Evaluating Effectiveness of Shallow and Deep Networks to Intrusion Detection System

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 shallow networks such as Logistic regression, Naive Bayes, k-nearest neighbor, decision tree, Ada boost, random forest, support vector machine and extreme learning machine and deep networks such as multi layer perceptron and deep belief network.

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	Data instances 10% data			
	KDD		NSL-KDD	
	Train	Test	Train	Test
Normal	97278	60593	67343	9710
DOS	391458	229853	45927	7458
Probe	4107	4166	11656	2422
R2L	1126	16189	995	2887
U2R	52	228	52	67
Total	**494021**	**311029**	**125973**	**22544**

Contd.

Algorithm	KDDCup '99'				NSL-KDD			
	Accuracy	Precision	Recall	F-score	Accuracy	Precision	Recall	F-score
LR	0.848	0.989	0.821	0.897	0.720	0.620	0.905	0.736
NB	0.929	0.988	0.923	0.955	0.728	0.622	0.935	0.747
KNN	0.929	0.998	0.913	0.954	0.788	0.677	0.971	0.798
DT	0.929	0.999	0.913	0.954	0.796	0.687	0.969	0.804
AB	0.925	0.995	0.911	0.951	0.774	0.662	0.970	0.787
RF	0.927	0.999	0.910	0.952	0.779	0.667	0.975	0.792
SVM	0.924	0.996	0.909	0.950	0.772	0.666	0.947	0.782

Table 2. Detailed results of various classical machine learning classifiers

Contd.

Network Layers	Number of Neurons	KDDCup '99'				NSL-KDD			
		Accuracy	Precision	Recall	F-score	Accuracy	Precision	Recall	F-score
MLP1	[60]	0.924	0.996	0.908	0.950	0.799	0.717	0.879	0.790
MLP2	[90,90]	0.934	0.995	0.922	0.958	0.811	0.701	0.879	0.817
MLP3	[120,120,120]	0.938	0.988	0.934	0.960	0.861	0.766	0.977	0.859
MLP4	[150,150,150,150]	0.939	1.000	0.924	0.960	0.866	0.768	0.988	0.864
DBN1	[200]	0.924	0.996	0.909	0.950	0.885	0.821	0.939	0.876
DBN2	[250,250]	0.929	0.998	0.913	0.954	0.896	0.814	0.984	0.891
DBN3	[300,300,300]	0.937	0.999	0.923	0.960	0.914	0.838	0.992	0.909
DBN4	[350,350,350,350]	0.997	1.000	0.997	0.998	0.973	0.944	0.996	0.969

Table 3. Summary of test results of various MLP and DBN networks

Contd.

KDDCup '99'											
Minimal	NORMAL		DOS		PROBE		U2R		R2L		ACC
Features	**TPR**	**FPR**	**TPR**	**FPR**	**TPR**	**FPR**	**TPR**	**FPR**	**TPR**	**FPR**	
MLP4	0.871	0.079	0.927	0.170	0.553	0.011	0.0	0.0	0.0	0.0	0.886
MLP8	0.995	0.092	0.938	0.015	0.712	0.002	0.0	0.0	0.01	0.0	0.921
MLP12	0.996	0.081	0.941	0.040	0.794	0.002	0.0	0.0	0.001	0.0	0.923
DBN4	1.0	0.081	0.938	0.099	0.0	0.0	0.0	0.0	0.0	0.0	0.912
DBN8	0.998	0.081	0.939	0.052	0.654	0.002	0.0	0.0	0.018	0.0	0.921
DBN12	0.999	0.743	0.248	0.095	0.0002	0.0	0.0	0.0	0.0	0.0	0.381
NSL-KDD											
MLP12	0.760	0.168	0.901	0.318	0.470	0.012	0.0	0.0	0.0	0.0	0.684
MLP8	0.999	0.530	0.55	0.044	0.464	0.0024	0.0	0.0	0.0	0.0	0.667
MLP4	0.871	0.079	0.927	0.17	0.553	0.011	0.0	0.0	0.0	0.0	0.885
DBN12	0.996	0.095	0.781	0.024	0.849	0.077	0.447	0.001	0.529	0.019	0.686
DBN8	1.0	0.065	0.807	0.043	0.773	0.108	0.358	0.008	0.387	0.003	0.799
DBN4	0.999	0.003	0.928	0.059	0.842	0.109	0.388	0.003	0.194	0.001	0.715

Table 4. KDDCup '99' and NSL-KDD attack detection rate with minimal feature sets such as 4, 8 and 12

Contd.

Algorithm	NORMAL		DOS		PROBE		U2R		R2L		ACC
	TPR	**FPR**	**TPR**	**FPR**	**TPR**	**FPR**	**TPR**	**FPR**	**TPR**	**FPR**	
						KDDCup '99'					
LR	0.969	0.185	0.841	0.07	0.073	0.002	0.0	0.0	0.0	0.0	0.833
NB	0.711	0.077	0.848	0.023	0.963	0.076	0.8	0.053	0.152	0.001	0.803
KNN	0.994	0.087	0.939	0.012	0.693	0.004	0.229	0.0	0.063	0.001	0.922
DT	0.995	0.085	0.941	0.004	0.745	0.002	0.343	0.002	0.125	0.0003	0.926
AB	0.99	0.625	0.383	0.03	0.116	0.002	0.0	0.0	0.003	0.0	0.487
RF	0.995	0.093	0.940	0.004	0.753	0.002	0.271	0.0	0.001	0.0	0.922
SVM	0.987	0.061	0.939	0.004	0.928	0.026	0.0	0.0	0.147	0.0001	0.926
ELM	0.997	0.073	0.940	0.005	0.809	0.009	0.157	0.001	0.172	0.002	0.929
						NSL-KDD					
LR	0.926	0.468	0.641	0.122	0.171	0.020	0.0	0.0	0.0	0.0	0.635
NB	0.269	0.083	0.762	0.165	0.539	0.02	0.806	0.258	0.365	0.104	0.478
KNN	0.976	0.333	0.73	0.031	0.589	0.038	0.179	0.0001	0.084	0.016	0.741
DT	0.971	0.334	0.756	0.012	0.715	0.032	0.328	0.002	0.01	0.019	0.753
AB	0.936	0.37	0.796	0.146	0.11	0.009	0.0	0.0	0.0	0.0	0.685
RF	0.975	0.408	0.749	0.013	0.618	0.02	0.254	0.0003	0.002	0.0002	0.741
SVM	0.977	0.242	0.697	0.014	0.913	0.108	0.0	0.0	0.011	0.0009	0.755
ELM	0.974	0.232	0.774	0.015	0.854	0.091	0.0	0.0	0.023	0.001	0.776

Table 5. Detailed results for KDDCup '99' and NSL-KDD using classical machine learning classifiers

Contd.

KDDCup '99'											
Network	NORMAL		DOS		PROBE		U2R		R2L		ACC
Layers	**TPR**	**FPR**	**TPR**	**FPR**	**TPR**	**FPR**	**TPR**	**FPR**	**TPR**	**FPR**	
MLP 1	0.989	0.091	0.939	0.015	0.771	0.003	0.0	0.0	0.001	0.0	0.919
MLP 2	0.981	0.095	0.938	0.019	0.674	0.003	0.0	0.0	0.001	0.0001	0.917
MLP 3	0.983	0.144	0.882	0.013	0.785	0.006	0.0	0.0	0.0003	0.0	0.876
MLP 4	0.984	0.134	0.899	0.021	0.669	0.003	0.0	0.0	0.0	0.0	0.887
DBN 1	0.988	0.078	0.941	0.051	0.616	0.002	0.0	0.0	0.134	0.002	0.922
DBN 2	0.988	0.076	0.939	0.022	0.709	0.003	0.0	0.001	0.332	0.003	0.928
DBN 3	0.979	0.071	0.959	0.023	0.708	0.003	0.0	0.0	0.001	0.001	0.933
DBN 4	0.953	0.082	0.937	0.127	0.105	0.003	0.0	0.0	0.0	0.0	0.902
NSL-KDD											
MLP 1	0.975	0.093	0.768	0.031	0.775	0.128	0.0	0.0	0.214	0.027	0.789
MLP 2	0.976	0.149	0.777	0.058	0.817	0.065	0.0	0.0	0.343	0.007	0.812
MLP 3	0.972	0.254	0.758	0.025	0.785	0.089	0.0	0.0	0.035	0.001	0.764
MLP 4	0.975	0.392	0.658	0.018	0.733	0.056	0.0	0.0	0.0	0.0	0.721
DBN 1	0.998	0.084	0.828	0.073	0.839	0.114	0.0	0.0	0.002	0.004	0.793
DBN 2	0.974	0.233	0.778	0.015	0.857	0.091	0.0	0.0	0.029	0.001	0.776
DBN 3	0.982	0.092	0.776	0.014	0.922	0.111	0.0	0.0	0.261	0.029	0.817
DBN 4	0.979	0.256	0.778	0.014	0.809	0.058	0.0	0.0	0.089	0.015	0.793

Table 6. Detailed results for KDDCup '99' and NSL-KDD using deep networks

Summary

- Shallow and Deep network is applied for network intrusion detection.
- Deep network performed well in comparison to the shallow networks.
- The primary reason to that is, a deep network passes the information through the several layers and nonlinearity in each layer facilitates to learn the distinguishable patterns between normal and attack connection records.

Future Work

- KDDCup '99' and NSL-KDD are most well-known and outdated. Moreover. these are not representative for today’s network traffic. Applying the proposed methodologies on the recent network traffic data set is essential. This will be remained as one of significant future work direction.

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