ISSN 2706-655X Vol.5, Issue 9: 28-33, DOI: 10.25236/IJFET.2023.050906

Design and Research of Security Software Based on Traffic Analysis

Zhong Manlin, Yin Hang, Zhou Jianhan, Lan Tianyu

Liaoning University of Science and Technology, Anshan, China

Abstract: *This project provides a security defense system and method against traffic attacks. The system includes: SDN switch, forwarding the ICMP request message and ICMP response message sent by the user terminal, monitoring the ICMP request message and ICMP response message, and forming ICMP information in case of abnormality; The SDN controller connected with the SDN switch receives the ICMP information reported from the SDN switch, senses the message forwarding path corresponding to the ICMP information, judges the location and type of the attacker, and sends a flow table to the SDN switch as the entrance routing function to implement the entrance filtering strategy to defend the attacker. This project adopts SDN architecture, which can accurately determine the location and type of attack of the attacker and execute the corresponding entrance filtering strategy, so as to effectively defend against ICMP Flood attacks.*

Keywords: *network security; Flow analysis; Trojan horse; Viruses; Security defense*

1. Preface

First, we use the deep learning model based on residual networks (Resnets) to identify and prevent network security threats, which is a popular and cutting-edge research direction at present.Our model uses the Keras deep learning framework, and constructs a residual network based on identity blocks and convolutional blocks.Compared with the traditional deep learning model, the model based on residual network can better avoid the problems of gradient disappearance and gradient explosion, and it is easier to achieve higher accuracy in the training process.We used the malicious sample API in the Cuckoo sandbox environment to test our model, and conducted performance evaluation on multiple datasets such as MNIST and Deeplearning.ai's public datasets.The results show that our model can have high accuracy, and has a better ability to identify and prevent threats such as malware.This is a new idea and tool for research and practice in the field of network security, which is expected to play an important role in practical applications.

Secondly, our data visualization exploration provides new ideas and possibilities for data analysis in the field of network security.We intend to use visualization techniques such as scatter plot matrix and parallel coordinate system to analyze and present network data and information.This method based on data visualization can help security researchers understand and identify anomalies and threats in the network more intuitively, and improve the detection and prediction ability of network security to a certain extent.In addition, our exploration can also provide new ideas and technical support for data visualization applications in other fields.

ICMP flood attacks can be divided into three ways: one is direct flood, which uses your own machine to attack others directly. This requires sufficient bandwidth. Direct attacks will expose your IP address, which is not common.One way is to forge an IP flood. It randomly forges an IP to flood, which is a relatively covert and insidious flood attack.The third way is called "Smurf" attack, which is the most covert and common attack method.The attacker sends ICMP Echo request packets to the network broadcast address, and sets the source IP address as a third-party victim, causing all hosts in the network to return ICMP Echo response packets to the third-party victim, which eventually leads to the third-party crash.

The existing ICMP Flood attack defense technology can be mainly divided into three aspects: detection and defense, enhanced tolerance, and attack source tracking.Since the existing defense technologies are all based on the traditional distributed network, it is difficult to achieve accurate and dynamic detection and defense and attack source tracking.

The existing detection methods for ICMP flood attacks mainly calculate the number of ICMP packets

ISSN 2706-655X Vol.5, Issue 9: 28-33, DOI: 10.25236/IJFET.2023.050906

passing in unit time. If it is greater than the peak value of ICMP traffic, it is considered as an ICMP attack.However, because the existing detection is isolated and distributed, it is impossible to accurately determine which kind of ICMP Flood attack and the exact source of the attack.The original network is not based on SDN architecture. It is difficult for distributed control to perceive the forwarding path of packets and the location of attackers. Therefore, it is impossible to accurately find the switch or router nearest the attacker for entrance filtering or rate limiting, and it is also impossible to accurately determine which ICMP Flood attack is.The root of ICMP Flood attack lies in the openness of ICMP services, the uncertainty of object-oriented, and the limitation and exhaustion of service provider resources. These factors determine that there is no perfect solution at present.It can be seen that the current protection against ICMP Flood attacks has some shortcomings both in theory and application, mainly reflected in the low accuracy and efficiency[1-3].

2. Project content

The research on feature selection of network traffic anomaly and the design of BP neural network model for network traffic anomaly detection have important academic value and application prospect. In order to reduce network traffic characteristics, this project hopes to be based on a dual feature selection algorithm based on correlation and improved binary cuckoo optimization.

1) The redundant features irrelevant to classification in the feature set are eliminated through the correlation measurement between features and features, and between features and categories; Then the feature selection is transformed into an optimization problem, and the swarm intelligence optimization algorithm is introduced. The improved binary cuckoo algorithm is used to search out the most favorable features from the feature subset to form the final optimal feature subset.

2) Differential evolution strategy and opposite learning strategy are introduced into the algorithm to accelerate the convergence speed of the algorithm. The improved algorithm is used to guide the BP neural network to find the best weight and threshold to complete the training of the anomaly detection model.

The filtering threat traffic software of this project is expected to be able to effectively check and analyze the traffic and data packets transmitted in the network under the support of machine learning, actively filter threat traffic, accurately identify network viruses and trojans and other threats, and improve network security defense capabilities[4-5].

3. Security defense system against traffic attacks

The security defense system against traffic attacks includes:

SDN switch forwards ICMP request message and ICMP response message sent by user terminal, monitors ICMP request message and ICMP response message, and forms ICMP information in case of abnormality;

The SDN controller connected to the SDN switch receives the ICMP information reported by the SDN switch, senses the message forwarding path corresponding to the ICMP information, judges the location and type of the attacker, and sends a flow table to the SDN switch as the entrance routing function to implement the entrance filtering strategy to defend the attacker.

When the SDN switch finds that the forwarding rate of the ICMP request message exceeds the specified threshold, the forwarding rate of the ICMP response message exceeds the specified threshold, or the destination IP of the ICMP request message is the network propagation address, it judges that an exception occurs and forms ICMP information.

The SDN controller receives the ICMP information, and then judges whether the forwarding rate of the ICMP response message exceeds the specified threshold when judging that the destination IP of the ICMP request message included in the ICMP information is the network propagation address. When judging that the ICMP response message exceeds the specified threshold, the entry filtering strategy corresponding to the stream table issued by the SDN controller is to discard the ICMP request message.

The SDN controller receives the ICMP information, and then judges whether the forwarding rate of ICMP request message and ICMP response message exceeds the specified threshold when the destination IP not including ICMP request message in the ICMP information is the network propagation address. If the forwarding rate of ICMP request message and ICMP response message exceeds the specified threshold. The entry filtering policy corresponding to the flow table issued by the SDN controller is to

ISSN 2706-655X Vol.5, Issue 9: 28-33, DOI: 10.25236/IJFET.2023.050906

limit the packet forwarding rate of the SDN switch as the entry routing function.

After the SDN switch sends the ICMP information, it continues to monitor the ICMP request message and ICMP response message. When it finds that the ICMP request message and ICMP response message are back to normal, it sends the defense removal request to the SDN controller. The SDN controller judges according to the defense removal request and obtains that the corresponding message forwarding rate is less than or equal to the specified threshold, then it removes the issued flow table.

4. Security defense methods for traffic attacks

The project's security defense methods against traffic attacks include:

Monitor the ICMP request message and ICMP response message sent by the forwarded user terminal through the SDN switch corresponding to the user terminal, and form ICMP information in case of abnormality;

Receive ICMP information for judgment, sense the message forwarding path corresponding to ICMP information, judge the location and type of the attacker, and send a flow table to the SDN switch as the entrance routing function to implement the entrance filtering strategy to defend the attacker.

The exceptions in ICMP information generated when exceptions are found include:

The forwarding rate of ICMP request message exceeds the specified threshold, the forwarding rate of ICMP response message exceeds the specified threshold, or the destination IP of ICMP request message is the network propagation address.

When it is judged that the destination IP of the ICMP message including the ICMP request message is the network propagation address, then it is judged whether the forwarding rate of the ICMP response message exceeds the specified threshold. When it is judged that the forwarding rate of the ICMP response message exceeds the specified threshold, the entry filtering strategy corresponding to the distribution flow table is to discard the ICMP request message.

When it is judged that the destination IP which does not include ICMP request message in ICMP information is the network propagation address, then it is judged whether the forwarding rate of ICMP request message and ICMP response message exceeds the specified threshold. When it is judged that the forwarding rate of ICMP request message and ICMP response message exceeds the specified threshold,The entry filtering policy corresponding to the distribution flow table is to limit the packet forwarding rate of the SDN switch as the entry routing function[6-8].

When the SDN switch finds an exception and forms ICMP information, it continues to monitor the exception. When the exception returns to normal, it requests to remove the defense of the entrance filtering strategy, judges the request, and obtains that when the corresponding message forwarding rate is less than or equal to the specified threshold, it removes the issued flow table.

5. System composition

1) Network packet capture

Timely collect user information, device information and network traffic information. At the same time, the system also needs to process these information to improve the efficiency of security analysis

2) Artificial Intelligence for Machine Learning Training

With the support of machine learning, complete the inspection and analysis of traffic and data packets transmitted in the network, and actively filter threat traffic.

3) Security operation terminal

Realize security attack risk assessment and check the accuracy of the prediction of the security identification module. If the accuracy is low, you can further increase learning instances or replace the pattern recognition algorithm.

4) Characteristic database

In addition to the initial training, in the process of software application, continuously collect new network packet characteristics that meet the requirements of security strategy for AI training.

ISSN 2706-655X Vol.5, Issue 9: 28-33, DOI: 10.25236/IJFET.2023.050906

6. Research methods:

1) Stream statistics design

(1) The design idea of flow statistics is shown in Figure 1.

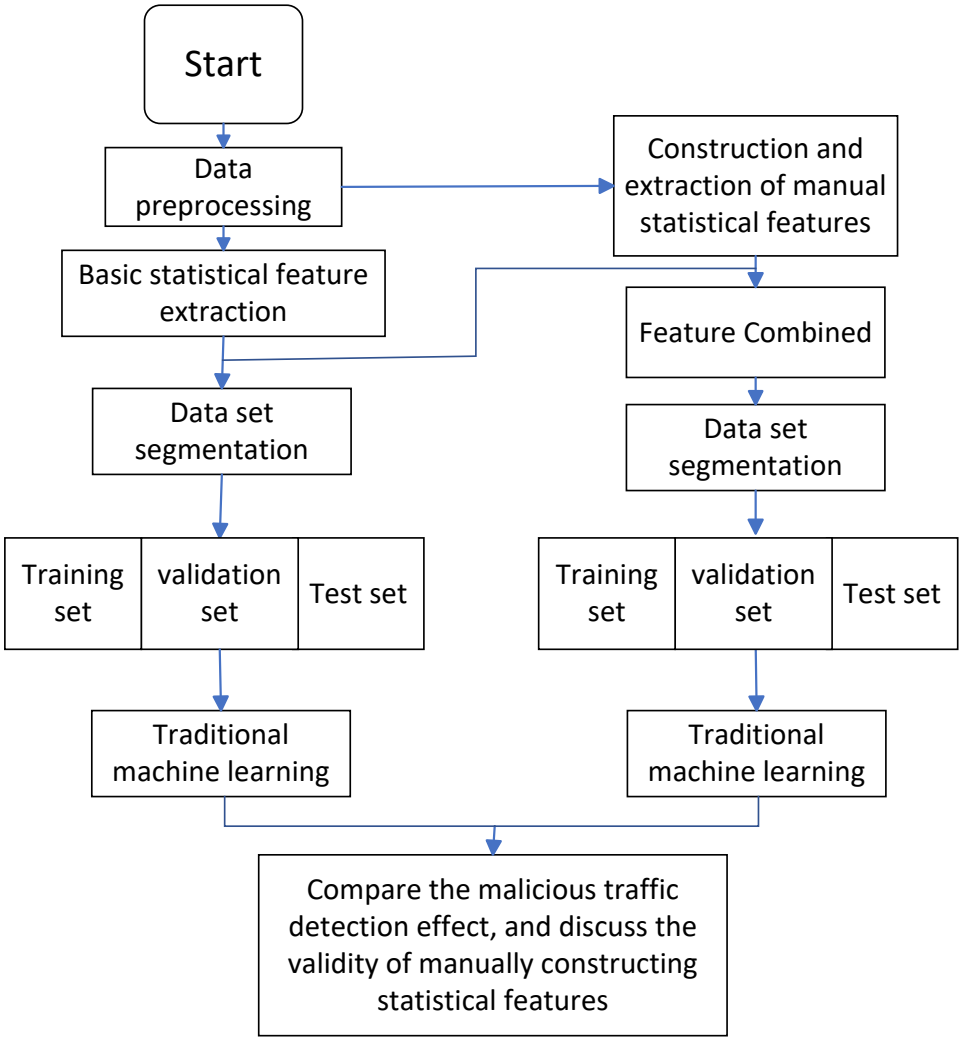

Figure 1: Stream Statistics Design

Figure 1 is the flow chart of the expected design. Firstly, based on the preprocessed network flow data, the flow statistical characteristics are extracted, which are 5 basic statistical characteristics and 17 manually constructed statistical characteristics; Then the traditional machine learning malicious traffic detection model is established based on 5 basic features and 22 statistical features including manually constructed statistical features respectively; Finally, the effectiveness of manually constructed statistical features is discussed by comparing the detection effects of the two types of models.

2) Design of flow trajectory diagram

Figure 2 shows the flow chart of the expected design. First, five tuple information is extracted based on the preprocessed network flow data, including port numbers, protocol numbers and IP addresses at both ends of the two-way flow, and the network flow that cannot obtain complete five tuple information is deleted; Secondly, according to the definition of traffic trajectories, the sharing of network flow IP addresses is analyzed and a graph is constructed; Then we use the node embedding algorithm to learn the node representation.

ISSN 2706-655X Vol.5, Issue 9: 28-33, DOI: 10.25236/IJFET.2023.050906

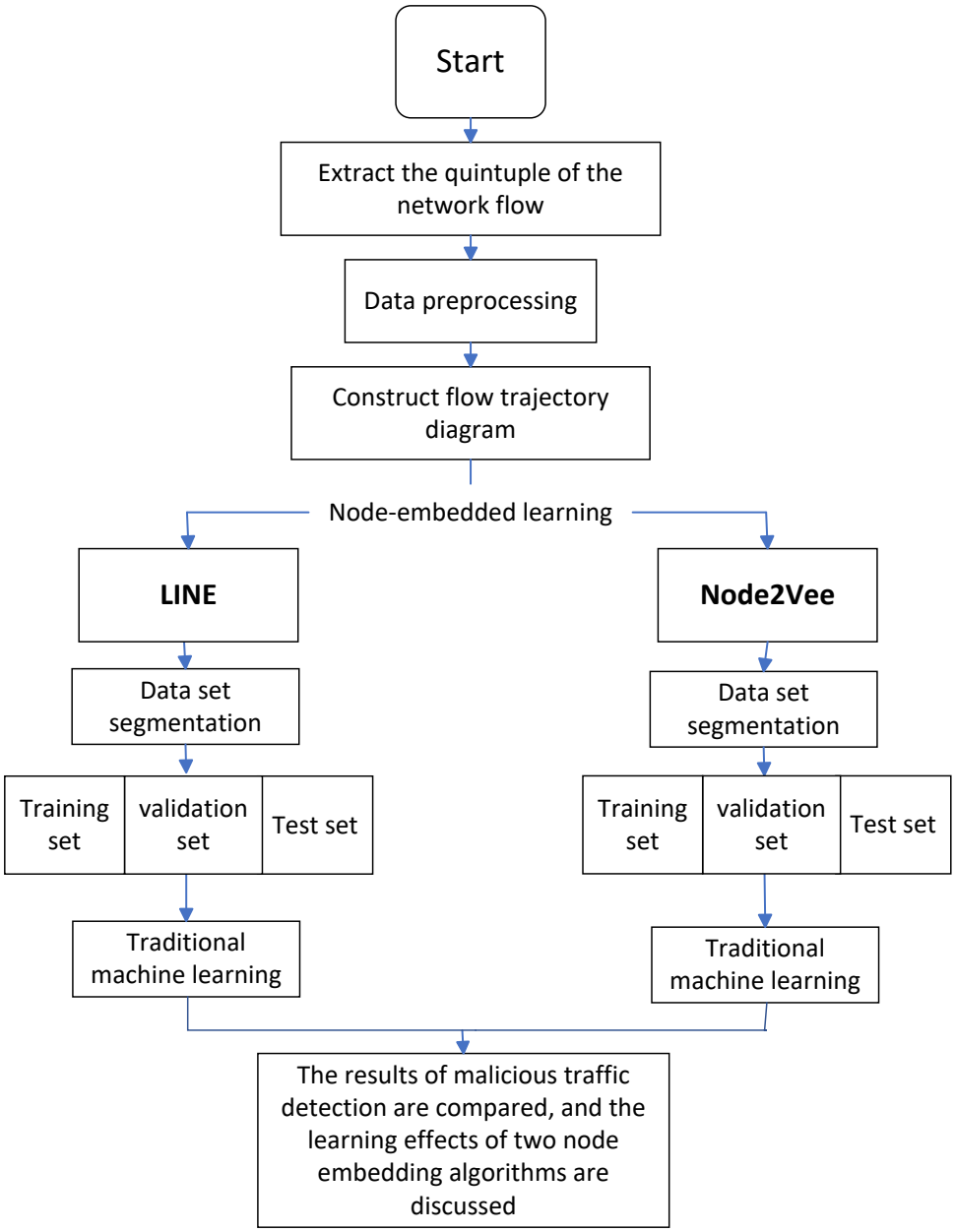

Figure 2: Flow Path

7. Conclusion

This patent adopts the SDN architecture. The SDN switch will report ICMP information dynamically. Based on this information, the controller can know where ICMP exception information occurs (entrance router or exit router). Finally, according to the generation conditions, it can accurately determine the location and attack type of the attacker and execute the corresponding entrance filtering strategy, so as to effectively defend against ICMP Flood attacks. Once the attacker stops attacking, the SDN controller will also disarm ICMPFlood based on the ICMP information reported by the switch, so as to release the flow table resources and maximize the effective management of the entire SDN network.

1) Compared with the traditional security technology for analyzing network traffic, which only relies on the known threat traffic database, the universality of different application scenarios is low, the update speed is slow, and it is difficult to meet the scenarios with high-level network security requirements. The security software based on traffic analysis can respond effectively through timely analysis, perception and early warning, thus reducing the losses caused by network attacks.☐☐

2) The packet sniffing technology based on big data and machine learning technology can provide a

ISSN 2706-655X Vol.5, Issue 9: 28-33, DOI: 10.25236/IJFET.2023.050906

more comprehensive flow analysis and filtering function. It uses computer software programming to unpack network IP packets into data flows for systematic automatic monitoring, so as to deeply understand the network conditions and alert network managers.

3) Combined with the characteristics of deep learning and traditional machine learning, encrypted malicious traffic detection is performed based on flow statistical characteristics, traffic trajectory, and fusion flow statistical characteristics and traffic trajectory respectively. This new efficient encrypted malicious traffic detection method based on neural networks uses convolutional networks as feature extractors to simultaneously train traffic trajectory graph structure and traffic statistical characteristics, and uses decision trees as classifiers to detect encrypted malicious traffic.

Acknowledgments

2023 Innovation and Entrepreneurship Training Program of Liaoning University of Science and Technology.

References

[1] Li Zhiming, Flow analysis system [J]. Computer Age, 2001 (12)
[2] Li Wenlin, Liu Chunwu. Design and Implementation of 10 Gigabit Network Traffic Analysis System [J] Information and Computer (Theoretical Edition), 2016 (16)
[3] Wang Qinggang, Gu Feng, Zhang Xuemei, Yu Rundong, Zhang Yi, Wang Yufan, Security early warning system based on campus network traffic analysis [J]. Network Security Technology and Application, 2022 (07)
[4] Zhou Xiaopeng. Network security based traffic analysis technology [J]. Information and Computer (Theoretical Edition), 2019 (12)
[5] Zhang Jian. Use traffic analysis to achieve fine network management [J]. China's Science and Technology Wealth, 2008 (07)
[6] Yao Weidong, New Value of Traffic Analysis: Neusoft NetFlow Technology [J]. Computer Security, 2006 (09)
[7] Liu Qing, Bandwidth management and control strategy based on traffic analysis [J]. Western Radio and Television, 2017 (12)
[8] Zhang Jingchun, Xie Xiaoning, Ma Yonghu. Development of traffic analysis system in the era of "Internet+" (Taking Zhicheng Network as an example) [J]. China New Communications, 2018 (15).