Secure Shell (SSH) Traffic Analysis with Flow Based Features Using Shallow and Deep networks

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

- Traffic classification serves as a primary mechanism for numerous network management activities counting from knowing simple network statistics to quality of service provisioning.
- Most commonly used methods are port based, payload based and flow features statistics.

Methodology

- Flow feature statistics such as protocol, minimum packet length (f&b), minimum inter-arival time (f&b), duration mean packet length (f&b), mean inter-arival time (f&b), total packets (f&b), maximum packet length (f&b), maximum inter-arival time (f&b), total bytes (f&b), standad deviation of packet lengths (f&b), standad deviation of inter-arival times (f&b) are passed to machine learning and deep learning algorithms

Contd.

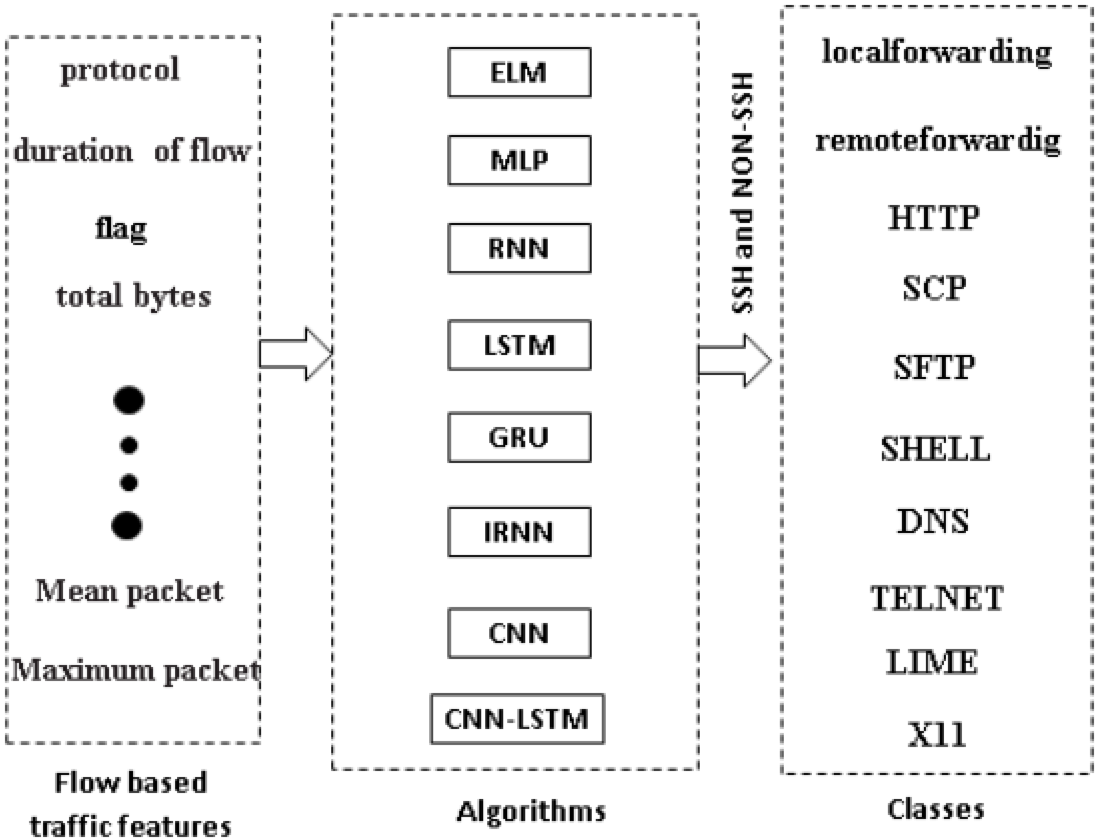

Figure 1. Architecture for classifying SSH traffic analysis

Description of the data set and Results

Public traces are from the NLANRs (National Laboratory for Applied Network Research) Active Measurement Project (AMP) [1] and Measurement and Analysis on the WIDE Internet (MAWI) [2]. Private trace is from Network Information Management and Security Group (NIMS) [3], [4].

Table 1. Description of Data set

Data set	Total SSH flows	Total NON-SSH flows
AMP	427,448	20,669,977
MAWI	19,016	19,954,825
NIMS	14,681	699,170

Contd.

Algorithm	Accuracy	Precision	Recall	F-score
ELM	0.958	0.992	0.964	0.978
MLP	0.962	0.982	0.979	0.981
RNN	0.967	0.980	0.986	0.983
LSTM	0.997	0.997	1.000	0.998
GRU	0.994	0.994	1.000	0.997
IRNN	0.974	0.983	0.991	0.987
CNN	0.974	0.995	0.978	0.986
CNN-LSTM	0.999	1.000	1.000	1.000

Table 2. Summary of test results with training data set MAWI and AMP and testing data set NIMS

Contd.

Algorithm	Accuracy	Precision	Recall	F-score
ELM	0.920	0.874	0.981	0.925
MLP	0.925	0.875	0.993	0.930
RNN	0.950	0.980	0.969	0.974
LSTM	0.965	0.992	0.972	0.982
GRU	0.962	0.992	0.970	0.980
IRNN	0.955	0.980	0.974	0.977
CNN	0.944	0.990	0.953	0.971
CNN-LSTM	0.979	0.990	0.988	0.989

Table 3. Summary of test results with training data set NIMS and testing data set MAWI and AMP

Contd.

Name of service	ELM		MLP		RNN		LSTM		GRU		IRNN		CNN		CNN-LSTM	
	TPR	FPR	TPR	FPR	TPR	FPR	TPR	FPR	TPR	FPR	TPR	FPR	TPR	FPR	TPR	FPR
LocalForwarding	1.0	0.0	1.0	0.0	1.0	0.0	1.0	0.0	1.0	0.0	1.0	0.0	1.0	0.0	1.0	0.0
RemoteForwarding	1.0	0.0	1.0	0.0	1.0	0.0	1.0	0.0	1.0	0.0	1.0	0.0	1.0	0.0	1.0	0.0
SCP	1.0	0.001	0.998	0.001	0.986	0.0	0.932	0.001	0.932	0.01	0.993	0.0	0.995	0.001	1.0	0.0
SFTP	0.939	0.0	0.886	0.0	0.968	0.0	0.947	0.001	0.866	0.01	0.973	0.0	0.917	0.0	1.0	0.0
SHELL	0.916	0.0	0.945	0.001	0.947	0.0	0.951	0.002	0.921	0.003	0.992	0.0	0.951	0.0	1.0	0.0
TELNET	0.992	0.0	0.976	0.0	0.984	0.0	0.984	0.002	0.984	0.002	0.992	0.0	0.988	0.0	1.0	0.0
FTP	0.965	0.0	0.789	0.0	0.904	0.0	0.934	0.001	0.934	0.0002	0.978	0.0	0.908	0.0	1.0	0.0
HTTP	0.99	0.002	0.96	0.002	0.982	0.002	0.948	0.002	0.948	0.002	0.99	0.001	0.983	0.001	1.0	0.0
DNS	0.697	0.04	0.553	0.004	0.712	0.013	0.991	0.001	0.991	0.002	0.592	0.002	0.599	0.004	0.992	0.0
lIME	0.951	0.114	0.996	0.174	0.984	0.111	0.996	0.009	0.992	0.009	0.996	0.154	0.996	0.152	0.999	0.003
X11	0.983	0.0	0.983	0.0	0.983	0.0	0.93	0.0	0.93	0.003	0.992	0.0	0.977	0.0	1.0	0.0
Accuracy	0.932		0.95		0.958		0.989		0.985		0.958		0.956		0.999	

Table 4. Summary of test results in classifying background applications running over SSH and NON-SSH using deep learning approaches

Summary

- The performance of machine learning and deep learning approaches are evaluated on classifying SSH.
- To know how machine learning and deep learning works on completely unseen data, we have trained both machine learning and deep learning approaches on public traces such as AMP, MAWI and the performance of them is evaluated on private trace such as NIMS and vice versa.
- Deep learning algorithms performed well in comparison to the machine learning algorithms in all the experimental settings.

Future Work

- The internet and its applications mainly peer-2-peer (P2P), voice over internet protocol (VOIP), multi-media are following constant transformation. Thus, the patterns of traffic are very dynamic. Thus the proposed technique can be applied on the recently released data set.

References

[1] "Nlanr," available at http://pma.nlanr.net/special.

[2] "Mawi," available at http://tracer.csl.sony.co.jp/mawi/.

[3] R. Alshammari and A. N. Zincir-Heywood, "A flow based approach for ssh traffic detection," in Systems, Man and Cybernetics, 2007. ISIC. IEEE International Conference on. IEEE, 2007, pp. 296–301.

[4] "Can encrypted traffic be identified without port numbers, ip addresses and payload inspection?" Computer networks, vol. 55, no. 6, pp. 1326–1350, 2011