Autonomous Model Update Scheme for DL-based Network Traffic Classifiers

Jielun Zhang

Advisor: Feng Ye, Ph.D.

Department of Electrical and Computer Engineering, University of Dayton

University of Dayton

Background

Network traffic classification is essential in access networks for end-to-end network management and measurement. State-of-the-art Deep Learning (DL) based classifiers, e.g., Convolutional Neural Network (CNN) based packet classifier in Fig.1(a), have high accuracy as a data-driven approach, where a classification result can be given with an input packet [1]. Such classifiers would need to be updated when a new application is in the network traffic. However, it is challenging to build and label a dataset of the new application from active network traffic. To tackle the issues, we design an autonomous update scheme for DL-based traffic classifiers [2].

Objectives

To allow the autonomous model update, we propose to

- Filter the data packets of a new application from active network traffic and build a corresponding training dataset.
- Update the current traffic classifier and evaluate the update scheme with an open dataset.

Preliminary – CNN-based Packet Classifier

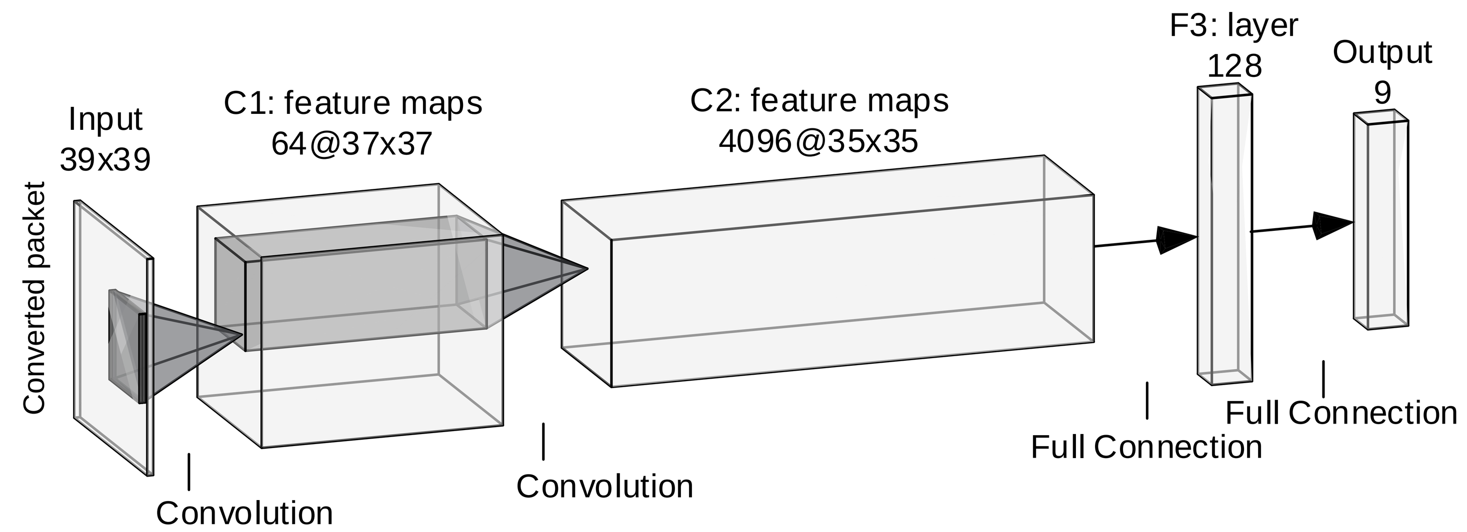


Figure 1(a): The proposed CNN-based packet classifier

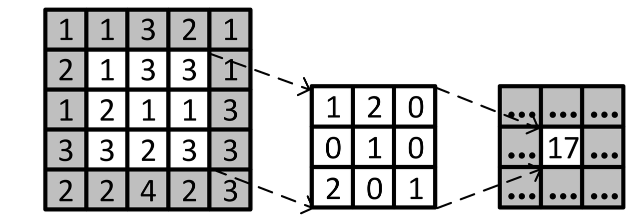


Figure 1(b): Convolution operation

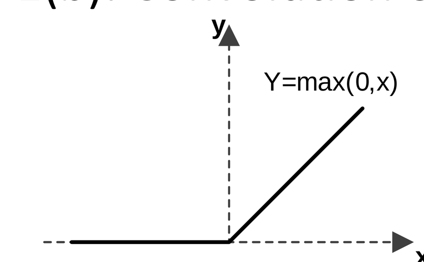


Figure 1(c): Activation function (ReLU)

Convolution: $c[i][j][k] = b[k] + \sum_{l} \sum_{s=1}^{W} \sum_{t=1}^{H} w[s][t][l][k] * I[(i-1)+s][(j-1)+t][l]$, *Activation:* $x[i][j][k] = \max\{0, c[i][j][k]\}$,

Fully connected (dense) layer: $\boldsymbol{y} = [y_1, y_2, \ldots, y_N] = (W^T \cdot \boldsymbol{x}) + \boldsymbol{b}$, *Softmax layer:* $\boldsymbol{s} = [s_1, s_2, \ldots, s_N] = \exp(y_n)/\sum_{i=1}^{N} \exp(y_i)$.

Autonomous Classifier Update Scheme

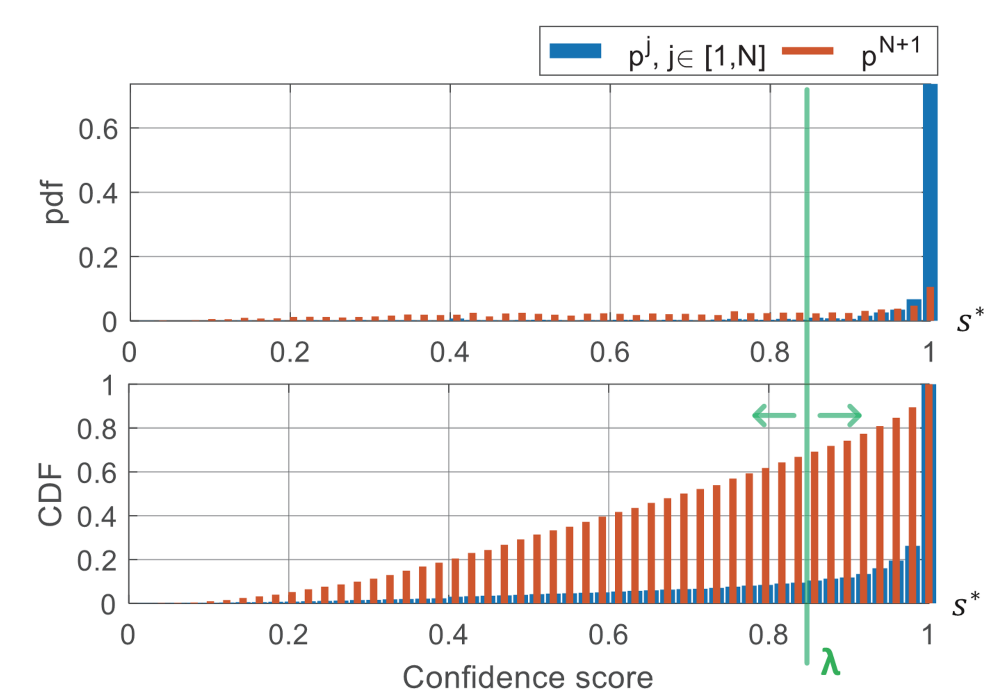


Figure 2: pdf and CDF of confidence scores

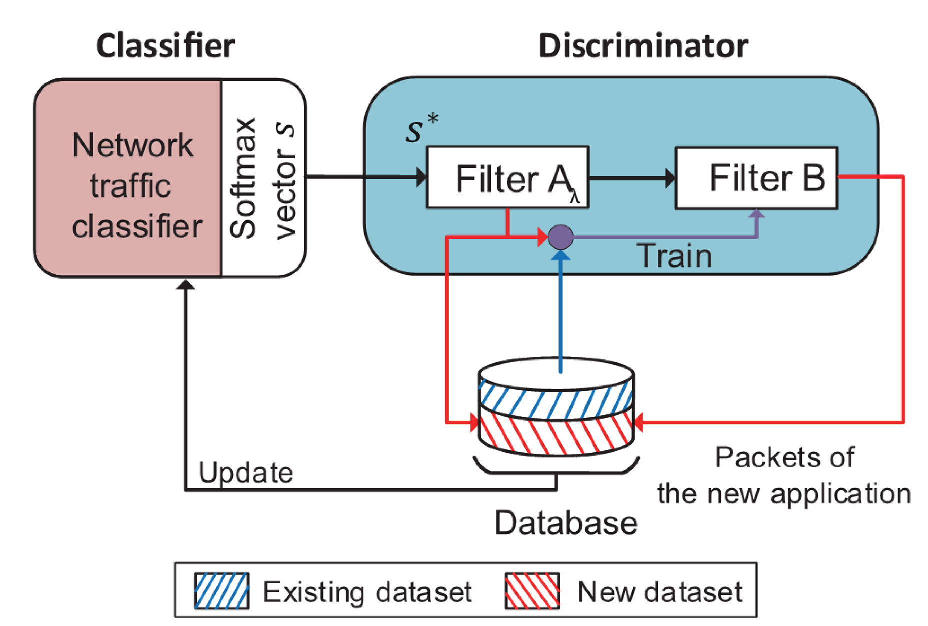


Figure 3: The proposed updating scheme

With the observation shown in Fig. 2 that confidence scores of the packets from the new application are usually lower than those of the known applications in the database, we propose an autonomous classifier update scheme shown in Fig. 3 which can be summarized as follows.

- Obtain confidence scores s* from the Softmax layer in the DL-based classifier.
- Filter A uses a threshold λ to filter the left part as the packets of the new application.
- Use packets in the old dataset and the filtered packets in filter A to train a binary classifier as filter B, which is capable of filtering a packet from the new application among the packets whose confidence scores locates on the right side of the λ.
- Refresh the database with the packets filtered by both filter A and filter B by labeling them as the packets of the new application.
- Update the original classifier with the refreshed database through transfer learning, where the original parameters are kept but the sizes of the last fully-connected layer and the Softmax layer are modified.

Dataset and Metrics

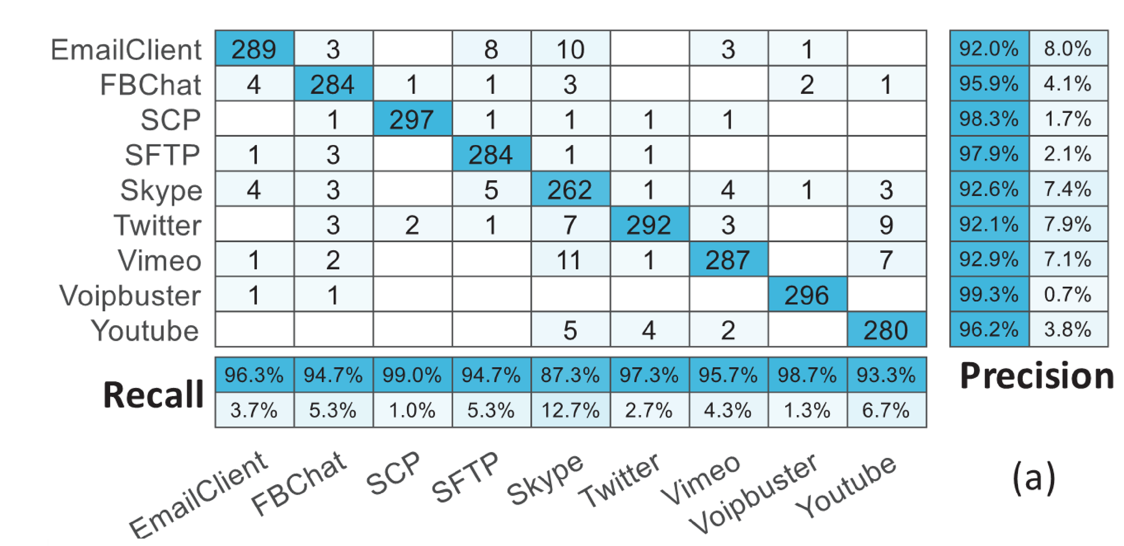
The dataset chosen for evaluation is selected from the "ISCX VPN-nonVPN dataset" (ISCXVPN2016) [3]. A total of 206,688 packets, including applications, such as Skype, Youtube, Vimeo, etc., are extracted from the dataset.

We use recall and precision as the performance metrics which are calculated as:

$$Recall = \frac{TP}{TP + FN} \qquad Precision = \frac{TP}{TP + FP}$$

TP: # of true positive instances properly classified as X.
FP: # of false positive instances classified as X incorrectly.
TN: # of true negative instances properly classified as X.
FN: # of false negative instances classified as not X incorrectly.

Evaluation Result



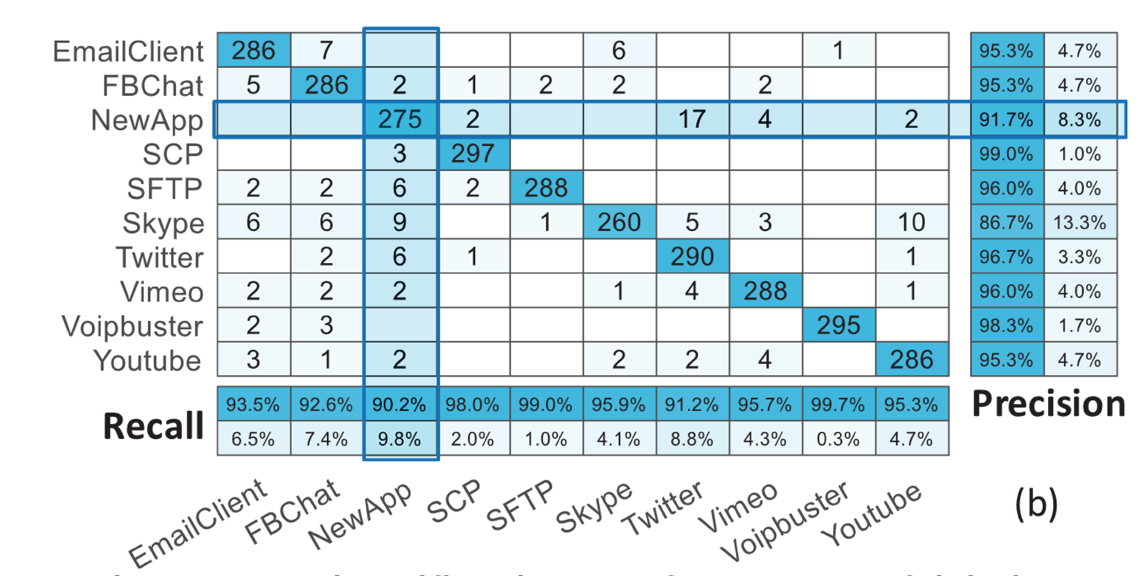


Figure 4: Classification performance of (a) the original classifier trained of 9 existing network applications; (b) updated classifier of 9 existing applications and 1 new application

The confusion matrix illustrated in Fig. 4 demonstrates that the proposed scheme updates the original model successfully. It enables the model to classify the packets from a new application with an average recall close to 95.1% and an average precision as 95.03%.

Jielun Zhang received a B.S. degree in electrical engineering from Shanghai Normal University, Shanghai, China; a B.S. degree in electronic and computer engineering technology and an M.S. degree in electrical engineering from the University of Dayton, Dayton, OH, USA. He is currently pursuing the Ph.D. degree from the Department of Electrical and Computer Engineering, University of Dayton, Dayton, OH, USA. His current research interests include artificial intelligence in networking and wireless communications.

[1] P. Wang, X. Chen, F. Ye and Z. Sun, "A Survey of Techniques for Mobile Service Encrypted Traffic Classification Using Deep Learning," in IEEE Access, vol. 7, pp. 54024-54033, 2019. doi: 10.1109/ACCESS.2019.2912896
[2] **J. Zhang**, F. Li, H. Wu and F. Ye, "Autonomous Model Update Scheme for Deep Learning Based Network Traffic Classifiers," 2019 IEEE Global Communications Conference (GLOBECOM), Waikoloa, HI, USA, 2019, pp. 1-6.
[3] Draper-Gil, Gerard, et al. "Characterization of encrypted and vpn traffic using time-related." Proceedings of the 2nd international conference on information systems security and privacy (ICISSP). 2016.