DOI : https://doi.org/10.56452/7-3-105

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

International Journal of Mechanical Engineering

Deep Neural Network Model Exploration and Utilization in Computer Network Incursion Detection

Abhishek Sharma

Asst. Professor, Department of Comp. Sc. & Info. Tech., Graphic Era Hill University, Dehradun, Uttarakhand India 248002

Abstract:

We reached in the era where we are now discussing about 6G in speed of internet speed of broadband and also the network topologies evolution is continuously speeding, and as the internet features and complexity grows incursion also grows and become more difficult to find out, and detection of this intrusion is pretty more and more heterogeneous. Due to this super big data flow and multiple algorithms and data paths used for incursion, it's being difficult to select the approach to be used for the detection of the incursion. One of the previous approaches for incursion detection is feature processing, which works on the feature extraction feature, but not too good in performance. Now a days people using Deep learning approaches which is performing well in incursion detection and also have great learning ability characteristic. We also have to enhance our incursion detection approaches according to that. In this research we use the deep neural network to train the data and we show improvement in accuracy of classification and recognition & also enhance the rate of incursion detection and also compare the data with conventional neural network.

Keywords: *Performance, Incursion detection, Deep learning, neural network.*

---

1. INTRODUCTION

India has been connected to the Internet for more than 20 years as first it was launched on 1986, for public access it is available from 1995 and the scale of the Internet market in India has augmented swiftly in recent years. Through the annual summary report of NIC, we can learn that by the end of 2015, the total number of websites had reached eight million, increased by 10%. The scale of the Internet users and the mobile phone users are increasing at a high speed, in 2022 it is reaching to 467 million social media users and 1.10 billion mobile users respectively [1]. The popularity rate of India's Internet has reached 58%. However, the

DOI : https://doi.org/10.56452/7-3-105

swift growth of info has also brought many network security problems. At the end of 2014, the 62189- booking official network was attacked by suspected hit the library, which led to the disclosure of personal information of more than 130 thousand users, and in year 2023, approx. 324620 incursion attacks are there. The incursion is around us, and our personal information may be stolen by invading attack initiators at any time [1-3]. There are a lot of problems in the traditional incursion detection system itself, which makes people urgently need a new incursion detection model to change the current situation. With a new force suddenly rises of deep learning in recent years, with its unique data feature learning ability, it brings new ideas to the processing of multi-feature incursion data. And its successful performance in the field of image recognition and speech recognition gives us the idea of applying it to the field of incursion detection.

2. STUDY FOUNDED ON INCURSION DETECTION AND DEEPLEARNING

2.1 Technical Features of Incursion Detection

In the existing security system, incursion detection system is responsible for intercepting network information in the system, analyzing and auditing information, and taking corresponding response measures to protect the system. Incursion detection system can be saidto be a collection of incursion detection hardware and software. Figure 1 shows the role of the incursion detection system. Nowadays, incursion detection scheme has been recognized by the security experts as the second security gates after the firewall. Incursion detection system can deal with the internal and external attacks in real time without disturbing the usual process of the system and protect the system in real time.

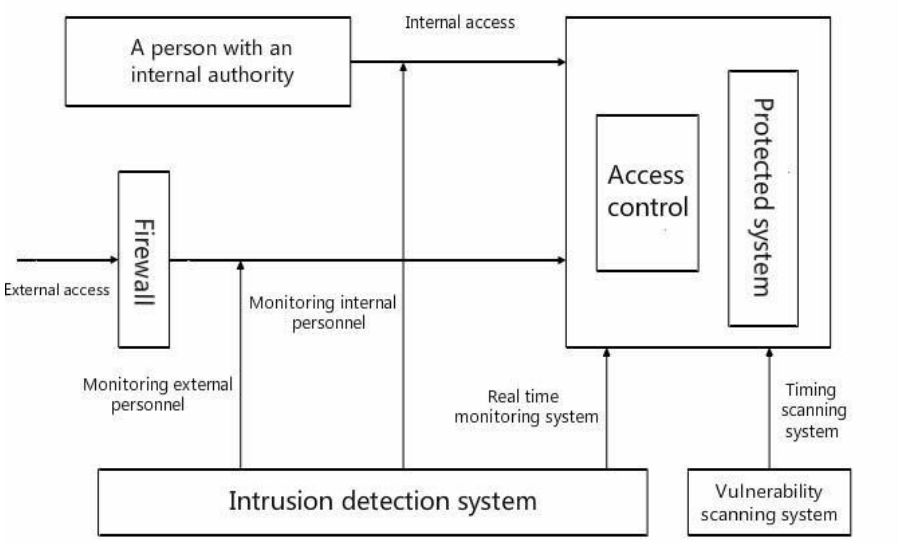

Fig 1: The role of incursion detection system

2.2 Exploration more on Deep Learning

Deep learning is the subdivision of Machine learning and AI. The essence of deeplearning

DOI : https://doi.org/10.56452/7-3-105

is to take analyses multiple datasets by building more hidden layer machine learning models and using alot of training data, get more useful data features, and ultimately achieve efficient classification accuracy. The purpose of deep learning is to establish and simulate the neural network of human brain to analysis data and process data, and to conduct data processing by imitating the operation mechanism of human brain. In deep learning, all feature data share the same network structure. This way is more conducive to extract deep layer feature and enhance the memory ability of network. The structure diagram of deep learning, as shown in Figure 2, the basic idea of deep learning: Each layer of network uses unsupervised method to carry on the characteristic learning; On the basis of the last training, each layer was trained with the method of unsupervised learning and the training result was taken as input to the next level.

Finally, the whole network is fine-tuned with supervised training, so that the input and output of the model are as similar as possible.

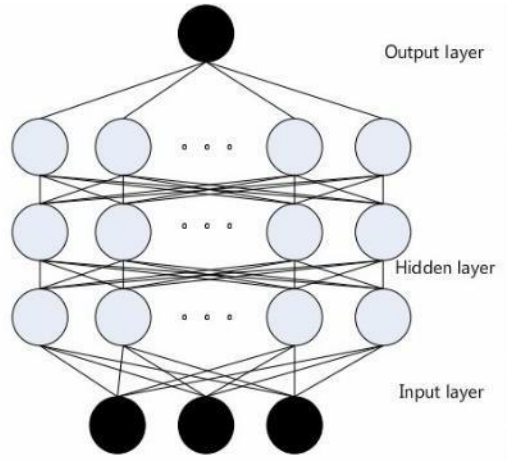

Fig 2: The structure diagram of deep learning

3. FORMATION OF SCIENTIFIC PROTOTYPICAL OF DEEP NEURAL NETWORK

Deep learning is mainly applied to audiovisual, pictures, linguistic processing system and so on, andthere is a very few research on the application of deep learning in incursion detection. In this article we are proposing an incursion detection module constructed by using deep confidence network, the whole module includes network detector module, data preprocessing module,DBN anomaly detection module, detection response module and others module. The specific module flow chart is shown in Fig 3.

3.1 Network Detection and Data Preprocessing

The basic component module of the network detector incursion detection system, the function of this module is to collect and intercept all flow information in the network. It inputs the captured information into the data preprocessing module for data preprocessing. Because the current network detector can be divided into two kinds: setting up router port listening and

DOI : https://doi.org/10.56452/7-3-105

Ethernet network monitoring. Because there is fiber or DDN special line to access networks, data monitoring cannot be effectively applied by Ethernet network broadcast characteristics, so the network detector uses router port and router monitor. In this model, data preprocessing module needs to process network information captured by network detectors, local storage network data and local new incursion data information. The function of data preprocessing is to process the original data through data processing to form effective data that can be input to the DBN module. Because the range of input data of DBN processing module is [0,1], and normalized data can effectively avoid the situation of low classification accuracy due to the large difference in data.

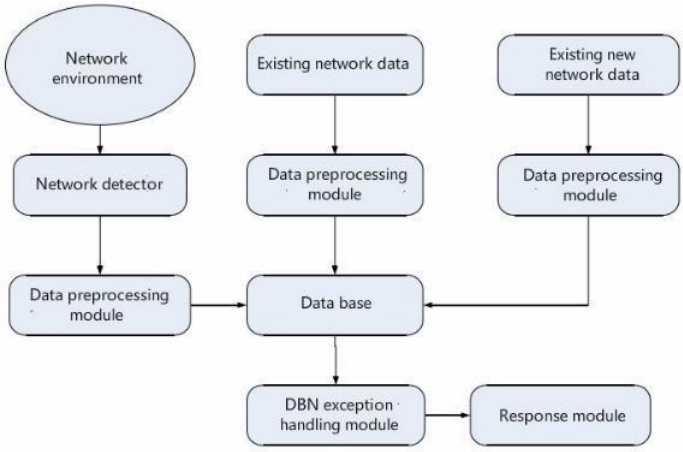

Fig 3: Incursion detection module based on deep confidence network

3.2 DBN Exception Handling Module

The DBN processing module is mainly carrying on an unsupervised learning of the preprocessed data in the data preprocessing module. It is the processing and abstraction of high dimensional data. The DBN module is divided into two steps in the training model. Training each layer of RBM network respectively, its characteristics are unsupervised and independent, and it ensures that when feature vectors are mapped to different feature spaces, the feature information is preserved as far as possible. The last layer of DBN is set up as a BP neural network. Taking the eigenvector of the upper RBM as an input vector to supervised train entity classifier and because the RBM of each layer is trained in the first step, it can only ensure that its own weight is mapped to the best of the feature vector of the layer. Our ultimate goal is to optimize the corresponding feature vectors for the overall weight value. According to the characteristics of BP neural network, BP neural network can propagate the error information from top to bottom to RBM of each layer, so as to fine tune the whole DBN network and achieve the global optimum.

3.3 Evaluation Criteria of Mathematical Model

In this paper, the incursion detection model based on the deep confidence network is mainly intended to achieve high data recognition rate, it can identify the new type of incursion data and the time that the model takes time to process the data. Therefore, the standard of the model is

DOI : https://doi.org/10.56452/7-3-105

the response time of the model, the total correct rate of data classification, and the accuracy rate of the new type of incursion data to correctly identify the classification.

Correct recognition rate of data:

$$T_{sum} = \frac{T_n + T_t}{Sum} \quad (1)$$

Among them, T_{sum}represents the correct rate of classification, $T_n$represents the correct identification number of$normal$type data, represents the correct identification number of intrusive data types, andSumrepresents the total number of test data sets.

(2) The correct recognition rate of new incursion data:

$$T_{new} = \frac{T_{nt}}{SumN} \quad (2)$$

Among them, T_{new} represents the correct recognition rate of new incursion data. T_{nt} represents the number of correct identifying new incursion detection data, and $SumN$represents the total amount of new incursion data tested.

4. APPLICATION OF DEEP NEURAL NETWORK IN COMPUTER NETWORK INCURSION DETECTION

4.1 Preprocessing of Experimental Data

The data set used in this paper is the KDDCUP 99 -10% data set and the KDDCUP99-Correct dataset. This data set has the problem of large data volume, inconsistent format and complex features. Professor Stolfo first used the data method to process the data set. The new dataset obtained was used in the KDD CUP competition held in 1999, thus forming the KDDCUP99 data set. Now, this data set is a detection data set in the field of network incursion detection. In this research mainly uses 10% data of the KDD99 data set, in the KDDCUP99 10% data set, and the number of network connection types.

Deep learning approach uses numerical data sets, so we have to preprocess the KDDCUP99 data. To process the character data set we uses mapping methods viz; TCP one-dimensional data is mapped to (1,0,0) 3D data, and the UDP is mapped to (0,1,0) 3D data, and ICMP is mapped to (0,0,1) 3D data. By analogy, 66 service types are mapped to multidimensional data based on this method. Through this data mapping method, the 41 - dimensional original data in the 10% KDDCUP 99 data is mapped to 118- dimensional feature data. The extreme value method is used for data normalization.

4.2 Experimental Simulation and Result Analysis

For simulation of this research and exploration MATLAB R2014a 32-bit (win 32) is used. And we examine to verify whether the model can be used effectively in incursion detection. MATLAB can omit a lot of data structure code, and it is more timeliness in the processing of experimental data. This article uses 3 layers of RBM and one layer of BP neural networks. The BP neural network plays the function of parameter tuning and classification. Because there are more than 490 thousand sets of 10% data sets in KDDCUP99. In order to improve the execution efficiency of MATLAB, and the data set screened Normal and Dos type data from the original

DOI : https://doi.org/10.56452/7-3-105

data set, and their number accounted for a very large proportion of the original dataset. Therefore, this experiment randomly selected 7477 Normal data, 3346 DOS types and 2000 Probe types. Because the data size of R2L and U2R type are small, the deep confidence network requires a large number of data sets for training.So, this article analyses all the R2L and U2R type data of the 10% data set in KDD CUP, and randomly extracts the attack data of U2R type in the KDDCUP99 data set and adds it to the experimental data set.

At random, 70% of the data collected in the experimental data was selected as the experimental training set, and the remaining 30% was used as the experimental test set. So the experimental training set has 9,800 data, and the experimental test set has 4201 data. In this article, to construct the DBN a three-layer RBM network is used. The number of characteristics of RBM is 118-40-15-5, and the number of iterations of BP neural network is 10. The impact ofthe number of BP iterations on the accuracy rate of the classification is discussed.

We can see clearly that when we set the number of iterations of restricted Boltzmann machine to 200 times, with the increase of BP iteration times, the accuracy of classification showed a steady growth trend. When the number of BP iterations is set to 75 times, the accuracy of classification has been stabilized, and the accuracy of classification has been stabilized at about 99.54%. At this point, if the number of iterations of the neural network is increased, the accuracy of classification will not be improved, instead, it will increase the running time of the program.

When new types of incursion data appear, the incursion detection method based on the deep confidence network can still effectively identify and classify the new type of attack type. The recognition rate of R2L is only 35.26%, and the reason is that the data sample of the training set R2L is too little, which leads to the deep confidence network cannot automatically identify the specific impact characteristics of this type. Therefore, the data recognition of R2L in the above table is low, but the recognition rate of the other three types of new type of incursion data has reached a high level. Therefore, the incursion detection method based on the deep confidence network can also identify the new data.

5. CONCLUSION

This research takes the current development status of incursion detection as the main line. First,a comprehensive introduction and analysis of incursion detection system is made, and the basic concept, basic structure, classification and detection methods of incursion detection are introduced in detail. At the same time, the deep learning of one of the main contents of this paper is expounded in a comprehensive way, which makes a paving for the research of the deep structure. A computer network incursion detection based on deep confidence network is proposed, and the effectiveness of incursion detection is verified by experiments. Therefore, the incursion detection model based on deep neural network has important research significance.

DOI : https://doi.org/10.56452/7-3-105

REFERENCES

1. Y. Zhang, P. Li and X. Wang, "Intrusion Detection for IoT Based on Improved Genetic Algorithm and Deep Belief Network," in IEEE Access, vol. 7, pp. 31711-31722, 2019, doi: 10.1109/ACCESS.2019.2903723.
2. 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
3. Wenlei Shi, Lei Xu, Dongli Peng, "Application of Deep Learning in Financial Management Evaluation", Scientific Programming, vol. 2021, 2021. https://doi.org/10.1155/2021/2475885
4. 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
5. Lei Lei, Wei Chen, Bing Wu, Chao Chen, Wei Liu, A building energy consumption prediction model based on rough set theory and deep learning algorithms, Energy and Buildings, Volume 240,2021,110886, ISSN 0378-7788, https://doi.org/10.1016/j.enbuild.2021.110886.