Using Long-Short-Term Memory Based Convolutional Neural Networks for Network Intrusion Detection

Chia-Ming Hsu, He-Yen Hsieh, Setya Widyawan Prakosa, Muhammad Zulfan Azhari, and Jenq-Shiou Leu(✉)

National Taiwan University of Science and Technology, Taipei, Taiwan
{d10402101,m10502103,d10702804,
d10702805,jsleu}@mail.ntust.edu.tw

Abstract. The quantity of internet use has grown dramatically in the last decade. Internet is almost available in every human activity. However, there are some critical obstacles behind this massive development. Security becomes the hottest issue among the researchers. In this study, we focus on intrusion detection system (IDS) which is one of the solutions for security problems on network administration. Since intrusion detection system is a kind of classifier machine, it is allowed to engage with machine learning schemes. Related to this reason, the number of studies related to utilizing machine learning schemes for intrusion detection system has been increased recently. In this study, we use NSL-KDD dataset as the benchmark. Even though machine learning schemes perform well on intrusion detection, the obtained result on NSL-KDD dataset is not satisfied enough. On the other hand, deep learning offers the solution to overcome this issue. We propose two deep learning models which are long-short-term memory only (LSTM-only) and the combination of convolutional neural networks and LSTM (CNN-LSTM) for intrusion detection system. Both proposed methods achieve better accuracy than that of the existing method which uses recurrent neural networks (RNN).

Keywords: Intrusion detection system · Deep learning · Long-short term memory · NSL-KDD dataset

1 Introduction

With increasing the number of internet users, the global internet use has escalated. The internet is very helpful almost in every human activity. However, it has a lot of vulnerability in term of security. The researchers have been handling the vulnerability, but the attacks become more dangerous day by day. An Intrusion Detection System (IDS) is one of the best inventions in computer security because the number of researchers who work for developing the performance of

J.-L. Chen et al. (Eds.): WiCON 2018, LNICST 264, pp. 86–94, 2019.
https://doi.org/10.1007/978-3-030-06158-6_9

intrusion detection is high. Furthermore, intrusion detection is the most fundamental part for network system administrator to monitor various malicious behavior inside a computer networking. Then, based on the method that is used by intrusion detection, it is considered as a classifier machine. Intrusion detection identifies every single network traffic and classifies it into which kind of category it belongs to, normal or malicious traffic. Thus, intrusion detection is able to utilize machine learning schemes to enhance its accuracy during classifying.

Even though conventional machine learning schemes are highly used for intrusion detection, they cannot present the result optimally. So, it triggers the researchers to apply deep learning to overcome this such an issue. The result that they can achieve is outstanding. Many of researchers use NSL-KDD dataset [1,2] as the benchmark as for the validation and evaluation of their implementation. In this study, we utilize two deep learning models in intrusion detection and NSL-KDD dataset as the benchmark as well. The first model is Long short-term memory (LSTM) which is used as the baseline and basic model. The second is the combination of convolutional neural networks (CNN) and LSTM is applied in this study. As a result, both our proposed methods achieve better accuracy than that of existing methods, particularly for KDDTest^{-21}.

We organize this paper as follows: Sect. 2 list of existing works related to the machine learning and deep learning implementation on intrusion detection. Next is Sect. 3 which describes our proposed methods. Afterward, Sect. 4 presents result and evaluation. The last section infers the work that we have done and discusses future works of our implementation.

2 Related Work

There are many researchers that employ various machine learning schemes. For instance, Kuang *et al.* [3] propose a novel support vector machine (SVM) which combine kernel principal component analysis (KPCA) and genetic algorithm (GA) for intrusion detection and use KDD Cup99 [4] as the dataset. Then, Reddy *et al.* [5] also use SVM as well for intrusion detection. Then, they adopt effective discriminant function to increase the accuracy.

Meanwhile, Ingre *et al.* [6] analyze the performance of NSL-KDD using Artificial Neural Networks (ANN). Then, Farnaaz *et al.* [7] propose intrusion detection system using Random Forest (RF) and NSL-KDD datasets to evaluate the performance of their model. In addition, Zhang *et al.* [8] build network intrusion detection system which is also based on RF but they use KDD Cup99 to assess the achievement of their model. However, there are some weaknesses in machine learning scheme. For instance, feature engineering and selection do not perform well for extracting the most representative features in big data and cause the decreasing of accuracy [9]. Since the intrusion detection encounters massive data in the traffic network, these classical machine learning schemes do not yield a better result.

Recently, the number of research on deep learning which is a branch of machine learning has risen. It induces deep learning implemented in many fields

[10–12] and intrusion detection system is no exception. For instance, the study of classifying intrusion detection using deep learning has been done by performing Recurrent Neural Networks (RNN) [13]. Authors have constructed the approach for classification task on NSL-KDD dataset and confirmed that deep learning scheme promises better result compared to traditional machine learning schemes.

From the fact that RNN can be used for Intrusion Detection System (IDS) and it gives promised result for classification the intrusion. The scheme to employ Long Short-Term Memory (LSTM) [14] for intrusion detection is proposed in this paper. The proposed scheme is evaluated on NSL-KDD dataset and we also compare it with RNN-IDS proposed by [13].

3 Methodology

In this study, we propose two deep learning models that we have evaluated on NSL-KDD dataset. The first model is an LSTM-only model which views the dataset as the time series while another model is CNN-LSTM which is basically almost the same as LSTM-only but in this model, we perform extracting important features vectors by using CNN.

3.1 Dataset Description

The NSL-KDD dataset was developed in 2009 and it has been utilized massively by researchers for the benchmark of intrusion detection experiments. The NSL-KDD dataset has refined KDD Cup99 dataset which has some drawbacks [15] that can affect the accuracy of the model. In addition, NSL-KDD has some the advantages such as training set not containing redundancy records and test set not containing duplicate records [1]. The NSL-KDD dataset consists of the KDDTrain^{+} as the training set while for the testing set, it has KDDTest^{+} and KDDTest^{-21}. There are 41 features and 1 additional feature as a label for each record. For the experiments, we apply two models of classification. The first model is binary classification which consists of two categories which are normal and abnormal illustrated in Table 1 while another model is five-categories classification which contains data such as normal, DoS (Denial of Service attacks), R2L (Root to Local attacks), U2R (User to Root attacks), and Probe (Probing attacks) as shown in Table 2. Moreover, KDDTest^{-21} is more difficult to be classified than that of KDDTest^{+}.

Table 1. Binary classification in NSL-KDD dataset-2 categories

	Total	Normal	Abnormal
KDDTrain^{+}	125973	67343	58630
KDDTest^{+}	22544	9711	12833
KDDTest^{-21}	11850	2125	9698

Table 2. Different classification in NSL-KDD dataset-5 categories

	Total	Normal	DoS	Probe	R2L	U2R
KDDTrain^{+}	125973	67343	45927	11656	995	52
KDDTest^{+}	22544	9711	7460	2421	2885	67
KDDTest^{-21}	11850	2125	4344	2402	2885	67

3.2 Data Preprocessing

Since LSTM is a variant of RNN, the input value must be a numerical value. NSL-KDD dataset contains three non-numerical features namely, `protocol_type`, `service`, and `flag`. These three features are converted into numerical form by using one-hot-encoding. Furthermore, the range of value in some features varies widely such as in `duration`, `src_byte`, and `dst_byte`. Thus, we need to normalize these features by employing feature scaling.

3.3 Long-Short Term Memory (LSTM)

LSTM is a special variant of RNN architecture which is able to learn long-term dependencies. LSTM is a network which is composed of cells (LSTM units) that are connected to each other. An LSTM unit consists of three kinds of the gate such as input gate, output gate, and forget gate as illustrated in Fig. 1.

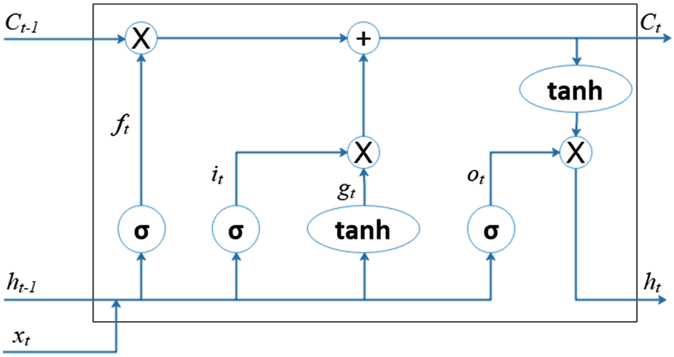

Fig. 1. LSTM Unit

Based in Fig. 1, a LSTM unit gets three input from the last step. The first is x_t which is a feature at time step t. The next is h_{t-1} which is the hidden unit from the last time step and the last is a memory cell that is represented by C_{t-1} which containts the information of previous steps. Then, input, output, and forget gate are represented by i_t, o_t, and f_t respectively at time step t and each gate has its own function. The forget gate gets rid of the information from the cell state based on h_{t-1} and x_t. Then, the input gate updates the information of memory cell by using i_t and g_t which is a hyperbolic tangent *(tanh)*. C_t is the new value of memory cell. The last is output gate that decides what the output looks like. The equation of all computation in a LSTM unit can be written as follows:

$$f_t = \sigma(W_{xf}x_t + W_{hf}h_{t-1} + b_f) \tag{1}$$

$$i_t = \sigma(W_{xi}x_t + W_{hi}h_{t-1} + b_i) \tag{2}$$

$$g_t = tanh(W_{xc}x_t + W_{hc}h_{t-1} + b_c) \tag{3}$$

$$C_t = f_t * C_{t-1} + i_t * g_t \tag{4}$$

$$o_t = \sigma(W_o x_t + W_{ho}h_{t-1} + b_o) \tag{5}$$

$$h_t = o_t * tanh(C_t) \tag{6}$$

Where W represents the weight of the gate and b denotes the bias.

3.4 Convolutional Neural Networks

CNN is a feed-forward artificial neural networks that can be applied to various schemes including classification and feature extraction. In this work, CNN is designed to be the feature extraction method. To obtain a robust feature that represents each class in the database, CNN is utilized before applying LSTM. Furthermore, LSTM receives a representative feature that can enhance the performance of our proposed scheme. In our evaluation, we will show the difference between the entire approach using CNN for feature extraction and without employing it.

3.5 Proposed Schemes

LSTM-Only Implementation. Figure 2 illustrates the implementation steps of LSTM-only model. Before we train the model, we preprocess the data. Then, we fit the data on the model to be trained. There are two layers in the LSTM-only model with 640 hidden nodes. The forget bias of each LSTM layer is set to 1. Once the training stage is done, we evaluate the proposed approach using the testing data to get the detection result.

CNN-LSTM Implementation. Figure 3 shows the implementation steps of CNN-LSTM model. We use the convolutional neural networks to obtain a set of robust features before applying LSTM. There are two convolutional layers with 32 kernel filters in each layer following by max pooling layer. Furthermore, we apply LSTM described above with the extracted features from convolutional neural networks.

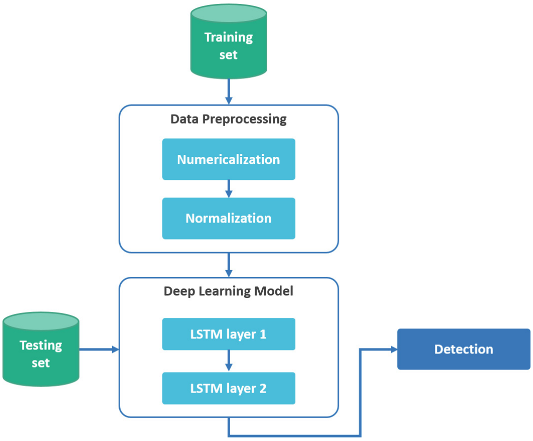

Fig. 2. Diagram of proposed method LSTM-only

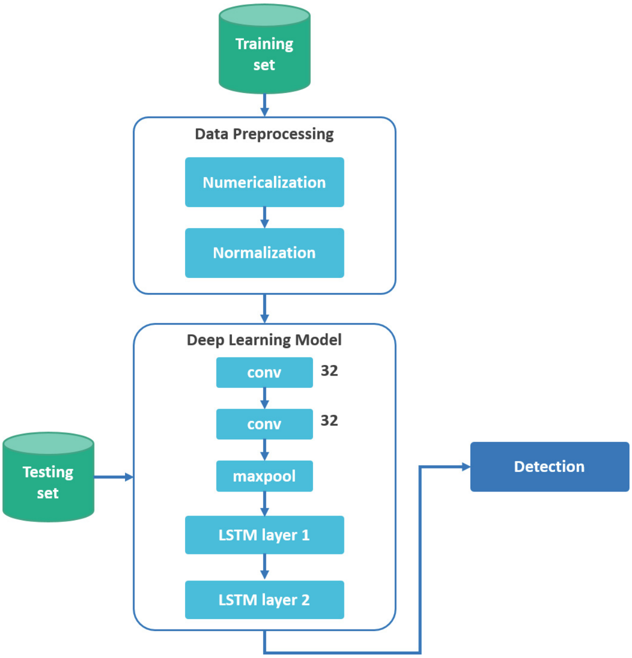

Fig. 3. Diagram of proposed method LSTM-only

4 Result and Discussion

After conducting experiments on NSL-KDD dataset, we compare our proposed methods to RNN-IDS [13] and the outcome of proposed methods perform higher accuracy both of KDDTest$^+$ and KDDTest^{-21} which is more complicated to

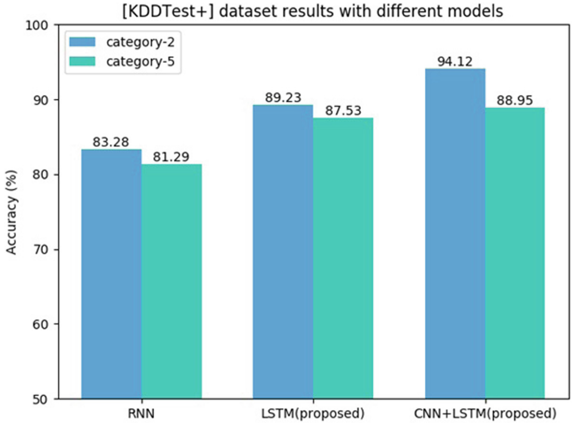

Fig. 4. The result of experiments on KDDTest^{+}

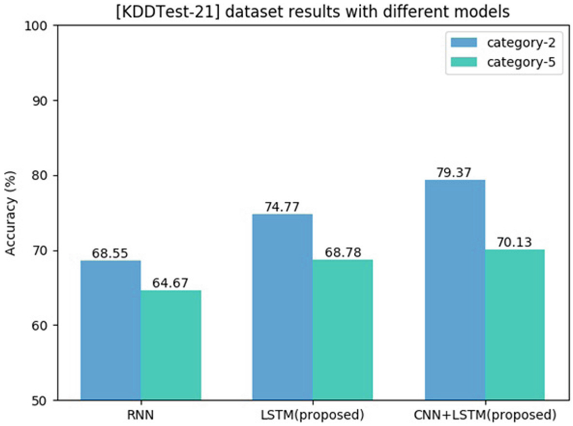

Fig. 5. The result of experiments on KDDTest^{-21}

be tested. Figure 4 depicts the experiment result on KDDTest^{+}. The result of LSTM-only and CNN-LSTM achieve higher accuracy for category-2 and category-5 than that of RNN-IDS which only reaches 83.28% and 81.29% for category-2 and category-5 respectively. LSTM-only obtains 89.23% and 87.53% for category-2 and category-5 respectively. Then, the second proposed method, CNN-LSTM gets higher accuracy with 94.12% and 88.95% for category-2 and category-5 respectively.

Figure 5 presents the experiment result on KDDTest^{-21}. Even though it is difficult to do classifying on KDDTest^{-21}, the proposed methods can perform well and surpass the performance of RNN-IDS. CNN-LSTM still obtains the highest accuracy with 79.37% and 70.13% for category-2 and category-5 respectively.

Then, LSTM-only also outpaces the outcome of RNN-IDS with 74.77% and 68.78% while RNN-IDS cannot gain 70% of the accuracy.

5 Conclusion

In this paper, we propose two deep learning models which are LSTM-only and CNN-LSTM to classify the packet traffic. To evaluate proposed methods, we conduct the experiment on NSL-KDD dataset which is often used by researchers for the benchmark. NSL-KDD dataset contains two test sets named KDDTest^{+} and KDDTest^{-21} which is hard to be classified. By utilizing LSTM, we can achieve higher accuracy on both test sets than that of the existing method. Moreover, after implementing CNN for feature extraction before LSTM layer, the accuracy of proposed method increases significantly.

References

1. Revathi, S., Malathi, A.: A detailed analysis on NSL-KDD dataset using various machine learning techniques for intrusion detection. Int. J. Eng. Res. Technol. **2**, 1848–1853 (2013)
2. Dhanabal, L., Shantharajah, S.P., Dr.: A study on NSL-KDD dataset for intrusion detection system based on classification algorithms. In: International Journal of Advanced Research in Computer and Communication Engineering, vol. 4, pp. 446–452 (2015)
3. Kuang, F., Xu, W., Zhang, S.: A novel hybrid KPCA and SVM with GA model for intrusion detection. Appl. Soft Comput. **18**, 178–184 (2014)
4. Hettich, S., Bay, S.D.: The UCI KDD Archive, University of California, Department of Information and Computer Science, Irvine, CA (1999). http://kdd.ics.uci.edu
5. Reddy, R.R., Ramadevi, Y., Sunitha, K.V.N.: Effective discriminant function for intrusion detection using SVM. In: International Conference on Advances in Computing, Communications and Informatics (ICACCI), pp. 11481153 (2016)
6. Ingre, B., Yadav, A.: Performance analysis of NSL-KDD dataset using ANN. In: International Conference on Signal Processing and Communication Engineering Systems (SPACES), pp. 9296 (2015)
7. Farnaaz, N., Jabbar, M.A.: Random forest modeling for network intrusion detection system. Procedia Comput. Sci. **89**, 213217 (2016)
8. Zhang, J., Zulkernine, M., Haque, A.: Random-forests-based network intrusion detection systems. IEEE Trans. Syst. Man Cybern. Part C (Appl. Rev.) **38**, 649–659 (2008)
9. Niyaz, Q., Sun, W., Javaid, A.Y., Alam, M.: A deep learning approach for network intrusion detection system. EAI Endorsed Trans. Secur. Saf. **16**, 21–26 (2015)
10. Xu, Y., Shi, L., Ni, Y.: Deep-learning-based scenario generation strategy considering correlation between multiple wind farms. J. Eng. **2017**, 2207–2210 (2017)
11. Wu, B.-F., Lin, C.-H.: Adaptive feature mapping for customizing deep learning based facial expression recognition model. IEEE Access **6**, 12451–12461 (2018)
12. Wang, T., Wen, C.-K., Wang, H., Gao, F., Jiang, T., Jin, S.: Deep learning for wireless physical layer: opportunities and challenges. China Commun. **14**, 92–111 (2017)

13. Yin, C., Zhu, Y., Fei, J., He, X.: A deep learning approach for intrusion detection using recurrent neural networks. IEEE Access **5**, 21954–21961 (2017)
14. Hochreiter, S., Schmidhuber, J.: Long short-term memory. Neural Comput. **9**, 1735–1780 (1997)
15. Kaushik, S.S., Deshmukh, P.R., Dr. Prof.: Detection of attacks in an intrusion detection system. Int. J. Comput. Sci. Inf. Technol. **2**(3), 982–986 (2011)