Network Data Visualization

Jonatan Schroeder

University of British Columbia

Nov 7, 2007

Papers covered

- Richard A. Becker, Stephen G. Eick, Allan R. Wilks, *Visualizing Network Data.* IEEE Transactions on Visualization and Computer Graphics (TVCG), Vol 1, No 1, March 1995, pp 16-28.
- Eleftherios Koutsofios et.al., *Visualizing Large-Scale Telecommunication Networks and Services.* Proceedings of IEEE Visualization 1999, pp 457-461.
- Bill Cheswick, Hal Burch, and Steve Branigan, *Mapping and Visualizing the Internet* USENIX, San Diego, CA, June 2000.
- G. Conti et.al., *Countering Security Analyst and Network Administrator Overload Through Alert and Packet Visualization.* IEEE Computer Graphics and Applications (CG&A), March 2006.

Motivation

- Increasing network measurement data
- Nodes, links and possibly spatial information
- Many variables
  - Directed or indirected links
  - Natural or abstract spatial layout
  - Categorical or quantitative data
  - Static or time-varying data

Natural graph representation

- Structure sometimes is secondary
- Links and nodes data is usually the focus
- Graph representation may hide important information
- Large volume of data

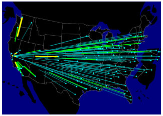
Covered approaches outline

- SeeNet (1995)
- Swift-3D (1999)
- Cheswick Internet map (2000)
- RainStorm/Rumint (2006)

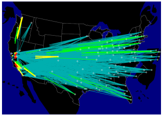
SeeNet

- Richard A. Becker, Stephen G. Eick, Allan R. Wilks, *Visualizing Network Data.* IEEE Transactions on Visualization and Computer Graphics (TVCG), Vol 1, No 1, March 1995, pp 16-28.
- **When**: 1995
- **What**: Telecommunication – long distance calls
- **Task**: Identifying overloads in specific circuits
  - Overloads during 1989 San Francisco earthquake
- **How**: Variation of graph representation, geographic information and matrix form

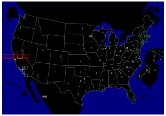
Visualization



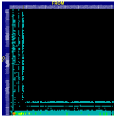
Visualization



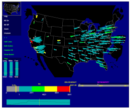
Visualization



Visualization



Visualization



Characteristics

- Parameter focusing
- Line shortening
- Zoom and pan

Critique

- Geographic information
- Direction using line shortening
- Multiple visualization options
- Several parameters
- Hard identification of incoming links

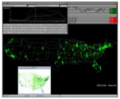
SWIFT-3D

- Eleftherios Koutsofios et.al., *Visualizing Large-Scale Telecommunication Networks and Services.* Proceedings of IEEE Visualization 1999, pp 457-461.
- **When**: 1999
- **What**: Telecommunication – link usage
- **Task**: Identifying unanswered/lost calls
- **How**: Geographic representation, bars and color-coding, 3D zoom

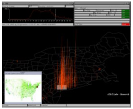
Characteristics

- Statistical 2D visualizations
- Pixel-oriented 2D visualizations
- Dynamic 3D visualizations

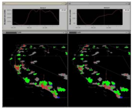
Visualization



Visualization



Visualization



Critique

- 3D visualization may be confusing
- Poor presentation
- Overlaping 3D bars over color-coding may hide information

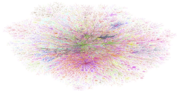
Internet Map

- Bill Cheswick, Hal Burch, and Steve Branigan, *Mapping and Visualizing the Internet* USENIX, San Diego, CA, June 2000.
- **When**: 2000
- **What**: Internet topology (`traceroute`)
- **Task**: Map the structure of the topology at a given time and during a period
- **How**: Graph representation, line charts, animation

Network Mapping

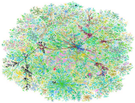
- Periodic tests in a intranet and in 90,000 nodes in the Internet
- Tests started in August 1998
- Search for DNS entries - specific networks and countries

Visualization

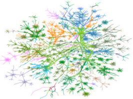


"Peacock-on-the-windshield"

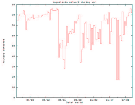
Visualization



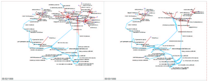
Visualization



Visualization



Visualization



Critique

- Graph representation interesting for local representation
- Filtering by DNS interesting, although not reliable for country-level
- Chart representation interesting for a singular specific task

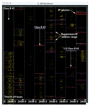
Rainstorm

- Bill Cheswick, Hal Burch, and Steve Branigan, *Mapping and Visualizing the Internet* USENIX, San Diego, CA, June 2000.
- **When**: 2006
- **What**: Security attacks on GeorgiaTeck campus network
- **Task**: Focus limited resources in real threatenings
- **How**: 2D map IP number × time, parallel coordinates

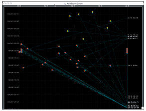
Motivation

- Georgia Institute of Technology uses 2.5 class B IP ranges
- Too much attacks data to analyse and filter
- Data obtained using Snort and Ethereal
- Study with students and professionals - overload
- Hard to deal with time-based data

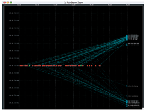
Visualization



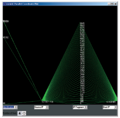
Visualization



Visualization



Visualization



Critique

- Describes user evaluation
- Identification of singular hosts and IP ranges
- Represents time
- Identification of multiple attacks to single host
- Visualization of the overall situation
- Multiple columns – department identification

Conclusion

- Best visualization for networks depends on the task
- Graph representation is limited
- Geographic information is an option, but also limited

Network Data Visualization

Jonatan Schroeder

University of British Columbia

Nov 7, 2007