Network Intrusion Detection using Fusion Features and Convolutional Bidirectional Recurrent Neural Network

Elsevier[1]

Radarweg 29, Amsterdam

Elsevier Inc[a,b], *Global Customer Service*[b,*]

[a]*1600 John F Kennedy Boulevard, Philadelphia*
[b]*360 Park Avenue South, New York*

Abstract

This template helps you to create a properly formatted LaTeX manuscript.

Keywords: `elsarticle.cls`, LaTeX, Elsevier, template

2010 MSC: 00-01, 99-00

1. Introduction

In recent years the number of internet users is increased rapidly. Emerging sectors such as social media, education, tourism, banking and so on are now connected by www and reachable through the internet. Rapid usage of services provided by the above sectors generates a massive amount of data over the internet. Cyber attacks are also increasing quickly with the growth of the internet. Attack on valuable data may break confidentiality, integrity and availability of policies of computer security.

There are several free hacking attacking tools widely present on the internet and their usage does not require any high skills. On the other hand, multiple protection software tools against attacks are also available. Some of the protection software tools are encryption methods, antivirus, firewalls, etc. However,

[☆] Fully documented templates are available in the elsarticle package on CTAN.
[*] Corresponding author
Email address: `support@elsevier.com` (Global Customer Service)
URL: `www.elsevier.com` (Elsevier Inc)
[1] Since 1880.

these software tools are not effectively preventing all types of threats. Hacking of client's passwords, getting or modifying client's sensitive information leads to loss of credibility of business providers with their clients.

The Intrusion Detection System (IDS) is a primary security mechanism that continuously monitors and filters out the network activities affected by the attack. IDS is widely used for the detection of various types of attacks. IDSs are broadly classified into two types, one is network-based and another one is host-based IDS. Network-based IDS detects malicious activities in network traffic by analyzing individual packets. Host-based IDS detects the malicious activities from logs. Combination of network and host-based IDS are widely used in various organization. However traditional methods show low performance in the detection of unseen threats. In this work, the main concentration is on network-based IDS.

In the literature different machine learning algorithms such as Naive Bayes (NB), Support Vector Machine (SVM), Random Forest (RF) and so on are used for intrusion detection. Different feature selection algorithms are used to select significant features from the data and used as input to the machine learning algorithms. Recently, deep learning models such as Convolutional Neural Network (CNN), Recurrent Neural Network (RNN) are also used for intrusion detection. DNN models omit feature selection stage and data itself considered as input features.

In this paper, architectures of CNN and RNN are combined to get Convolutional Recurrent Neural Network (CRNN). CNN captures significant features from each feature vector and RNN captures sequential information from the input features. CRNN takes the advantages of both the architectures. Bidirectional Long Short-Term Memory (LSTM) is used as RNN. Hence, the proposed model is also referred to as Convolutional Bidirectional Recurrent Neural Network (CBRNN). Input features and their first and second-order derivatives are fused at different levels to train CBRNN.

Rest of the paper is organized as follows. Section 2 gives in detail the proposed method for intrusion detection. Section 3 discuses the results and section 4 concludes the work.

2. Network intrusion detection

The proposed network intrusion detection system consists of two stages. One is fusion feature generation and another is the design of CBRNN architecture. Each stage is explained below in brief.

2.1. Generation of fusion features

The input dataset of network intrusion is a combination of different features of the form discrete, continuous and categorical values with varying ranges and resolution. Even a few features of the dataset may be null or infinite. Current machine learning/deep learning algorithms are not compatible with such data types. Hence, the dataset is preprocessed first to get significant features suitable for classification. Further, first and second-order derivates are computed from preprocessed features of size $M \times N$ using (1) and (2).

$$d_m = \begin{cases} c_{m+1} - c_m & \text{if } m = 1 \\ c_m - c_{m-1} & \text{otherwise} \end{cases} \tag{1}$$

$$a_m = \begin{cases} d_{m+1} - d_m & \text{if } m = 1 \\ d_m - d_{m-1} & \text{otherwise} \end{cases} \tag{2}$$

The first (d_m) and second-order (a_m) derivative features are also known as delta and delta-delta (acceleration) features respectively and widely used as supplementary features in speech/speaker recognition tasks. Preprocessed features and their first and second-order derivatives are fused (concatenated) to get fusion features.

2.2. Convolutional Bidirectional Recurrent Neural Network

Two CBRNN architectures of the proposed work are given in Figure 1 and 2. Both the architectures consist of one 1D CNN layer followed by Relu activation function and 1D max-pooling operation. The output of the CNN layer is fed as

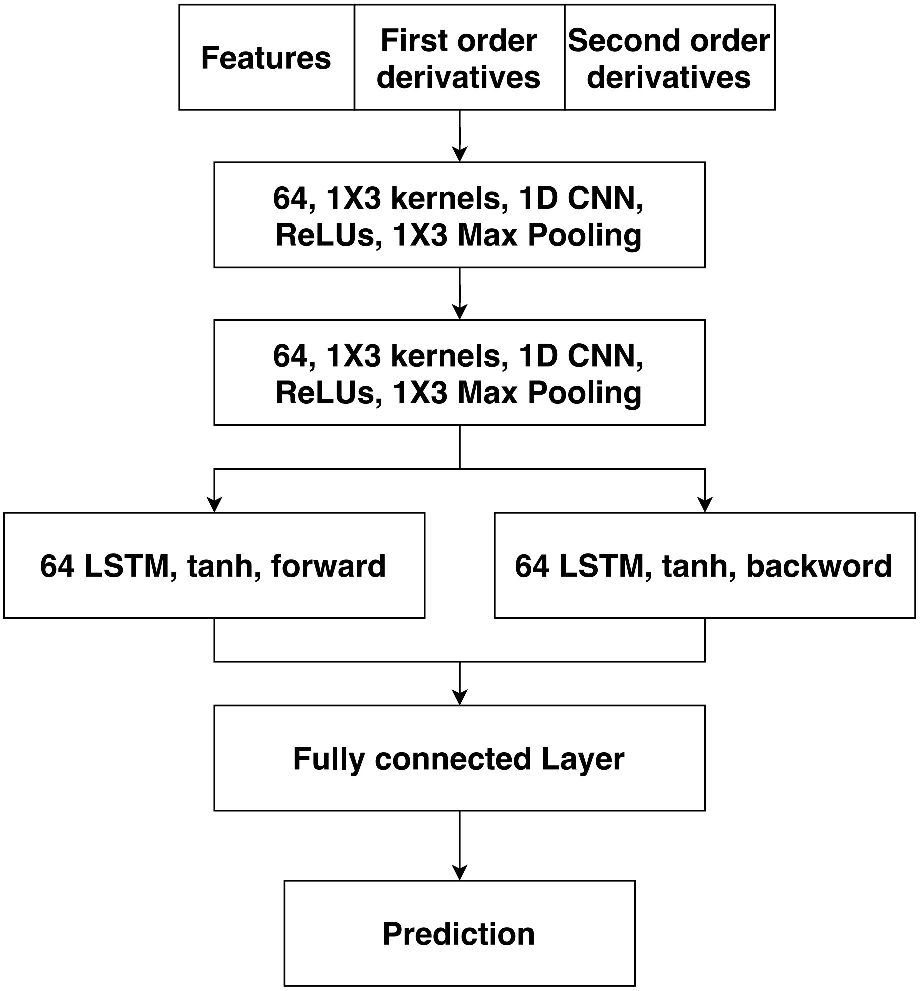

Figure 1: A boat.

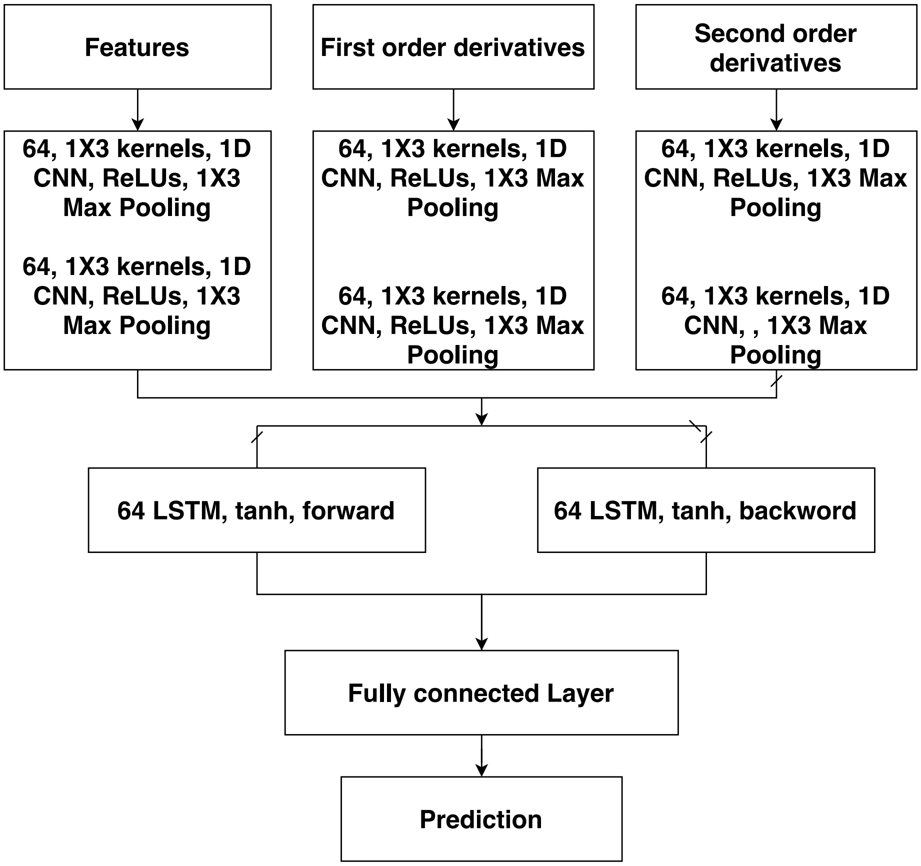
Features
First order derivatives
Second order derivatives
64, 1X3 kernels, 1D CNN, ReLUs, 1X3 Max Pooling
64, 1X3 kernels, 1D CNN, ReLUs, 1X3 Max Pooling
64, 1X3 kernels, 1D CNN, ReLUs, 1X3 Max Pooling
64, 1X3 kernels, 1D CNN, ReLUs, 1X3 Max Pooling
64, 1X3 kernels, 1D CNN, ReLUs, 1X3 Max Pooling
64, 1X3 kernels, 1D CNN, , 1X3 Max Pooling
64 LSTM, tanh, forward
64 LSTM, tanh, backword
Fully connected Layer
Prediction

Figure 2: A boat.

Table 1: Confusion matrix of all categories over the UNSW-NB15 dataset with features and First Derivative of Features using Early Fusion classifier.

Actual	Predicted										
	Normal	Generic	Exploits	Analysis	Backdoor	DoS	Fuzzers	Reconn	Shellcode	Worms	Recall()
Normal	**24735**	1	3574	8	0	6	7714	851	111	0	0.67
Generic	148	**18146**	403	0	0	12	149	10	3	0	0.96
Exploits	1019	0	**9114**	0	0	17	906	63	13	0	0.82
Analysis	16	0	658	**1**	0	0	2	0	0	0	0.00
Backdoor	15	0	544	0	**4**	0	18	2	0	0	0.01
DoS	215	6	3460	0	0	**75**	308	22	3	0	0.02
Fuzzers	753	0	1914	0	0	4	**3104**	256	31	0	0.51
Reconn	34	4	726	0	0	6	253	**2473**	0	0	0.71
Shellcode	20	6	91	0	0	2	187	26	**46**	0	0.12
Worms	6	0	34	0	0	0	4	0	0	**0**	0.00
Precision()	0.92	1.00	0.44	0.11	1.00	0.61	0.25	0.67	0.22	0.00	

Table 2: Performance of our proposed methods for Binary Classification using the UNSW-NB15 Dataset.

Method	Order of Derivative	Training Accuracy	Validation Accuracy
Early Fusion	First	89.24	75.67
	Second	91.04	78.58
Late Fusion	First	88.07	75.63
	Second	89.67	76.54

input to a bidirectional LSTM layer, the output of the bidirectional LSTM is input to the fully connected output layer with a sigmoid or softmax activation function. Each layer of CBRNN architecture is explained below in brief.

2.2.1. CNN layer

In this work, there are two ways are proposed to consider input to the CNN: preprocessed features and their first and second-order statistics are fused to get features of size $M \times N \times 3$ and fed as input to the CNN of CBRNN. This fusion is also known as early fusion. In another case, preprocessed features and their first and second-order statistics of sizes $M \times N \times 1$ are fed as input to the three separate CNNs. The outputs of these CNNs are fused and fed as input to the RNN. This fusion is also known as late fusion.

Table 3: Performance of our proposed methods for Multiclass Classification using the UNSW-NB15 Dataset.

Method	Order of Derivative	Accuracy	Precision	Recall	F1-score
Early Fusion	First	70.08	0.79	0.70	0.71
Late Fusion	First	62.10	0.72	0.62	0.63

3. Bibliography styles

There are various bibliography styles available. You can select the style of your choice in the preamble of this document. These styles are Elsevier styles based on standard styles like Harvard and Vancouver. Please use BibTEX to generate your bibliography and include DOIs whenever available.

Here are two sample references: [1, 2].

References

[1] R. Feynman, F. Vernon Jr., The theory of a general quantum system interacting with a linear dissipative system, Annals of Physics 24 (1963) 118–173. doi:10.1016/0003-4916(63)90068-X.

[2] P. Dirac, The lorentz transformation and absolute time, Physica 19 (1-–12) (1953) 888–896. doi:10.1016/S0031-8914(53)80099-6.