ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

TIK Communication Systems

Prof. B. Plattner

MA/SA:

Animated Visualization of Network Traffic through Frequent Itemsets

Visualization is a strong approach to make complex data accessible to humans in a way that draws from our ability to visually capture important trends within seconds. This holds for almost any area including the monitoring of computer network traffic we are interested in.

We aim at exploring new techniques of animated visualizations to extend the toolbox of useful perspectives onto network traffic.

In this context we use frequent itemset mining (FIM) as a way to extract frequent patterns from large masses of network traffic data to separate important from less important details. The results of the FIM mining we display as a graph with frequent items as circular nodes having a size equivalent to their popularity, items as rectangular nodes annotated by their name/value, and edges linking nodes together based on their co-occurrence. Figure 1 shows a simple example that illustrates the prevalence of local and remote web servers, the dominance of two particular local DNS servers accessed by two-packet flows as well as all remote DNS servers. Finally, we see that NTP traffic (on port 123) is a popular application, too.

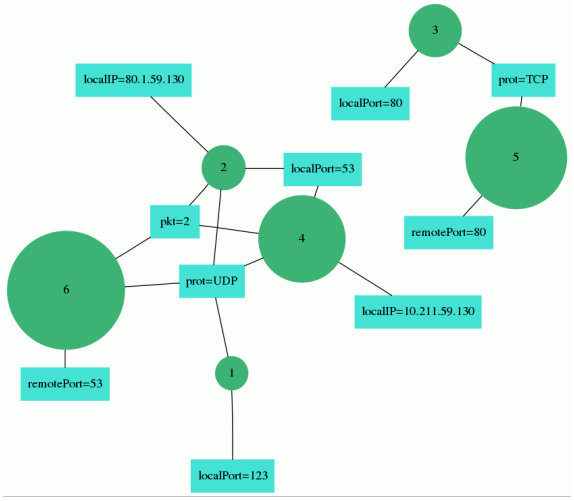

Figure 1: Visualization of frequent itemsets as found in a 10 min time interval during the 30th of July 2010 at 10:00 am. We set the threshold for a minimal itemset size to 5%.

While static displays convey information about a traffic snapshot, in contrast, animated visualizations bear the potential to make important trends and interesting anomalies intuitively visible.

Therefore, the goals of this thesis work are:

1. In a first introductory step the student uses the static FIM visualization approach to experimentally study filtering strategies to remove less interesting details from visualization. A basic software for this task and access to a large network traffic monitoring data archive is provided by us.

2. Next, dynamic graph layout algorithms that display sequences of graphs in such a way that identical parts remain stable over time have to be studied.

3. Then, a tool has to be programmed that implements the animated FIM visualization using a sliding window approach. Optionally, filtering strategies can be included that suppress less interesting parts from the animation and/or highlight most important trends.

4. Depending on work progress and student interests an integration of this new visualization approach into the NfSen network monitoring framework could be an additional task.

Requirements: C/C++, networking basics. This thesis work offers practical as well as theoretical tasks including the development of Internet traffic analysis software.

Interested? Please contact us for more details!

Contacts

- Prof. Eduard Glatz: eglatz@tik.ee.ethz.ch, ETZ H83