Applying Convolutional Neural Network for Network Intrusion Detection

Vinayakumar R[1], K.P Soman[1] and Prabaharan Poornachandran[2]

[1]Centre for Computational Engineering and Networking (CEN), Amrita School of Engineering, Coimbatore, Amrita Vishwa Vidyapeetham,

Amrita University, India.

[2]Center for Cyber Security Systems and Networks, Amrita School of Engineering, Amritapuri, Amrita Vishwa Vidyapeetham,

Amrita University, India.

Outline

- Introduction
- Methodology
- Description of the data set and Results
- Summary
- Future Work
- References

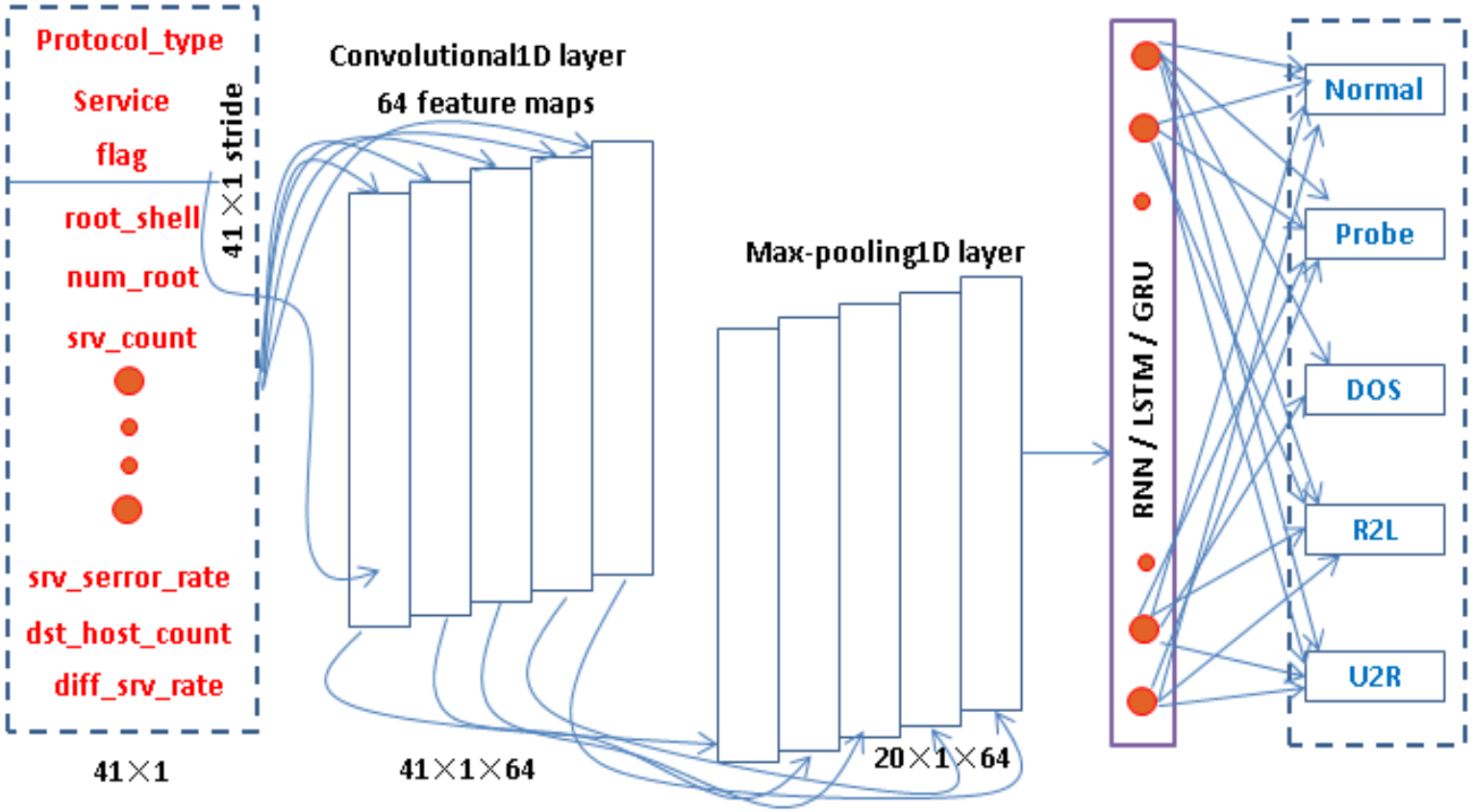
Introduction

- Information and communication technology (ICT) systems are essential for today's rapidly growing powerful technologies. At the same time, ICT system has been encountered by various attacks.
- Network intrusion detection system (NIDS) is a tool used to detect and classify the network breaches dynamically in ICT systems in both academia and industries.

Methodology

- Feature sets of connection records are passed to deep networks such as Multi-layer perceptron, convolutional neural network (CNN) and hybrid of CNN and recurrent neural network (RNN) and its variants such as long short-term memory, gated recurrent unit

Contd.



- Figure 1. Architecture of CNN and its hybrid network, all layers and its connections are not shown

Description of the data set and Results

Network intrusion detection data sets: DARAPA / KDDCup ’99’ [1] and NSL-KDD [2].

Table 1. Description of Data set

Attack category	Full data set	10 % data set			
	KDDCup 99	KDDCup 99		NSL-KDD	
	Train	Train	Test	Train	Test
Normal	972780	97278	60593	67343	9710
DOS	3883370	391458	229853	45927	7458
Probe	41102	4107	4166	11656	2422
r2l	1126	1126	16189	995	2887
u2r	52	52	228	52	67
Total		494021	311029	125973	22544

Contd.

Algorithm	Accuracy	Precision	Recall	F-score
CNN 1 layer	0.999	0.999	0.999	0.999
CNN 2 layer	0.998	0.999	0.998	0.999
CNN 3 layer	0.801	0.804	0.994	0.889
CNN 1 layer-LSTM	0.94	0.998	0.928	0.961
CNN 2 layer-LSTM	0.997	0.999	0.996	0.998
CNN 3 layer-LSTM	0.964	0.999	0.956	0.977
CNN 1 layer-GRU	0.922	0.995	0.907	0.949
CNN 2 layer-GRU	0.981	0.999	0.976	0.988
CNN 3 layer-GRU	0.936	0.999	0.921	0.958
CNN 1 layer-RNN	0.821	0.999	0.778	0.875
CNN 2 layer-RNN	0.973	1.0	0.967	0.983
CNN 3 layer-RNN	0.938	0.997	0.926	0.960

Table 2. Summary of test results for KDDCup '99' in classifying the connection records as either normal or attack

Contd.

Algorithm	Normal		Dos		Probe		u2r		r2l		Accuracy
	TPR	FPR	TPR	FPR	TPR	FPR	TPR	FPR	TPR	FPR	
MLP 8	0.760	0.168	0.901	0.318	0.470	0.012	0.0	0.0	0.0	0.0	0.684
CNN-LSTM 8	0.998	0.092	0.766	0.022	0.873	0.052	0.238	0.0	0.784	0.01	0.878
CNN 8	0.998	0.117	0.801	0.026	0.825	0.052	0.104	0.0	0.556	0.013	0.857
MLP 4	0.999	0.530	0.55	0.044	0.464	0.002	0.0	0.0	0.0	0.0	0.667
CNN-LSTM 4	0.999	0.082	0.862	0.062	0.863	0.067	0.209	0.005	0.248	0.002	0.846
CNN 4	0.997	0.104	0.831	0.079	0.712	0.063	0.03	0.0	0.326	0.007	0.827
MLP 4	0.871	0.079	0.927	0.17	0.553	0.011	0.0	0.0	0.0	0.0	0.885
CNN 4	1.0	0.015	0.943	0.145	0.607	0.040	0.0	0.0	0.306	0.009	0.852
CNN-LSTM 4	1.0	0.031	0.916	0.166	0.591	0.032	0.328	0.002	0.283	0.003	0.839

Table 3. Summary of test results for minimal feature sets of KDDCup '99' in multi class classification setting

Contd.

Algorithm	Normal		Dos		Probe		u2r		r2l		Accuracy
	TPR	FPR	TPR	FPR	TPR	FPR	TPR	FPR	TPR	FPR	
MLP 6 layer	0.996	0.081	0.941	0.040	0.794	0.002	0.0	0.0	0.001	0.0	0.923
CNN 1 layer	0.999	0.053	0.941	0.003	0.887	0.011	0.0	0.0	0.654	0.003	0.944
CNN 2 layer	0.999	0.020	0.974	0.002	0.969	0.013	0.286	0.0	0.636	0.0	0.970
CNN 3 layer	0.999	0.022	0.975	0.003	0.925	0.012	0.343	0.0	0.633	0.0	0.970
CNN 1 layer-LSTM	0.998	0.054	0.942	0.007	0.882	0.012	0.0	0.0	0.530	0.002	0.941
CNN 2 layer-LSTM	0.999	0.028	0.974	0.008	0.781	0.005	0.0	0.0	0.712	0.002	0.970
CNN 3 layer-LSTM	0.997	0.006	0.995	0.014	0.868	0.004	0.0	0.0	0.745	0.001	0.987
CNN 1 layer-GRU	0.998	0.073	0.941	0.009	0.857	0.003	0.171	0.001	0.347	0.001	0.934
CNN 2 layer-GRU	0.999	0.031	0.972	0.005	0.873	0.004	0.0	0.0	0.724	0.001	0.969
CNN 3 layer-GRU	0.999	0.013	0.991	0.002	0.873	0.011	0.0	0.0	0.484	0.001	0.977
CNN 1 layer-RNN	0.987	0.073	0.941	0.017	0.861	0.005	0.243	0.0	0.312	0.001	0.931
CNN 2 layer-RNN	0.995	0.031	0.974	0.014	0.760	0.005	0.0	0.0	0.693	0.0	0.967
CNN 3 layer -RNN	0.999	0.027	0.974	0.004	0.912	0.007	0.029	0.0	0.674	0.001	0.969

Table 3. Summary of test results for KDDCup '99' in categorizing attacks to their corresponding categories

Summary and Future work

- The convolutional neural network (CNN) is proposed for intrusion detection by modeling network traffic events of TCP/IP packets.
- For comparative study, MLP network is used.
- CNN and hybrid of CNN and RNN and its variants performed well in comparison to the MLP network.
- The attacks to ICT systems and networks are diverse and continuously evolving gradually. Thus, the efficacy of the proposed mechanism has to be verified on the recently release network intrusion detection data set.

References

[1]http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html

[2] M. Tavallaee, E. Bagheri, W. Lu, and A. A. Ghorbani, “A detailed analysis of the kdd cup 99 data set,” in Computational Intelligence for Security and Defense Applications, 2009. CISDA 2009. IEEE Symposium on. IEEE, 2009, pp. 1–6