Network Security Monitoring Method Based on Deep Learning

Tianxi Yu 1*, Xiaoyao Yin 2, Menglin Yao 3, Tong Liu 4

1 Kunming Medical University, Kunming, Yunnan, 650000, China
2 Rose-Hulman Institute of Technology, Terre Haute, IN, 47803, US
3 University of Bristol, Bristol, BS8 1TH, England
4 University of California, Irvine, CA, 92697, US

* Corresponding author’s e-mail: 201824019@kmmu.edu.cn

Abstract: With the rise and rapid development of mobile communication, big data and artificial intelligence technology, we are entering the era of mobile Internet. With the continuous intellectualization of network security and infrastructure, information technology has been widely used in the field of industrial control, making network security more and more open, which brings a new network security control system to the traditional relatively closed industrial control system. This paper mainly introduces the network security monitoring method based on deep learning. In this paper, the network security monitoring method based on deep learning is studied, and the network security monitoring planning is designed by using image analysis, and the feasibility of detection model and deep learning is analyzed reasonably. A network security monitoring method based on deep learning is designed. Through data collection, feature extraction and neural network model training of network security power consumption information, non-invasive network security monitoring is realized. This method can detect network security information attacks that cannot be found at the network level, and improve the security performance of network security. The experimental results show that the network security monitoring method for deep learning increases the network security efficiency by 24%. The limitations of the research on network security monitoring method for deep learning and the methods and paths to provide good network security monitoring planning for image analysis application are analyzed, discussed and summarized, so as to enrich the academic research results.

1. Introduction

Based on the deep learning network security monitoring method, the network security protection strategy of network security equipment is studied, the traffic message information of network security is collected, and the information attack detection of network security equipment is realized by data cleaning, feature extraction and model training, and the network security is monitored [1-2]. Various heterogeneous data sources are standardized and integrated, and data is analyzed and processed by correlation analysis and security situation prediction technology to improve the accuracy of alarm, find potential threats in the network, and predict the network security trend in the future [3-4].

With the development of science and technology and the rapid development of Internet, the rules of classification algorithms are difficult to be given directly through programming, but they are often easily obtained by learning algorithms [5-6]. Akerkar r believes that the classification process first
needs to process the actual data into the data that the computer can understand (data preprocessing) [7]. Levy thinks that learning data has too many features, so it may need to select features, select a group of most representative from feature sets, avoid dimension disaster problems, etc. [8]. For the security protection strategy of network security, we collect the bypass information of network security equipment, and then capture the time sequence change of network security power consumption through LSTM neural network, and realize the security monitoring of network security [9-10]. However, there are errors in their experimental process, resulting in inaccurate results.

The innovation of this paper is to propose a research on the network security monitoring method based on deep learning. The research aims at the research of network security monitoring method based on deep learning, and analyzes the effective countermeasures of deep learning. In this paper, network security detection model is trained to achieve network level security protection. The method can detect the attack behavior of network security from the network level effectively. The model also has good robustness and generalization performance, and can improve the security performance of network security. This paper aims to find a new way for the development of network security monitoring system which is suitable for in-depth learning.

2. Network Security Monitoring in Depth Learning

2.1. Filtering Method in Deep Learning
Filter is proposed in this paper. This is to give weight to each one-dimensional feature of data set, and then select the features with large weight according to the weight sorting. This feature selection method is independent of the following learning algorithm. It integrates the selection of feature subset into the training of learning algorithm, and takes the performance of learning algorithm as the standard embedded feature subset: for specific learning algorithm, the feature subset with the highest accuracy is learned. The selection process of feature subset and the training process of learning algorithm are integrated to achieve the above two processes in the same optimization stage. During the training process of learning algorithm, the selection predictive model of feature subset is automatically completed: the classification results directly tell the probability model of which data belongs: the classification results tell us the probability that the data belongs to each class, it may be easy to determine which type of probability it belongs to or may be difficult to determine.

The process of establishing the detection model, that is, the training process of the model must first prepare the training set, a good training set should fully cover all intrusion modes and user use modes, which needs to be improved in use. Firstly, the association rules and frequent sequence patterns of training sets are mined by association analysis and sequence analysis. The frequent association patterns within security events are obtained by using association rules based on central features. Then, frequent sequence patterns within security events are obtained from these associations. Then, data gathering and feature selection are made by using these patterns, and feature calculation module is used. According to the constructed feature set, the security events are reprocessed and the processed results are saved in the feature library. Finally, the detection model generation module uses classification analysis and cluster analysis to learn the rules of intrusion detection automatically from the feature library, and establishes the detection model. It is an effective algorithm to monitor network security by using this function properly, which has the following forms.

\[
V \mathbf{\cdot} I = \sqrt{3} V \mathbf{\cdot} I
\] (1)

The calculation value of network security monitoring algorithm is, and the formula is as follows;

\[
3I = I + I + I = 3U \alpha \sigma C
\] (2)

The following formula shall be used for the test:

\[
I = \frac{V \cos \alpha - V \cos \gamma}{R + R - R}
\] (3)
2.2. Detection Model
The process of using the detection model is the process of real-time detection of security events by using the detection model. The detection of security events is essentially a data classification problem. According to the detection model, the detected events are divided into normal, abnormal or specific intrusion classes. According to the feature set constructed in the training process, the feature calculation module is used to calculate the features of the event, and the calculation results are given to the pattern matching module, which classifies the calculation results according to the decision rules of the detection model. For misuse detection, if it is consistent with a decision rule, it will be judged as intrusion and the corresponding type of alarm will be output; for exception detection, if the response category obtained by the decision rule is different from the actual corresponding center feature, or no matching rule can be found, it will be judged as abnormal data and the abnormal alarm will be output. Finally, the data of the feature library and the intrusion category just detected are returned to the detection model generation module. The detection model generation module learns the rules of intrusion detection again to update the detection model and ensure the real-time update of the model.

3. Detection Model Analysis of Deep Learning

3.1. Safety Monitoring System
Association analysis engine is one of the core components of security monitoring system, which consists of four components: event standardization, association engine, response management and association rule base. It is mainly to realize the centralized association analysis of IDS, firewall and system log, merge and associate a large amount of event information, analyze the events that have serious impact on the network and key systems, and analyze the key information needed in the event set management, such as attack source, attack means and affected devices.

Event Standardization: the collection terminal collects security events from various security devices, which are different and difficult to analyze. We need to unify and standardize the events to facilitate the analysis and use of the association engine in the future: we need to apply association rules to correlate the standardized events with each other or with vulnerabilities and network services. The new associated alarm events are generated and provided to the response correlation module for processing. For example, if a large number of warning events from the same source IP are received from IDS, firewall and other security devices in a certain period of time, an event that the IP address is initiating a network attack will be generated.

3.2. Detection Application in Network Security System
Response management: after the network attack event is found, according to the type and severity of the event, the responsible person of the corresponding asset needs to be informed by e-mail or SMS to deal with the security event, so as to reduce the risk. The process of data processing first collects the security event from each device, and then standardizes the security event. After compression, merging and filtering, the results are stored in the event database. Through the security event trigger, the security event is associated with the detection model (i.e. trigger event Library) to find threats or intrusions. And generate alarm information, and then take measures to release the alarm information or other ways of processing.

One of the core problems of network security monitoring application is event correlation, which is the recognition of the relationship between and among multiple events in a period of time, that is, the recognition of event pattern. In the past, this kind of identification usually depends on people's intuition and experience, or based on the analysis of attack patterns and system weaknesses by security experts, which is very time-consuming and inefficient, and not accurate enough. It is often only effective for known intrusion behavior, and can not find new intrusion. Therefore, we use data mining technology to analyze log data and automatically generate detection model to avoid manual analysis and coding detection model, which greatly improves the efficiency of pattern recognition and rule
construction. It is suitable for both anomaly detection and misuse detection, and can effectively discover known and unknown attack patterns. The specific results are shown in Table 1.

| Way of Communication | Short Message | Gsm Circuit | Gprs          |
|----------------------|---------------|-------------|---------------|
| Transmission Rate    | Full Duplex   | Full Duplex | Full Duplex   |
| Reliability          | Piece         | Connection  | Maximum       |
| Time Delay           | Large Fluctuation Range | Small | Medium |

4. Image Analysis of Deep Learning

4.1. Image Analysis Technology

With the continuous improvement of intrusion technology and the increasing amount of information of network security data, the performance of intrusion detection system can not meet our needs. With the maturity and popularization of deep learning technology, especially the excellent performance in the field of feature learning, we have found a breakthrough. In this paper, the research of deep learning for network security detection is taken as the direction of exploration, focusing on the intrusion detection algorithm based on deep learning. Using nsl-kdd data set, the traditional classification detection algorithm is analyzed and improved, and its implementation in tensorflow machine learning platform is explored.

In the pedestrian tracking subsystem, no corresponding measures are taken for the interference of similar objects, which makes it difficult for two pedestrians with similar appearance characteristics to distinguish the position of the target after the intersection, resulting in the loss of tracking. At the same time, in the case of tracking loss, no effective correction scheme is taken to let the algorithm look for the target again. Solving these problems is of great significance for more stable target tracking. In the face detection subsystem, the face detection effect is poor for the face with large scale change, especially when the face occupies less pixels, which leads to the blurring of the face. But at this time, the face can still be determined by the pedestrian's body frame, Therefore, face detection can be combined with pedestrian detection to improve the detection effect of small targets. The specific results are shown in Figure 1. Compared with the traditional network security system, the face detection system has higher accuracy in multiple detection.

![Figure 1. mental model work](image_url)
4.2. Face Recognition Analysis under Security Monitoring System
In the pedestrian recognition subsystem, the recognition accuracy is lower when the camera has a large difference in the brightness and angle of view. For the multi person parallel scene, it can not only retrieve according to the current target, but also extract the pedestrian appearance characteristics to improve the accuracy of the retrieval. Because the scale of pedestrian in the task is different in the surveillance video, the appearance feature requires high scale invariance. The algorithm proposed in this paper directly deforms the training samples with different resolutions to fixed resolution, which will cause the appearance features of the target to take place a certain process due to the specific results of time relationship as shown in Table 2.

Table 2. Statistical table of sample library

| Communication speed (MBS) | Number of processors | Processing capacity MPS | Average load rate (%) |
|---------------------------|----------------------|-------------------------|-----------------------|
| Number of Transformers    | 4                    | 515                     | 8                     |
| Total Sample              | 4                    | 377                     | 160                   |
| Training Samples          | 2                    | 380                     | 106                   |
| Validation Sample         | 2                    | 515                     | 54                    |

With the development of image analysis technology, the installation of security monitoring camera has been gradually popularized, whether in the street or in indoor public places, security monitoring plays an important role. Through the tracking of pedestrian targets, we can extract the motion features to find out whether its behavior is normal or not; we can extract the trajectory of its motion to determine whether it has retrograde, wandering in sensitive areas and other abnormal behaviors; we can count the crossing at the designated location to determine the size of the flow of people. Through the face detection function, we can count the number of faces in a certain area, so as to determine the density of the crowd, so as to timely dredge the abnormal crowd with high density; we can learn the features of the face, so as to realize the face recognition function; we can further obtain various attributes of the face, such as gender, age, expression and other features, to analyze the potential abnormal behavior. Through the pedestrian re identification function, we can find the personnel in the database in real time, so as to realize the security control and other functions. The specific results are shown in Figure 2. In many experiments, the image analysis technology generally has a higher safety factor than the camera.

![Figure 2. Questionnaire](image-url)
5. Conclusions
In this paper, although the network security monitoring method based on deep learning is still insufficient. Deep learning network security monitoring supports network access and access, which brings great challenges to the protection of network security. On the one hand, for the network security devices constituted by the operating system, the firmware vulnerability of the operating system is easy to be exploited by the attacker, and the attacker can use the network security devices as a springboard to attack the network security devices on the user side. And then through the network security equipment penetrated into the workstation and master station, so as to realize the control of other network security equipment. There are still many in-depth contents in the research of network security monitoring method based on deep learning, and there are still many steps in the research of network security monitoring method, which are not involved because of space and personal ability. In addition, the practical application effect of image analysis related experiments can only be compared with the traditional model from the theoretical and simulation level.

References
[1] Doukas D I, Chrysochos A I, Papadopoulos T A, et al. Volume Element Method for Thermal Analysis of Superconducting DC Transmission Cable[J]. IEEE Transactions on Applied Superconductivity, 2017, PP(99):1-1.
[2] Hassabis D, Kumaran D, Summerfield C, et al. Neuroscience-Inspired Artificial Intelligence[J]. Neuron, 2017, 95(2):245-258.
[3] Prasad A, Kulkarni R, Jiang S, et al. Cocaine Enhances DC to T-cell HIV-1 Transmission by Activating DC-SIGN/LARG/LSP1 Complex and Facilitating Infectious Synapse Formation[J]. Scientific Reports, 2017, 7:40648.
[4] Isuru M, Hotz M, Gooi H B, et al. Network-constrained thermal unit commitment for hybrid AC/DC transmission grids under wind power uncertainty[J]. Applied Energy, 2020, 258(Jan.15):114031.1-114031.17.
[5] Camerer C F. Artificial Intelligence and Behavioral Economics[J]. NBER Chapters, 2018, 24(18):867-71.
[6] Hassabis, Demis. Artificial Intelligence: Chess match of the century[J]. Nature, 2017, 544(7651):413-414.
[7] Akerkar R, Michel Plantié, François Troussset. Editorial. In International Journal on Artificial Intelligence Tools[J]. International Journal on Artificial Intelligence Tools, 2017, 26(02):-
[8] Levy, Frank. Computers and populism: artificial intelligence, jobs, and politics in the near term[J]. Oxford Review of Economic Policy, 2018.
[9] Dande P, Samant P. Acquaintance to Artificial Neural Networks and use of artificial intelligence as a diagnostic tool for tuberculosis: A review[J]. Tuberculosis, 2018, 108:1.
[10] Doukas D, Syrpas A, Labridis D P. Multi-Terminal DC Transmission Systems based on Superconducting Cables Feasibility Study, Modeling and Control[J]. IEEE Transactions on Applied Superconductivity, 2018:1-6.