DOI : https://doi.org/10.56452/7-3-111

ISSN: 0974-5823 Vol. 7 No. 3 March, 2022

International Journal of Mechanical Engineering

Cyberspace security protection by using Fine tuning and classification method of deep learning

Pardeep Singh

Associate Professor, Department of Computer Science, Graphic Era Hill University, Dehradun, Uttarakhand India 248002

***Abstract*:**

We can assume the attacks and defender as an opponent participant of a cyber space game, from which the attacker player is more laborious and active then another defender player which remain most of the inactive or passive. One of the important reasons that why defender player is remain passive is that it rely on the basic hard coded control mechanism. This can be once known by the attacker he or she can breach it easily. To make the defender more powerful there is a need that we mix the human brain real time intelligence with the computer, so that defender can resist all the complex attacks.

This real time human and computer intelligence can be achieved by Deep learning. This article shows hybrid incursion detection scheme which uses multi-layer depth structure for unsupervised feature learning and fine-tuning algorithm is used to transform the model to achieve the best expression of features and classification method is used to identify the incursion data.

keywords: Cyberspace security, hybrid incursion detection scheme, Deep learning, unsupervised feature learning, computer intelligence

I. INTRODUCTION

In this network era computer network security has become a major concern, railway ticket website database, passport websites, twitter, bank accounts websites, and defense websites remain on point of the attackers, to defend from the attacks such as the leakage Intrusion or incursion detection system is used. Incursion detection system (IDS) is an independent system which completes the incursion detection function, is a combination of software and hardware [5]. It can detect the incursion behavior or attempt of unauthorized objects against the system, and monitor the illegal operation of authorized objects to system resources. There are two types of detection performed by the IDS, one is anomaly detection and other is misuse detection. Misuse detection is a process of "summarizing incursion characteristics and determining attacks", and its main feature is the establishment of feature base. Anomaly detection technology is based on the user behavior characteristics and the use of system resources to determine whether there is incursion [6-8].

As networks grows, data flow also grows which leads to the complex incursion

DOI : https://doi.org/10.56452/7-3-111

behaviour. In addition, there are many problems in the traditional incursion detection system itself, which makes people urgently need a new incursion detection model to change the current situation. It makes a newbreakthrough in incursion detection. However, in fact, these methods often appear as classifiers in incursion detection systems to distinguish whether the network behavior is normal. These methods often do not play a learning role in the characteristics of attack behavior. With the diversification, complexity and huge of incursion data, incursion detection system is required to perform better in data processing and feature learning. With the rapid development of deep learning in recent years, with its unique data feature learning ability, it brings a new idea to deal with multi feature incursion data, and its successful performance in the field of image recognition and speech recognition makes us have the idea of applying itto the field of incursion detection.

II. INCURSION DETECTION SYSTEM

With the increasing complexity of the current network environment, incursion detection system has become an indispensable part of the network security system [9-10].

A. The Concept of Invasion

In a broad sense, incursion is a collection of illegal activities that attempt to destroy the confidentiality, integrity, controllability or availability of computers. From the perspective of classification, incursion includes six types: trial incursion, camouflage attack, denial of service, leakage, security control penetration and malicious use.

The combination of software and hardware for incursion detection constitutes the incursion detection system. The working principle of incursion detection is: collect information from different links and analyze the information, find the characteristics of trying to generate incursion activities, and automatically respond to the detected behavior, including cutting off the network, recording events or warnings, etc.

In order to solve the problem of the cooperation ability of different incursion detection systems this paper shows a common incursion detection framework (CIDF). CIDF is a set of specifications, which defines the standard language for IDS to express incursion detection information, which is used to express system events, analysis results and response indicators. IDS is logically divided into various task oriented components, and the communication protocol between IDS components is defined. The model is shown in Figure 1. It divides IDS into four components:

(1) Event generators (event generators);
(2) Event analyzers;
(3) Event data bases;
(4) Response units.

DOI : https://doi.org/10.56452/7-3-111

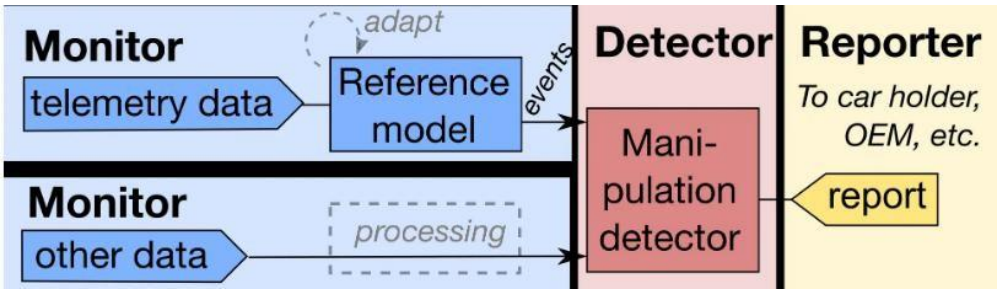

Fig.1 CIDF Model

CIDF designates the data collected and processed by IDs as events. Generally speaking, the collected data includes the traffic packets in the network, and can also be the audit log of the computer system and other information. The function of event generator is to obtain information from the whole IDS environment and provide it to other processing modules. Then, the event analyzer analyzes the data and generates the analysis results. The response unit works after the event analyzer finds the abnormal data with the sign of incursion. It can terminate the process, cut off the connection, change the attribute or just give a simple warning. Event database is responsible for storing the data obtained by event generator and event analyzer and the results of analysis.

In this model, it includes the following main functions:

(1) Monitor and analyze user and system activities:

(2) Detect system configuration and existing vulnerabilities;

(3) Statistical analysis of abnormal behavior;

(4) Identify known attacks;

(5) Evaluate the integrity of system core files or key information or important data files;

(6) Manage operating system logs to identify violations of security policies.

B. Basic Structure of Incursion Detection System

1) General Model of Incursion Detection

General incursion detection framework (CIDF) is proposed by DARPA. As mentioned above, its main work includes four parts: IDS architecture, communication mechanism, description language and application programming interface (APD). At present, most IDS devices are based on the general model of CIDF. According to this model, IDS devices from different manufacturers can cooperate with each other through corresponding communication protocols.

2) Denning Model of Incursion Detection

Denning model is the earliest model, which is independent of the specific system and input. It is an abstract model, which provides a reference for most use models. The model consists of six modules: subject, object, audit record, activity profile, exception record and activity rule. The model has the idea of rule-based, some existing activities may lead to rule learning, and add new rules, but its biggest defect is the lack of the current incursion detection most needed vulnerability information and attack methods and other knowledge. Figure 2 is a schematic diagram of Denning model.

DOI : https://doi.org/10.56452/7-3-111

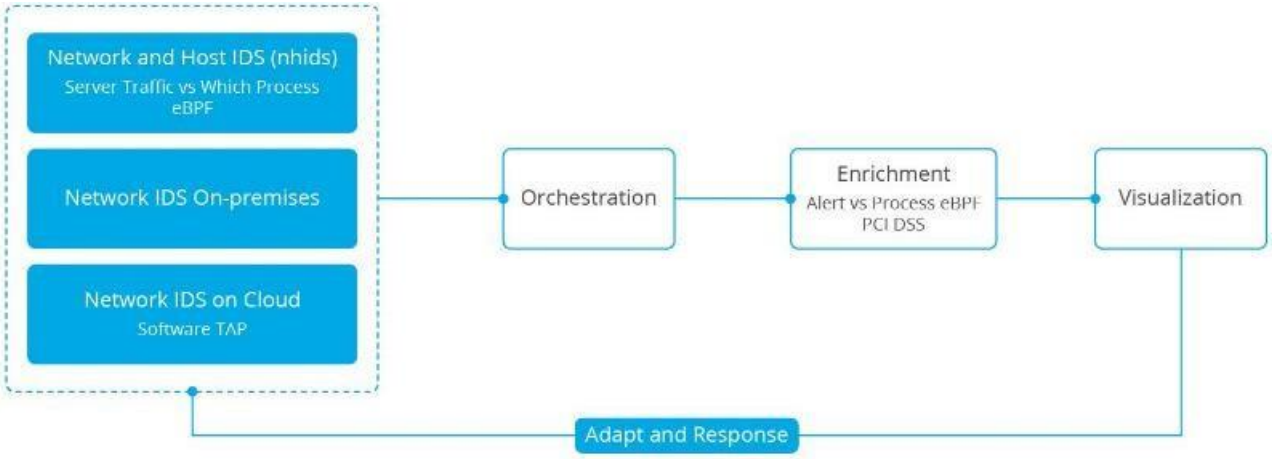

Fig.2 Denning Model of Incursion Detection

C. Classification and Detection Methods of Incursion Detection Technology

Through the analysis of IDS, we can know that the first step of incursion detection is to collect data from different nodes of the network system with incursion behavior, and then send these data to the incursion analysis engine for processing. The task of incursion analysis is to rely on various incursion detection and analysis technologies and methods to find traces of incursion from a large number of data. IDS detection and analysis technology is mainly divided into two categories: anomaly detection and misuse detection.

Here is a brief introduction to misuse detection and exception detection:

(1) Misuse detection

A variety of misuse detection techniques, also known as “geometry based attack detection” are used to detect misuse characteristics. By using these features for feature matching or rule matching, if the matching behavior is generated, it indicates that an attack has occurred. The main problem to be solved in misuse detection is how to write all possible attack feature libraries and feature libraries different from normal behavior. Table 1 lists the main advantages and disadvantages of misuse detection.

Table I Characteristics of Misuse Detection

Advantage	Shortcoming
High detection rate	It is difficult to build feature library
Low false positive rate	Unable to detect unknown attacks

(2) Anomaly detection

Anomaly detection technology is also known as behavior-based detection, it is based on the user's behavior and the use of system resources to determine whether there is an incursion behavior. Anomaly detection assumes that all incursion activities are abnormal to the activities of normal agents. According to this theory, if there is a behavior rule base of normal activities for the system, then the behavior of the agent can be used to judge whether it deviates from the normal activities of the system, so as to identify the incursion

DOI : https://doi.org/10.56452/7-3-111

behavior. The key of this detection method is how to define a “normal” state. At the same time, anomaly detection can only identify those behaviors that are different from normal activities, and cannot know the specific incursion situation. Table 2 shows the advantages and disadvantages of anomaly detection.

Table II Characteristics of Anomaly Detection

Advantage	Shortcoming
No prior knowledge of security defects	Higher false positive frequency
Easily detect new attacks	Low efficiency in dynamic environment

III. Deep Learning

A. Common Models of Deep Learning

1) Compiler

Automatic encoder is a typical unsupervised feature learning algorithm, which makes full use of the characteristics of artificial neural network (ANN). To some extent, the research of artificial neural network is inspired by biology. It is composed of a series of simple units which are densely connected with each other, forming a hierarchical network system. In such a network system, given its input I, the weights of the network structure are obtained through the adjustment training of the multi-layer network and the adjustment of its parameters, and the final output O is obtained. If it is adjusted several times, I and O are the same or the error is minimized. Naturally, many different feature representations of input I are obtained (each layer represents a representation). Through experimental research, it is found that the new and optimal feature data learned from the original data can greatly improve the error of the model, improve the prediction accuracy of the model, and even have more outstanding effect than the current classification algorithm in classification problems.

Automatic encoder is a kind of multi-layer forward neural network, which can reduce the dimension of high-dimensional data by transforming the specific feature vector into abstract feature vector to get the low dimensional feature vector. Its working principle is shown in Figure 3. Since the self-coding network is an unsupervised learning method, its whole structure is composed of encoder and decoder. The encoding process is used to reduce the dimension of data, the decoding process is used to reconstruct the data, and the process can be regarded as the reverse process of encoding.

DOI : https://doi.org/10.56452/7-3-111

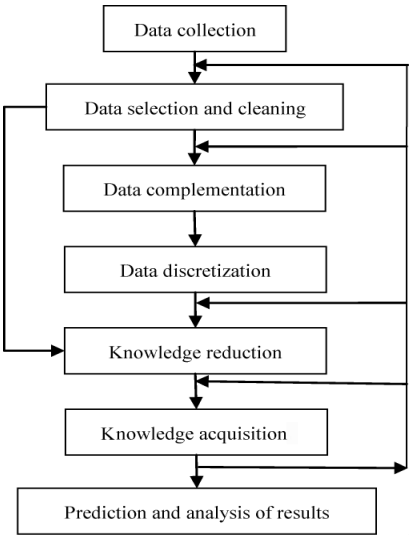

Fig.3 The Principle of Self Coding Network

2) Convolutional Neural Network

Convolutional neurons are simple elements and complex elements (called simple elements and complex elements respectively, namely s elements and C elements). The surface polymerized by S-element is S-element, and the layer polymerized by S-element is S-layer. The same relationship exists among C-element, C-element and C-layer. The network structure is shown in Figure 4:

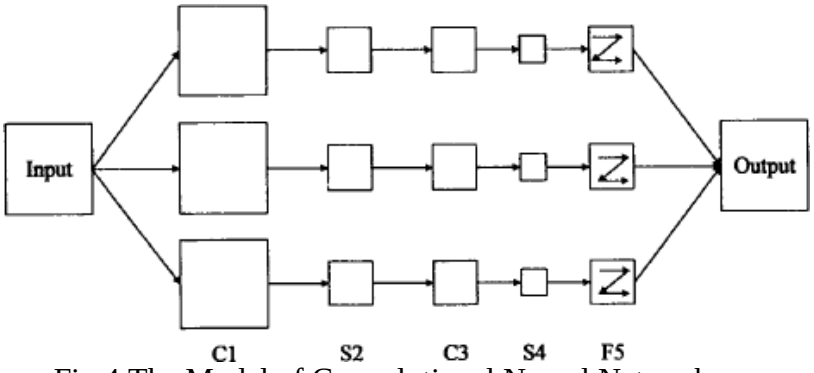

Fig.4 The Model of Convolutional Neural Network

B. Bp Neural Network

BP neural network is a kind of one-way propagation multi-layer feedforward network, which adopts the back propagation algorithm. BP network includes input layer, hidden layer and output layer. Figure 5 is one of its models.

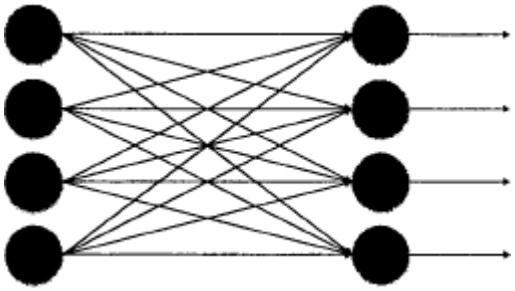

Fig.5 Bp Neural Network Model

DOI : https://doi.org/10.56452/7-3-111

The theory of neural network has been proved that as long as the number of hidden layer nodes is enough, the single layer BP neural network can approximate any nonlinear function of finite discontinuity with any precision. At the same time, the more the number of hidden layers, the more links of error transmission, and the lower the performance of the network. Therefore, according to the experimental results, BP neural network usually adopts three-layer structure.

The realization process of BP algorithm is as follows:

Input: the training sample is v_i, (i = 1,2,. , m);

Output: fine tuned model parameter θ= {W, b, c};

(1) For each training sample v_i

(2) Calculate the actual output v_i of the output node

(3) The error gradient between the actual output and the ideal output (v_i) of the output node is calculated

$$\delta_k = v_i(1-v_i)(v_i - v_i') \quad (1)$$

(4) The error gradient of hidden layer element h is calculated

$$\delta_h = v_h(1-v_h)\theta_{hk}\delta_k \quad (2)$$

Here, θ_{hk} is the connection weight of hidden layer unit h to the next layer node k, and δ_k is the output of node k calculated according to the excitation function.

(5) Calculation weight update

$$\theta_{ij} = \theta_{ij} + \Delta\theta_{ij}$$

$$\Delta\theta_{ij} = \eta O_i \delta_j \quad (3)$$

In the implementation process of BP algorithm, η is the learning rate, and the optimal value of learning rate is determined by many experiments. O_i is the output of node i, O_j is the output of node j, and δ_j is the recursive error gradient of node j. Then, the weights obtained from the input of all training data sets are updated, and the new weights are calculated according to the updated weights. Until the output error (expressed by variance) reaches the minimum value, that is:

$$E = \sum \left| \sum \left(d_{sz} - O_{sz} \right) \right|^2 \square \ \varepsilon \quad (4)$$

DOI : https://doi.org/10.56452/7-3-111

$s \setminus z \quad)$

Here s is the training sample sequence, Z is the output node sequence, d_{sz} is the ideal output of sample s at node Z, O_{sz} is the actual output of sample s at node Z.

IV. INCURSION DETECTION BASED ON DEPTH STRUCTURE

A. From Shallow Structure to Deep Structure

Research shows that deep network structure has stronger function expression ability than shallow network structure. For a simple network, nodes can be added in the following two ways (as shown in Figure 6). The first way is to increase horizontally to a certain level of the network to make the network more "fat"; the second way is to expand the network vertically to make it stack into a more hierarchical network and finally form a "deep" structure. Relatively speaking, in the case of adding the same number of nodes to the network, the second way is more compact and less cumbersome than the first way, and its function expression ability is also better than the first way. The key point is that the expression of the second depth structure is similar to the structure of human cerebral cortex processing information, which abstracts from the bottom layer to the top layer to achieve feature extraction.

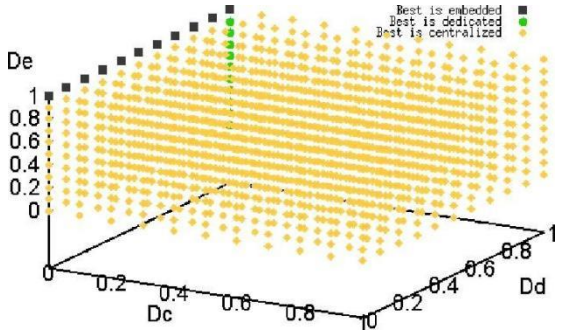

Fig.6 Transformation of Network Structure

In the process of incursion, the generation of attacks is often hierarchical, including a variety of basic attributes and means, which constitute a rich way of attack. It is the level by level expression of depth structure that makes it possible to extract and filter incursion data when dealing with a large number of incursion detection data, which is of great help to the detection performance of incursion detection system.

B. Hybrid Incursion Detection Model Based on Depth Structure

According to the diversity and complexity of the current incursion data set, and the more real-time and adaptive of incursion detection system. Combined with the excellent performance of deep learning technology in feature expression, this paper proposes a general model of Hybrid Incursion Detection System Based on deep structure. In this model, the incursion detection system is divided into three modules: data acquisition and processing module, feature learning module, incursion recognition and classification module.

(1) Data acquisition and processing module

This module is mainly used to collect incursion information. According to the needs of the latter model, the preprocessing of feature data may include the following parts: data filtering, normalization, normalization and so on. Among them, the purpose of data filtering

is to reduce the amount of data directly processed by the incursion detection system, remove some redundant information, and reduce the impact on the later model training; the purpose of standardization is to unify the data from multiple IDS sources or digitize the data format. Through standardized processing, all data will form “standardized“ data, which is partial to processing; normalization is to limit the data to be processed within a certain range, which not only brings convenience for later data processing, but also ensures the convergence of later model generation.

(2) Feature learning module

This module mainly extracts the features of the collected data by feature dimension reduction. By reducing the amount of data noise, the later incursion recognition performance is more stable. This module can use feature dimension reduction method to extract and select features. After this step of feature extraction and selection, incursion detection system will have higher incursion recognition rate.

(3) Incursion identification and classification module

Through the use of machine learning methods (Bayesian, support vector machine, etc.) for incursion data classification and recognition.

C. Comparison of Feature Learning Experiments Based on Depth Structure

In order to compare and analyze the feature learning performance of several deep learning methods mentioned above, this paper uses three depth structures of automatic encoder, CNN and DBN to do feature learning comparative experiments on NSL-KDD data set. During the experiment, we use two feature learning methods:

The first is to use the traditional shallow network learning application mode, that is, to use shallow structure to train the original input data and use Softmax to classify it. Specifically, CNN directly uses the training set for supervised training, and then tests the test set samples. On the other hand, DBN conducts several unsupervised pre-training of RBM, then adds a classification output layer to form DBN structure, and makes the trained RBM parameters as the initial weights of the whole network, then uses supervised BP algorithm to fine-tune the whole network, and finally uses the adjusted DBN to classify the test set. The process of SAE is similar to that of DBN. These processes have no obvious feature extraction, and feature extraction and classification become a whole.

The second is to use deep structure for feature learning. The training method is the same as the first one. After the training is completed, we remove the last layer of the network and use the front structure as the feature extractor. Then, the features of training samples and test samples are extracted respectively, and the dimension of features is the number of nodes in the last layer of the network. At last, the popular softmax and linear SVM are used for classification experiments. The comparison of this partof experiments is listed in Table 3.

DOI : https://doi.org/10.56452/7-3-111

Table III Experimental Results of Feature Comparison

Method	Structure	Recognition rate	
		Mode 1 (Softmax)	Mode 2 (SVM)
SAE	122-50-5	86.32%	87.36%
	122-100-80-50-25-5	90.97%	91.25%
CNN	1-4C-2S-4C-2S-5	87.14%	87.26%
	1-6C-2S-12C-2S-5	91.37%	91.42%
DBN	122-50-5	89.16%	90.25%
	122-100-80-50-25-5	93.69%	93.81%

The experimental results show that in the aspect of structure selection, the deep structure feature learning has better advantages than the traditional shallow learning method. No matter what kind of classification method is used, the deep structure has more advantages than the shallow structure in the classification recognition rate.

V. CONCLUSION

After completing this basic research work, this paper focuses on the comprehensive analysis and design of the hybrid incursion detection model based on depth structure, and uses this method to solve specific incursion detection problems. The traditional method of feature learning and the method of depth structure are deeply studied, and this method is applied to incursion detection, and a hybrid incursion detection model based on depth structure is proposed. With reference to the proposed hybrid incursion detection model, the deep structure feature learning under this model is compared experimentally, and it is concluded that DBN method has good feature learning advantages in incursion data, which paves the way for the following specific work.

REFERENCES

[1] Wei Yonglian, Yi Feng, Feng Dengguo, Yong W, Yifeng L. Network Security Situation Assessment Model Based on Information Fusion. Computer Research and Development, 2009, 46 (3): 353-362

[2] Xu Guoguang, Li Tao, Wang Yifeng. A Network Security Real-time Risk Detection Method Based on Artificial Immune. Computer Engineering, 2005,31 (12): 945-949

[3] Jiang Wei, Fang Binxing, Tian Zhihong. Network Security Evaluation and Optimal Active Defense Based on Attack Defense Game Model. Acta Computer Sinica, 2009, 32 (004): 817-827

[4] Miao Yongqing. Stochastic Model Method and Evaluation Technology of Network Security. China Science and Technology Investment, 2017, 4: 314

[5] Bao Xiuguo, Hu Mingzeng, Zhang Hongli. Two Quantitative Analysis Methods for Survivability of Network Security Management Systems. Acta Communication Sinica, 2004, 25 (9): 34-41

[6] Epistemological View: Data Ethics, Privacy Trust on Digital Platform, Harsh, R., Acharya, G., Chaudhary, S., 2018 IEEE International Conference on System, Computation, Automation and Networking, ICSCA 2018, 2018, 8541166

[7] Enhance the Data Security in Cloud Computing by Text Steganography, Sanghi, A., Chaudhary, S., Dave, M., Lecture Notes in Networks and Systemsthis link is disabled, 2018, 18, pp. 241–248

[8] Li Weiming, Lei Jie, Dong Jing. an Optimized Real-time Network Security Risk Quantification Method. Acta Computa Sinica, 2009 (04): 793-804.