Classification of Network Attacks with LSTM Architecture Method

Fuat TÜRK[1], *

[1] *Faculty of Engineering, Computer Engineering, Çankırı Karatekin University, Çankırı, Turkey*

Abstract

Detection of unknown attacks in network traffic is an extremely important issue due to the increasing dependency of systems on the internet today. Until recently, traditional machine learning models were generally preferred for network security detection. Nowadays, it is not being preferred as much as before. Even though machine learning models can acquire a wide variety of features, they require the manual design of network traffic, obtaining a low-rate accuracy. On the other hand, an attack detection system is a very critical situation for protecting information from malicious treatment. Attack detection systems are a system mechanism that can classify data as normal or attacked. The LSTM model is proposed for systems that can operate with higher accuracy as an alternative to classical machine learning models. The proposed LSTM model can automatically learn the basic features of the hierarchy and does not require manual design principles. This model has been tested with the publicly available NSL-KDD dataset acquiring 80% accuracy. Experimental results show that the model can be used as an alternative to other methods.

Keywords: *Network Attacks, LSTM architecture, NSL-KDD data set, Network Attack classification*

1. Introduction

Today, network security has become a more important issue due to the increasing use of network-based devices. With the development of internet technology, internet services offered to people have also diversified. Therefore, the probability of facing various security threats is more likely to increase [1]. In addition, intrusion detection into network systems is becoming more and more difficult [2]. In particular, how to detect unexpected malicious network traffic is an important issue. [2-3].

Network traffic can be divided into two basic categories, normal traffic, and malicious traffic. From this point of view, attack detection can be considered a classification problem. By effectively detecting and blocking malicious traffic, and improving the performance of classifiers, system accuracy can be greatly improved. Machine learning (ML) methods are widely used in intrusion detection to identify malicious traffic. However, these methods require basic learning and feature selection. On the other hand, they have difficulties in attribute selection. Also, they cannot effectively solve the huge intrusion data classification problem that leads to low recognition accuracy and a high false alarm rate. Nowadays, deep learning-based intrusion detection methods have started to replace ML methods. [4-5].

Shrivas and Devangan performed a highly accurate study on the NDSL-KDD dataset using the Artificial Neural Network (ANN) and Bayesian Net with Gain Ratio (GR) feature selection method [6]. Abhirop et al. tried three different ML algorithms. In this study, Support Vector Machine (SVM), Naive Bayes (NB) and Neural Network (NN) methods were used to detect the attack system. The researchers opted for the open-source protocol to collect group features to generate the training data. ML techniques were based on five features, and experimental results show that SVM gives a low accuracy rate compared to the last two classifiers. [7]. In the study of Serinelli et al., a passive defense system aimed at monitoring and protecting computer networks is introduced. It has also been tried to provide guidance on the selection and execution of methodology for training Machines and Deep Learning models. Their goal is to minimize the Attack Undetected percentage, False Alarm Rate percentage, and overall test time [8]. Staudemeyer and Omlin have tested the performance of the Long Short-Term Memory (LSTM) network in classifying intrusion traffic. The study results indicate that LSTM can learn all network attacks hidden in the training data. [9].

*Corresponding author. *e-mail address: fuatturk@karatekin.edu.tr*

2. Materials and Methods

2.1. NSL-KDD dataset

NSL-KDD is a dataset designed by Tavalaee et al. [10]. This dataset is open to access for everyone. It contains a total of 37 attack types, where 27 attacks are used by the test dataset and 23 attacks are used by the training dataset for experiments. It includes 41 features and 5 network attacks in total. There are 5 types of network attacks one of which is normal and the other 4 are Research Attacks (Probe), Denial of Service attacks (DoS), User-to-Root (U2R), and Remote-to-Local (R2L) [11,12]. The removal of excess records of NSL-KDD helps the classifier produce unbiased results, and it is its most important advantage over other datasets.

2.2. LSTM Architecture

LSTM networks were designed by Hochreiter and Schmidhuber to predict special cases that Recurrent Neural Networks (RNN) cannot solve. A structure is available in LSTM networks to calculate hidden states. The memory cells in the LSTM are the structures that hold the previous state and the input information. These cells are the mechanisms that decide which data to keep or which data to delete. Then they merge the previous state with the current memory. With such an approach, long-term dependencies are eliminated and data sets are maintained. The LSTM structure is given in Figure 1. The gate given as input controls when the new information should enter the memory, the forget-memory gate controls the forgetting of the existing information and the recall of new data. The final stage decides when the information in the cell will be used at the exit [13].

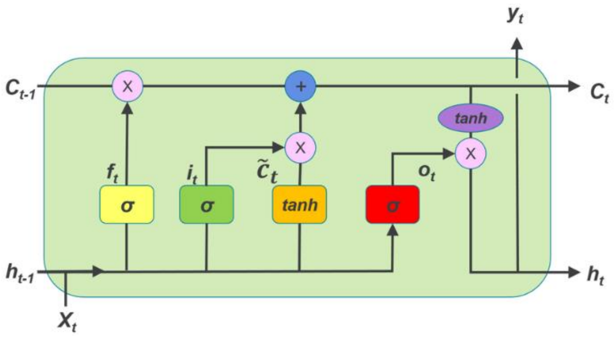


Figure 1. LSTM architecture [14]

The basic structure of the proposed LSTM architecture is shown in Figure 2. The output is arranged in 5 types with the softmax function. Unit means the size of the inner cells in LSTM. Here, the unit value is set to 50.

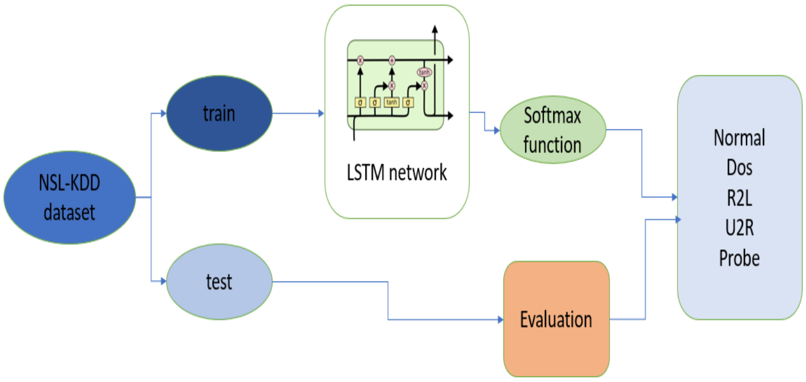


Figure 2. Proposed LSTM architecture and workflow diagram

3. Results and Discussion

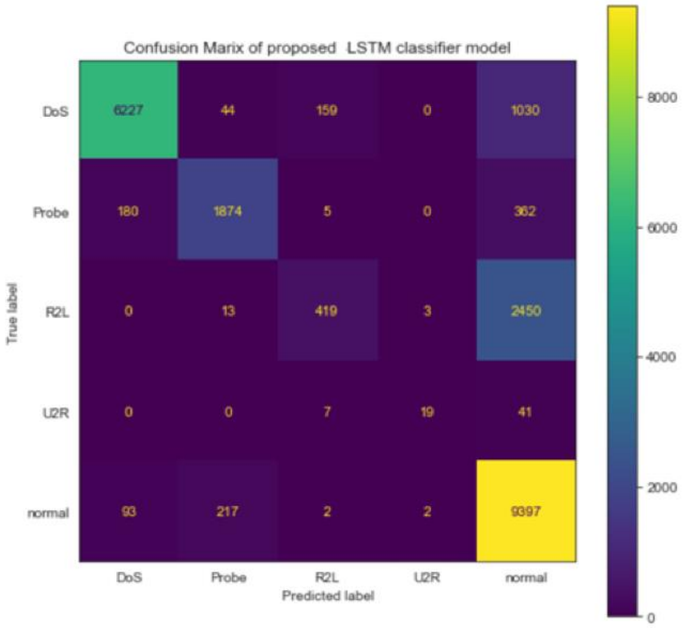
3.1. Performance metrics with LSTM architecture.

The performance metrics obtained as a result of training the NSL-KDD data set with the LSTM network are shown in Table 1.

Table 1. LSTM architecture performance metrics

	Precision	Recall	F1-Score
Dos	0.83	0.96	0.89
Probe	0.77	0.87	0.82
R2L	0.15	0.71	0.24
U2R	0.28	0.79	0.42
Normal	0.97	0.71	0.82
Accuracy(avg)		0.80	

The confusion matrix is shown in Figure 3. It is seen that the success of the R2L and U2R attack types is low and is confused with the normal type. When we look at other types, we can say that success is higher. In Figure 4 the ROC curve analysis for the LSTM classifier is shown. When the ROC analysis is carefully examined, it can be said that R2L is a comparatively low area, and the calculated areas for the other types are close to each other. However, we can talk about classification success because all types have a curve above the mid-level area.



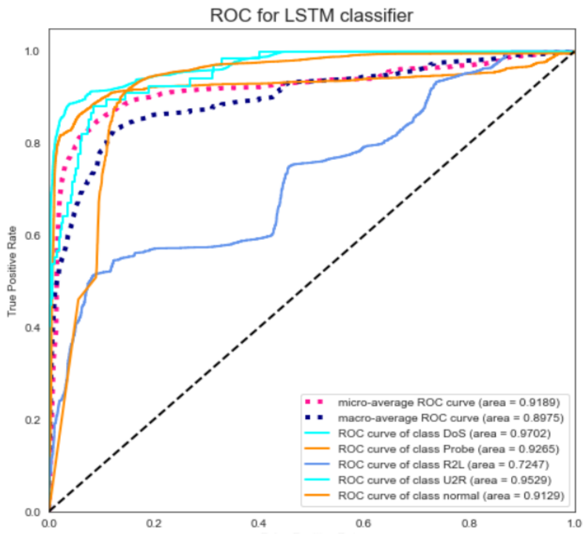


Figure 3. LSTM architecture confusion matrix values

Figure 4. ROC analysis graph for LSTM architecture

3.2. Evaluation results

As a result of the data obtained from the existing graphics and tables, it can be recommended to use LSTM networks as an alternative to machine learning and classical Convolutional Neural Networks in the detection of network attacks. Here, studies can be carried out to increase the detection rates of R2L and U2R classes with low accuracy values. At this stage, the selection of hyperparameters, and updates on the network structure design may be recommended. Apart from this, the NSL-KDD data set can be merged with other data sets or the samples can be increased in the number of classes with low success. As a result of these processes, I think that networks trained with high accuracy can be a good application option for attack detection and classification, especially in all server-based systems.

References

[1] IEEE Xplore Full-Text PDF: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8988230. Accessed 20 Jul 2022.

[2] Zarpelão, BB., Sanches, M.R., Kawakani C.T., Carlisto D. A. *A survey of intrusion detection in Internet of Things*, 2017. Doi: 10.1016/j.jnca.2017.02.009

[3] Network intrusion detection | IEEE Journals & Magazine | IEEE Xplore. https://ieeexplore.ieee.org/abstract/document/283931?casa_token=kjdXNtV8njIAAAAA:09FAGw-yog7dsRJcdPlDmUpnqH8429q5GpdGU1upj_Pi_TEdCj_QCTdoWOhuIn0Nc7Z8jytR7b8. Accessed 20 Jul 2022

[4] Kuang, F., Xu, W., Zhang, S. A novel hybrid KPCA and SVM with GA model for intrusion detection. *Applied Soft Computing*, 18:178–184, 2014. Doi: 10.1016/j.asoc.2014.01.028

[5] Garg, S., Batra, S. A novel ensembled technique for anomaly detection. International Journal of *Communication Systems*, 30: e3248, 2018. Doi:10.1002/DAC.3248

[6] KumarShrivas, A., Kumar, D.A. An Ensemble Model for Classification of Attacks with Feature Selection based on KDD99 and NSL-KDD Data Set. IJCA 99:8–13., 2014. Doi:10.5120/17447-5392

[7] IEEE Xplore Full-Text PDF: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8600196. Accessed 20 Jul 2022.

[8] Serinelli, BM., Collen A., Nijdam, NA. Training Guidance with KDD Cup 1999 and NSL-KDD Data Sets of ANIDINR: Anomaly-Based Network Intrusion Detection System. *Procedia Computer Science*, 175:560–565, 2020. Doi: 0.1016/J.PROCS.2020.07.080

[9] Staudemeyer, RC., Omlin, CW. Evaluating performance of long short-term memory recurrent neural networks on intrusion detection data. ACM International Conference Proceeding Series 218–224, 2013.https://doi.org/10.1145/2513456.2513490

[10] Tavallaee, M., Bagheri, E., Lu, W., Ghorbani, AA. A detailed analysis of the KDD CUP 99 data set. IEEE Symposium on Computational Intelligence for Security and Defense Applications, CISDA, 2009. Doi:10.1109/CISDA.2009.5356528

[11] A Revıew On Kdd Cup99 And Nsl Nsl-Kdd Dataset.: EBSCOhost. https://web.s.ebscohost.com/ehost/pdfviewer/pdfviewer?vid=0&sid=63cfb8b5-e09c-4bf3-b523-9c94f4219456%40redis. Accessed 20 Jul 2022.

[12] A Comparative Analysis of Intelligent Techniques for Detecting Anomalous Internet Traffic - ProQuest. https://www.proquest.com/openview/f57c4b057a2a89dbd1757e77abf5812d/1?pq-origsite=gscholar&cbl=18750. Accessed 20 Jul 2022.

[13] Hochreiter S, Schmidhuber J (1997) Long Short-Term Memory. Neural Computation 9:1735–1780. https://doi.org/10.1162/NECO.1997.9.8.1735

[14] Uzun Kısa Dönemli Bellek (Long / Short Term Memory) (LSTM). Available at: https://medium.com/@batincangurbuz/uzun-k%C4%B1sa-d%C3%B6nemli-bellek-long-short-term-memory-lstm-c526980c28b1, 2022.