University College London

Dept. Computer Science

Automatic Feature Selection for Website Fingerprinting

Interim Report

Axel Goetz

Supervisors:

Dr. George Danezis

Jamie Hayes

January 26, 2017

1 Current Progress

We have updated some requirements that were mentioned in the project plan. Rather than first collecting a large dataset of website traces over a long period of time, we decided to start with existing datasets to perform some experiments. Then later, if we get the opportunity to do so, we can still collect our own data.

Given the nature of the challenge, a majority of the time will be spend on researching models that perform automatic feature selection. After careful examination, there are only two couple deep learning methods that seem to be appropriate, a *RNN Encoder Decoder* or a *Bidirectional RNN Encoder*. We also considered using a *Stacked Autoencoder* but it did not seem to be appropriate as it requires a fixed-length vector as an input. Hence, if we were to use it, we either have to pad or compress the traces, which are both not elegant solutions. In addition to simply training these models on the data, we might perform *denoising* on the them, which essentially means learning the models to distinguish uncorrupted data from corrupted data. This final step allows us to fine tune the encoders to get a consistent performance even if some of the data is noisy.

Although we have started experimenting with some of these models, they have not been fully implemented. However we are still on schedule for doing so.

Finally, we have also selected a set of previously successful website fingerprinting attacks. An environment has been set up, some of these models have been implemented and the infrastructure is in place to extract a set of hand-picked features from the raw data. This will allow us to quickly perform a performance comparison with the manually engineered features and the automatically selected ones.

2 Remaining Work

The first priority is to fully implement a *RNN Encoder Decoder* or a *Bidirectional RNN Encoder* and fine tune it. Next, we have to perform the analysis on how appropriate our automatically engineered features are compared to hand-picked ones. So this includes finishing the implementation of existing models, and the infrastructure to extract the features.

Next, we need to pick a set of criteria that we will use to compare the predictive power of several models. Using these criteria we will then have to perform a thorough analysis of how the automatically engineered features compared to the hand-picked ones.

Finally, after all of the above has been completed, we will focus on finished writing the final report. If there is still time remaining, we might still try to collect our own data over an extended period of time.