Universe Scientific Publishing

ORIGINAL ARTICLE

A Review of Intrusion Detection Technology Based on Deep Reinforcement Learning

Juquan Yu*, Rui Zhou, Ziming Wang, Zixing Wang

Beijing Institute of Technology, Beijing 100081, China. E-mail: yujuquan9936@yeah.net

Abstract: With the rapid development of modern science and technology, all kinds of network attacks are updated constantly. Therefore, the traditional network security defense mechanism needs to be further improved. Through extensive investigation, this paper presents the latest work of network intrusion detection technology based on deep learning. Firstly, this paper introduces the related concepts of network intrusion detection technology. On this basis, we further evaluate the performance of three common deep learning models in intrusion detection, and conclude that DBN algorithm has some strong advantages. Afterwards, it also puts forward several improvement strategies of intrusion detection models.

Keywords: Deep Learning; Intrusion Detection; Feature Selection

1. Introduction

Intrusion Detection System (IDS) is the core of network security. IDS can be divided into misuse detection and anomaly detection according to the strategies they adopt. Misuse intrusion detection depends on existing pattern database[1]. It analyzes the known attack behaviors, establishes corresponding attack signature database, and then directly detects the attack signatures that have been covered in the pattern database. Anomaly detection firstly constructs the normal behavior description of computer system or network connection, and then judges whether the intrusion occurs by analyzing the deviation degree between the detected behavior description and the normal behavior description.

At present, misuse detection has been well-developed and has achieved large-scale application. However, as misuse detection is merely based on the statistics of known attack signatures and responses to attack data, its main limitation is that it can only detect known intrusion but cannot detect unknown intrusion.

Anomaly detection focuses on abnormal site behaviors that deviate from normal website behaviors. Obviously, anomaly detection is not as good as misuse detection for detecting known attacks. However, since anomaly intrusion detection can detect abnormal behaviors via analysis of network traffic, it has an enormous advantage in detecting some specific attacks such as encryption attack and 0day attack. Based on its unlimited development and application prospects, anomaly intrusion detection has been widely studied.

2. Feature selection and extraction

doi: 10.18686/esta.v7i4.164

The primary task of anomaly intrusion detection is to extract the flow-level behavior characteristics of network traffic from the original network data and analyze them. These features can be analyzed in four aspects.

2.1 Classic features

Many characteristics related to statistics can be extracted for use. For example, the average packet length, the number of bytes per data stream, etc. The effectiveness of classic features for data traffic classification has been verified in many researches. For instance, in one research conducted by Mr. Mohamad and his team, a hybrid deep learning model is proposed. By using CNN to extract meaningful statistical features from IDS's big data, the reliability of classic features in intrusion detection is proved as well.

2.2 Data-content features

Data-content features are obtained from specific load fields of data packages. Packets are transmitted in network in the form of binary bitstreams. The storage of grayscale image or RGB image is also realized in the form of binary bitstreams. Based on the similarity between data packets and images, it is natural to transform network flow packets into images for processing. The method of combining images which contain the features of data packets with CNN permits researchers to instruct the computer to automatically learn from training data and form models of different network traffic. In order to find the characteristics of the traffic, Zhang, *et al*.[2] map the original hexadecimal code to decimal numbers. Then they classify the data stream through the improved hierarchical network model. Experiments in two different training data sets show that the model can achieve 99.9% accurate classification rate.

2.3 Temporal features

Temporal features include the arrival interval of data packets or the continuous transmission direction of data packets. The temporal characteristics that can reflect the relationship among flows have been widely used in many kinds of network environments, and have been verified in various data sets. Sliding window method is a typical method to extract temporal characteristics, but the traditional sliding window does not consider the window span time, or the complexity of the runtime algorithm. An improvement of the current mainstream data flow algorithm is the decay window model[3]. This method of the decay window technology uses the structure of an improved tree to maintain and update the summary of the data-flow regularly. It can be verified that the algorithm can achieve better clustering quality, smaller memory cost and higher data processing ability.

2.4 Protocol features

The protocol features contain the hidden structural information about network traffic, which can be used to detect attacks that focus on protocol vulnerabilities. A large number of fields of normal network protocol can be learned by the IDS so as to obtain the transferring relationship of protocol states, and then analyze abnormal behaviors.

3. Tasks of intrusion detection

The basic requirement of intrusion detection is to classify different network attacks. In addition, intrusion detection based on deep learning should provide support for encryption attack and 0day attack detection.

3.1 Attack classification

Attack classification requires not only to distinguish normal traffic and abnormal traffic, but also to identify the attack types of abnormal traffic. In the field of network attack detection, compared with traditional features-extraction algorithms, deep learning has a better features-extraction effect. For example, the use of unsupervised deep learning automatic encoder model for training[4] not only eliminates the influence of human factors in traditional features-extraction, but also preserves the classified information of features as much as possible. Via this method, the detection of unknown network attacks would be more accurate.

3.2 Detection of encryption attacks

In the traditional handshake phase of encryption protocol, both sides of communication often need to negotiate the encryption requirements in plaintext. By acquiring the data related to the encryption in the handshake phase, we can predict the nature of the packets. In addition, we can analyze the behavior mode of encrypted traffic by using the length of data packets, or the time interval and order of message transmission, so as to establish the normal traffic model of encrypted data. On

this basis, if we further study the content of encrypted traffic, we can achieve high-precision intrusion detection rate of encrypted traffic. Through the way of deep learning, we can extract all kinds of behavior characteristics of encrypted traffic, which can help us to realize the recognition and classification of encrypted traffic. Wang Wei[5] proposed an end-to-end encrypted traffic detection scheme based on CNN, so as to solve the problem of traditional machine learning-based intrusion detection methods which require manual extraction of data features. This method based on deep learning technology can achieve automatic extraction of flow characteristics and type recognition. It has proved that this method can greatly improve the accuracy and efficiency of data extraction compared with traditional methods.

3.3 Detection of 0day vulnerabilities

"0Day" attack, refers to the security vulnerability that is used maliciously by hackers immediately after it is found. Although the traditional misuse detection has a high accuracy for the detection of known attacks, it has no power to parry the new security vulnerability of 0Day attacks. However, the method based on anomaly detection can detect the 0Day attack or the variation of known attack. For example, Mr. Nerella *et al*.[6] have used the manifold alignment method of TL to transform the source domain and the target domain into a common potential space, which can avoid the problem caused by different characteristic spaces and different marginal probability distributions between domains. In the transformed space, a method of generating target soft tags is proposed by using clustering program to compensate for the lack of target instances, so as to improve the effect of 0Day attack detection.

4. Comparison of deep learning models

4.1 Comparison test of AE, CNN and DBN

In order to reflect the feature learning performance of different models, this part will carry out feature learning experiments on the NSL-KDD data set. In the experiments, two kinds of feature learning methods were used[6].

The traditional application mode of shallow network learning was used. Specifically, CNN conducted supervised training; DBN trained multiple RBM layer by layer without supervision, and then fined the weights of the whole network through the supervised BP algorithm; the process of SAE is similar to that of DBN. All three models trained the original input data through shallow structure.

Feature learning was carried out through depth structure. The learning and training methods are the same as the first method above, but after the training, the last layer of the network needs to be removed. Moreover, the feature extractor is made through the front structure, so that the training samples and test samples are separately extracted.

Both DBN and SAE adopted shallow 122-50-5 and deep 122-100-80-50-25-5 structures; CNN adopted 1-4c-2s-4c-2s-5 and 1-6c-2s-12c-2s-5 structures, with the convolution template set as 5×5.

The Experimental Results of Feature Comparison

Method	Structure	Recognition rate	
		(softmax)	(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%

Figure 1. The experimental results are as follows.

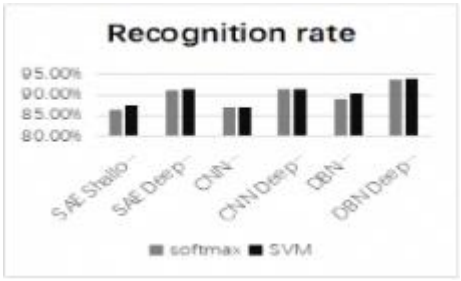

Figure 2. The histogram of feature comparison.

It can be seen that no matter what kind of deep learning models and classification methods were adopted, the effect of feature learning with deep structure is better than the traditional shallow network learning. It can be seen from the above charts that when SVM classification and SoftMax are adopted, the accuracy of SAE, CNN and DBN is higher than that of shallow-learning. Comparing the three learning models, we can conclude that DBN model has a greater advantage in recognition than SAE and CNN model.

4.2 Comparison of DBN and other feature-based learning methods (PCA)

The above experiments have confirmed the effect of DBN. In order to improve the accuracy of intrusion detection more intuitively, we displayed the comparison of DBN and PCA in the data set of NSL-KDD. Firstly, we reduced feature dimensionality by using DBN and PCA, and then SVM classification method is used to analyze and recognize the dimensionality of the reduced data. During the training, 20, 30, 40 and 70 percentage of the training data were used for the experiments.

Comparation of DBN and Other Feature method

Training data	PCA	DBN
20%	73.65%	91.57%
30%	72.91%	91.82%
40%	73.51%	92.93%
70%	73.82%	92.42%

Figure 3. Comparison of DBN and other methods.

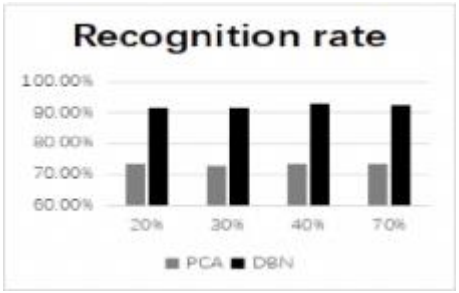

Figure 4. The histogram of DBN and PCA.

As it can be seen from the above charts, DBN has an overwhelming advantage over traditional feature learning methods in all data stages. At 70% of training data, DBN is 18.6% higher than PCA, which shows that DBN is more adaptable to feature extraction in high-dimensional space.

5. Model improvement of intrusion detection

Although CNN and AE do not perform as well as DBN, both models still have the potential for significant improvement. Here we introduce two improvements of them.

5.1 Improvement of CNN

The core of CNN is convolutional kernel, which

makes CNN better at processing image data. Hence, we introduce an improved scheme of convolutional expansion, combining it with auto-encoder. The training process is divided into three stages. In the first stage, the model is transformed into a number vector by a session-based data preprocessing module, which we use as the image book of the pre-training. In the second stage, the extended convolutional auto-encoder learns important hierarchical feature representation from a large number of unlabeled training samples. The reason for using the extended convolutional auto-encoder is that it can achieve greater processing power under the same computing power. At the same time, because the activation function of the extended convolutional auto-encoder is ReLU, there is no gradient vanishing problem. After the construction of full connection layer, SoftMax classifier for extracting features and classifying is introduced. In the last stage, the backward-propagation algorithm and a few of labeled samples are used to further optimize the features learned from the unsupervised pre-training process, so as to optimize the model parameters. There is no pooling layer in this model, which avoids the information loss caused by pooling operation.

5.2 Improvement of SAE: SDA

The second improvement scheme is called stack noise reduction auto-encoder (SAE). We first need to preprocess the data. The network session can well reflect the association among network packets, which determines that data preprocessing module here is session-based. The data preprocessing in this part will extract a small number of basic features in the head of the network packet and the load of the network application layer. The above two items together constitute the data set, which is taken as a training sample of stacked denoising auto-encoder (SDA). The training of trestle noise reduction auto-encoder model can be divided into two stages: the first stage is a layer-by-layer unsupervised training stage where input is the unlabeled data set. Then the models are trained layer by layer greedily. In more detail, the first noise reduction auto-encoder completes the training by minimizing the input and output reconstruction errors. Then the next encoder uses its last encoder's outcomes as its own input. Multiple noise reduction auto-encoders are stacked into multi-layer neural network to extract the feature mark of data. The second stage is a supervised fine-tuning stage. The main structure is SoftMax classifier, which classifies the data with features description that is acquired from the hidden layer. The whole neural network is trained as a multi-layer perceptron. Each layer is the same noise reduction auto-encoder. All parameters are optimized by verifying the data with tags, and the early shutdown system is used to avoid over-fitting.

6. Conclusion

This paper mainly focuses on the development of intrusion detection system. At the beginning, we systematically introduced the development of IDS and some related researches of it. After that, we put forward some suggestions for improving the two models. All in all, intrusion detection has become a popular research subject in the field of network security nowadays. We strongly believe that with the clear research direction, the gradual improvement of theoretical structure, the optimization of learning model and the intrusion detection system based on deep learning will continue to develop and progress.

References

1. Ju H, Lee D, Hwang J, *et al*. PUMAD: PU metric learning for anomaly detection. Information Sciences 2020; 523: 167–183.
2. Zhang Y, Chen X, Jin L, *et al*. Network intrusion detection: Based on deep hierarchical network and original flow. IEEE Access 2019; (7): 37004–37016.
3. Wang D. Density-based data stream ing based on damped window model. Bulletin of Science and Technology 2013; (6): 40–43, 46.
4. Sameera N, Shashi M. Deep transductive transfer learning framework for zero-day attack detection. ICT Express 2020; 6(4): 361–367.
5. Wang W. Deep learning for network traffic classification and anomaly detection [PhD thesis]. Hefei: University of Science and Technology of China; 2018.
6. Yang K. Intrusion detection based on deep learning (in Chinese) [master's thesis]. Beijing: Beijing Jiaotong University; 2015.