ISSN: 2688-8645

DDoS Attack Target Detection based on AM+BPNN

Jing Chen*

Guangdong University of Science & Technology, Dongguan, China

Abstract

The computer has developed from a single machine to a multi-machine network. The development of the network has penetrated into people's life, and similarly, the problem of network security has also followed. Distributed Denial of Service (DDoS) attack is one of the most popular network attacks at present. How to effectively detect DDoS attack targets and take urgent protective measures has become one of the difficulties in the research community. In this paper, a method of detecting DDoS attacks by using CNN neural network with attention mechanism (AM) is proposed by using the characteristics of a large amount of data in DDoS attacks. The technology used in this method is relatively mature, the implementation is simple, the cost is low, and it has certain practical significance.

Keywords

DDoS Attack Detection; CNN; AM.

1. Introduction

Distributed denial of service attack is one of the current mainstream network attacks, because it can forge the source IP address. Therefore, with the advent of the era of big data, target attack detection is an important problem in the field of network security and other scientific research. At present, deep learning has become a familiar term, and its application fields are also quite extensive. Target attack detection based on deep learning and artificial intelligence has also become a research trend. Research in various fields has also achieved certain results, such as the identification and detection of attack sources in DoS attacks [1]. The two prominent features of concealment and distribution make it difficult to detect and trace the source, which brings unpredictable losses to many companies. Research on the detection of DDoS attacks has become an urgent problem to be solved. Convolutional neural networks [2-4] have achieved remarkable results in object detection. CNN-based methods can be roughly divided into two types, one-stage algorithm: represented by YOLO[3], SDD[2]; two-stage algorithm. Both algorithms are limited by the size of the target area in the attack route image.

Reference [5] proposes a target detection method based on improved Faster R-CNN. What it improves is the utilization of feature map information to achieve better accuracy. However, this paper does not consider the condition of real-time response time. Reference [6] designed a feature block based on multi-scale receptive field to enhance the receptive field of the network and improve the detection accuracy. However, the model has poor practicability due to the deep network layer and too many training parameters. Reference [7] proposed to use the secondary fusion structure to shorten the relative path between feature levels, and use the multi-branch fusion module to make up for the lack of upper and lower semantics, so as to improve the detection accuracy. However, the real-time performance of detection is not considered.

In literature [8-10], the current detection of DDoS attacks is mainly based on statistical detection methods and artificial intelligence-based detection methods. Statistics-based detection mainly uses statistical methods to analyze the characteristics of DDoS attacks and then detect them. The detection based on artificial intelligence mainly includes detection based on classification algorithm, clustering algorithm and deep learning algorithm. The classification

ISSN: 2688-8645

algorithm uses SVM to detect the three flooding attacks of TCP, UDP and ICMP; there is also a KNN algorithm based on the modular distribution to detect attacks. The clustering algorithm uses the traditional K-means to add the army to enhance the detection effect; there are also detection methods based on the improved AP clustering algorithm. Deep learning algorithms use CNN and RNN models for detection; there are also attack detection methods based on BP neural network. This paper proposes a method of detecting DDoS attacks using a convolutional neural network with an attention mechanism. Using the feature that a large amount of request data will arrive at the victim within a period of time during a DDoS attack, it can quickly detect whether the host or server is attacked. A DDoS attack was carried out, so that an emergency response can be made to reduce the unwarranted losses caused by the DDoS attack.

1.1. DDoS Attacks

A denial of service (DoS) attack refers to the use of network protocol flaws or direct brute-force means to exhaust the victim's resources. The purpose is to make the target host or network unable to provide normal services, stop responding or crash. It is not an attack on the target host or related equipment. With the development of the network, a distributed denial of service (DDoS) attack is a simultaneous attack by multiple attackers in different locations to one or more target hosts. Because the attack is launched from different locations, it is called a distributed denial of service attack. The following figure is the principle of DDoS attack, as shown in Figure 1.

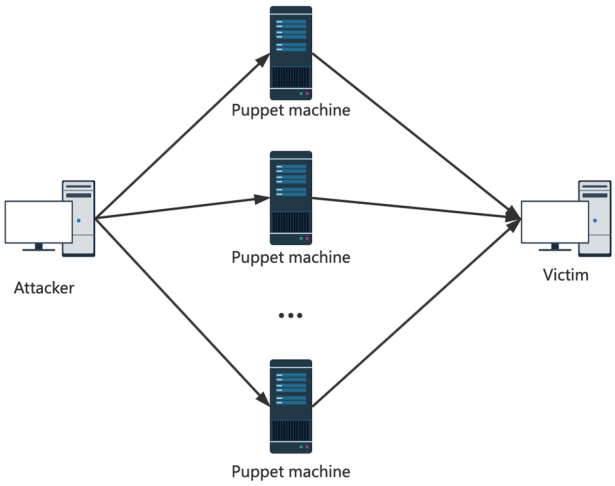

Figure 1. DDoS attack principle

As can be seen in Figure 1, the attacker forged IP addresses and attacked the victim from different locations, thereby hiding his real address, achieving the purpose of concealed attacks and evading tracking.

1.2. CNN

Convolutional Neural Network (CNN) is a multi-layer supervised learning neural network, which contains convolutional layers, downsampling layers and fully connected layers. Among them, the fully connected layer can be thought of as our reverse neural network (BPNN).

1.3. Attention Mechanism

In the learning process of the neural network, different weights will be given to different features, then. The attention mechanism is to change the weight of the original features with the same weight, that is, to attach great importance to certain features, which can accelerate

ISSN: 2688-8645

the convergence of faster related models and achieve better results, so that the final learning effect is better. optimization.

1.4. Status of DDoS Attack Detection

At present, the detection of DDoS attacks is mainly based on statistical detection methods and artificial intelligence-based detection methods. Statistics-based detection mainly uses statistical methods to analyze the characteristics of DDoS attacks and then detect them. The detection based on artificial intelligence mainly includes detection based on classification algorithm, clustering algorithm and deep learning algorithm. The classification algorithm uses SVM to detect the three flooding attacks of TCP, UDP, and ICMP; there are also KNN-based algorithms that use modular distribution to detect attacks. The clustering algorithm is improved by the traditional K-means to enhance the detection effect; there are also detection methods based on the improved AP clustering algorithm. Deep learning algorithms use CNN and RNN models for detection; there are also attack detection methods based on BP neural network.

2. DDoS Attack Detection by AM+CNN

DDoS attacks generally forge fake IP addresses, and use the fake IP addresses to send a large number of data packets to the attacked target, so as to achieve the resource of the target host or exhaust the network bandwidth resources. Then we can use the feature of the arrival of a large number of irregular data packets within the same time interval to determine whether a DDoS attack has occurred. Figure 3 is a schematic diagram of an improved CNN with an attention mechanism added. It is divided into three major modules, namely data preprocessing, feature selection and CNN detection learning.

2.1. Data Preprocessing

Due to redundant or invalid data in the data, data filtering needs to be performed on the originally acquired data. In the process of network transmission, there will be invalid data packets or data packets with lost information, which will have a certain impact on the accuracy of our DDoS attack detection. Therefore, before learning the neural network, it is necessary to filter out the originally obtained dirty data packets according to certain rules, leaving data useful for detection.

2.2. Feature Selection

In the filtered data, information such as the transmission timestamp of the data packet, the protocol representation in the data set, the source port number, and the serial number of the client can be obtained by extracting the header information of the data packet. In the research of this paper, according to certain feature selection rules, the required features are retained and the useless features are removed. Since this study mainly focuses on the number of packets arriving at the attacked end within a certain time interval, we mainly focus on the transmission timestamp of the packets.

2.3. Image Generation

The filtered data and calculation rules are used to calculate the correlation strength between events, and an event table is established. Using the event table and the correlation strength, a strength matrix is obtained, and then the matrix is converted into an strength map.

2.4. Detection Learning

Because this paper takes the transmission timestamp of the data packet as the point that needs to be paid attention to, in the CNN that introduces the attention mechanism, the timestamp is taken as the key feature to see if there are a large number of data packets coming at the same

ISSN: 2688-8645

time, in order to achieve the correct The resource of the target host is exhausted, so more weight is assigned to it. The intensity map is fed into a CNN for learning. In the process of learning, if the detection effect is not good, the threshold can be adjusted and re-learned, so as to optimize the effect.

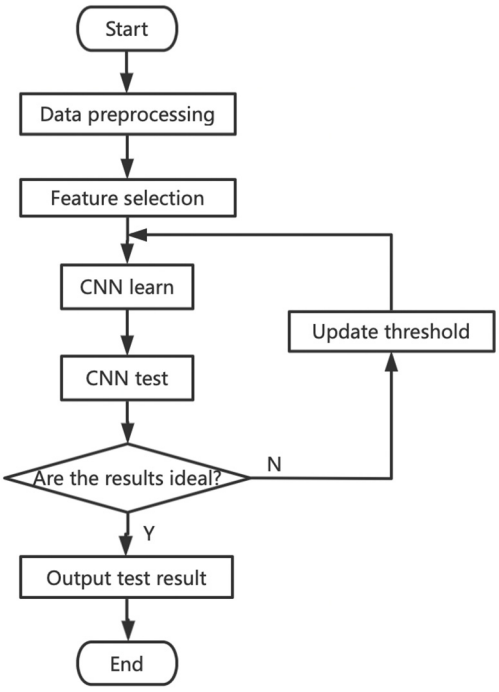

Figure 2. DDoS attack detection by AM+CNN

3. Conclusion

This paper proposes a DDoS attack detection method based on the attention mechanism of convolutional neural network, which focuses on considering whether a large number of data requests reach the attacker in a period of time. However, if a user requests a large amount of data, this method will have a certain false alarm rate, so it is necessary to consider which feature should be weighted to improve the detection accuracy.

Acknowledgments

This work was supported by Natural Science Project of Guangdong University of Science and Technology (GKY-2021KYQNK-6 & GKY-2021KYYBK-24).

References

[1] Jin Wang, Yi Guohong, Hong Hanyu, Chen Siyuan. Real-time vehicle detection based on convolutional neural network [J]. Computer Engineering and Applications, 2021,57(05):222-228. (in Chinese).

[2] Shaoqing Ren, Kaiming He, Ross Girshick, and Jian Sun.Faster R-CNN: Towards real- time object detection with regionproposal net- works. In NIPS, 2015.

[3] Wei Liu, Dragomir Anguelov, Dumitru Erhan, ChristianSzegedy, Scott Reed, Cheng -Yang Fu, and Alexander CBerg. SSD: Single shotmultibox detector. In ECCV, 2016.

[4] J. Redmon, S. Divvala, R. Girshick, and A. Farhadi. Youonly look once: Unified, real - time object detection. arXivpreprint arXiv:1506.02640 v4, 2015.

ISSN: 2688-8645

[5] Guo Xingang, Zhang Peidong, Liang Jinming, Wang Shuai. Improved Faster R-CNN target detection method [J]. Journal of Changchun University of Technology, 2020, v.41;No.170(05):64-70. (in Chinese).

[6] Liu Xiangyu, Yang Chaoyu. Target detection algorithm of multi-branch convolution block [J]. Journal of Chifeng University (Natural Science Edition), 2020, 36(10): 17-22. (in Chinese).

[7] Pan Qiuyu, Wang Wei, Wang Mingming, Wang Daoshun. Target detection method based on convolutional feature modeling [J]. Computer Application Research, 2021, 38(03): 928-931. (in Chinese).

[8] Zeng Xiaojie. DDOS attack detection based on neural network [J]. Electronic Technology and Software Engineering, 2018(8): 200-200. (in Chinese).

[9] Zhang Jinglong. Overview of DDOS attack detection methods [J]. Science and Technology Economics Tribune, 2020, v.28;No.710(12):23-24. (in Chinese).

[10] Tang Kunjian. DDoS attack detection method based on load prediction [J]. Network Security Technology and Application, 2018, No.205(01):14-15. (in Chinese).