"Visualization and Monitoring of Network Traffic"

Dagstuhl Seminar 09211, May 17-20, 2009

-Executive Summary-

Daniel A. Keim (Universität Konstanz, DE)
Aiko Pras (University of Twente, NL)
Jürgen Schönwälder (Jacobs Universität - Bremen, DE)
Pak Chung Wong (Pacific Northwest National Lab., US)
Florian Mansmann (Universität Konstanz, DE)

Keywords. Computer Networks, Internet, Monitoring of Networks and Services, Visualization Animation

1 Motivation

The seamless operation of the Internet requires being able to monitor and visualize the actual behaviour of the network. Today, IP network operators usually collect network flow statistics from critical points of their network infrastructure. Flows aggregate packets that share common properties. Flow records are stored and analyzed to extract accounting information and increasingly to identify and isolate network problems or security incidents. While network problems or attacks significantly changing traffic patterns are relatively easy to identify, it tends to be much more challenging to identify creeping changes or attacks and faults that manifest themselves only by very careful analysis of initially seemingly unrelated traffic pattern and their changes. There are currently no deployable good solutions and research in this area is just starting. In addition, the large volume of flow data on high capacity networks and exchange points requires to move to probabilistic sampling techniques, which require new analysis techniques to calculate and also visualize the uncertainty attached to data sets.

2 Goals and Content of the Seminar

The aim of the seminar is to bring together for the first time people from the networking community and the visualization community in order to explore common grounds in capturing and visualizing network behaviour and to exchange upcoming requirements and novel techniques. The seminar also targets network operators running large IP networks as well as companies building software products for network monitoring and visualization. We believe that bringing experts from two usually separate fields together makes this seminar unique and we expect that the intensive exchange in a Dagstuhl seminar setting has high potential to lead to joint follow-up research.

The following research questions were suggested for discussion:

- What are suitable data analysis and visualization techniques that can operate in real-time and support interactive online operation?
- How can monitoring and visualization techniques be made scalable?

- How can distributed monitoring systems be self-organizing and adapt dynamically to changes in network and service usage?
- How can algorithms aggregate data within the network and trade accuracy of the measurement results against data collection overhead?
- What are suitable sampling techniques and how does sampled data impact data analysis techniques and data visualization?
- Which filtering, zooming, and correlation techniques can be applied in real-time?
- What are good techniques for visualizing unusual traffic patterns or very rare patterns?
- What are effective methods to detect and visualize intrusions, like (distributed) scan attempts and denial of service attacks.

While this item list was helpful as an orientation, not all of the items were actually covered during the seminar. Moreover, other concerns, such as NetFlow storage and retrieval, were emphasized in the presentations and discussions.

3 The Participants

The seminar gathered 36 researchers from the following 10 countries:

Country	Number of participants
Australia	1
Brasil	1
France	1
Germany	16
Israel	1
Netherlands	5
New Zealand	1
South Korea	1
Switzerland	3
USA	6

Most participants come from universities or state-owned research centers (33) while 3 participants were employed by industry or industrial research centers.

4 The Program

Monday (2009-05-18)

After the opening, the morning sessions featured the keynote talks:

Visualization Keynote
- Jack van Wijk: Network Visualization

Networking Keynote(s)
- Harald Weikert: Network Traffic Visualization with IsarFlow
- Felix Wu: On Detection and Analysis of BGP Anomalous Dynamics

In the afternoon sessions, short talks of the participants presented the participants' research activities in the fields of networking and visualization:

1)	Keith Andrews, TU Graz	The Usability of Information Visualisation Techniques for Network Monitoring
2)	Nevil Brownlee, University of Auckland	Collecting and Analysing Traffic Flow Data
3)	Isabelle Chrisment, Université Henri Poincaré - Nancy I	Measurements and Analysis of P2P Exchanges
4)	Stephan Diehl, Universität Trier	Working Group Results "We have a hammer, find a nail"
5)	Falko Dressler, Universität Erlangen	High-speed Monitoring and Intelligent data pre-selection for Attack Detection
6)	Glenn A. Fink, Pacific Northwest National Lab.	Cyber Analytics: Challenges and solutions for computer security
7)	Carsten Goerg, Georgia Institute of Technology	Interactive Exploration of Typed Networks
8)	Hans Hagen, TU Kaiserslautern	Visualization and Monitoring of Network Traffic
9)	Simon Leinen, Switch - Zürich	Visualizations in Network Operations and Management: What Works, What Doesn't, and What's
10)	Lars Linsen, Jacobs University - Bremen	Cluster Visualization in Network Traffic
11)	Florian Mansmann, Universität Konstanz	Monitoring and Intrusion Detection with NFlowVis
12)	John McHugh, Dalhousie University	FloVis a visual paradigm for forensic network data analysis
13)	Cristian Morariu, Universität Zürich	Distributed Traffic Analysis
14)	Stephen North, AT&T Research - Florham Park	Network Visualization and Service Monitoring Research in a Large ISP
15)	Adam Perer, IBM - Haifa	Improving Exploration of Networks by Integrating Statistics and Visualization
16)	Ramin Sadre, University of Twente	Three Remarks on Visualization
17)	Taghrid Samak, DePaul Univ. - Chicago	Using Space-Filling Curves in Visualization of Network Traffic
18)	Sebastian Schmerl, BTU Cottbus	Explorative Visualization of Log Data to support Signature Development and Forensic Analysis
19)	Carsten Schmoll, FhG FOKUS - Berlin	Fraunhofer FOKUS - interests in Visualization
20)	Juergen Schoenwaelder , Jacobs Universität - Bremen	Flow Pattern Analysis
21)	Mike Sips , MPI für Informatik - Saarbrücken	Exploring and Modeling the Local Behavior of Personal Machines
22)	Anna Sperotto , University of Twente	Working with network data: visualizing data relations
23)	Alexandru C. Telea , University of Groningen	Visualization of Large Network Structures: Bundled Edges or Node-Link Layouts?

The evening session was reserved for demonstrations of research prototypes accompanied by cheese and wine.

Tuesday (2009-05-19)

Four working groups were formed in order to inspire fresh and novel research. Thereby, particular care was taken that the groups are mixed in a way that each one contained experts of both fields. Each of the following questions was assigned to two working groups.

1) What could be applications of visualization in the area of network monitoring?
2) What visualization could be useful to solve networking problems?

After the 90 min discussions within the working groups, the results were shared and discussed with all participants of the seminar.

The social program of the event was scheduled on Tuesday afternoon. It included a wine tasting in the historic city Trier.

Wednesday (2009-05-20)

The morning of the last day of the seminar was reserved for discussions, conclusions and the closing remarks of the organizers.

5 Conclusions

The Visualization and Monitoring of Network Traffic seminar was a fertile meeting in which researchers from diverse background met. It included industry and academia, senior and junior researchers, multi-national representation, and people coming from several disciplines. This diversity resulted in interesting and useful discussions, new understandings of the fundamental concepts and problems in the field, and in new collaborations on an array of problems which were not well defined or identified prior to this seminar.

Several work groups during the seminar not only generated new insights into specific topics in the field of visual network monitoring, but also initiated ongoing joint work, with group members continuing the work they started at the seminar.
The seminar included multiple presentations and discussions. In particular, the largely disjoint research communities Networking and Visualization exchanged their methods and unsolved problems resulting in fruitful discussions and awareness of the respectively other field.

This seminar clearly illustrated the diversity, relevance, and fertility of the topics we presented and discussed. The intensity of the participants' involvement leads us to believe that the interactions fostered by the seminar will generate a lot of follow-up research, and eventually lead to practical use as well.