RadialNet

An Interactive Network Topology Visualization Tool with Visual Auditing Support

João Paulo S. Medeiros[1], Selan Rodrigues Santos[2]

<joaomedeiros@dca.ufrn.br>, <selan@dimap.ufrn.br>

[1]Department of Computer Engineering and Automation – DCA
[2]Department of Informatics and Applied Mathematics – DIMAp
Federal University of Rio Grande do Norte – UFRN

Frascati, Italy, Oct. 2008

Agenda

- Introduction
  - Motivation
  - Requirements
  - Related work
- Network Security
  - Nmap
- Visualization
  - Reference Model
- RadialNet
  - The Application
  - Some Features
  - Case Studies
- Final Considerations

Introduction

Motivation

- Data retrieval and visualization is a challenge for large networks;
- Data presentation is generally textual;
- Information Visualization can be applied to network related data;
- These techniques can be used to provide an effective network topology representation.

Introduction

Requirements

A network visualization tool must...

- Be able to represents large networks (more than hundreds of nodes);
- Provide mechanisms to navigate the network topology and its data;
- Afford a simple and complete (all data) visual representation;
- Get rid of or offer solutions for data occlusion.

Introduction

Related Work

There are problems with existing network visualization tools:

- fe3d: the three-dimensional approach implies data occlusion;
- Nagios: the radial visualization is good, but it lacks features;
- Cheops-ng: it is not based on solid information visualization techniques.

Network Security

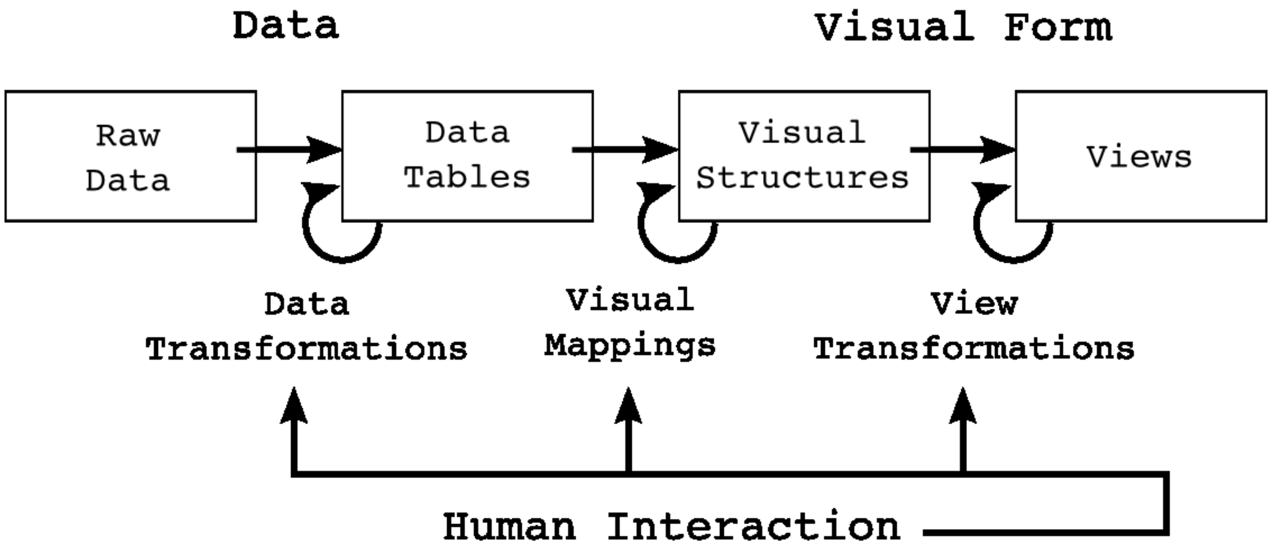
Nmap

Tool used to acquire network data. Features:

- Detect networks devices (routers, firewalls, wireless access points, ...);
- Detect remote operating system (OS fingerprinting);
- Perform Ports scan and service discovery (FTP, DNS, HTTP, ...);
- Discover Network topology (using Traceroute);
- Determine link latency and route disruption.

Visualization

Reference Model (Stuart Card)

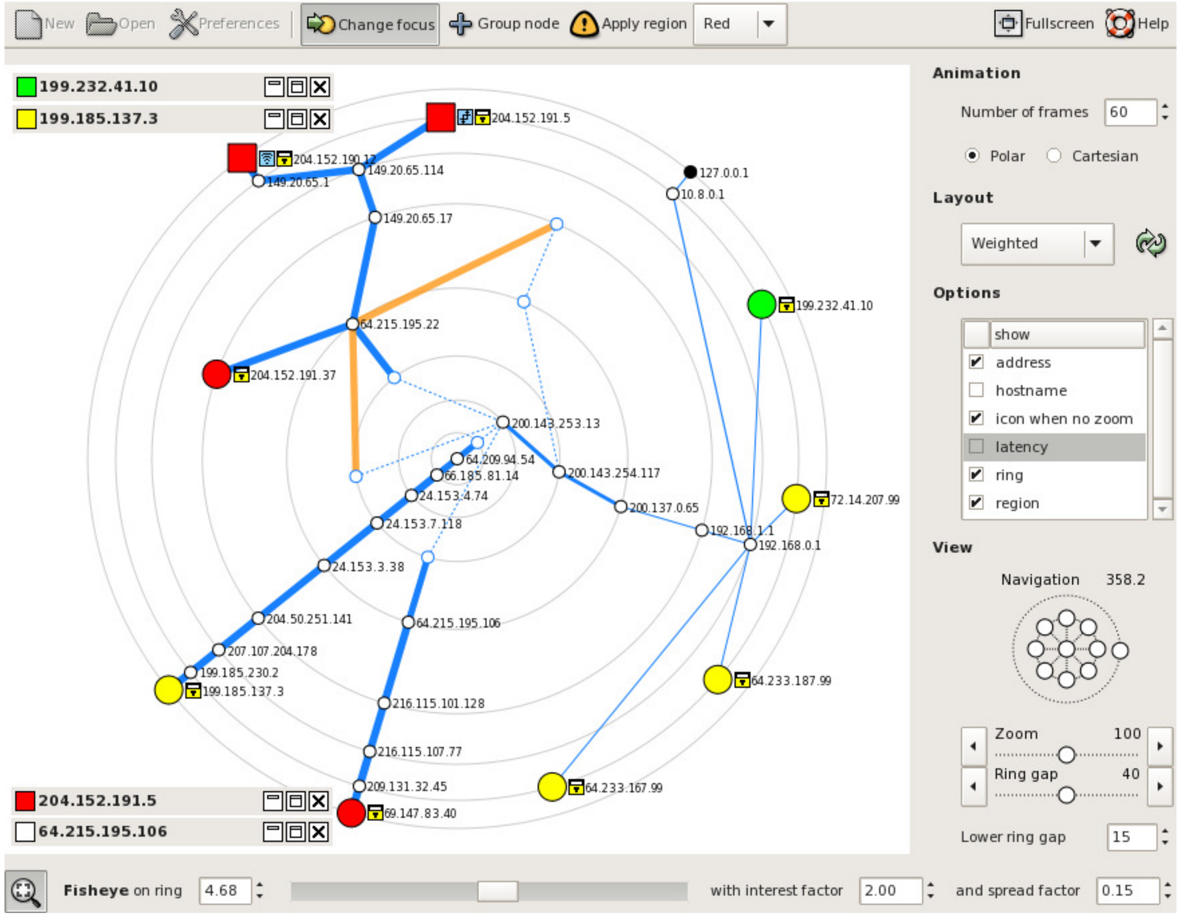


Used reference model.

Reference Model (phases)

- Data Transformation
  - Data tables organized in variable types;
- Visual Mappings
  - Association between data tables and retinal variables;
  - Node-links diagrams (radial layout);
  - Visual marks + graphical properties;
- View Transformations
  - Navigation (animation, zooming, panning, reorganization of nodes);
  - Detail-on-demand;
  - Strategies to handle occlusion (filtering, fisheye distortion, subgraph collapsing).

The Application



Animation

Number of frames 60

● Polar ○ Cartesian

Layout

Weighted

Options

- show
- ☑ address
- ☐ hostname
- ☑ icon when no zoom
- ☐ latency
- ☑ ring
- ☑ region

View

Navigation 358.2

Zoom 100

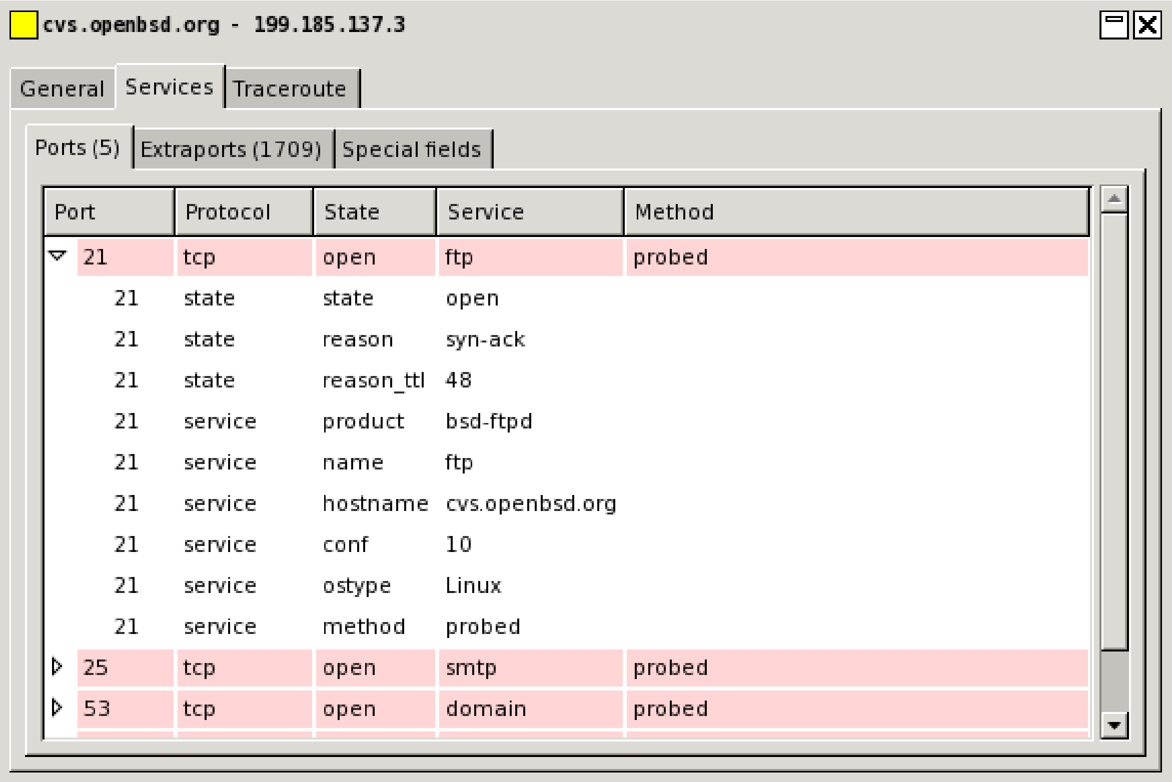
Ring gap 40

Lower ring gap 15

Fisheye on ring 4.68 with interest factor 2.00 and spread factor 0.15

`http://www.dca.ufrn.br/~joaomedeiros/radialnet/`

Some Features



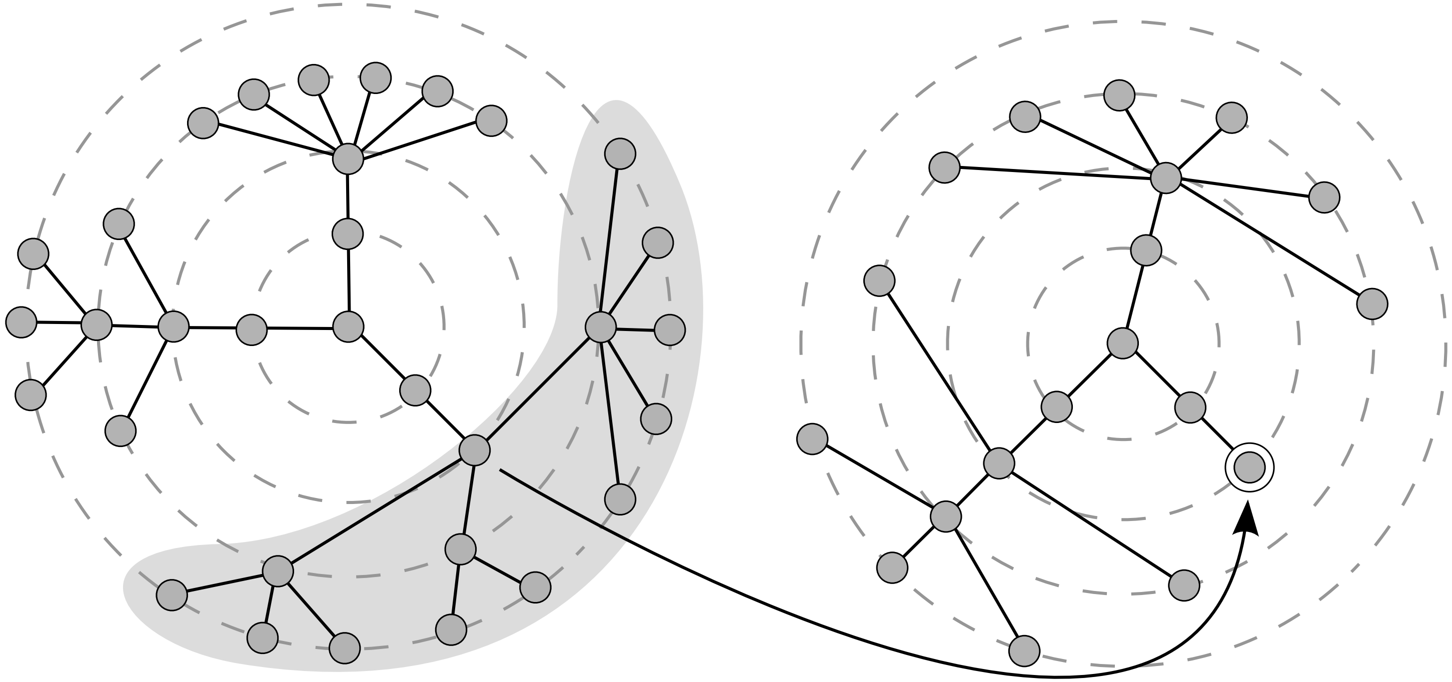
cvs.openbsd.org - 199.185.137.3

Port	Protocol	State	Service	Method
21	tcp	open	ftp	probed
21	state	state	open	
21	state	reason	syn-ack	
21	state	reason_ttl	48	
21	service	product	bsd-ftpd	
21	service	name	ftp	
21	service	hostname	cvs.openbsd.org	
21	service	conf	10	
21	service	ostype	Linux	
21	service	method	probed	
25	tcp	open	smtp	probed
53	tcp	open	domain	probed

- ▷ Open ports details;
- ▷ Filtered ports;
- ▷ Running services information;
- ▷ Detailed traceroute.

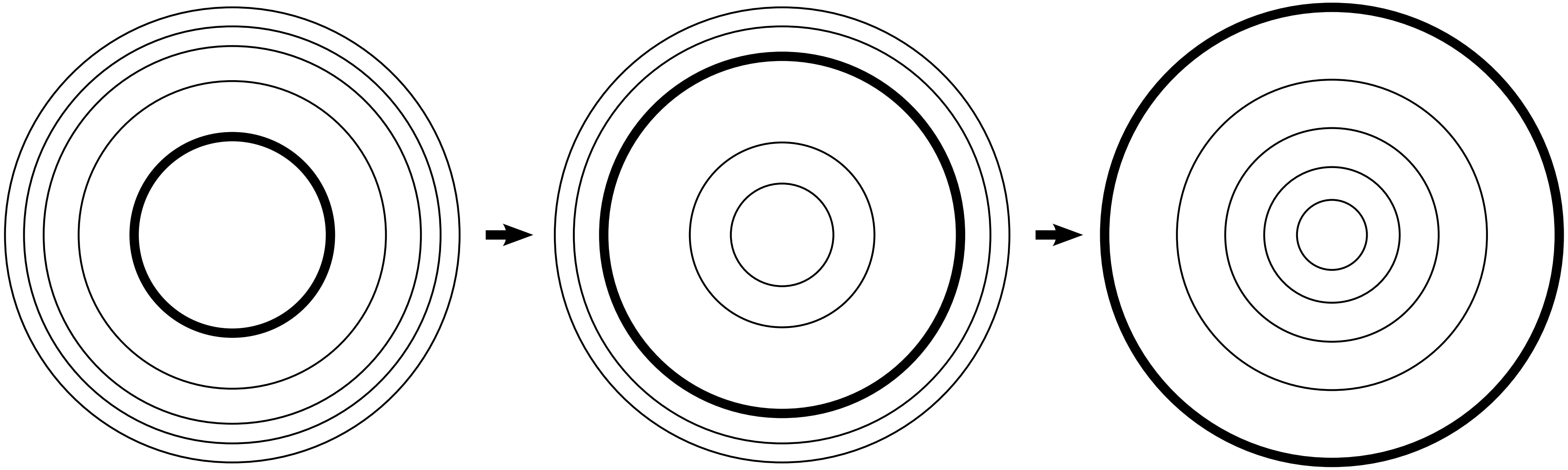
Detail on demand.

Some Features



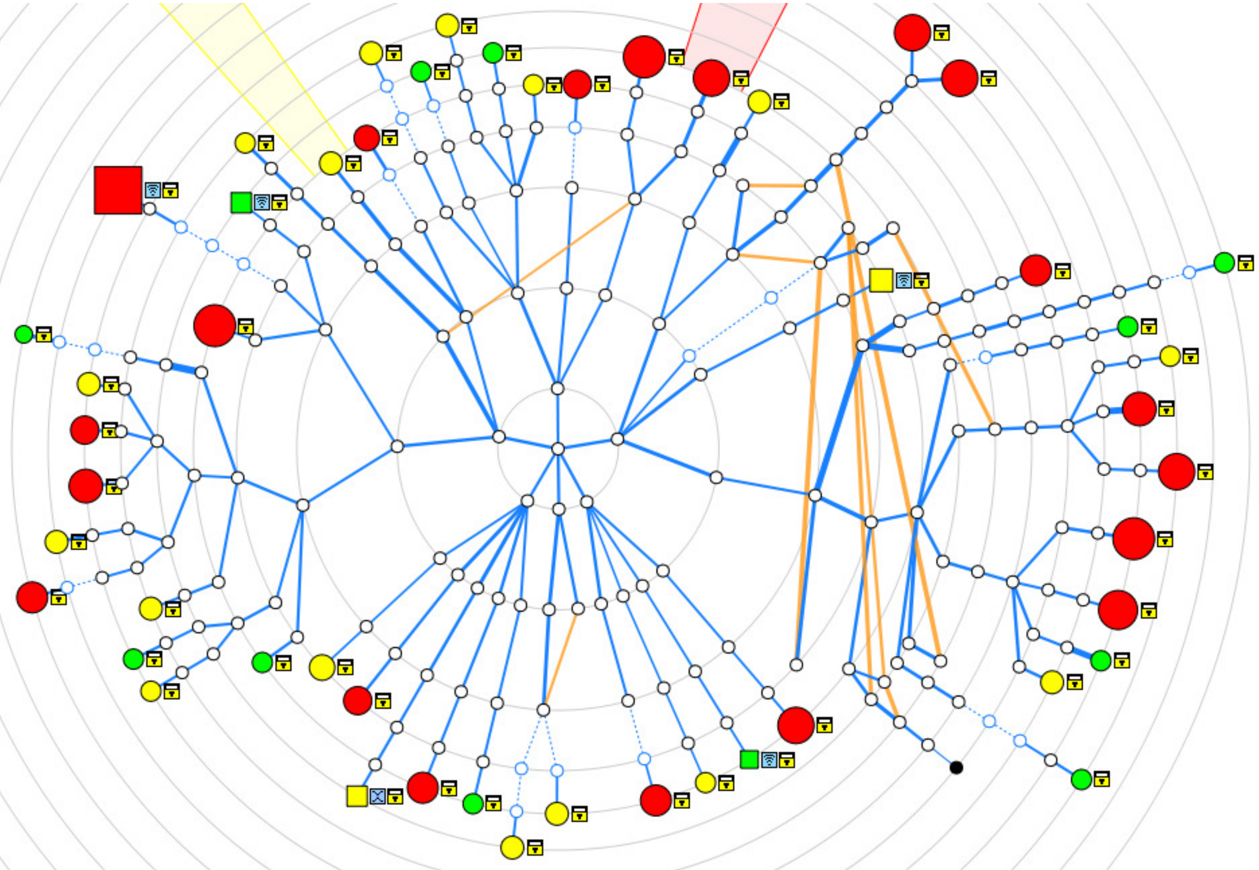
Collapsing (grouping) nodes.

Some Features



Fisheye based effect.

Case Study – Brazilian Universities



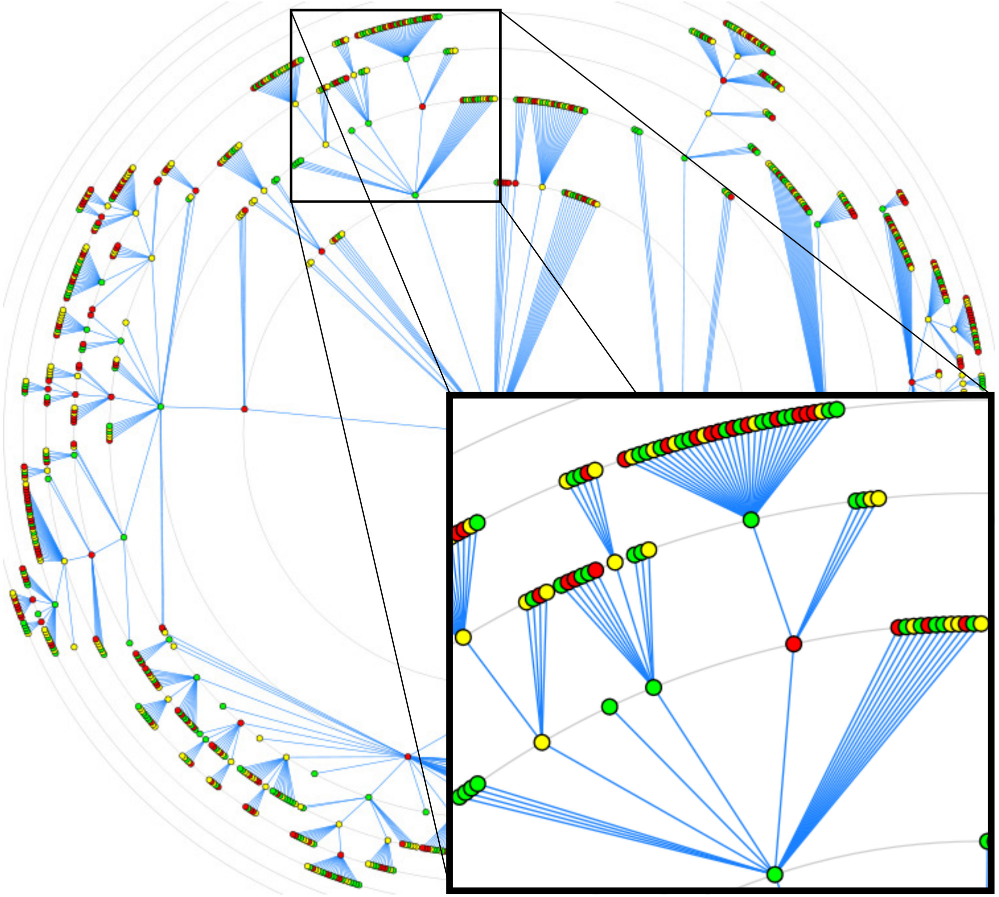
- Node shape;
- Color and size;
- Line thickness;
- Icons;
- Orange lines;
- Dashed lines.

50 Brazilian universities (238 nodes).

Case Study – Brazilian Universities

- Several hosts have security problems;
- All hosts have filtered ports;
- We can identify switches, routers and WAPs;
- Alternative routes;
- Hop counting;
- Network bottlenecks.

Case Study – Large Networks



Visualization of 1000 nodes.

To handle occlusion:

- Filtering;
- Subgraph collapsing;
- Fisheye distortion.

Final Considerations

Nmap/Umit Integration

- Radialnet was developed during Google Summer of Code 2007;
- Has been integrated to Umit (Nmap frontend);
- Added to Nmap/Zenmap.

Conclusion

- Information Visualization models and techniques can help network security management!

Future Work

- Perform a cross-referencing between captured data and NIST vulnerability database;
- Use other tools to acquire data can extend RadialNet applicability:
  - Network administration;
  - Load balancing analysis.

Contact

joaomedeiros@dca.ufrn.br