heig-vd
Haute Ecole d'Ingénierie et de Gestion
du Canton de Vaud
http://www.heig-vd.ch

Travail de diplôme 2006

HEIG-VD
Route de Cheseaux 1
CH - 1401 Yverdon-les-Bains

Peer-to-Peer Detection

Traffic Analysis

Most of the **traffic classification** currently used on IP networks is based under the assumption that layer 4 (TCP or UDP) port numbers present in IP packets headers can define the layer 7 protocol of the communication. Unfortunately this assumption is no longer true due to many protocols using dynamic ports such as Peer-to-Peer protocols, VoIP and so on.
To solve this issue at least two ways exist, (1) trying to apply better algorithms to the transport layer information we already have and (2) analyzing more informations than we currently do, like the whole packets including payload. This diploma mainly focused on the second solution but, nonetheless, presented an insight of the first one.

Behavior Analysis

This first solution called **behavioral analysis** is based on ongoing research which tries to model the way Peer-to-Peer networks are working and infers some common characteristics of theirs traffic. Those models does not require access to the IP packets payload.

Deep Packet Inspection

Deep Packet Inspection works by using protocol signatures, usually in the form of regular expressions, which are applied to the payload of IP packets in order to determine the layer 7 protocol used. This method has to be implemented on the network probes because it requires access to the IP packets payload.
Because the pattern matching operation on traffic can quickly become very complex and resource intensive, some companies have manufactured dedicated hardware. Most of the time this kind of hardware is based a regular expressions matching engine implemented on a FPGA.
During this diploma, in the office of *Eneo Tecnología* in Seville, a network probe doing traffic classification with hardware accelerated pattern matching has been developed. This development, see figure 1, was based on (a) the free software **pmacct**, a multi protocol network probe developed by Paolo Lucente and (b) the NodalCore C-2000 Serie card as well as the Linux C API from the company *Sensory Networks*, see figure 2.

Results

The result of the development is a working but performance-wise suboptimal Network Probe doing traffic analysis using an hardware accelerated pattern matching engine. This can serve as a proof of concept and has given ideas about future works on the subject, moreover extensive benchmarks have been developed.

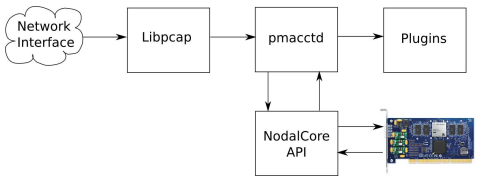

FIGURE 1: Hardware Accelerated Network Probe Design

FIGURE 2: Sensory Networks' C-2000 Card

Auteur: François DEPPIERRAZ
Répondant externe: Jaime NEBRERA
Prof. responsable: Hervé DEDIEU
Sujet proposé par: Eneo Tecnologia

Hes·so
Haute Ecole Spécialisée
de Suisse occidentale