DDoS Attack Detection Method under Deep Learning in the Context of SDN-OpenFlow

CURRENT STATUS: UNDER REVIEW

EURASIP Journal on Wireless Communications and Networking

Gang Ke
Dongguan Polytechnic
ekang95@126.comCorresponding Author

Ruey-Shun Chen
Dongguan Polytechnic

Y.C. Chen
University of California Davis

Naixue Xiong
Tianjin University

Yuan Tian
Nanjing Institute of Technology

Najla Al-Nabhan
King Saud University

DOI: 10.21203/rs.3.rs-20700/v1

SUBJECT AREAS
Systems Biology Artificial Intelligence and Machine Learning

KEYWORDS
DDoS attack detection, SDN-OpenFlow, Deep learning, Network security
Abstract

This paper is to study the DDoS attack detection method based on deep learning (DL) under SDN-OpenFlow, to contribute to network security. This paper applies DL to DDoS attack detection to expect excellent research results. The DDoS problem of this study belongs to the binary classification problem. Therefore, the content of this research is carried out by judging whether the characteristic data of the OpenFlow flow table is normal or not. Under normal circumstances, this kind of binary classification problem uses the probability value between 0 and 1 to express its tendency result. Therefore, after comprehensive consideration, this paper chooses to use the back-propagation neural network (BPNN) as the neural network structure of the model. Regarding the small-scale data, the performance of this method is more general. However, in the case of large-scale data, the detection accuracy, false alarm rate (FAR), and testing time of this method are all excellent. Compared with other attack detection methods, the one proposed by this paper has certain advantages in various aspects. The DL-based DDoS attack detection method can effectively detect attack status, providing an important theoretical basis for the study of attack detection.

1. Introduction

With the information industry expanding and the information technology developing, the Internet has become an indispensable part of people's lives. However, during the development of the Internet, the requirements for network equipment have become higher\(^1\text{-}^3\). It is difficult for traditional network equipment to meet the current real demands. Therefore, major equipment manufacturers have begun to add other protocols or functions to make up for the new problems and needs that have arisen. However, this approach increases the complexity of network equipment. The current operation and maintenance of network equipment are difficult. With the increase in Internet traffic, these problems will continue to deteriorate\(^4\text{-}^5\). Software-Defined Network (SDN) is a network architecture that separates the data layer from the traffic layer of the network. Its core protocol is OpenFlow. This new type of network architecture can increase the utilization of network resources through centralized control\(^6\). SDN can effectively solve the resource load problems faced by major equipment manufacturers and improve the performance of load balancing. However, because of its flexibility,
SDN is more vulnerable to distributed denial of service (DDoS) attacks. DDoS attacks make the network equipment unsustainable due to excessive traffic by creating attack traffic, which causes the system to malfunction. At present, the frequency of DDoS attack events is getting higher, and the attack traffic generated is also increasing. Thus, the problem of network security is serious at present. Therefore, this paper studies the DDoS attack detection method under SDN-OpenFlow architecture. DDoS attacks can only be prevented if they are detected. Research on DDoS attack detection is a main concern of scholars worldwide.

Abidoye et al. (2017) studied DDoS attacks received by wireless sensor networks and proposed a message analyzer solution for wireless sensors. It can detect damaged sensors that are vulnerable to DDoS attacks, and all leaked messages sent by the attacker to the base station through the sender node. The method was compared with other related protocols, which showed the effectiveness of the method. Kim (2019) used basic neural networks as well as long-term and short-term recursive neural network methods to study DDoS attacks, extracting values that represent attack characteristics from the data set. Two methods were used to perform preprocessing to study the impact of learning previous traffic on sequential traffic analysis and the impact of learning one data set on applying to another. Also, whether the algorithm can be used for recent attack traffic was determined. The experimental results showed that the pre-processing method used, the neural network architecture and hyperparameters, as well as the optimizer, were suitable for DDoS attack detection. Simpson (2018) conducted research on increasing DDoS attack intensity. This article introduced an interaction mode between vulnerable peripheral services and indirectly related autonomous systems, enabling autonomous systems to arrange local filtering under the remote-service control with assurance. Also, a performance evaluation was proposed, showing that the mechanism was feasible in the emerging trend of operators' willingness to improve the hardware's programmability through SDN technology and to reduce the attack on downstream customers. In addition, it was analyzed to prove that the conscious attack on the mechanism did not cause the autonomous system to suffer other attacks. Mehmood et al. (2018) proposed a method of
applying a Naive Bayes classification algorithm to the invasion testing system. The system was deployed in the entire network in the form of multi-agents to sense abnormal behaviors or irregular traffic and actions of nodes. They also discussed the basic concepts related to essay work and the latest research in similar fields \[12\]. Since none of the current algorithm research for attack detection can reach the standard of excellence, this paper conducts related research on attack detection. This paper researches the DL-based DDoS attack detection method under SDN-OpenFlow. It applies DL to DDoS attack detection to expect excellent research results. The DDoS problem of this study belongs to the binary classification problem. Therefore, the content of this research is carried out by judging whether the characteristic data of the OpenFlow flow table is normal or not. Under normal circumstances, this kind of binary classification problem uses the probability value between 0 and 1 to express its tendency result. Therefore, after comprehensive consideration, this paper chooses to use the BPNN as the neural network structure of the model.

2. Method
2.1 SDN-OpenFlow network
SDN performs centralized management of the network by dividing the control layer and the data layer. Also, the network resources are reasonably configured according to requirements to avoid resource waste. The SDN network does not require hardware adjustments to the original network equipment, which can effectively save application costs \[13\]. The SDN network has an application layer, a control layer, and an infrastructure layer. The application layer can provide users with various user interface programs. Users can choose and develop various modules according to their needs to achieve personal customization requirements. The controller customizes the relevant strategies based on the user's demands and transmits customized rules to the data and the control layer. The control layer is to control the network structure. The infrastructure layer is used to achieve the conversion between data \[14\].

OpenFlow realizes the design idea of SDN and promotes the development of SDN technology. It is one of the main ways to achieve SDN technology. OpenFlow introduces the concept of “flow” and uses a "flow table" that can meet various functions for data transmission. At the same time, the flow table
can be accessed remotely through the OpenFlow protocol. In this way, the entire network structure becomes an abstract structure with a multi-user program interface to facilitate various studies\[^{15}\].

2.2 DDoS attack form

There are three main forms of DDoS attacks: IP spoofing, slow connection attack, and flooding attack.

(1) IP spoofing: a widely used attack method. The principle is that the IP packets produced by the action are false source IP addresses to imitate the identity of other systems or senders. In the malicious attack request to the target system, a large number of fake source IPs are randomly generated. If the target defense is weak, the authenticity of the attack source cannot be analyzed for the malicious request received, to achieve the purpose of hiding the attacker\[^{16}\]. For the “reflection” DDoS attack, it is characterized by the use of a service protocol flaw of the target system, and the non-equivalence of the input and output. A malicious request with a small throughput was sent to the target. The target system returns a large number of reactions due to its protocol flaws. The network bandwidth is blocked and the host system resources are occupied. At this time, if the request of the attacker adopts the real source address, it will be swallowed by a huge reaction with hurting himself\[^{17}\]. Then, it is imperative for attackers to take IP spoofing measures.

(2) Slow connection attack: HTTP slow attack is to use HTTP legal mechanism, and try to keep the connection as long as possible after the connection is established, without releasing, to reach the HTTP service attack. The attacker sends a POST request, constructs a message, and submits data to the server, with setting the message length to a large value. Also, in subsequent transmission, only one small message is sent each time. It causes the server to wait for data and the connection is always occupied.

(3) Flooding attack: The flooding attack is a three-way handshake mechanism using TCP. The attacker uses a fake IP address to send a request to the attacked end. The response message sent by the attacked end will never be sent to the destination. Then, the attacked end will cause a lot of resource consumption in the process of waiting to close this connection. If the number of such connections is large, the resources of the host will be exhausted. Then, the attacker will achieve its purpose.

The above three are the most basic DDoS attack forms. In actual life, DDoS attack forms often appear
in the form of mixed-use.

2.3 DDoS attack detection

The DDoS attack is threatening for Internet security. Thus, DDoS attack detection is the research focus of researchers in various countries. DDoS attack detection is to control the source of the attack to effectively prevent DDoS attacks. However, prevention alone is not the answer to current network security issues. Detection is an important step to prevent DDoS attacks.

DDoS attack detection is divided into three modes based on misuse, anomaly, and hybrid. DDoS attack detection based on misuse can be performed by collecting the data packets currently encountering the attack and comparing them with the characteristic parameters of the DDoS attack. DDoS attack detection based on misuse and anomaly needs to be performed by establishing a model. The former requires a negative behavior model, while the latter requires a positive behavior model. The relevance ratio and false alarm rate (FAR) of the former are not high, but the maintenance cost is high, which is not conducive to transplantation and expansion. The latter has a higher relevance ratio and FAR, but this method can detect the characteristics of the attack. The detection of hybrid modes is usually carried out in the form of data mining. The characteristic parameters in the attack are extracted and detected using the misuse detection method.

2.4 DDoS attack detection based on DL

The characteristics of the OpenFlow flow table represent the current network status of the switch. The network conditions where DDoS attacks occur are not the same as under normal circumstances, and their flow table characteristics are also different. Therefore, in the traditional rule-based attack detection process, the following problems exist.

(1) Difficult rule setting: Different rules need to be set in the face of different types of attacks. Because there are many types of attacks, there are many types of rules. Also, there must be no interference between the rules. It causes a lot of inconvenience to the maintenance of these rules, and some types of attacks can cause multiple changes. Thus, in the process of setting the rules, it is necessary to accurately find the changed part to formulate the rules. This process also brings difficulties for the formulation of rules.
(2) Difficult to find rule thresholds: The setting of thresholds is important because it is related to the division of traffic. However, network traffic has strong randomness and fluctuations exist. Thus, the characteristics produced will fluctuate with it. In practice, there is no clear distinction between normal traffic and attack traffic. Therefore, setting the threshold is difficult.

(3) Difficult data analysis: The flow table data will continue to increase during the network operation. Setting the threshold is difficult by depending on humans to find rules. Also, it needs to take much equipment maintenance time. The data will become a large burden. Therefore, the increase in the data volume does not represent an increase in the accuracy.

Because of the above difficult problems, this paper uses DL to formulate rules.

DL is a new machine learning area, and its motivation is to establish and simulate the neural network of the human brain to perform the analytical learning. It imitates the mechanisms of the human brain for the interpretation of data, such as images, sounds, and text. DL belongs to a type of unsupervised learning. Its notion comes from the study of the artificial neural network (ANN). In fact, the multilayer perceptron containing multiple hidden layers belongs to a DL structure. Combining low-level characteristic, the attribute categories or characteristics of more abstract high-level representation are formed to find out distributed characteristic representations of data\(^{18}\).

The idea of DL is consistent with that of the ANN. Generally speaking, neural networks are machine learning architecture. All individual units are linked together in weights. The training is performed on these weights through the network. Thus, it can be called a neural network algorithm. The idea of the ANN algorithm comes from imitating the thinking way of the human brain. The human brain receives input signals through the nervous system and makes a reaction accordingly. The external stimulation is received by using neurons to receive electrical signals converted by the nerve terminal. Then, it is hoped that the brain's thinking is simulated through artificial neurons, and the ANN is created.

Artificial neurons make up the computing unit of the ANN, and the structure of the ANN describes the connecting method of these neurons. Neurons can be organized in layers. The layers can be connected to each other. In the past, many factors prevented it from adding many layers. With the algorithms updating, the data volume increasing, and the GPU developing, many layers can be used
to develop neural networks, which has resulted in the deep neural network. In fact, DL is synonymous with the deep neural network\(^{[19]}\).

The DDoS problem of this study belongs to the binary classification problem. Therefore, the content of this research is carried out by judging whether the characteristic data of the OpenFlow flow table is normal or not. Under normal circumstances, this kind of binary classification problem uses the probability value between 0 and 1 to express its tendency result. Therefore, after comprehensive consideration, this paper chooses to use BPNN as the neural network architecture.

The layer number in the neural network and the neuron number will have a serious impact on the performance of the model. Therefore, the layer number in the neural network and the neuron number need to be studied in detail before they can be determined. However, as far as the current research status is concerned, there is no effective related method for selecting the neuron number and the layer number. Only manual screening can be performed. Thus, in this process, it will take a lot of time to test and explore, finally determining the optimal value \(^{[20]}\). According to previous research experience in this aspect, the performance is better when the network is large and deep. Therefore, this paper adjusts network architecture based on this principle. In terms of the neuron number and the layer number, it uses the method of network layer priority to study.

In addition to the above two parameters, the activation function has a serious influence on the model’s performance. In the current related studies, the use of the ReLU activation function has become the first and mainstream choice. Also, the activation function performs better in many aspects. Thus, the activation function of the network layer in this paper is the ReLU activation function.

2.5 Experimental environment for DDoS attack detection based on DL

The experimental environment in this paper includes the front-end platform, SDN controller, BPNN model and network simulation environment. The simulation tool used is mini-net, which can simulate a complete network structure.

The front-end platform is developed using Java Swing. The URL provided by Floodlight is used to obtain network topology information and DDoS attack detection results. Also, the attack alarms and
abnormal switch locations are realized. The SDN controller is Floodlight. The controller has more complete functions and can perform route calculation and flow table calculation. Java is used for controller development. The bottom layer of the BPNN model uses Theano. The network simulation environment is the OpenFlow switch, host, and server. The numbers are 7, 16, and 1 respectively. To simulate the real network situation, this paper uses the traffic control tool in the Linux system to set the bandwidth and delay.

3. Results And Discussion
3.1 Test data acquisition
To have enough data for subsequent simulation experiments, this paper first conducts simulation experiments of five types of DDoS attacks and normal conditions. After the simulation, multiple pieces of feature data are generated, as shown in Fig. 1.

The feature data under normal conditions in Fig. 1 comes from different network busy levels. The five types of attack feature data also include different attack strengths, different numbers and positions of attackers, and different victim positions.

3.2 Comparison results of the small data relevance ratio
In the research of this paper, the support vector machine and decision tree are used as control detections to study the relevance ratio of DDoS attack relevance ratio of various methods in the case of small data. The comparison results are shown in Fig. 2.

The figure above shows the comparison of the relevance ratio between the DL model and the other two models under a small data scale. The horizontal axis is various types of DDoS attacks, and the vertical axis is the relevance ratio. It can be seen from the figure that in the case of a small data scale, the relevance ratio of the DL model in the face of flooding attacks has a slight advantage, but it has not shown its detection advantage in other aspects. The detection performance is not outstanding.

3.3 Comparison results of the small data FAR
The FAR of the DDoS attack relevance ratio of various methods regarding small data is studied. The comparison result is shown in Fig. 2. The model with a lower FAR performs better.

The figure above shows the comparison of the FAR between the DL model and the other two models
under a small data scale. The horizontal axis is various types of DDoS attacks, and the vertical axis is the FAR. It can be seen from the figure that under the condition of a small data scale, the FAR of the DL model is at a low level, but its performance is not in an excellent state. The overall performance is similar to the decision tree.

3.4 Comparison results of relevance ratios under big data scale
As the scale of the training data expands, the performance of each model also changes to some extent. The relevance ratio of DDoS attack relevance ratio of various methods under the large data scale regarding the small data is studied. The comparison results are shown in Fig. 4.

The figure above shows the comparison of the relevance ratio between the DL model and the other two models under the big data scale. The horizontal axis is various types of DDoS attacks, and the vertical axis is the relevance ratio. It can be seen from the figure that in the case of a small data scale, the relevance ratio of DL in the face of IP spoofing attacks has a strong advantage. Also, the relevance ratio of flooding attack, UDP Flood and slow connection attacks are all excellent, which is almost the same as the decision tree detection method. But it performs poorly in HTTP Flood. Because in HTTP Flood, attackers use real IP addresses and imitate the use of real users to attack. For this type of attack, the flow-based attack detection method does not have a good testing effect. Since the decision tree model has a relatively high FAR, the relevance ratio is relatively high. In general, the DDoS attack detection model based on DL performs well and has certain advantages over other models. However, this model is not suitable for all attack states.

3.5 Comparison results of the FAR under large data scale
Because of the change in the data volume, the FAR of each model also changes to a certain extent. The comparison result of the FAR under the big data scale is shown in Fig. 5.

The figure above shows the comparison of the FAR between the DL model and the other two models under the big data scale. The horizontal axis is various types of DDoS attacks, and the vertical axis is the FAR. From the figure, regarding a large data scale, the DL method has the lowest FAR. In the actual situation, the normal network usage situation is far more than the attack situation. Thus, a low FAR is a necessary condition for DDoS attack detection. From the above figure, although the
relevance ratio of the decision tree method performs well overall, the FAR is generally high, which is more than twice that of the DL method. Therefore, after comprehensive consideration, it is found that the performance of the DL method is better.

3.6 Comparison results of testing time
Testing time is also an important parameter in DDoS attack detection. The length of the testing time is related to the subsequent response. Thus, comparing the testing time of several models, the results are shown in Fig. 6.

From the figure, in terms of testing time, the decision tree takes little time because of its special structure. The DL method takes more time to detect. However, considering the low FAR and high relevance ratio of DL, its testing efficiency is high. Therefore, the DL method can meet the needs of attack scenarios when detecting.

3.7 Comparison results of other algorithms
Compared to the traditional BPNN detection model, comparison results of the accuracy rate are shown in Fig. 7.

Compared with the traditional BPNN model, as shown in the figure above, the testing accuracy rate of both has gradually increased. The relevance ratio based on the DL method in this paper is relatively high. However, with the larger training data, the gap between the two will become smaller.

The comparison of the testing time between the two is shown in Fig. 8.

From the above figure, the testing time based on the DL method is generally low. The testing time based on the BPNN method is higher. Therefore, on the whole, the detection method based on DL in this paper performs better.

Compared with the traditional comentropy method, the comparison result of its testing accuracy rate is shown in Fig. 9.

From the above figure, the testing accuracy rate based on the DL method is generally higher than that of the traditional comentropy method. The comparison results of the testing time between the two is shown in Fig. 10.

From the above figure, the traditional comentropy method generally takes a long time. Therefore,
from all aspects, the detection method based on DL in this paper is excellent.

Compared with the method of extreme learning machine, the comparison results of the accuracy rate is shown in Fig. 11. The comparison results of the testing time between the two is shown in Fig. 12. From Figs. 11 and 12, in the comparison of the testing time and accuracy rate of the two, the accuracy rate based on the DL test algorithm in this paper is higher, and the time is relatively short. Therefore, the detection method based on DL is more excellent.

The results of comparison with the k-Nearest Neighbor (KNN) algorithm are shown in Figs. 13 and 14. From Figs. 13 and 14, the testing time and accuracy rate of the two methods is not much different. However, the more the subsequent training data, the better the DL detection method in this paper, and the shorter the time.

Compared with SOM (Self-organizing feature mapping) detection method, the results are shown in Figs. 15 and 16. From Figs. 15 and 16, the testing time and accuracy rate of the two are not much different, which indicates that both of them have good performance in DDoS attack detection. However, the method proposed by this paper has certain advantages. Its testing accuracy rate is higher, and the testing time is shorter.

4. Conclusion
This paper researches the DL-based DDoS attack detection method under SDN-OpenFlow. After comparing with various other algorithms, the method of this paper is excellent in all aspects and can meet the needs for attack detection. The innovation is that DL has been applied to DDoS attack detection and it has obtained relatively excellent research results. Although some achievements have been obtained in this research, there are still some shortcomings. The DL model of this research also needs a certain degree of human adjustment, and it cannot be completely intelligent. It will be considered in the next research to obtain a more intelligent detection model. Due to time, the research on attack types is not complete. Therefore, the detection effect of other attack types cannot be reflected at present. Thus, the next step is to continue this research, expand the scope of attack detection, and consolidate the research results of the paper.
Declarations

Acknowledgement

The authors extend their appreciation to the Deanship of Scientific Research at King Saud University for funding this work through Research Group no. RG- 1441-331.

1. Declarations section

- Availability of data and materials (Mandatory for Biology and Medical journals)

Data sharing not applicable to this article as no datasets were generated or analysed during the current study

- Competing Interest (Mandatory)

The authors declare that they have no competing financial interests.

- Funding (Mandatory)

The authors extend their appreciation to the Deanship of Scientific Research at King Saud University for funding this work through Research Group no. RG- 1441-331.

- Authors Contribution (Mandatory)

Gang Ke, Ruey-Shun Chen carried out the DDoS attack detection method studies, participated in the experimental design and drafted the manuscript. Y. C. Chen carried out the Deep learning research. Naixue Xiong participated in the experimental design and performed the statistical analysis. Yuan Tian, Najla Al-Nabhan conceived of the study, and participated in its design and coordination and helped to draft the manuscript.

- Acknowledgements (optional)

Not applicable

- Authors Information (optional)

Not applicable

List Of Abbreviations

deep learning (DL)

Software-Defined Network (SDN)

distributed denial of service (DDoS)
back-propagation neural network (BPNN)

artificial neural network (ANN)

k-Nearest Neighbor (KNN)

SOM (Self-organizing feature mapping)

false alarm rate (FAR)

References

1. Mehmood A, Mukherjee M, Ahmed S H, et al. NBC-MAIDS: Naïve Bayesian classification technique in multi-agent system-enriched IDS for securing IoT against DDoS attacks. The Journal of Supercomputing, 2018, 74(10), pp. 5156-5170.

2. Krasnov A E, Nadezhdin E N, Nikol'skii D N, et al. Detecting DDoS attacks by analyzing the dynamics and interrelation of network traffic characteristics. Vestnik Udmurtskogo Universiteta. Matematika. Mekhanika. Komp'yuternye Nauki, 2018, 28(3), pp. 407-418.

3. Yan Q, Huang W, Luo X, et al. A multi-level DDoS mitigation framework for the industrial internet of things. IEEE Communications Magazine, 2018, 56(2), pp. 30-36.

4. Kolias C, Kambourakis G, Stavrou A, et al. DDoS in the IoT: Mirai and other botnets. Computer, 2017, 50(7), pp. 80-84.

5. Saied A, Overill R E, Radzik T. Detection of known and unknown DDoS attacks using Artificial Neural Networks. Neurocomputing, 2016, 172, pp. 385-393.

6. Bawany N Z, Shamsi J A, Salah K. DDoS attack detection and mitigation using SDN: methods, practices, and solutions. Arabian Journal for Science and Engineering, 2017, 42(2), pp. 425-441.

7. Somani G, Gaur M S, Sanghi D, et al. DDoS attacks in cloud computing: Issues, taxonomy, and future directions. Computer Communications, 2017, 107, pp.30-48.

8. Wang A, Chang W, Chen S, et al. Delving into internet DDoS attacks by botnets: characterization and analysis. IEEE/ACM Transactions on Networking, 2018, 26(6), pp.
9. Abidoye A P, Obagbuwa I C. DDoS attacks in WSNs: detection and countermeasures. IET Wireless Sensor Systems, 2017, 8(2), pp. 52-59.

10. Kim M. Supervised learning-based DDoS attacks detection: Tuning hyperparameters. ETRI Journal, 2019, 41(5), pp. 560-573.

11. Simpson S, Shirazi S N, Marnerides A, et al. An inter-domain collaboration scheme to remedy ddos attacks in computer networks. IEEE Transactions on Network and Service Management, 2018, 15(3), pp. 879-893.

12. Mehmood A, Mukherjee M, Ahmed S H, et al. NBC-MAIDS: Naïve Bayesian classification technique in multi-agent system-enriched IDS for securing IoT against DDoS attacks. The Journal of Supercomputing, 2018, 74(10), pp. 5156-5170.

13. Zheng J, Li Q, Gu G, et al. Realtime DDoS defense using COTS SDN switches via adaptive correlation analysis. IEEE Transactions on Information Forensics and Security, 2018, 13(7), pp. 1838-1853.

14. Osanaiye O, Cai H, Choo K K R, et al. Ensemble-based multi-filter feature selection method for DDoS detection in cloud computing. EURASIP Journal on Wireless Communications and Networking, 2016, 2016(1), pp. 130.

15. Zhang Y Y, Lu G H, Li P F. A Survey of Deep Learning Methods for SDN Network Intrusion Detection System. Computer Applications, 2019, 39(S2), pp. 147-151.

16. Somani G, Gaur M S, Sanghi D, et al. Combating DDoS attacks in the cloud: requirements, trends, and future directions. IEEE Cloud Computing, 2017, 4(1), pp. 22-32.

17. Praseed A, Thilagam P S. DDoS attacks at the application layer: Challenges and research perspectives for safeguarding Web applications. IEEE Communications Surveys & Tutorials, 2018, 21(1), pp. 661-685.
18. Gupta B B, Badve O P. Taxonomy of DoS and DDoS attacks and desirable defense mechanism in a cloud computing environment. Neural Computing and Applications, 2017, 28(12), pp. 3655-3682.

19. Behal S, Kumar K. Detection of DDoS attacks and flash events using novel information theory metrics. Computer Networks, 2017, 116, pp. 96-110.

20. Toklu S, Şimşek M. Two-layer approach for mixed high-rate and low-rate distributed denial of service (DDoS) attack detection and filtering. Arabian Journal for Science and Engineering, 2018, 43(12), pp. 7923-7931.

Figures

Figure 1

Number of training and test records (Figure1: The feature data under normal conditions comes from different network busy levels. The five types of attack feature data also include different attack strengths, different numbers and positions of attackers, and different victim positions.)
Comparison of relevance ratios under small data scale (Figure 2): The figure above shows the comparison of the relevance ratio between the DL model and the other two models under a small data scale. The horizontal axis is various types of DDoS attacks, and the vertical axis is the relevance ratio. It can be seen from the figure that in the case of a small data scale, the relevance ratio of the DL model in the face of flooding attacks has a slight advantage, but it has not shown its detection advantage in other aspects. The detection performance is not outstanding.)
Comparison of the FAR under small data scale (Figure 3: The figure above shows the comparison of the FAR between the DL model and the other two models under a small data scale. The horizontal axis is various types of DDoS attacks, and the vertical axis is the FAR. It can be seen from the figure that under the condition of a small data scale, the FAR of the DL model is at a low level, but its performance is not in an excellent state. The overall performance is similar to the decision tree)
Comparison of relevance ratios under big data scale (Figure 4: The figure above shows the comparison of the relevance ratio between the DL model and the other two models under the big data scale. The horizontal axis is various types of DDoS attacks, and the vertical axis is the relevance ratio. It can be seen from the figure that in the case of a small data scale, the relevance ratio of DL in the face of IP spoofing attacks has a strong advantage. Also, the relevance ratio of flooding attack, UDP Flood and slow connection attacks are all excellent, which is almost the same as the decision tree detection method. But it performs poorly in HTTP Flood.)
Comparison of the FAR under big data scale (Figure 5: The figure above shows the comparison of the FAR between the DL model and the other two models under the big data scale. The horizontal axis is various types of DDoS attacks, and the vertical axis is the FAR. From the figure, regarding a large data scale, the DL method has the lowest FAR.)
Comparison of testing time (Figure 6: From the figure, in terms of testing time, the decision tree takes little time because of its special structure. The DL method takes more time to detect. However, considering the low FAR and high relevance ratio of DL, its testing efficiency is high. Therefore, the DL method can meet the needs of attack scenarios when detecting.)
Comparison of the accuracy rate compared with traditional BPNN method (Figure 7: Compared with the traditional BPNN model, as shown in the figure 7, the testing accuracy rate of both has gradually increased. The relevance ratio based on the DL method in this paper is relatively high. However, with the larger training data, the gap between the two will become smaller.)
Comparison of testing time compared with traditional BPNN method (Figure 8: From the figure 8, the testing time based on the DL method is generally low. The testing time based on the BPNN method is higher. Therefore, on the whole, the detection method based on DL in this paper performs better.)
Comparison of testing accuracy rate compared to the traditional comentropy method

(Figure 9: From the figure 9, the testing accuracy rate based on the DL method is generally higher than that of the traditional comentropy method.)
Comparison of testing time compared to traditional comentropy method (Figure 10: From the figure 10, the traditional comentropy method generally takes a long time. Therefore, from all aspects, the detection method based on DL in this paper is excellent.)
Comparison of testing accuracy rate compared with the extreme learning machine method (Figure 11: From Figures 11, in the comparison of the accuracy rate of the two, the accuracy rate based on the DL test algorithm in this paper is higher. Therefore, the detection method based on DL is more excellent.)
Figure 12

Comparison of testing time compared with the extreme learning machine method (From Figures 12, in the comparison of the testing time of the two, the time based on the DL test algorithm in this paper is relatively short. Therefore, the detection method based on DL is more excellent.)
Figure 13

Comparison of testing accuracy rate compared with KNN method (From Figures 13, the accuracy rate of the two methods is not much different. However, the more the subsequent training data, the better the DL detection method in this paper.)
Comparison of testing time compared with KNN method (From Figures 14, in the comparison of the testing time of the two, the time based on the DL test algorithm in this paper is short. Therefore, the detection method based on DL is more excellent.)
Comparison of testing accuracy rate compared with the SOM method (Figure 15: From Figures 15, in the comparison of the accuracy rate of the two, the accuracy rate based on the DL test algorithm in this paper is higher.)
Comparison of testing time compared with the SOM method. Figure 16: Compared with SOM (Self-organizing feature mapping) detection method, the method proposed by this paper has certain advantages, the testing time is shorter.