Identification of Cybersecurity Elements Based on Convolutional Attention LSTM Networks

Yingying Hu*, Runjie Liu*, Ziyu Ma

*Supercomputer Center, Henan, China

*ierjliu@zzu.edu.cn

Abstract: As the first step of cybersecurity situational awareness, the accuracy of cybersecurity element recognition will directly affect the results of situational understanding and situational prediction. In this paper, we propose a network element recognition method based on the convolutional attention mechanism combined with a long- and short-term memory network. The input network traffic data is successively passed through the convolutional neural network, attention mechanism, and long- and short-term memory network, which not only takes into account the influence degree of different network attributes on different network behaviors but also realizes that the feature information extracted in the early stage can be circulated in the network, thus providing a discriminant basis for the final network behaviors. To verify the effectiveness of our proposed method, we perform experimental validation on the KDD-Cup 1999 (kdd-99) dataset. The results show that our proposed method achieves an accuracy of 98.48% in the identification of network security elements. In addition to this, we also compare and analyze our proposed algorithm with other mainstream algorithms, and the results also validate the effectiveness of our proposed method.

Keywords: Attentional mechanisms, CNN, LSTM, Cybersecurity elements recognition

1. Introduction
With the continuous development of network technology, the requirements for network security are increasing [1-3] and with the increasing number of attacks and intrusions in the network, how to protect personal information and property security in the network is particularly important. Because the number of network nodes in traditional network systems is limited and there is less information about data traffic in the network, devices such as firewalls, intrusion detection systems, and network administrators can effectively monitor the security status of the network in real-time and deal with certain abnormal states in a timely manner.

However, in the era of big data, especially driven by the fifth-generation mobile communication network (5G) technology, the development of the Internet of Things (IoT) technology is also further promoted due to the low latency and high bandwidth characteristics of 5G networks. The need to interconnect all surrounding objects as network nodes so that various objects can interact with each other in real-time has led to significant changes in the traditional network size and inter-network structure. Compared to the traditional user-as-node approach, the number of current network access terminals is increasing [4], thus resulting in the exponential growth of data and traffic information in the network, and due to the continuous improvement of various network protection devices, network attacks are becoming more and more hierarchical, diverse and complex, so how to effectively carry
out network security defense is imminent. In addition, in the face of a variety of real-time network information, it is increasingly difficult for network managers to identify the factors that have a large impact on the network from the massive multi-source heterogeneous data, thus easily causing a series of problems such as untimely processing of network information, identification errors and delayed perception. Therefore, accurate identification of network security elements will play an important role in situational awareness capabilities.

2. Related work
How to effectively carry out the traffic data information in the network is going to have an important impact on the final network state analysis. It is popular to firstly pre-process the network information in the data set using different approximation algorithms so as to ignore the redundant feature information in the data in order to improve the accuracy of identification. By dividing practical network scenarios into two categories, attack defense analysis, and security measurement, the data in the network is processed in real-time by introducing Game theoretic [5] and good results have been obtained. The correlation between each attribute feature is studied to enhance the is being effect on various categories [6]. [7] used a novel feature selection technique based on rough set (RS) and hypergraph (RSHGT) theory to identify the best feature subsets and achieved good results. [8] established a network security identification system based on convolutional neural networks and achieved good experimental performance. However, with the increasing amount of multi-source heterogeneous network security information, the ability to efficiently mine and evaluate security posture elements from multi-source heterogeneous data will be limited. To solve this problem, [9] proposed a contextual inference method for security posture awareness models based on semantic ontologies and user-defined rules, and invoking ontology techniques can provide a unified formal description to solve the semantic heterogeneity problem in cybersecurity.

We extract features from the input multi-source heterogeneous network data based on the convolutional attentional LSTM model [10] to achieve the recognition and classification of different network behaviors. The convolutional neural network (CNN) extracts features from the input information through the convolutional layer; the attention mechanism adaptively adjusts the contribution of different features to the recognition result, which speeds up the convergence of the model and reduces the training time; finally, the features are input into the long-short-time network (LSTM) to achieve the continuation of the extracted early features in the network. Real-time report transmission improves the accuracy of model classification.

3. Proposed Method

3.1. Framework of model
The network security element recognition model based on convolutional attention LSTM effectively avoids the problem of overfitting through the CNN model's parameter sharing mechanism. The LSTM model avoids the long-distance dependency problem of traditional deep learning methods, and at the same time adopts the attention mechanism to effectively analyze the correlation between the input and output of the model, thus realizing the element identification. The model framework is shown in Fig 1:
The model consists of two parts:

a) CNN network-based feature extraction model: convert the string part of the kdd99 dataset into numbers, and convert the input kdd features into an 8*8 matrix for input into the convolutional neural network, and use the convolutional neural network to complete the extraction of shallow features.

b) Attention-LSTM construction: The shallow features captured by the convolutional neural network are combined with the attention mechanism to realize the important distribution of different features by calculating the probability of relevant features, so that the network always focuses on the relevant features that have a great influence on the result; in addition, in order to avoid the disadvantage that the early features cannot be utilized by the convolutional neural network in the feature extraction process, we solve the long dependency problem of features by introducing the LSTM structure. Finally, the output features extracted from the network are fully connected and classified, and the output data are input to the softmax classifier to finally determine whether the input network behavior is abnormal.

### 3.2. Algorithmic implementation

In order to accelerate the convergence of the model, we train the data batches into the network through mini-batch. Firstly, the data are encoded and input into the convolutional neural network, while the feature re-extraction structure of Attention-LSTM is input, and the error is calculated by cross-entropy function, as in Eq. 1. Finally, the classification accuracy is obtained by full connection operation. Experiments show that 3*3 convolutional kernels have better feature extraction capability, so we set the convolutional kernels to 3*3, and the algorithm is as follows:

$$L = - \sum_{i=1}^{N} y^{(i)} \log \hat{y}(i) + (1 - y^{(i)}) \log (1 - \hat{y}(i))$$

(1)
1) The first convolution uses 16 convolution kernels of the same size, so the size of the kernels is 3*3*16; set the value of the Stride of the convolution operation is 1 and set the padding = 1. And use RELU for the first convolution after the result of the nonlinear operation, the output size is 8*8*16;

2) Pooling after the first convolution: kernel size is 2*2, the output size is 4*4*16;

3) the second convolution: the use of 32 convolution kernels, so the size of the convolution kernels; the use of RELU on the second convolution of the data after the nonlinear processing;

4) Pooling after the second convolution;

5) Use softmax functions to normalize weights, as in Eq. 2;

\[ a_i = \frac{e^{sim_i}}{\sum_{j=1}^{m} e^{sim_j}} \]  

(2)

Where \( a_i \) is the value of i corresponding weight factor.

4. Experiment

The dataset used in this paper is KDD-Cup99[11], which contains a total of 41 conditional attributes and one label attribute, and the distribution Tab of intrusions of each category in the dataset is shown in Tab 1. Among them, the label attributes can be classified into five types: probe, Dos, U2R, R2L, and Normal. In this paper, some sample features in the dataset are selected for training, and the data contains 345814 training samples and 148206 test samples in total. In this paper, we validate our proposed method based on the PyTorch platform.

| Types of attacks | Training data | Test data |
|------------------|---------------|-----------|
| Nomal            | 345814        | 148206    |
| Probe            | 8214          | 8332      |
| Dos              | 335244        | 107040    |
| U2R              | 104           | 456       |
| R2L              | 2252          | 32378     |

Tab.1 Distribution of intrusive behavior

To verify the validity of the method proposed in this paper, we use the accuracy rate of the test set recognition as an indicator to judge the classification ability of the model proposed in this paper. The accuracy rate is calculated by the following formula.

\[ A = \frac{TP + TN}{TP + TN + FP + FN} \]  

(3)

where: A denotes accuracy, TP denotes the number of correctly classified attack samples, TN denotes the number of correctly classified normal samples, FP denotes the number of misclassified attack samples, and FN denotes the number of misclassified normal samples.

By comparing our proposed method with that proposed by previous researchers, as shown in Fig 2, the experimental results show that our proposed network model achieves better performance in recognition accuracy than other classification algorithms;
Fig. 2 Comparison of the accuracy of different algorithms

5. Conclusion
In this paper, we study how to effectively identify anomalous traffic information in a network. In addition, we introduce an attention mechanism to identify and transmit important features, considering that the input data sequences show different contributions to the final result. Therefore, we propose an element recognition method based on the convolutional attention LSTM network, and by conducting experiments on kdd99 dataset, the accuracy reaches 98.48%, and the experimental results verify the effectiveness of our proposed method. Compared to the previous algorithm, higher recognition accuracy is achieved, so that our proposed model can truly re-reflect whether there are anomalies in the network traffic, which is of some practicality. In the next work, we will study the root cause analysis of multi-indicator fusion alarms.

References
[1] Sngo, H H 2020 Proc. of the 3rd Int. Conf. on Mechatronics and Intelligent Robotics Procedia Computer Science (kunning) (Amsterdam: ELSEVIER SCIENCE BV) pp 84-87
[2] Mohanta B K, Jena D, Satapathy U and Patnaik S 2020 Survey on IoT Security: Challenges and Solution using Machine Learning, Artificial Intelligence and Blockchain Technology Internet of Things 11 p 100227
[3] Yuan J and Luo X 2019 Regional energy security performance evaluation in China using MTGS and SPA-TOPSIS Science of The Total Environment 696 p133817
[4] McGinthy J Wong M L J and Michaels A J 2019 Groundwork for neural network-based specific emitter identification authentication for IoT J. IEEE Internet of Things 6 p 6429
[5] Liang X and Xiao Y 2012 Game theory for network security IEEE Communications Surveys & Tutorials 15 p 472
[6] Kayacik H G, Zincir-Heywood A N and Heywood M I 2005 Proc. of the 3rd annual Conf. on privacy, security and trust (New Brunswick) Vol. 94 (Saarland: Schloss Dagstuhl) pp 1723-1722
[7] Raman M G, Kirthivasan K and Sriram V S 2017 Development of rough set–hypergraph technique for key feature identification in intrusion detection systems Computers & Electrical Engineering 59 p 189
[8] Gu Z, Nazir S, Hong C and Khan S 2020 Convolution neural network-based higher accurate intrusion identification system for the network security and communication Security and Communication Networks 2020
[9] Xu G, Cao Y, Ren Y, Li X and Feng Z 2017 Network security situation awareness based on
semantic ontology and user-defined rules for Internet of Things IEEE Access 5 p 21046

[10] Hochreiter S and Schmidhuber J 1997 Long short-term memory Neural computation 9 p 1735

[11] Pfahringer B Winning the KDD99 classification cup: bagged boosting ACM SIGKDD Explorations Newsletter 1 p 65