EG UK Theory and Practice of Computer Graphics (2013), pp. 1–2
Silvester Czanner, Wen Tang (Editors)

NetVis: A network traffic visualization tool

SUBMISSION ID

AFFILIATION ID

Figure 1: *New EG Logo*

Abstract

Computer network traffic visualizations attempts to deliver improved understanding of traffic on a network to an observer. Many existing tools opt for graph or plot-based visualizations to detect patterns or outliers in the data, but still largely provide a segmented view of any data feed. In this paper, we present a novel network traffic visualization framework that makes use of a variety of complementary visualizations to obtain better situational awareness. Our proposed solution is to look at different.. more

Categories and Subject Descriptors (according to ACM CCS): I.3.3 [Computer Graphics]: Picture/Image Generation—Line and curve generation

1. Introduction

JH: A few guidelines to writing:

- No need to mention this is a student group paper as this is being submitted to a research conference. The editors will know because we have to sign up as a student paper (there is a best student paper prize), but the reviewers won't know.
- Keep your language as formal as possible: Avoid 'I' and limit the use of 'we'. No banter or double-ententres. Text should be clear and concise.
- Pseudo-code/Maths is welcomed if needed. Typesetting using the program package: http://en.wikibooks.org/wiki/LaTeX/Algorithms
- No references in the abstract. No footnotes in the paper.
- Other general EG paper writing guidelines can be found below (commented out).
- Conference submission guidelines: http://www.eguk.org.uk/TPCG13/submission/submission.html
- JH will submit the final copy of the paper.
- JH: Better title is welcomed if you have one! :)

2. Related Work

JH will write this

3. NetVis Architecture

Describe the architecture, how traffic is read and processed, the format of the CSV, why was it designed the way it is? Add diagram How real-time is it? What filtering do you support + protocols? How modular is the code base, can one simply script in another vis?

4. NetVis Visualizations

4.1. GUI

Describe the GUI in detail

4.2. Attribute Distribution

4.3. Dataflow

Port scan attack example?

4.4. Spinning Cube

The spinning cube is an implementation of an existing visualization tool known as the spinning cube of potential doom [**?**].

4.5. Traffic Volume

4.6. Heat Map

4.7. Activity Groups

5. Discussion

Why were the five vis picked? how do they complement each other?

5.1. User Workflow

Describe a typical workflow of an analyst, include a workflow diagram (e.g. UML or CONOPS (concept of operations, see)) Describe how the visualisations complement each other Describe how many alerts it can process at any time and accumulative.

5.2. Advantages

List them

5.3. Limitations

List them

5.4. Future Work

Future work includes streaming in live data, improving vis.. This will be addressed by.. Be sure to reveal some, but not too much

6. Conclusion

In this paper we have presented..