Technische Universität München
Lehrstuhl für
Netzarchitekturen & Netzdienste
Prof. Dr. Georg Carle

02.11.2009

Bachelorarbeit

Classification of Traffic Flows using DPI *

* Eine deutsche Themenenbeschreibung erhalten Sie gerne auf Anfrage.

Motivation

Network operators want to know which kinds of services and applications are responsible for the network traffic. However, traffic classification based on port numbers is no longer efficient since many new applications choose or negotiate port numbers dynamically or reuse registered ports of other services in order to pass firewalls. One solution is to look into the packet payload and search for characteristic signatures which enable the identification of the underlying protocol and application. This procedure is commonly known as **Deep Packet Inspection** (DPI).

Goal of this bachelor thesis is to integrate DPI functionality into an existing monitoring tool for online and offline classification of packet flows and bidirectional connections. The classification results shall provide a “ground truth” for other traffic classification approaches which do not rely on packet payload, such as statistical classification techniques and Machine Learning.

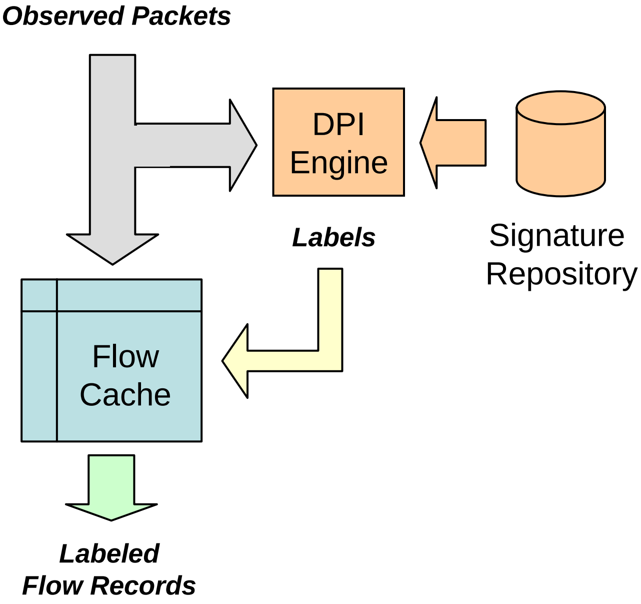
Task Description

DPI functionality is to be integrated into the open-source monitoring software **VERMONT** [1]. One use-case is to include a label into each flow record which carries the classification result for that specific flow or connection.

Instead of defining a new set of signatures or classification algorithms, signatures and methods of existing traffic classification tools shall be reused as far as possible. Therefore, the work will start with a study of available open-source DPI solutions, such as Open DPI [2].

[1] http://www.history-project.net

[2] http://opendpi.org



Requirements

Linux skills, programming skills in C/C++

Contact

Gerhard Münz, Lothar Braun
Email: {muenz|braun}@net.in.tum.de Tel.: 289-18008, 289-18010