Encrypted Traffic Classification with Recurrent Neural Networks

GitHub: https://github.com/imaginebreake/RNNTraffic

Group 8:

Tianyi Gao (Gavin)

scytg1@nottingham.ac.uk

Yuwei Zhu (Tony)

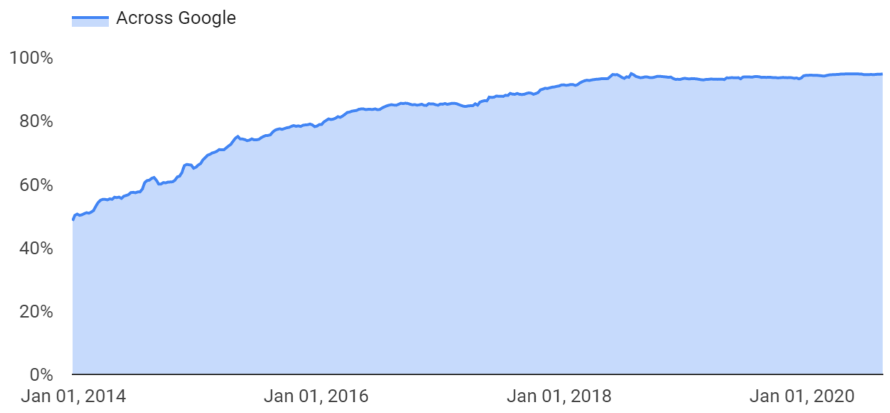
yuweizhu_tony@163.com

ST106 Final Project, September 2020

Overview

1. Introduction
2. Related Work
3. Background
4. Methodology
5. Conclusion
6. Future work

1 Introduction



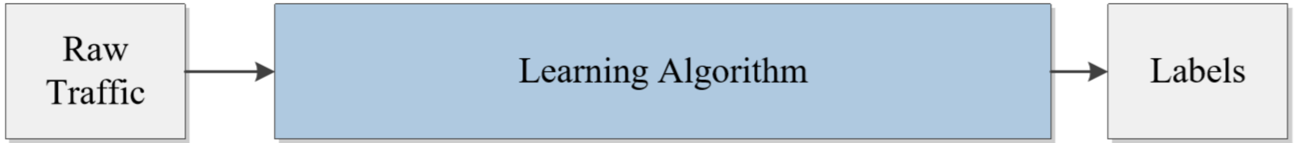
Encrypted traffic (HTTPS) across Google

- **The need for network traffic classification**
  - Malware traffic detection
  - Quality of service (QoS)
- **New change and challenge**
  - Application layer encryption: High percentage of encrypted traffic
  - Transport layer encryption: Big market size of VPN service
- **Current best approach – End-to-end 1D CNN model**
- **Our contributions**
  - 1D CNN model r**eproduction**
  - **RNN model** on VPN / Non-VPN binary classification
  - **RNN model** on detailed type classification (Email, Chat, P2P and Streaming)

2 Related Work

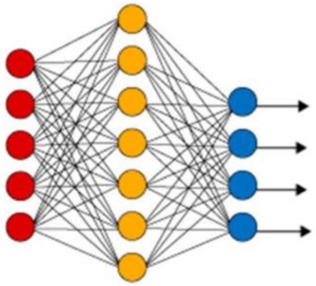
- Previous generation methods
  - Port-based methods
  - Deep packets inspection
  - Statistics methods
- **Neural network methods**
  - **End-to-end 1D CNN model**

a) Divide-and-conquer model

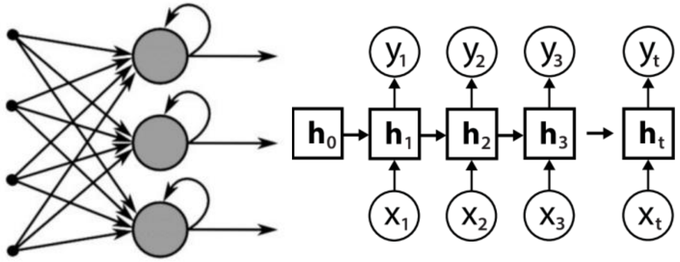


b) End-to-end learning model

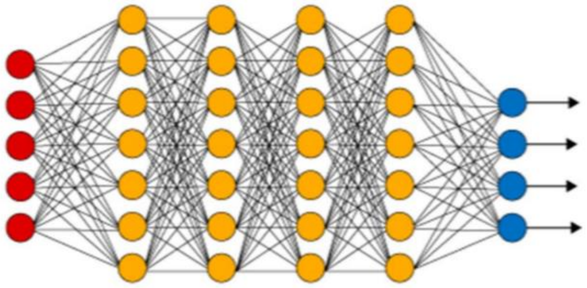
3 Background



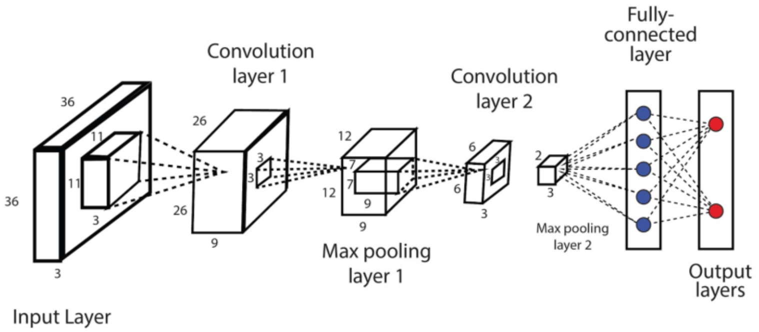
Neural Networks



Recurrent Neural Network (RNN)



Deep Neural Networks



Convolutional Neural Network (CNN)

4.1 Method - Data Processing

Network Traffic Captured **.pcap Files**

Here, large pcap files are splitted by SplitCap tool to each session.

Separate Sessions **small .pcap files**

Each session is read byte by byte as **raw 8-bit unsigned integers**. In this case, sessions larger than 1,500 bytes are **trimmed** to 1,500 bytes, and sessions smaller than 300 bytes are discarded, and the other sessions are **self-repeated** up to 1,500 bytes.

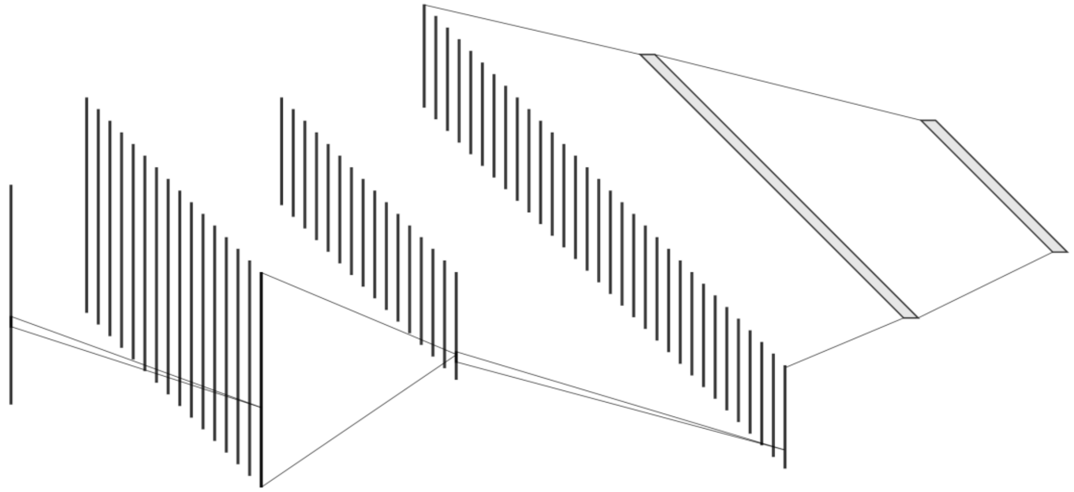
Normalised Sessions **.csv files**

4.2 Method - 1D CNN Model Reproduction

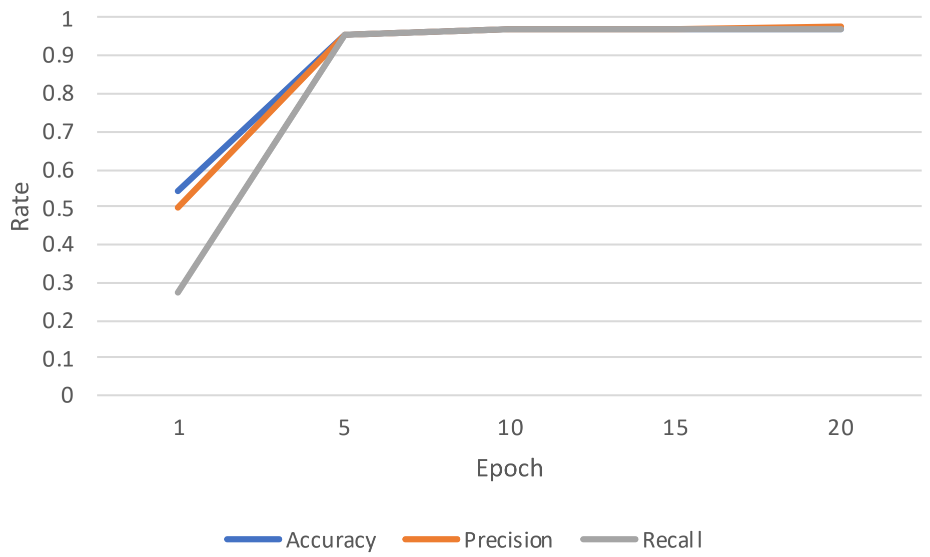
We reproduced the end-to-end 1D CNN model for binary non-VPN/VPN traffic classification.

All the network traffic data were split into 3 sets for training (80%, 5930 records), validation (10%, 741 records) and testing (10%, 742 records).

After 20 epochs of optimization, the model ended up with the validation result of: **97.30% Accuracy, 97.46% Precision, 97.22% Recall**.



Reproduced model architecture



Evaluation data on validation set during training

4.3 Method – RNN Model

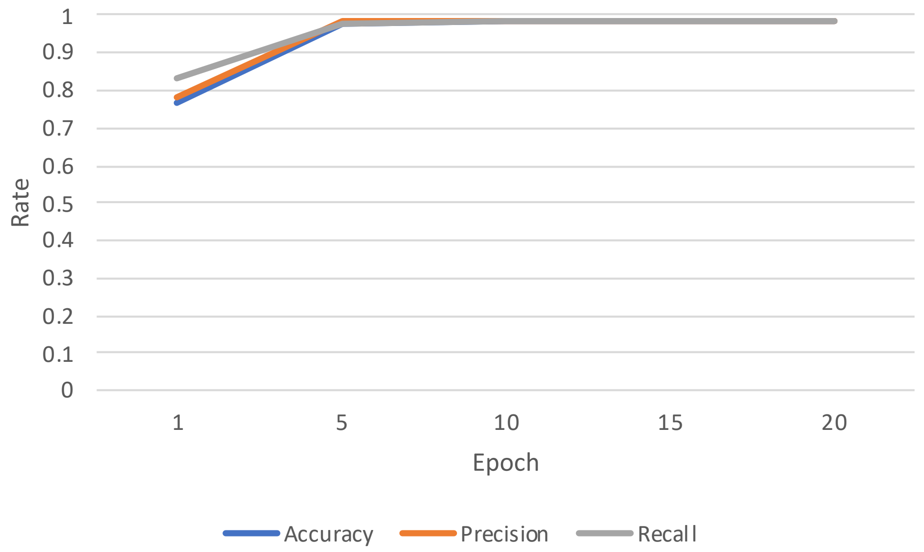
We proposed three brand new RNN models on different tasks. The train/validate/test dataset settings is same as the 1D CNN one. In practice, bidirectional LSTM neuron units are applied instead of simple RNN neuron units.

4.3.1 non-VPN/VPN Binary Classification

The RNN architecture is listed and the model ended up with the validation result of: **98.25% Accuracy, 98.38% Precision, 98.16% Recall**.

Layer number	Layer type	Input size	Output size	Comment
0	LSTM	1500	512 * 2	1 inner layer, bidirectional
1	Dense	1024	128	ReLU applied
2	Dense	128	2	
3	Log Softmax	2	2	

RNN Model for non-VPN/VPN Binary Classification



Evaluation data on validation set during training

4.3.2 Detailed Type of Traffic Classification on RNN Model

For this task, same RNN model for VPN traffic and non-VPN traffic were designed. And separate model is trained. The RNN architecture is listed.

The result of traffic type under VPN on validation set is: **95.21% Accuracy, 87.69% Precision, 92.88% Recall**.

The result of traffic type under non-VPN on validation set is: **83.38% Accuracy, 84.91% Precision, 85.08% Recall**.

Layer number	Layer type	Input size	Output size	Comment
0	LSTM	1500	512 * 2	1 inner layer, bidirectional
1	Dense	1024	128	ReLU applied
2	Dense	128	4	
3	Log Softmax	4	4	

RNN Model for Detailed Traffic Type Classification

5 Conclusion

- This paper has implemented the binary classification of VPN and non-VPN traffic based on **CNN model and RNN model**. And the results of both models were **considerably well** while the RNN model has performed slightly better than the CNN model.
- Then, in order to categorize the network traffic into four detailed types (i.e. Email, Chat, P2P and Streaming), **RNN model** has been applied on VPN traffic and non-VPN traffic respectively. The results of this classification were not as good as those of the binary classification between VPN and non-VPN traffic, but they were **also acceptable**.

Model	Accuracy	Precision	Recall
4.2	98.11%	98.24%	98.02%
4.3.1	98.25%	98.39%	98.15%
4.3.2 A	95.49%	89.11%	92.02%
4.3.2 B	86.88%	86.96%	87.83%

Results on evaluation of test set

6 Future work

Potential further advancement of this paper might be:

- More effective methods of data representation,
- Further tuning of hyperparameters of the models,
- Trying out other advanced machine learning methods,
- etc.

References

[1] url: https://transparencyreport.google.com/https /overview.

[2] Herve Abdi. “A neural network primer”. In: Journal of Biological Systems 2.03 (1994), pp. 247–281.

[3] Yves Chauvin and David E Rumelhart. Backpropagation: theory, architectures, and applications. Psychology press, 1995.

[4] Sharan Chetlur, Cliff Woolley, Philippe Vandermersch, Jonathan Cohen, John Tran, Bryan Catanzaro, and Evan Shelhamer. “cudnn: Efficient primitives for deep learning”. In: arXiv preprint arXiv:1410.0759 (2014).

[5] Alberto Dainotti, Antonio Pescape, and Kimberly C Claffy. “Issues and future directions in traffic classification”. In: IEEE network 26.1 (2012), pp. 35–40.

[6] Jason A Donenfeld. “WireGuard: Next Generation Kernel Network Tunnel.” In: NDSS. 2017.

[7] GerardDraper-Gil,ArashHabibiLashkari,Mohammad Saiful Islam Mamun, and Ali A Ghorbani. “Characterization of encrypted and vpn traffic using time-related”. In: Proceedings of the 2nd international conference on information systems security and privacy (ICISSP). 2016, pp. 407–414.

[8] Jawad Khalife, Amjad Hajjar, and Jesus Diaz-Verdejo. “A multilevel taxonomy and requirements for an optimal traffic-classification model”. In: International Journal of Network Management 24.2 (2014), pp. 101–120.

[9] Yann LeCun, Yoshua Bengio, et al. “Convolutional networks for images, speech, and time series”. In: The handbook of brain theory and neural networks 3361.10 (1995), p. 1995.

[10] Tomáš Mikolov, Stefan Kombrink, Lukáš Burget, Jan Černock, and Sanjeev Khudanpur. “Extensions of recurrent neural network language model”. In: 2011 IEEE international conference on acoustics, speech and signal processing (ICASSP). IEEE. 2011, pp. 5528–5531.

[11] Sebastian Ruder. “An overview of gradient descent optimizationalgorithms”.In:arXivpreprintarXiv:1609.04747 (2016).

[12] Petr Velan, Milan Čermák, Pavel Čeleda, and Martin Drašar. “Asurvey ofmethods forencryptedtraffic classification and analysis”. In: International Journal of Network Management 25.5 (2015), pp. 355–374. doi: 10.1002/nem.1901.

[13] VPN Market Size and Share 2020-2026: Global Research Report. url: https://www.gminsights.com/industryanalysis/virtual-private-network-vpn-market.

[14] Wei Wang, Ming Zhu, Jinlin Wang, Xuewen Zeng, and Zhongzhen Yang. “End-to-end encrypted traffic classification with one-dimensional convolution neural networks”. In: 2017 IEEE International Conference on Intelligence and Security Informatics (ISI). IEEE. 2017, pp. 43–48.

[15] Baris Yamansavascilar, M Amac Guvensan, A Gokhan Yavuz, and M Elif Karsligil. “Application identification via network traffic classification”. In: 2017 International Conference on Computing, Networking and Communications (ICNC). IEEE. 2017, pp. 843–848.

Q & A

Thanks For Watching