Computer Network Security Analysis Modeling Based on Spatio-temporal Characteristics and Deep Learning Algorithm

Lihua Wu¹*, Tian Deng²

¹Jiangxi Vocational College of Mechanical & Electrical Technology, China, 330013
²NanChang Institute of Science and Technology, Nanchang, China, 330108

*Corresponding author e-mail: 81171962@qq.com

Abstract. With the computer network in the industry, business, politics, finance, military and other social fields in the application of more and more extensive, the society on the computer network is also more and more dependent. However, because of its wide area distribution, heterogeneity and dynamic characteristics, computer network is very vulnerable to security threats from various aspects. In order to better maintain computer network security, this paper studies computer network security analysis modeling based on space-time characteristics and deep learning algorithm. First of all, this article through to the computer network security connotation and the present situation analysis, points out the main problems of network security model, and thus build a combination of deep learning algorithm, a simulation model of network security analysis results show that the intercept network attack rate increased by 32.12% than that of the traditional model, verify the validity of the model. Through the construction of the model, it is expected to contribute to the improvement of computer network security analysis.

Keywords: Spatio-temporal Characteristics, Deep Learning Algorithm, Computer Network Security, Simulation Modeling

1. Introduction

Unknown network threats are network threat attacks that have not been discovered or documented, including denial of service, malicious code, packet sniffing, and spam. There are many insecure factors in the network, mainly from hacker attacks, software vulnerabilities and internal personnel attacks[1-2]. Hackers often attack and destroy networks through vulnerabilities. Once the network is attacked by hackers, it will have a huge impact on people in real life[3-4].
Lee Jae-Hong's aim was to develop a computer-aided detection system based on a deep convolutional neural network algorithm and to assess its potential usefulness and accuracy in the diagnosis and prediction of periodontal damage. Combined with the pre-trained deep CNN architecture and self-trained network, periapical radiography images were used to determine the optimal CNN algorithm and weight. With the increasing popularity of multi-modal data on the Internet, cross-modal retrieval of large-scale multimedia databases has become an important research topic. Hash - based cross - pattern retrieval assumes that there is a potential space for multi - pattern feature sharing. To solve these problems, Wen Qu proposed a new hashing algorithm based on deep learning. Specifically, MDLH USES a deep neural network to encode heterogeneous features into compact common representations and learns hash functions based on the common representations. The parameters of the whole model are fine-tuned in the supervision training stage. Dong Yuan proposed an age classification framework based on deep learning. This algorithm USES deep convolutional neural network to extract advanced complex age-related visual features and predict the age range of the input face. Due to the lack of age-marked face images, Dong Yuan adopted the migration learning strategy to train deep convolution. In addition, in order to describe the relationship between tags constituting ordered sequences, a new loss function was defined in the training process of age classification task.

This paper proposes a deep learning method based on convolutional neural network and cyclic neural network to automatically extract the spatiotemporal characteristics of network traffic in order to reduce the human cost. Based on this, a network security analysis model is constructed to improve the model's ability to detect emerging unknown threats.

2. Computer network security and deep learning algorithms

2.1. Computer network security

With the rapid development of computer technology and Internet, the process of global informatization is accelerating, and malicious activities against the network are also increasing. How to effectively ensure the normal operation of the network has become a very critical problem. In order to prevent malicious intrusion and damage to the network, resulting in the loss of information resources, network administrators urgently need to be able to accurately and timely understand the current situation and future security trends of the entire network, timely detect attacks and harmful behaviors, and implement emergency response. In order to develop a reasonable network security setting and resource allocation emergency strategy, to achieve the purpose of in-depth prevention and defense, it is necessary to timely evaluate the network security situation, predict the future development situation, and timely understand the network situation. The evaluation and prediction of network security situation has been paid more and more attention and become the hotspot of network security management research.

2.2. Deep learning algorithm

The successful application of deep learning in image, voice, text and other aspects has aroused the interest of researchers, who try to apply deep learning in the field of network threat detection to improve the effect of threat detection and the ability of feature learning. Many threat detection systems treat threats as exceptions and identify network threats by means of exception detection.
For the frame diagram of network structure, the internal structure of network traffic reveals its temporal and spatial characteristics. The original byte stream vector of network traffic was first transformed into a tensor with a size of N *n* channels, and then used as the input of spatial-temporal feature extraction network. Among them, channels was taken as 1, and softmax classifier used cross entropy loss:

\[
L = \sum_{(h_i, y_i) \in X} H(\text{softmax}(h_i), y_i)
\]  

(1)

The computational complexity of the model is analyzed as follows. The computational complexity of the spatio-temporal feature extraction algorithm is influenced by the characteristic dimension d of network flow data, the number n of network flow data and the network structure:

\[
c_i = f[w \cdot x_{i(r+i-1)}]
\]  

(2)

3. Design of simulation experiment

3.1. Experimental background

With the development of network information technology, the era of big data has come. Faced with the rapid increase of network information, the network threat detection system needs more effective and automated detection methods. At the same time, the network infrastructure and network topology are constantly changing, and the traditional detection methods need to adapt to the changes of network environment. Time feature and space feature are two commonly used characteristics of network traffic, while the existing network threat detection technology has a common problem, that is, with the development of network infrastructure and the change of network topology, the detection accuracy will decline.

3.2. Experimental design

SplitCap flow cutting tool was used to perform network flow cutting on MAWILab, and the detection unit of network threat detection task was obtained. For network flow, five-tuple (source IP address, destination IP address, source port, destination port, and transmission protocol) is used to fuse with log file information to obtain network traffic with labels. Finally, fixed-length network byte stream is obtained by interception and padding. In order to reduce labor cost, deep learning network is used to extract features automatically.

The evaluation indexes used in this paper are accuracy, weighted F1(weighted_F1), recall (weighted_F1) and precision (weighted_precision). Accuracy rate is the ratio of all samples accurately predicted to the total number of samples. Because the network traffic data used in this paper is of multiple categories, the threat detection is actually of multiple categories. The experimental results are shown in Table 1.

| Methods | 784 d | 1600 d |
|---------|-------|-------|

Table 1. Experimental results
| Method                        | Accuracy | Recall rate | F1 with weights | Accuracy | Recall rate | F1 with weights |
|-------------------------------|----------|-------------|-----------------|----------|-------------|-----------------|
| MLP (Multilayer Perceptron)   | 0.738    | 0.739       | 0.709           | 0.742    | 0.742       | 0.714           |
| CNN(Convolutional Network)    | 0.794    | 0.794       | 0.772           | 0.806    | 0.806       | 0.795           |
| LSTM(Long and Short Memory)   | 0.816    | 0.856       | 0.801           | 0.811    | 0.811       | 0.807           |

4. Analysis of research results

4.1. Computer network security analysis modeling based on space-time characteristics and deep learning algorithm

As shown in Figure 1, the quality of feature extraction is indirectly reflected by the quality of the task. Softmax classifier was used to classify the results of different feature extraction, and the accuracy, weighted F1 value, weighted recall rate and weighted accuracy rate were observed on data in 784 and 1600 dimensions. It can be seen that the CNN method which extracts network traffic spatial characteristics has a poor classification result, while the LSTM method which extracts network traffic temporal characteristics has an improved classification result. The classification result of this method is the best. The experimental results show that different characteristics have different effects on network traffic detection, and the spatial and temporal characteristics are better, followed by the temporal characteristics, and the spatial characteristics are worse.

![Figure 1](image_url)

**Figure 1.** Comparison of temporal and spatial feature extraction efficiency
Network attack detection methods can be divided into three types: rule-based, machine-learning and deep-learning. In common network unknown threat detection research, relevant features are firstly extracted manually, and then model training is carried out, so the detection effect depends on the quality of feature extraction of feature engineering and other technologies. In the two studies using MAWILab data set, 29 features of the MAWILab data set were artificially extracted by feature engineering and detected by deep convolutive neural network, with an accuracy of 67.86%. When the extreme value theory was used for anomaly detection, 86% true positive rate and less than 4% false positive rate were obtained for flow anomaly detection of MAWILab data set. The internal structure of network traffic reveals its time and space characteristics, which are also commonly used in network traffic detection. Aiming at the problem of feature dependence and artificial experience dependence, the spatio-temporal feature extraction method of network byte stream based on deep learning algorithm is proposed in this chapter. Compared with the previous method, the cost of artificial construction and feature extraction is saved. The experiment on 1600 dimensional data has an accuracy of 89.85%.

As shown in Figure 2, compared with the traditional computer network security analysis modeling, the computer network security analysis modeling based on deep learning algorithm is obviously superior to the traditional modeling in accuracy, recall rate and other aspects. Computer network security, including users in their process of information transmission or storage of confidentiality, integrity and effectiveness of the proposed requirements, the guarantee of the security policy is the precondition of the realization of good computer network security, the intruder procedure to damage or steal information is the process of the damage to the safety measure slightly, security policy level is low, there is no guarantee that lead to network security. Qualitative analysis and quantitative analysis can be realized through the model. Among them, the qualitative analysis is mainly used to find out the cause of privilege promotion event and all fault modes when privilege promotion event occurs. The quantitative analysis is mainly to analyze the failure efficiency of the network system against all kinds of attack events, and to solve the incidence of privilege enhancement events, so as to evaluate the security of the network system.

Figure 2. Comparison between traditional and optimized modeling
In addition, the TTP can run as a process on a particular node in the cluster, but the node scrambler machine itself must be strictly secured to the scrambler secret key. Otherwise, after the long-term key stored on the entire TTP is leaked, the scrambler secret key distributed by the entire single scrambler system itself may also be cracked by the system. In the actual scrambling secret key defense mechanism, each node in the TTP responsible for performing the task of scrambling secret key protection for single machine will first automatically obtain the scrambling secret key according to the security requirements of network protocol, and then they will run the video node assigned by Map-Reduce for scrambling. The Hadoop stand-alone scrambling system can run much faster than other traditional video stand-alone scrambling systems (all using the same scrambling algorithm in the case of the network), with an average running data of 80MB/s, and the number of nodes in the cluster is 3.

4.2. Suggestions for Computer Network Security Analysis Modeling Based on Space-time Characteristics and Deep Learning Algorithms

Security requirements related to computer networks are often aimed at the same Internet environment, and users' own data privacy can be protected. Not because the cause of the individual accident suddenly facing the risk of leakage or damage, and, in many scenarios, the demand of the network security is based on security policy as its guarantee, namely through the application of the security policy can be judged whether the main body of a computer network to another network main body whether have access permissions, or determine their level of have access rights. The network security policy of modern computer mainly covers the following several important aspects: the specific access policy of the organization itself, the specific policy of mandatory access control, the autonomous access control policy and so on.

When modeling the network access permissions to the computer user's identity authentication to access standard, the computer to access network construction as a whole can plan for the five basic levels: the first as the Root, can be referred to as "for the computer system administrator, corresponding descriptions for all permissions, which users can access network resources all at the same time, covered all system in computer network equipment, files, and process all the access control and network security. The second is SUP-user, which can be described as having access rights much lower than that of the system administrator but much higher than that of the individual ordinary users, having access rights to computer files and programs. The third is User, which corresponds to a User that can be described as an individual common operating system. At present, the application of Tcp/IP network protocol is the important foundation of modern computer access to the network, the Internet network hosts between any independent of equipment must have a difference between other host IP address, this agreement is the foundation by using ICMP network protocol to get the computer network routing, transfer time and accessibility of the target network and related information. In the model on the relationship between the computer and network link between the main body, can be in Tcp/IP protocol between computer and network security of the network connection relations can be expressed as a connected set of any two separate devices in the network environment the safety of the linkage between the connection relationship can be built into a subset of the collection of the connection.

5. Conclusion
In this paper, spatial and temporal characteristics are combined with deep learning algorithm to optimize the modeling of network security analysis. The model can be used to extract features directly from the original network traffic. There is no need to make rules manually, nor to construct new features of new unknown threats artificially, so as to reduce labor costs. It is suitable for network security detection system in the form of big data. Moreover, the simulation model of adaptive depth domain proposed in this paper has been proved by experiments to be effective in analyzing and detecting network unknown threats.

Acknowledgments

This work was supported by the Research on teaching reform of colleges and Universities in Jiangxi Province(No.JXJG-18-27-10).

References

[1] Zhang Yu . Research on the computer network security evaluation based on the DHFHCG operator with dual hesitant fuzzy information[J]. Journal of Intelligent and Fuzzy Systems, 2015, 28(1):199-204.

[2] Guo Jincheng , Fan Dan , Che Haoyuan , et al. An approach to network security evaluation of computer network information system with triangular fuzzy information[J]. Journal of Intelligent & Fuzzy Systems, 2015, 28(5):2029-2035.

[3] Fourie I . Computer Network Security and Cyber Ethics (4th ed.)[J]. Online Information Review, 2015, 39(2):271-271.

[4] Yu Ning . The Risk Evaluation Research of Computer Network Security based on Grey Clustering[J]. International Journal of Security and its Applications, 2016, 10(8):191-200.

[5] Jae-Hong L , Do-Hyung K , Seong-Nyum J , et al. Diagnosis and prediction of periodontally compromised teeth using a deep learning-based convolutional neural network algorithm[J]. Journal of Periodontal & Implant Science, 2018, 48(2):114-.

[6] Qu Wen , Wang Daling , Feng Shi , et al. A novel cross-modal hashing algorithm based on multimodal deep learning[J]. Science China Information Sciences, 2017, 60(9):092104.

[7] Dong Yuan , Liu Yinan , Lian Shiguo . Automatic age estimation based on deep learning algorithm[J]. Neurocomputing, 2016, 187(apr.26):4-10.

[8] Gao Hui , Wu Jiang , Wei Cun , et al. MADM method with Interval-valued Bipolar Uncertain Linguistic Information for Evaluating the Computer Network Security[J]. IEEE Access, 2019, PP(99):1-1.

[9] Seungwon Shin, Haopeil Wang, Guofei Gu. A First Step Toward Network Security Virtualization: From Concept To Prototype[J]. IEEE Transactions on Information Forensics & Security, 2015, 10(10):2236-2249.

[10] Catherine Pearce, Sherali Zeadally. Ancillary Impacts of Multipath TCP on Current and Future
Network Security[J]. IEEE Internet Computing, 2015, 19(5):58-65.