Network Security Simulation Visualization

Ali Shiravi, Hadi Shiravi, and Ali A. Ghorbani {ali.shiravi, hadi.shiravi, ghorbani}@unb.ca

Introduction

Information visualization has matured over the past years and has been applied to a variety of applications. It has been only few years that this work been applied to the network security domain and other related information assurance problems.

Measuring the amount of damage caused by an attack is of great value. From this information network administrators can respond to these threats and ultimately protect the organizations data integrity and confidentiality.

Modeling and simulation is one of the corner stone's of Computer Science and its applications are widely acknowledged in network security evaluation. Here at NSL, we have developed an assessment tool to analyze the state of the network, in relation to different attack scenarios.The development of such security simulations and modeling tools present an interesting challenge which motivates the further research of visualizing information obtained from simulation.

Background

The basic idea with focus–plus–context–visualizations is to enable viewers to see the object of primary interest presented in full detail while at the same time getting a overview–impression of all the surrounding information — or context — available.

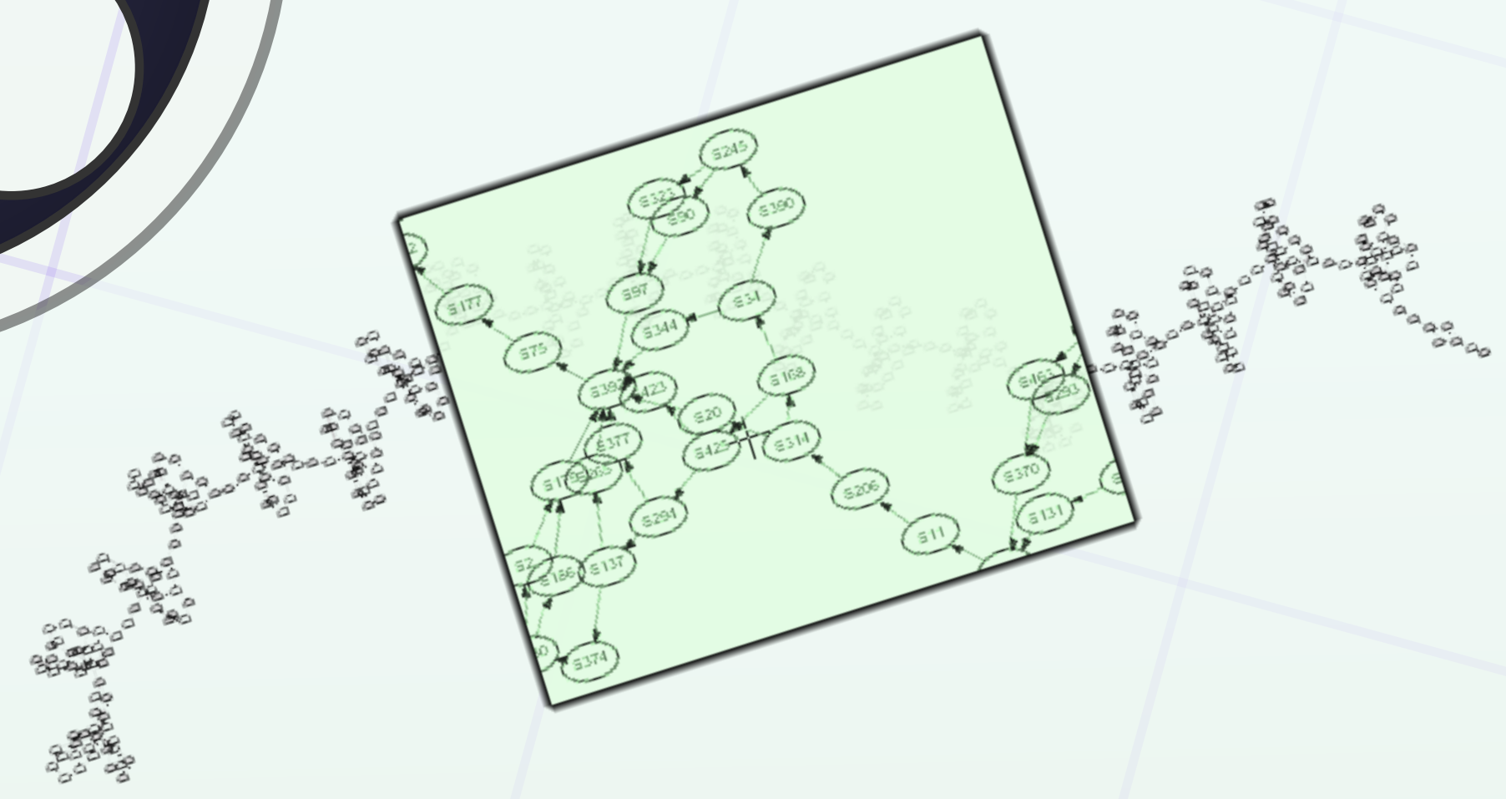
The currently existing focus-and-context methods are:

- Spatial methods. The image created with an existing visualization is distorted to allow more space for the currently more important objects, and less for the context. (e.g. fish-eye views, etc.)
- Dimensional methods. Users can move a focus over a visualization to display different data about the same objects. These methods don't display more objects, but they allow more or different data dimensions of the already displayed ones. (e.g magic lenses, etc.)
- Cue methods. In an existing visualization, objects that meet certain criteria are stressed by assigning visual cues to them so that they are more prominent to the viewer without hiding the context. An example of such a method is to use color saturation and brightness.

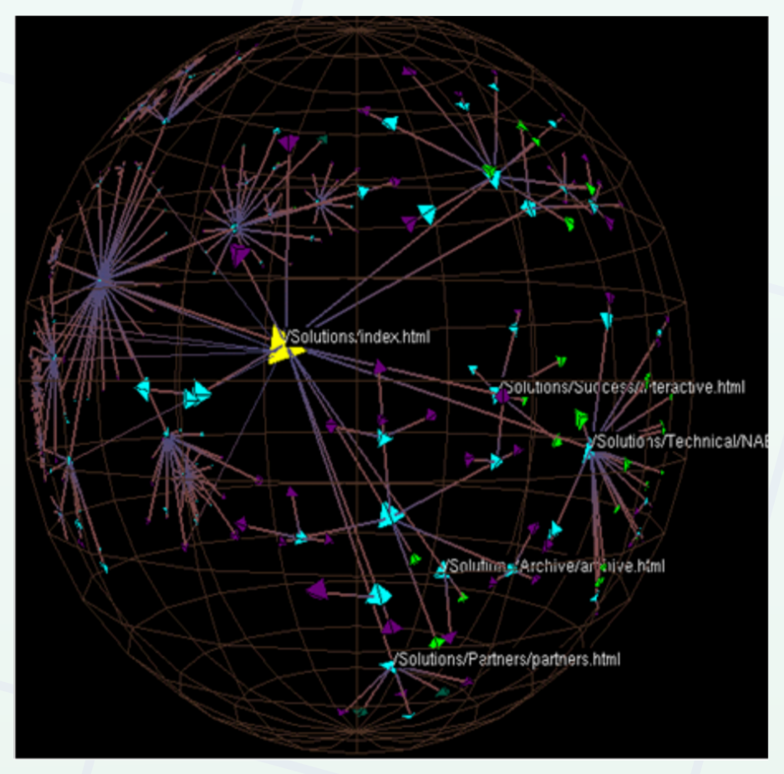
The ultimate goal is to apply current visualization techniques for the information obtained from the simulation. From our primary analysis of this information, we have decided to focus our work on utilizing techniques referred to as "context and focus" methods. The amount of data and information available to visualize in this project is substantial, but what is more important than that is to present this vast amount of inter-related information to showing detail and context simultaneously.

Some this information is as below.
Network topology, Connectivity, Infection dispersion, Affected Hosts
Reachability , Network impact, Attacker attributes (IP, DNS resolution)
Access paths, Offence presentation, Network traffic statistics
Potentially exposed data (IP, Asset, service properties, significance)
Specific Host info (no. of vulnerabilities, online time, open ports, etc.)
Flow statisticsProtocol statisticsVulnerability infoFirewalls (open ports, blocked IPs, vulnerabilities, exposure, etc.), Security analysis

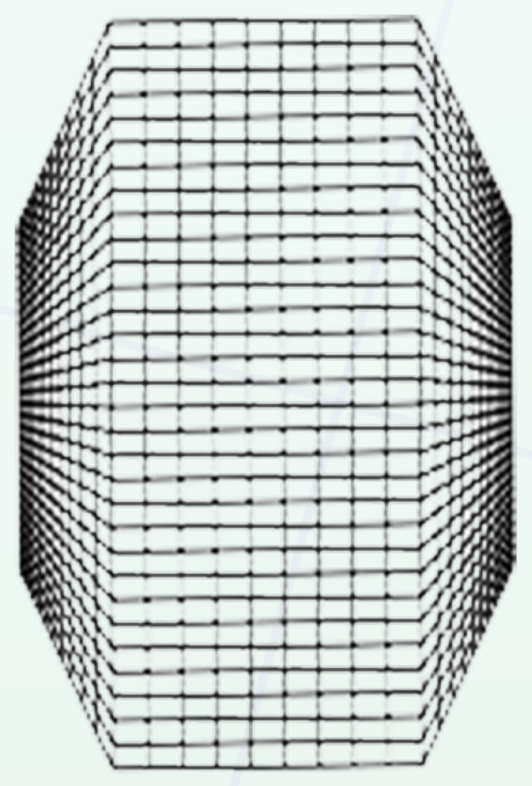
Objectives



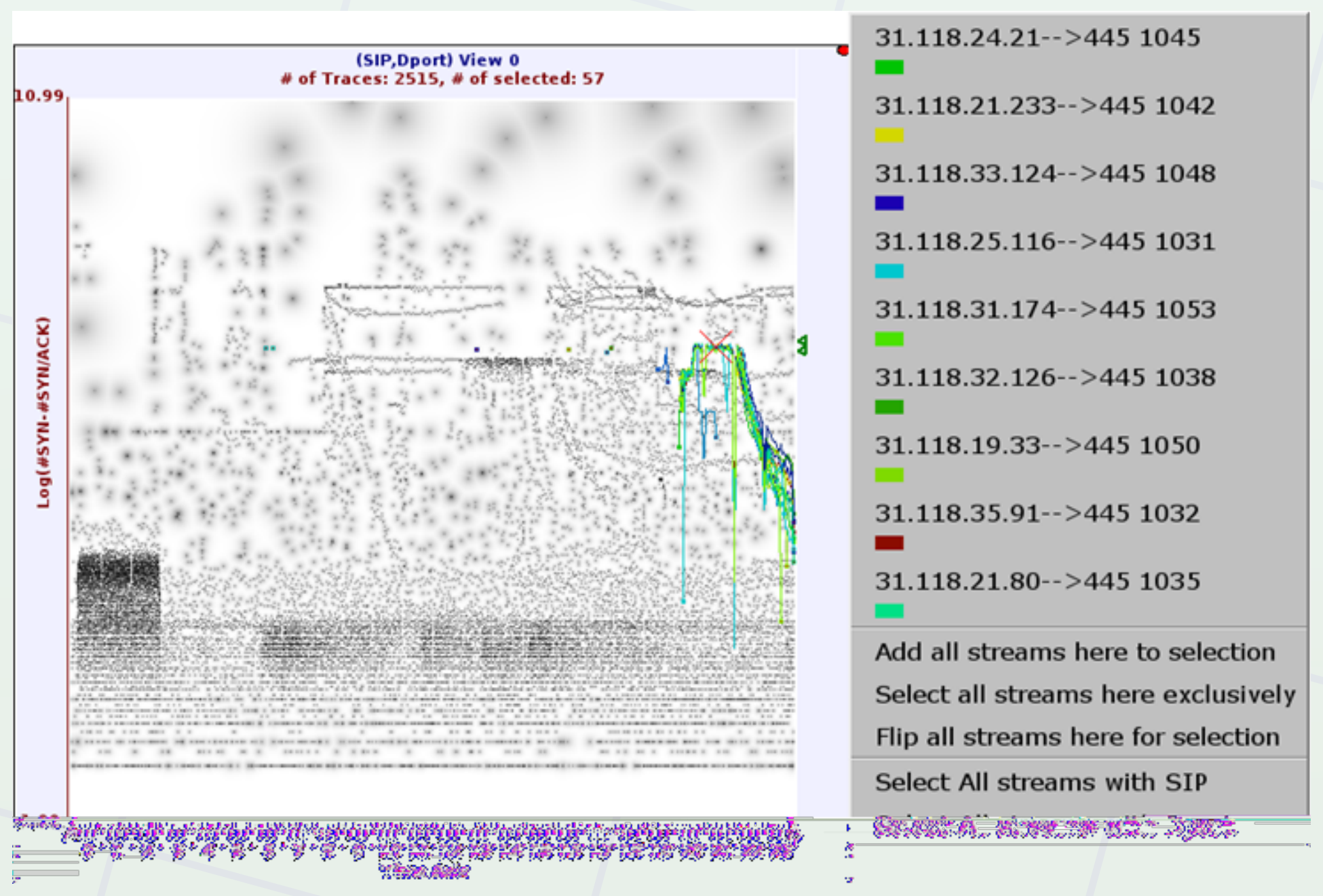
Magnification



3D Hyperbolic Space



Perspective Wall

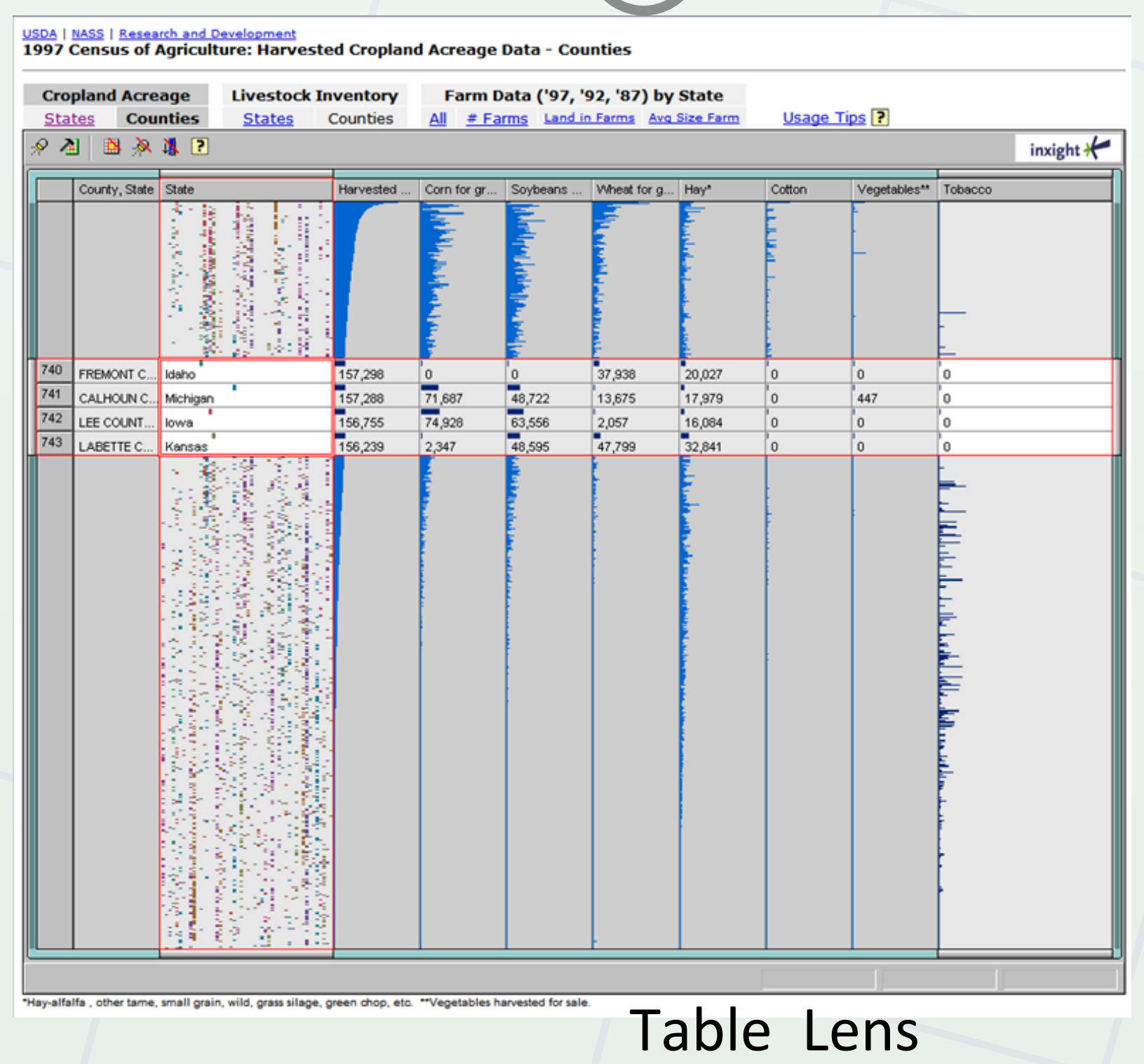


(SIP,Dport) View 0
# of Traces: 2515, # of selected: 57

31.118.24.21-->445 1045
31.118.21.233-->445 1042
31.118.33.124-->445 1048
31.118.25.116-->445 1031
31.118.31.174-->445 1053
31.118.32.126-->445 1038
31.118.19.33-->445 1050
31.118.35.91-->445 1032
31.118.21.80-->445 1035

Add all streams here to selection
Select all streams here exclusively
Flip all streams here for selection
Select All streams with SIP

Histographs



USDA | NASS | Research and Development
1997 Census of Agriculture: Harvested Cropland Acreage Data - Counties

	County, State	State	Harvested ...	Corn for gr...	Soybeans ...	Wheat for g...	Hay*	Cotton	Vegetables**	Tobacco
740	FREMONT C...	Idaho	157,298	0	0	37,938	20,027	0	0	0
741	CALHOUN C...	Michigan	157,288	71,687	48,722	13,675	17,979	0	447	0
742	LEE COUNT...	Iowa	156,755	74,928	63,556	2,057	16,084	0	0	0
743	LABETTE C...	Kansas	156,239	2,347	48,595	47,799	32,841	0	0	0

*Hay-alfalfa , other tame, small grain, wild, grass silage, green chop, etc. **Vegetables harvested for sale.

Table Lens

Examples of Focus and Context

network
security
laboratory

UNIVERSITY OF
NEW BRUNSWICK
UNB