Computer Network Security Analysis Modeling Based on Deep Learning Algorithm

Yinxing Li1,*

1Xi’an Traffic Engineering Institute, Xi’an, Shaanxi, China, 710300

*Corresponding author e-mail: Linyinxing11@163.com

Abstract. With the continuous development of human civilization and the continuous progress of computer technology, computer network has been widely used in our life, which has brought great convenience to people's production and life. As the computer network plays an increasingly important role in daily life, the security of computer network has been paid more and more attention. Therefore, this paper studies the modeling of computer network security analysis based on deep learning algorithm. Starting from the types, levels and main problems of security needs, this paper analyzes the threats faced by the system equipment, access rights, and the main connection relationship, and makes a visual description of the network threats from the perspective of the purpose of the attack is to enhance higher permissions. The security analysis and modeling work is applied to the security fault tree method of computer system and the attack method of network information system. Through research and analysis, starting from the current state of computer network security, this paper deeply studies the analysis and modeling of computer network security, and realizes the evaluation of current computer network security. The accuracy rate of the proposed method for intrusion detection reaches 91.6%.

Keywords: Computer Technology, Deep Learning, Network Security

1. Introduction

With the continuous development of modern society and economy, the rapid development and spread of computer and computer network[1-2], computer and network have gradually become an indispensable part of people's life. The technology of computer network and communication has changed the way of people's daily production and life and people's entertainment life mode, and has improved the quality and level of people's life. However, the problem of computer and network security has been attached great importance and attention by the society. At present, the problem of computer and network security is a global social problem. Many scholars at home and abroad have
done in-depth research in the field of computer security, and carried out a detailed study and analysis of computer security strategy, security protection, security detection, data recovery, security response and other research results, the establishment of PPDRR network security model. Through PPDRR China Network Security\textsuperscript{[3\textendash}5\textsuperscript{]} network security model, we can carry out security analysis and reliability evaluation on China's computer network security and computer information system technology status, and detect whether the software management system of the computer used and the network security status information of the computer information system are safe. PPDRR China's network security model is an active risk defense network security model. It regularly checks the system information of the computers used to release the network security, actively finds the information technology vulnerabilities that may affect the computer system security, and timely takes measures to deal with the risks.

Since 2015, the research on the application of deep learning\textsuperscript{[6\textendash}8\textsuperscript{]} in Cyberspace Security has gradually risen, causing widespread concern in the academic community. At present, deep learning is mainly used in malware detection and intrusion detection. Compared with traditional machine learning, deep learning improves the detection efficiency and reduces the false alarm rate. The deep learning algorithm gets rid of the dependence on Feature Engineering, and can automatically and intelligently identify attack features\textsuperscript{[9\textendash}10\textsuperscript{]}, which helps to find potential security threats. However, at this stage, the academic community has not a comprehensive and thorough understanding of the application of deep learning in Cyberspace Security. On this basis, this paper discusses the application of deep learning in Cyberspace Security.

Based on the current situation of computer network security based on learning algorithm, this paper classifies the application of some existing deep learning algorithms in the research of computer network security, In view of the current computer network system security attack fault tree analysis method and computer network security information system network attack trend diagram analysis method, this security trend graph analysis modeling and design work is applied, the current computer system network security analysis and evaluation can be basically realized.

2. Deep Learning Algorithm Training

2.1. Calculating the Training Error of Network

Based on deep learning algorithm, this paper uses small batch training method to train the algorithm. Batch input the selected graphics into the network to propagate them forward. Finally, the output error of each pixel is obtained. Then the average value of the sum of the output errors of all pixels in the batch sample image is taken as the output error to obtain the training error. At the same time, the training error of the network is calculated by formula (1-2).

\[ P(x = k) = \frac{\exp(a_i)}{\sum \exp(a_i)} \]  \hspace{1cm} (1)

\[ L = -\frac{1}{N} \ln[P(x = k)] \]  \hspace{1cm} (2)

In the above two formulas, \( i \in (1, K - 1) \cap (1, N - 1) \), \( P(x = k) \) represents the probability that a pixel
x belongs to k category. \( a_i \) represents the eigenvalue of the i category, K represents seven image object categories, \( L \) represents the final output error value, and \( N \) represents the total number of all pixels in a batch of images.

2.2. Establishing Network Topology Model

Computer network security is the goal that enterprises and countries have been pursuing. Cultivate information technology professionals, connect various equipment, and ensure the security of information data. In the network system, the storage and transmission of information data need some special media. Through this model, the system structure is optimized, and the computer equipment is connected by point and line, which increases the difficulty of attack and ensures the network security. At present, the division of the security level of the existing computer network security analysis model is mainly because the foundation of the Department is not very reasonable, and the Department is too single and simple. In addition, the difference between the application of computers and transmission tasks is also suspected of repetition. Finally, the research on vulnerability analysis of security network in the existing models is relatively weak, and the analysis and utilization of vulnerability need to be further strengthened. In the information age, computer plays a very important role in the network and people's daily life. However, there may also be some natural factors that affect network security, such as computer network, such as the leakage, tampering and illegal dissemination of computer network information, the loopholes of computer network and malicious software, and malicious attacks by hackers. In order to effectively improve network security, it is necessary to clarify the security attributes of computer network security, this paper establishes a set of computer network security attribute research model, and actively take some measures to protect the network, reduce the occurrence of network security vulnerabilities, and ensure network security.

3. Experimental Background and Design

3.1. Experimental Background

The security attributes of computer network include security requirements, system equipment, access rights, and main connection mode and computer vulnerability. Security requirements refer to the security of computer users for their own information, which is the basic requirement for integrity and confidentiality of information; system network equipment security refers to different personal computers, and the security performance of network system infrastructure equipment and security equipment is directly related to the user's security to a large extent, whether the computer or the network management system. For example, wireless routers, switches and other network servers are the core equipment of the system. As the name implies, the management system sets the network access rights of different degrees of use as confidentiality or security, and the evaluation system reasonably evaluates, classifies and protects the access rights of the system. The advantage of the main model connecting the computer model is the first connection point between the computer and the network, Because the information transmitted from the network system to the computer is easy to cause security problems, it is necessary to test the computer model regularly and take corresponding
protective measures; the weak link of computer model refers to the major errors in system design or software programming of some computer application software. These weaknesses determine the basic technical attributes of computer and network security.

3.2. Experimental Design

In this paper, the mobile phone virus intrusion data of Siemens project is used to carry out experiments in the laboratory. Siemens project mobile phone virus data set has 40 million pieces of data, a total of 69 fields. At present, 1239, 588, 215 types of data are extracted from the data, and the data distribution is shown in Table 1. A total of 22 fields are used, including 7 continuous features, 15 category features and 2 category labels. As the input of neural network, it is necessary to preprocess the data. For continuous features, it is necessary to use the minimum maximum normalization to balance the influence of each dimension feature on the target, and the classification features need to be coded.

| Attack type | Data volume |
|-------------|-------------|
| Training data | |
| 1239 | 73329 |
| 588 | 36524 |
| 215 | 9631 |
| Test data | |
| 1239 | 29834 |
| 588 | 15864 |
| 215 | 3540 |

4. Discussion

4.1. Analysis of Computer Network Security Modeling Based on Deep Learning Algorithm

This paper realizes the construction of trestle sparse self-coding network based on tensor flow, and verifies the detection effect on the data of Siemens mobile phone virus detection project and KDDCUP99 intrusion data in our laboratory. In this paper, a four layer stack sparse self-coding network of 100-80-60-40 is implemented. The corresponding sparse factor is set to 0.2-0.2-0.2, and the perceptron neural network with the same number of layers is also implemented. The detection
effect of deep feature learning algorithm based on trestle sparse self-coding network is shown in Figure 1.

![Figure 1](image)

**Figure 1.** Detection effect of stack sparse self-coding network algorithm in Siemens virus data set

It can be seen from Figure 1 that the classification method based on nonlinear deep features based on deep learning has a better overall detection effect than the classification method based on principal component analysis in F1 value. The unsupervised and non-linear feature extraction method based on deep learning for computer network security is proposed in this paper. Compared with the DNN softmax method, the overall effect of F1 value is significantly improved. At the same time, the trestle sparse self-coding network only needs 25 pre training times and 33 micro tuning network times, while DNN softmax takes 213 iterations. This experiment shows that trestle sparse self-coding can extract deep features, and the trestle sparse self-coding network has better generalization ability because of the sparsity limitation. The trestle sparse self-coding network can converge faster by pre training and fine tuning the network.

In this paper, the proposed intrusion detection method based on trestle sparse self-coding network is applied to 15% of KDDCUP99 data sets for multi classfication, instead of extracting part of the data for training or only making binary classification prediction. The detection effect of the algorithm is shown in Figure 2.

![Figure 2](image)

**Figure 2.** The detection effect of trestle sparse self-coding network algorithm in KDDCUP99 dataset

As can be seen from Figure 2, the intrusion detection method based on stack sparse self-coding network feature extraction has better detection effect than the traditional PCA softmax and DNN
softmax. However, the detection effect of Probe, R2L, and U2R is relatively poor. As can be seen from Figure 2, the proportion of data volume between normal type and probe type, r2l type and u2r type in training data is 47.21, 84.91 and 1589.07 respectively. Through analysis, it is found that there is data imbalance between categories in KDDCUP99 data.

4.2. The Development of Computer Network Security Analysis Model

At present, computer network engineers and experts at home and abroad have made a full and in-depth study on these problems. After a lot of calculation and repeated experiments, a practical PPDRR computer network security analysis model is established. The security model analyzes the problems existing in computer information technology and network security, and discusses the security status of its information system engineering and software system through the analysis of different stages of the network. It is an active defense model, which can detect, discover and solve problems in computer network system regularly.

When installing the computer system, we should fully consider the security performance of the system, check whether the structure and function of the specific computer system and network fully meet the requirements, whether our network can effectively achieve the degree of completely preventing computer intrusion, and whether it can ensure that our network system is fully suitable for the current economic and social development and needs. The function and security of the computer should fully embody the advanced technology of computer technology and network equipment, promote the economic development, ensure political stability and avoid the situation that is difficult to solve. In the event of failure, we should accurately use the technical theory and work experience to infer the cause of failure and make improvement. The specific attributes of computer network security can more effectively formulate protection measures, analyze and detect system vulnerabilities from different angles, and protect the privacy and security of users, enterprises and countries. Security demand is the most concerned problem in the field of science and technology development and economic exchange. Without security, we cannot carry out reasonable economic transactions and hinder the development of enterprises and individuals. Security requirement is not only a single technical requirement, but also a joint embodiment of various technical levels. When breaking through the computer network security barrier, it will affect the overall security and cause protection alarm. The huge computer not only needs advanced network technology and equipment support for network and system, but also has a set of system and equipment with perfect functions on the basis of which to ensure the safety of huge computer to network system and equipment is also an important content and attribute of huge computer to network security. Any progress and development of computer technology must be inseparable from the technical support of computer equipment. The two complement each other. It can automatically search and test computer technology on specific equipment to meet the requirements of work, store relevant work data and information, and protect network information security. In the process of using computer to search and access the network, the computer will automatically save the search and access rights in the computer. According to the different network user identity information, login user account and login password information are automatically identified, the computer network search and access rights related information will also be automatically identified, to improve the processing quality and security of network data and computer information for the huge network computer. The security of huge computers to the network not only means that the data and information stored in the network are not monitored by illegal
elements, but also the control of personal and enterprise information.

5. Conclusion

This paper mainly studies the analysis and modeling of computer network security based on deep learning algorithm. In the current era background, the network used by computer has been inseparable from the production and life of the people, so the importance and guarantee of using computer for network security is more and more recognized and valued by more and more people, In this paper, in-depth study of the current status of the development of computer network security, what are the possible threats to computer network security, as far as possible to clarify the security attributes of computer network security, to establish a computer network security research model based on deep learning, in order to protect the computer network from threats and ensure network security.

References

[1] Upadhyay R K , Kumari S , Misra A K . Modeling the virus dynamics in computer network with SVEIR model and nonlinear incident rate[J]. Journal of Applied Mathematics and Computing, 2017, 54(1):485-509.

[2] Grana J , Wolpert D , Neil J , et al. A likelihood ratio anomaly detector for identifying within-perimeter computer network attacks[J]. Journal of Network and Computer Applications, 2016, 66(may):166-179.

[3] Acemoglu D , Malekian A , Ozdaglar A . Network Security and Contagion[J]. Journal of Economic Theory, 2014, 166(3):536-585.

[4] Liyanage M , Abro A B , Ylianttila M , et al. Opportunities and Challenges of Software-Defined Mobile Networks in Network Security[J]. IEEE security & privacy, 2016, 14(4):34-44.

[5] Zhou H , Wu C , Jiang M , et al. Evolving defense mechanism for future network security[J]. IEEE Communications Magazine, 2015, 53(4):45-51.

[6] Levine S , Pastor P , Krizhevsky A , et al. Learning hand-eye coordination for robotic grasping with deep learning and large-scale data collection[J]. The International journal of robotics research, 2018, 37(4-5):421-436.

[7] Lv Y , Duan Y , Kang W , et al. Traffic Flow Prediction With Big Data: A Deep Learning Approach[J]. IEEE Transactions on Intelligent Transportation Systems, 2015, 16(2):865-873.

[8] Zhou J , Troyanskaya O G . Predicting effects of noncoding variants with deep learning-based sequence model,[J]. Nature Methods, 2015, 12(10):931-934.

[9] Dovydaitis J , Jasinevicius R , Petrauskas V , et al. Training, Retraining, and Self-training Procedures for the Fuzzy Logic-Based Intellectualization of IoT&S Environments[J]. International Journal of Fuzzy Systems, 2015, 17(2):133-143.

[10] Wang G , Liu F , Pang Y , et al. Coal mine intellectualization: The core technology of high
quality development[J]. Mtan Xueba/Journal of the China Coal Society, 2019, 44(2):349-357.