Visualizing Source-Destination Relationships of Network Traffic in the Internet

Florian Mansmann

Department of Computer and Information Science, University of Konstanz, Germany
mansmannn@inf.uni-konstanz.de
http://infovis.uni-konstanz.de/~mansmann

ABSTRACT

Network communication has become indispensable in business, education, and government. With the pervasive role of the Internet as a means of sharing information across networks, its misuse for destructive purposes, such as spreading malicious code, compromising remote hosts or damaging data through unauthorized access, has grown immensely in the recent years. The vast number of security incidents and other anomalies overwhelms attempts at manual analysis, especially when monitoring activity on service provider backbone links.

The classical way of monitoring the operation of large network systems is by analyzing the system logs for detecting anomalies. In this work, we present *Hierarchical Network Map*, an interactive visualization technique for analyzing network flow behavior by means of user-driven visual exploration. Our approach is meant as an enhancement to conventional analysis methods based on statistics or machine learning.

We superimpose a hierarchy on IP address space, and study the suitability of Treemap variants for each hierarchy level. Because viewing the whole IP hierarchy at once is not effective in most analysis tasks, we evaluate layout stability when eliding large parts of the hierarchy, while maintaining the visibility and ordering of the data of interest. A case study demonstrates how interactive visualization can be applied to gain deeper insight into large network traffic data sets.

The interdisciplinary approach integrating data warehouse technology, information visualization, and decision support, brings about the benefit of efficiently collecting the input data and aggregating over very large data sets, visualizing the results, and providing interactivity to facilitate analytical reasoning.

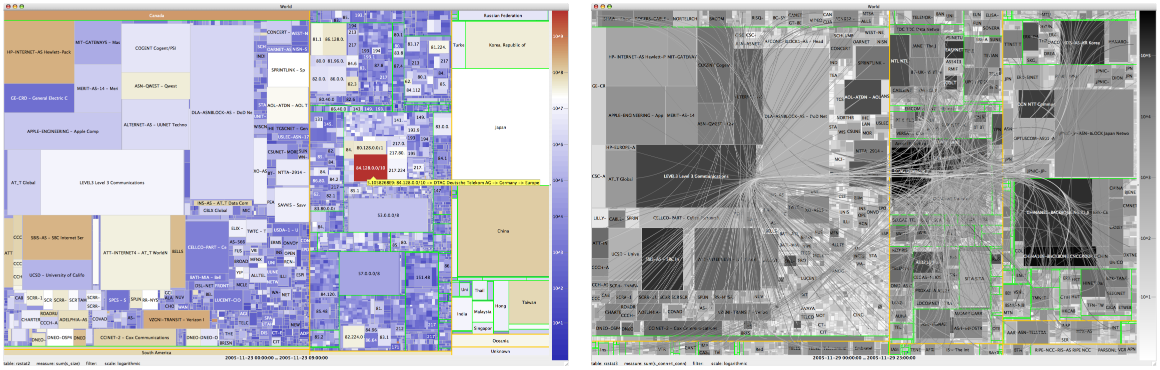

Figure 1: Multi-resolution HNMap approach (left) extended through edge bundles (right)