to the journal. We confirm that the content of the manuscript has not been published or submitted for publication elsewhere.

Code, Data, and Materials Availability

This article does not cover code, data, or material availability studies. There are no codes, data, and available materials to support this study.

References

1. L. Zheng, "Research on the performance evaluation method for cold chain logistics of agriculture products based on BP neural network mode," *Open Cybern. Syst. J.* **9**(1), 2168–2172 (2015).
2. K. L. Shi, "Research on the network information security evaluation model and algorithm based on grey relational clustering analysis," *Rev. Fac. Ing.* **14**(1), 69–73 (2017).
3. J. Pang, "Research on e-commerce applications based on neural network," *J. Comput. Theor. Nanosci.* **13**(8), 5227–5230 (2016).
4. J. Gu, Y. Pan, and H. Wang, "Research on the improvement of image edge detection algorithm based on artificial neural network," *Optik* **126**(21), 2974–2978 (2015).
5. Y. P. Jiang, C. C. Cao, and X. Mei, "A quantitative risk evaluation model for network security based on body temperature," *J. Comput. Netw. Commun.* **2016**(4), 1–10 (2016).
6. Z. Xu et al., "Study on security risk assessment of power system based on BP neural network," *J. Comput. Theor. Nanosci.* **13**(8), 5277–5280 (2016).
7. Z. L. Yang et al., "RNN-Stega: linguistic steganography based on recurrent neural networks," *IEEE Trans. Inf. Forensics Security* **14**(5), 1280–1295 (2019).
8. H. Ma et al., "Integrated software fingerprinting via neural-network-based control flow obfuscation," *IEEE Trans. Inf. Forensics Security* **11**(10), 2322–2337 (2016).
9. L. X. Shuo et al., "Collaborative filtering algorithm based on improved nearest neighbors," *Comput. Eng. Appl.* **39**(1), 58–53 (2015).
10. B. Q. Xiao et al., "Design of china's financial security early warning system based on GA-ANN," *Xitong Gongcheng Lilun yu Shijian/Syst. Eng. Theor. Pract.* **35**(8), 1928–1937 (2015).

11. B. Tan et al., "Representational learning approach for power system transient stability assessment based on convolutional neural network," *J. Eng.* **2017**(13), 1847–1850 (2017).
12. L. Yang, X. Y. Geng, and X. D. Cao, "A supervisory control and data acquisition network security attack recognition method based on multi-agent," *J. Comput. Theor. Nanosci.* **13**(4), 2504–2511 (2016).
13. Y. Tang et al., "Network security situational assessment method based on improved D-S evidence theory," *J. Nanjing Univ. Sci. Technol.* **39**(4), 405–411 (2015).
14. E. Hodo et al., "Threat analysis of IoT networks using artificial neural network intrusion detection system," *Tetrahedron Lett.* **42**(39), 6865–6867 (2017).
15. J. Butts and S. Shenoi, "Critical infrastructure protection IX," *Comput. Fraud Security* **417**(4), 11–15 (2017).

Zilong Wang received his PhD from Nanjing University of Aeronautics and Astronautics in 2007. He previously did his postdoctorate at the Peking University from 2010 to 2011. His research interests include information security, cryptography, and network security protocol.

Lin Shi is a doctoral candidate and received his master's degree from the University of Electronic Science and Technology. His research interests include computational intelligence, information security, and big data analysis.

Ning Chen received his master's degree in engineering from Hohai University, China. His research interests include information collection, information security, and automatic control.

Jie Chen received his master's degree from Nanjing University, China. His research interests include computational intelligence, software design, and applications.