The area of network traffic classification, which aims at labeling network traffic according to application or application type, is constantly evolving. When classification based on port inspection got deployed, applications started using dynamic ports. Then, the deployment of deep-packet inspection caused some applications to use encryption or variable length padding. Every new application development triggers new traffic classification techniques. Often each technique is tested in different environments and using proprietary network traces making it hard to reproduce the results, compare techniques, and fully understand the limits and benefits of each technique.

This paper presents a tool to benchmark traffic classification techniques, called NeTraMark. NeTraMark is extensible, so researchers can plug-in their techniques to compare to other classification algorithms. NeTraMark already includes implementations of eleven existing classification algorithms ranging from port and deep-packet inspection to graph-based classifiers. It also implements a number of evaluation metrics and a visualization module. Researchers can easily compare the results of classification techniques under the same metrics. Since publicly available full-payload traces are rare, NeTraMark can be deployed at different sites to run on locally available data sets. In summary, NeTraMark combines a number of features that should facilitate the life of developers of traffic classification techniques. The source code is available, so we should all contribute with our own algorithms and techniques. A community effort should lead to better standards for evaluating traffic classification techniques.

Public review written by

Renata Teixeira
Laboratoire d'Informatique de Paris 6 (LIP6)
CNRS and UPMC Sorbonne Universités, France