2023 IEEE 11th Joint International Information Technology and Artificial Intelligence Conference (ITAIC) | 979-8-3503-3366-4/23/$31.00 ©2023 IEEE | DOI: 10.1109/ITAIC58329.2023.10408809

Research on Detecting DDoS Attacks on SDN Platform Based on Bi LSTM Algorithm

Sui Xiangning, Li Qinan
College of Electronic and Information Engineering, Lanzhou Jiaotong University, Lanzhou 730070, Gansu Province, China
849789058@qq.com, room707@mail.lzjtu.cn
Corresponding Author: Sui Xiangning   Email: 849789058@qq.com

***Abstract*—Low-rate Distributed Denial of Service (L DDoS) attack has significant features of periodic attack traffic due to its small attack traffic, strong concealment, and huge harm. There is a deficiency in L DDoS attack detection in the existing SDNs that ignores temporal feature detection in attack traffic. While the Bi LSTM algorithm has advantages in temporal feature detection. Based on it, L DDoS attack detection scheme in SDN platform is proposed. Firstly, the five feature vectors in the flow table of the SDN switch-timestamp, average number of flow packets, average bit of flow packets, port rate, flow rate and source rate are calculated in real-time computing. Then they are sent into the Bi LSTM model to judge abnormal traffic and temporal feature detection for predicting the periodic time of L DDoS. Hence, it can make accurate detection of L DDoS, improving the accuracy and real time. The results show that the accuracy of L DDoS abnormal traffic detection reaches 99.2%.**

***Keywords*—sdn; ddoS; Bi LSTM ; RYU controller**

I. Introduction

DDoS attacks are the biggest cybersecurity threat facing Internet-related organizations [1]. By collecting network traffic data in real time and applying abnormal detection methods to network attacks in potential large scale network traffic is an important cornerstone for maintaining network security, which can strongly protect the interests of people's property.

L DDoS is a new type of DDoS attack [2], which has the features of stronger stealth, smaller traffic and attack traffic with periodicity. According to it, we need to analyze the timing characteristics of L DDoS attack traffic, summarize the timing pattern of L DDoS attack, and predict the time of the appearance of the next attack, so as to more accurately detect the L DDoS attack, and provide technical support to mitigate the subsequent L DDoS attacks on SDN platforms.

SDN can dynamically control network devices and implement security policies through the use of programmable controllers [3], which has the advantage of being able to monitor all traffic information, react to all attacks and improve network security [4]. This implementation of network virtualization provides a new experimental way for the research of new Internet architecture, and also it promotes the development of the next generation of the Internet, which has great potential for development.[5]

Compared with LSTM and other algorithms, Bi LSTM can utilize the advantage of bidirectional LSTM algorithm to correlate the temporal eigenvectors in the feature values, solving the problem that LSTM algorithm is not good enough in terms of efficiency for feature extraction. And it is more conducive to the detection of abnormal traffic.

Therefore, in this paper, a Bi LSTM-based L DDoS detection method in SDN is proposed for the significant features of L DDoS attack traffic with periodicity. The method statistically analyzes the temporal sequence of L DDoS attacks in real time, predicts the time of appearance of L DDoS attacks in the future and solves the problem of predicting the temporal sequence of L DDoS attacks, thus improving the accuracy of L DDoS attack detection.

II. Current Status of Domestic and Abroad Research

In recent years, both machine learning and deep learning algorithms have been widely applied to network security [6-7]. As a new type of DDoS attack, L DDoS has gradually been emphasized by researchers. Many researchers have proposed various abnormal detection methods for L DDoS attacks in SDN networks, which are different from the traditional methods.

Qi Benben et al. used recurrent neural network (RNN) for L DDoS detection and traffic classification [8-9], not being able to capture the dependency between feature vectors. LSTM algorithms have also been gradually applied to L DDoS detection [10], but there is a research gap between this detection method and Bi LSTM. Z. Liu et al. [11] proposed a DCNN Q-learning based method for CPSS LR in DDoS detection and defense method, which utilizes a deep convolutional neural network and locally sensitive features to extract the optimal feature distribution of the raw data for automatic learning, and employs a deep reinforcement learning network as a decision maker to improve the decision accuracy of attack detection.

Jadhav et al. [12] proposed an optimal objective entropy-based approach to detect L DDoS attacks, which has the problem of small distance values between normal and abnormal traffic and high false alarm rate.

Lijuan Li et al. [9] proposed a multi-type L DDoS detection method based on hybrid deep learning and it used up to more than eighty types of feature vectors for training. The disadvantages are time consuming and resources consuming and fails to capture long-term dependencies in temporal feature vectors.

Kaur et al. [13] proposed a high bandwidth attack method using self-similarity to detect TCP targets. It analyzes the effect of low-rate attacks on the self-similarity characteristics of the traffic and also it used the H-index to identify attacks by combining the legitimate traffic and the threshold value. This method is only effective for low-rate attacks based on TCP and depends on the threshold parameter value, which is easily to be affected by the randomness of the network environment and cannot achieve excellent detection results. What's worse, this detection method cannot do the analysis of the temporal nature of abnormal traffic.

Thus, periodic L DDoS attack detection in SDN platforms still suffers from the inability to capture long-term dependencies.

III. BiL STM-BASED DETECTION SCHEME

A. *Theoretical foundations*

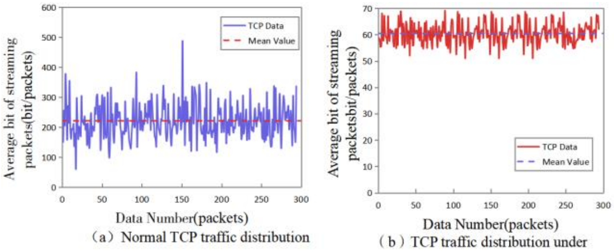
1) *Principles of L DDoS Attacks*

The principle of L DDoS attack is to periodically send high-speed pulsed suppression streams through the security vulnerability of the adaptive mechanism existing in network protocols or application service protocols, thus degrading the quality of target network service.

L DDoS attack flows usually choose periodic short duration high-speed pulsed malicious traffic to attacks. When the L DDoS attack flow suddenly launches an attack, a large amount of attack data flows into the network and the bottleneck link is seriously overloaded, which leads to frequent packet loss of normal TCP flows. It activates the TCP/IP congestion control mechanism to reduce the sending rate of normal TCP flows and the normal TCP throughput in the network is seriously lowered. At this point, the attack flow gradually occupied network resources, and the attacker will think that the network is in a "congested state'' and therefore reduce the output traffic, this will occur "denial of service''. For example, Figure 1 in the flow of packets in the average bit, the average normal traffic 220bit/packets, L DDoS attack traffic average of 60bit/packets, the attack traffic is only 27% of the normal TCP traffic, the normal TCP traffic throughput is seriously low, network service delays and even "denial of service". The throughput of normal TCP traffic was severely reduced and network services were delayed or even "denied service".

When the L DDoS attack flow is silent, legitimate TCP flows slowly return to the normal state and this state continues until the next L DDoS attack flow suddenly appears. Periodic L DDoS attack flows cause the network state to continuously switch between "congestion avoidance" and "congestion recovery", leading to a vicious cycle, with traffic oscillations that are very sharp and decreasing in mean value, as shown in Figure 1.

This morphological distribution anomaly is what distinguishes L DDoS attacks from other kinds of DDoS attack features, and is not easy to be forged. The average rate of L DDoS attack streams is low, but they can be well hidden in normal network traffic, and are difficult to be detected by detection algorithms targeting traditional DDoS attacks. However, according to its attack principle, the characteristics of L DDoS attack such as, duration, attack period and pulse intensity are also representative, in which the combination of periodicity and short-time high-speed pulse characteristics and matching network traffic with them can be used to discover L DDoS attack.



（a） Normal TCP traffic distribution

（b） TCP traffic distribution under

Fig. 1. TCP traffic distribution in normal state and LDDoS attack state conditions

2) *BiL STM*

The neural network structure model of BiL STM is shown in Fig. 2 and consists of two LSTM layers, which process input data in both directions [14].

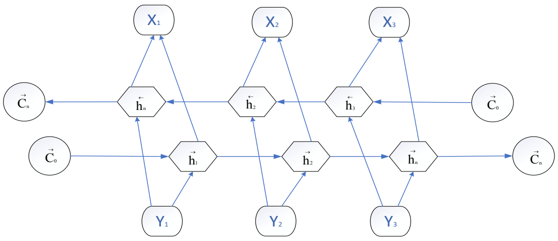


Fig. 2. Model of BiL STM neural network structure

The LSTM layer is a recurrent unit which includes input gates as well as output gates [15]. The output layer determines how much information the nerve cells at the back can get from the previous memory unit, while the forgetting gate at the other end, along with the input gate, determines the amount of information that can be stored in the existing memory unit. The output of each LSTM layer is connected and passed to the fully connected layer for classification [16].

For time series prediction, BiL STM uses bi-axial operation of forward computation and backward computation. The horizontal axis in Fig. 2 represents the bi-directional flow of the time series, and the vertical axis represents the unidirectional flow of temporal features from the input layer to the hidden layer and from the hidden layer to the output layer. To predict the time, the forward hidden vector value $\overrightarrow{h_2}$ and the new hidden vector value it generates $\overrightarrow{h_{\mathrm{n}}}$, and the backward term hidden vector value $\overrightarrow{h_1}$ and the new hidden vector value it generates $\overrightarrow{h_{\mathrm{n}}}$ are computed respectively. After inputting the two previous and subsequent vector values into the sequence, the outputs are combined to obtain the result $\overrightarrow{Y_{\mathrm{n}}}$. The formula is calculated as in equation (1), equation (2):

$$\overrightarrow{h_{\mathrm{n}}} = LSTM\left(X_{\mathrm{n}}, \vec{h}_{\mathrm{n}}\right) \tag{1}$$

$$Y_{\mathrm{n}} = \tanh\left(W_{\vec{n}y}\vec{h}_n + W_{\vec{n}y}\vec{h}_n + b_y\right) \tag{2}$$

LSTM () in Eq. (1) is a one-way LSTM computation method. The tanh () function in Eq. (2) is the hyperbolic tangent activation function. $W_{\vec{n}y}\vec{h}_n$ is the weight matrix of each layer linked to the hidden state of the antecedent, and b_y represents the bias term.

This model is trained using the Adam optimizer [17] and the binary cross-entropy loss function [18].

The formulas for the Adam optimizer are shown as Eqs. (3)(4)(5):

$$m_t := beta_1 \times m_{t-1} + (1 - beta_1) \times g \tag{3}$$

$$v_t = beta_2 \times v_{t-1} + \left(1 - beta_2\right) \times g \times g \tag{4}$$

$$\mathrm{var}\,iable := \mathrm{var}\,iable - lr_t \times m_t \Big/ \left(\sqrt{v_t} + \varepsilon\right) \tag{5}$$

Equation (3) calculates the first-order exponential smoothing value of the historical gradient, which serves to obtain the gradient value with enough momentum [19] . Equation (4) calculates the first order exponential smoothing value of the squared historical gradient to get the learning rate of each weight parameter. Equation (5) calculates the variable update values, which are proportional to the first order exponential smoothing value of the historical gradient and inversely proportional to the first order exponential smoothing value of the squared historical gradient [20].

The binary cross-entropy loss function is calculated as shown in equation (6):

$$L = -\left(y\log\left(p\right) + \left(1 - y\right)\log\left(1 - p\right)\right) \tag{6}$$

In Equation (6) y is the label (value 0 or 1) in the traffic feature, and p denotes the label that has been passed through the neural network prediction obtained the confidence level of the corresponding category[21].

B. Program design and realization

The three-tier architecture of the system solution is shown in Fig. 3 and is installed in the ryu controller for real-time monitoring of the real traffic environment and making records.

The first layer is the flow meter collection + feature extraction module. In this module the real flow information is detected and recorded by extracting the flow table information on the ryu controller and then the real flow feature values are extracted and output to the second layer.

The second layer is BiL STM attack detection module. The trained BiL STM detection model is installed in this module, which detects the existence of abnormal traffic in real time and records the detected abnormal traffic and normal traffic respectively according to the real traffic feature information transmitted from the first layer, and transmits the recorded real traffic information to the third layer.

The third layer is the timing detection module. We use BiL STM in this module to analyze the timestamp data collected from the first part of the detected anomalous traffic data in terms of temporal sequence, and then based on the analyzed temporal pattern, we predict the time when other anomalous traffic is likely to appear afterwards and record the output. Meanwhile, in this module, we summarize the performance and correctness of the anomalous traffic with respect to the collected eigenvalues.

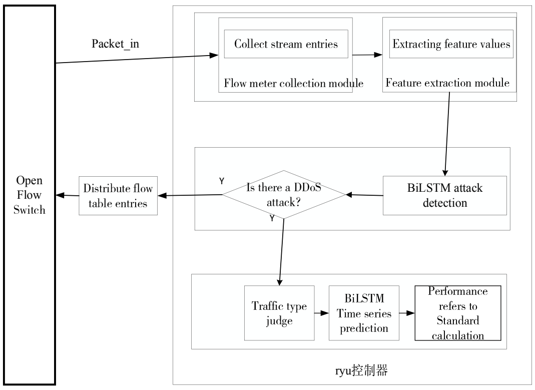

Packet_in
Collect stream entries
Flow meter collection module
Extracting feature values
Feature extraction module
Open Flow Switch
Distribute flow table entries
Y
Is there a DDoS attack?
Y
BiLSTM attack detection
Traffic type judge
BiLSTM Time series prediction
Performance refers to Standard calculation
ryu控制器

Fig. 3. Schematic diagram of the architecture

The flowchart of the identification of anomalous traffic using the model generated by BiLSTM training to characterize the traffic in the flow table information detected on the ryu controller is shown in Fig. 4. This part is installed in the BiLSTM attack detection module at the second layer of the architecture.

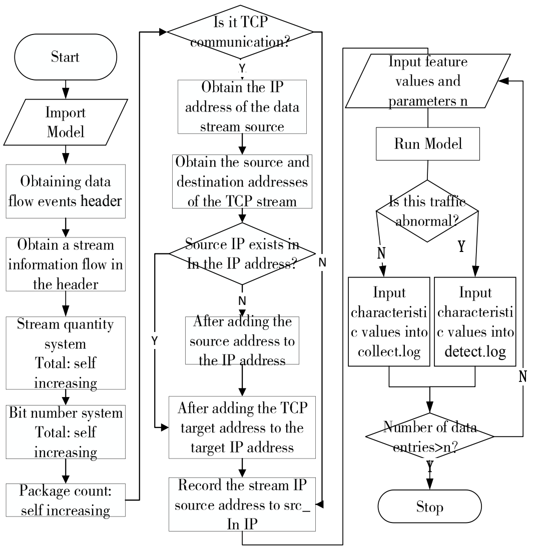

Start
Import Model
Obtaining data flow events header
Obtain a stream information flow in the header
Stream quantity system Total: self increasing
Bit number system Total: self increasing
Package count: self increasing
Is it TCP communication?
Y
Obtain the IP address of the data stream source
Obtain the source and destination addresses of the TCP stream
Source IP exists in In the IP address?
Y
N
N
After adding the source address to the IP address
After adding the TCP target address to the target IP address
Record the stream IP source address to src_ In IP
Input feature values and parameters n
Run Model
Is this traffic abnormal?
N
Y
Input characteristic values into collect.log
Input characteristic values into detect.log
Number of data entries>n?
N
Y
Stop

Fig. 4. Flowchart of core code one

The second part corresponds to the temporal analysis module of the architecture, in which the timestamp data of the previous part about the detected anomalous traffic is analyzed for temporal sequence through using the BiLSTM in this module. After that the analyzed temporal patterns are used to predict the possible time of occurrence of other anomalous traffic and record the output.

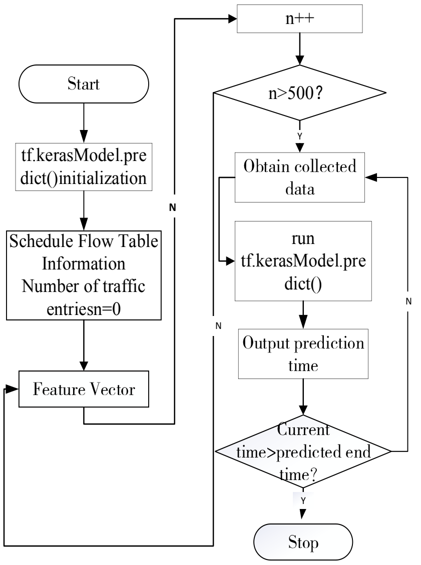

n++
Start
n>500?
Y
tf.kerasModel.predict()initialization
N
Obtain collected data
Schedule Flow Table Information Number of traffic entriesn=0
run tf.kerasModel.predict()
N
N
Output prediction time
Feature Vector
Current time>predicted end time?
Y
Stop

Fig. 5. Core Code II Flowchart

IV. EXPERIMENTAL TREATMENT AND ANALYSIS OF RESULTS

A. Introduction to the experimental environment

The experimental hardware environment was a NVIDIA GeForce RTX 3060 Laptop GPU with 16 GB of graphics memory, IAMD Ryzen 7 5800H with Radeon Graphics 3.20 GHz, and the software environment was Ubuntu 18.04.4 operating system, Python 3.6.1, torch1.10. 2+cpu, ryu 4.34, mininet2.3.1b1 environment for training.

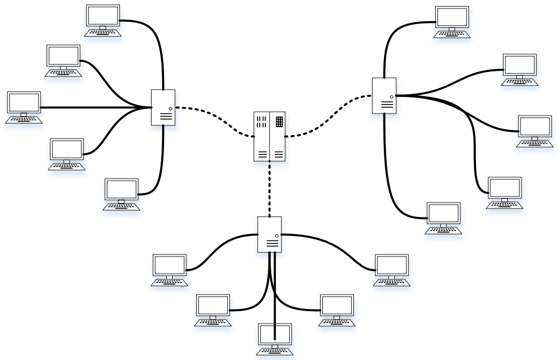


Fig. 6. Schematic diagram of topology for experimentation

The experimental topology is shown in Figure 6, which consists of 15 hosts, 3 OpenFlow switches to form a network and connect to the Internet. The link bandwidth between the OpenFlow switches is 10Mb/s and the bandwidth of the link between each host and the switch is 100Mb/s, and the latency of all the links is 10ms.

B. Data pre-processing

We simulated a low-rate TCP protocol-based Shrew attack on an SDN platform.

Firstly, we preprocess the real-time raw network traffic data extracted from the flow table and extract the following features: timestamp (date, time), flow average packet count, flow packet average bit, port rate, flow rate, source IP rate, and traffic type (normal traffic label:0, abnormal traffic label:1).

After preprocessing, a total of 30,000 pieces of traffic data are used to conduct model training, including 15,000 pieces of normal traffic and 15,000 pieces of abnormal traffic. In order to reduce the data uncertainty, 100 rounds of training are repeated each time, in which the legitimate traffic and attack traffic, the ratio of the training set to the test set is 2:1, and 10% of the data in the training set is selected as the validation set to validate the model's capability.

There is a substantial increase in the stream rate of abnormal traffic data during L DDoS attacks. As shown in Fig. 7, the flow rate of abnormal traffic is maintained at about 100 entries/second, while the flow rate of normal traffic is maintained at about 6 entries/second. This indicates that a large number of packets are sent during the L DDoS attacks.

By contrast, the source IP rate of anomalous traffic received by the host has risen dramatically relative to normal traffic.

There is a substantial increase in the source IP rate received by the host during L DDoS attacks. As it can be seen from Fig. 8, the source IP rate of abnormal traffic is maintained at around 96 packets/s and the source IP rate of normal traffic is maintained at around 1.4 packets/s.

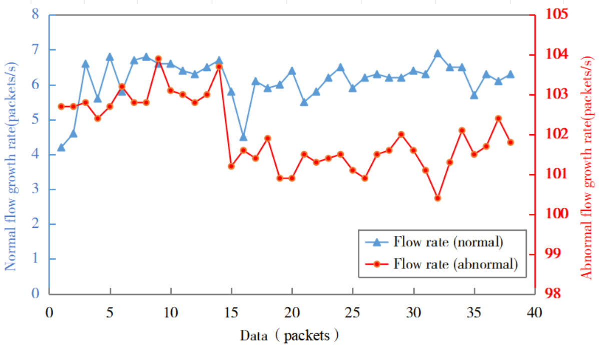


Fig. 7. Comparison of normal abnormal flow stream rates

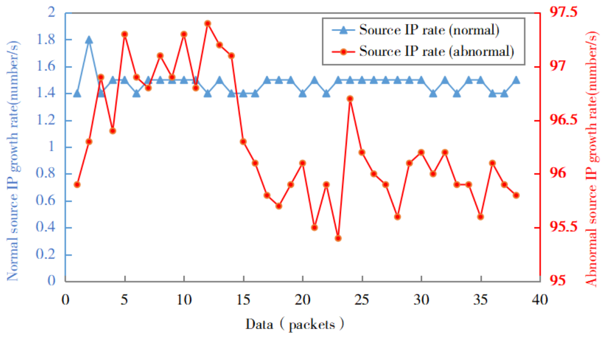


Fig. 8. Comparison of IP rate of normal abnormal traffic sources

C. *Bi LSTM model*

As it can be seen from Fig. 9, this model's accuracy gradually climbs during training and stabilizes after the 12th round with the accuracy gradually converging to 99.2%.

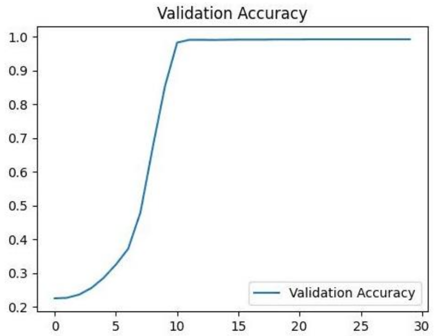


Fig. 9. Verification of accuracy

After completing the training, the validation set this model is utilized for training. As it can be seen in Fig. 10, this model is trained with a gradual decrease in the model deficiency value, which stabilizes after the 30th round and tends to zero.

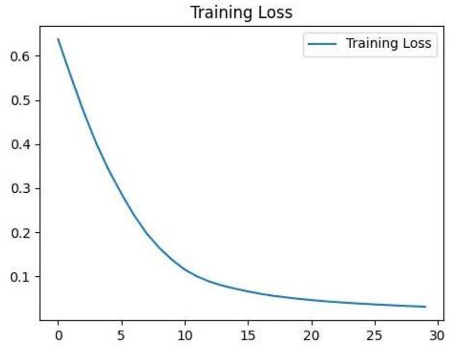


Fig. 10. Validation set missing values

When this model was tested for detection using the test set data, the accuracy of the test set in determining anomalous traffic was calculated to be 99.2%.

D. *Analysis of experimental results*

Experiments were conducted using four algorithm models, Bi LSTM, SVM, Random Forest, and LSTM, for performance analysis and comparison, with metrics of normal traffic false alarm rate 0FP, abnormal traffic false alarm rate 0FP, accuracy TP, and average elapsed time TE. And the results are shown in Table 1.

From the data in Table 1, it can be concluded that as the amount of data detected in real time increases, the Bi LSTM model takes less time to reach 0.13ms, and the accuracy of Bi LSTM for traffic monitoring is up to 99.2%, which is a significant improvement compared with other algorithms. It proves that this model can improve the judgment of traffic data features from more data, thus improving the performance of its own model.

TABLE I. COMPARISON OF EXPERIMENTAL RESULTS ON THE ACCURACY OF DIFFERENT ALGORITHMS FOR ANOMALOUS TRAFFIC VERIFICATION

mould	0FP	1FP	TP	TE (ms)
Bi LSTM	0	1.036%	99.221%	0.13036
SVM	0	2.983%	97.179%	0.24209
Random Forest	0	2.818%	97.047%	0.31254
LSTM	0	1.654%	98.016%	0.17523

Bi LSTM advantage lies in the temporal analysis and the comparison of experimental results of temporal prediction accuracy is shown in Table 2. When the interval time of the attack initiation is 0.5h, the time difference between the prediction time and the real time of the attack suffered is no more than 10s, which is regarded as a successful prediction. It can be seen that when the number of detected anomalous traffic data used for analysis is higher, the accuracy of timing prediction is higher; And the longer the time interval pattern in the periodic attack of LDDoS attack traffic, the more accurate the prediction results are.

TABLE II. COMPARISON OF EXPERIMENTAL RESULTS OF TIMING PREDICTION UNDER DIFFERENT CONDITIONS

BiLSTM	100 flows	500 flows	1000 flows
Interval 0.5h	99.23%	99.36%	99.53%
Interval 1h	99.56%	99.62%	99.73%
Interval 2h	99.65%	99.76%	99.81%

From Table 3, it can be seen that the predicted timestamp data and the real-time detected anomalous traffic data appeared at a time with good overlap. The time of the anomalous traffic data appeared at the time of prediction failure is also not much different from the time of this anomalous traffic actually appeared, and the prediction accuracy rate reaches 99.8%, which proves that this scheme has a relatively good performance in timing prediction.

TABLE III. COMPARISON OF THE TIME OF OCCURRENCE OF ABNORMAL FLOW WITH THE TIME OF PREDICTION

BiLSTM	Time of appearance of this attack	Predicted time of next attack
Time point 1	12:26:01	12:56:11
Time point 2	12:56:01	13:26:09
Time point 3	13:26:01	13:56:30
Time point 4	13:56:01	14:26:10
Time point 5	14:26:01	14:56:11

Experiments show that when a host on the SDN platform is subjected to an L DDoS attack, the accuracy of the timing analysis and the prediction of the future emergence time using Bi LSTM is as high as 99.8%. The accuracy improves as the time difference between the emergence of the anomalous traffic increases and the number of time points used to collect the prediction.

V. 5 CONCLUSIONS

In this paper, we propose a BiL STM-based L DDoS detection scheme in SDN, which is applied to preprocess the network traffic data and train a model to identify malicious flows. The controller uses the ryu controller under the control of OpenFlow protocol to realize the operation of the flow table, and the experimental results show that this method has high accuracy and can effectively detect L DDoS attacks in SDN.

The innovation of this paper is to build a model to detect L DDoS using BiL STM and record the detection results. We built an SDN platform and turned on periodic low-rate DDoS attacks. At the same time, the author began to collect traffic data in real time and extracted traffic features, after which the traffic features were input into the model for anomaly determination. Then, the time features were input as vectors into the BiL STM model for timing analysis, and the timestamped feature values of the previous portion about anomalous traffic were analyzed through the timing analysis for accurately predicting the time of occurrence of the anomalous traffic afterward and appearance time of the traffic.

The experimental results show that the method has a high accuracy of 99.2%, which can effectively detect periodic L DDoS attacks in SDN, while the accuracy in timing prediction is up to 99.8%. The summarized results of the performances of this experiment prove that the method has good performance.

By deploying BiL STM models in controllers in SDN networks, DDoS attack traffic with periodic low rates can be identified, thus contributing to the reliability and stability of SDN platforms. Future work includes improving the performance of the BiL STM model and exploring more advanced deep learning methods to detect L DDoS attacks with periodicity on SDN platforms.

ACKNOWLEDGMENT

This work was supported by the Gansu Provincial Natural Science Foundation project "Research on Anti Adaptive Attack of Consensus Algorithm Based on SM2 Linkable Ring Signature" No.22JR5RA356.

REFERENCES

[1] Radware:Data leakage will become the biggest cyber attack problem[J]. Electronic Product Reliability and Environmental Testing,2017,35(03):35.

[2] Jiang Wanming,Guo Chun,Jiang Chaohui. A low rate DDoS attack detection method based on BiLSTM[J]. Computer and Modernization,2020(05):120-126.

[3] Wang Juan,Wang Jiang,Jiao Hongyang et al. An OpenFlow-based real-time conflict detection and resolution method for SDN access control policies[J]. Journal of Computing,2015,38(04):872-883.

[4] Guo Sha. Research on DDoS attack detection in SDN network environment[D]. Lanzhou Jiaotong University,2021.

[5] ZHANG Zhaokun,CUI Yong,TANG Shuangzhuang et al. Research progress of software-defined networking (SDN)[J]. Journal of Software,2015,26(01):62-81.

[6] Sun Xin. Research on DDoS Attack Detection and Traceability Technology Based on SDN [D]. Nanjing University of Science and Technology,2020.

[7] JING ZHU,ZHONGDONG WU,LONGBIN DING,YANGYANG WANG. DBN-based DDoS attack detection in SDN environment[J]. Computer Engineering, 2020,46(04):157-161+182.

[8] QI Benben. Research on SDN anomaly detection based on deep learning[D]. Zhejiang Gongshang University,2020.

[9] Basit M U,Zeshan I,Zeeshan F K, et al. A Deep Learning Based Method for Network Application Classification in Software-Defined IoT[J]. International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems,2022,30(03).

[10] Ren Zhongyan,Han Li,Jia Fanxing et al.Research on low-speed port scanning detection module based on LSTM under SDN architecture[J]. Information Record Material,2023,24(02):242-245.

[11] Li Lijuan,Li Man,Bi Hongjun et al. Hybrid deep learning based multi-type low-rate DDoS attack detection method[J]. Journal of Network and Information Security,2022,8(01):73-85.

[12] Zengguang L,Xiaochun Y,Yuemei H. CPSS LR-DDoS Detection and Defense in Edge Computing Utilizing DCNN Q-Learning[J]. IEEE Access,2020,8.

[13] JADHAVN, PATIBM. low-rate DDOS attack detection using optimal objective entropy method[J]. International Journal of Computer Applications,2013,78(3): 33-38.

[14] KAUR G, SAXENA V, GUPTA J P. Detection of TCP targeted high bandwidth attacks using self-similarity[J]. Journal of King Saud University: Computer and Information Sciences, 2020, 32(1): 35-49.

[15] LIN Zhaoliang,LI Jinguo,HUANG Runyi.DDoS attack detection based on federated learning and CNN-BiLSTM in V2G networks[J]. Computer Application Research,2023,40(01):272-277.

[16] JIA Jing,WANG Qingsheng,CHEN Yongle et al. DDoS attack detection method based on attention mechanism[J]. Computer Engineering and Design,2021,42(09):2439-2445.

[17] Madoga,Xu Zhen,Huang Liang,Jing Yang,Naisan Li. An SDN controller blind DDoS attack protection method and system [P]. cn103561011a, 2014-02-05.

[18] Yan Q, Yu R, Gong Q, et al. Software-Defined Networking (SDN) and Distributed Denial of Service (DDoS) Attacks in Cloud Computing Environments:A Survey, Some Research Issues, and Challenges[J].IEEE Communications Surveys & Tutorials,2016,8(1): 602- 622.

[19] Lee S, Kim J, Shin S, et al. Athena: A framework for scalable anomaly detection in software-defined networks [C].Proceedings of 2017 the 47th Annual IEEE/ IFIP International Conference on Dependable Systems and Networks (DSN'17).2017:249-260.

[20] Leen De Baets,Joeri Ruyssinck,Thomas Peiffer,Johan Decruyenaere,Filip De Turck,Femke Ongenae,Tom Dhaene. Positive blood culture detection in time series data using a BiLSTM network.[J]. CoRR,2016, abs/1612.00962.

[21] S. M. Mousavi and M. St-Hilaire, "Early detection of DDoSattacks against SDN controllers," in Proc. Int. Conf. Comput. .Commun.(ICNC) , Feb. 2015, pp. 77-81.