VAST 2013 Mini-challenge 2: Visualizing Network Status for Assessment and Response

Mohan Krishna Kodali, Ujwal Manjunath, and Andrew A. Schaefer

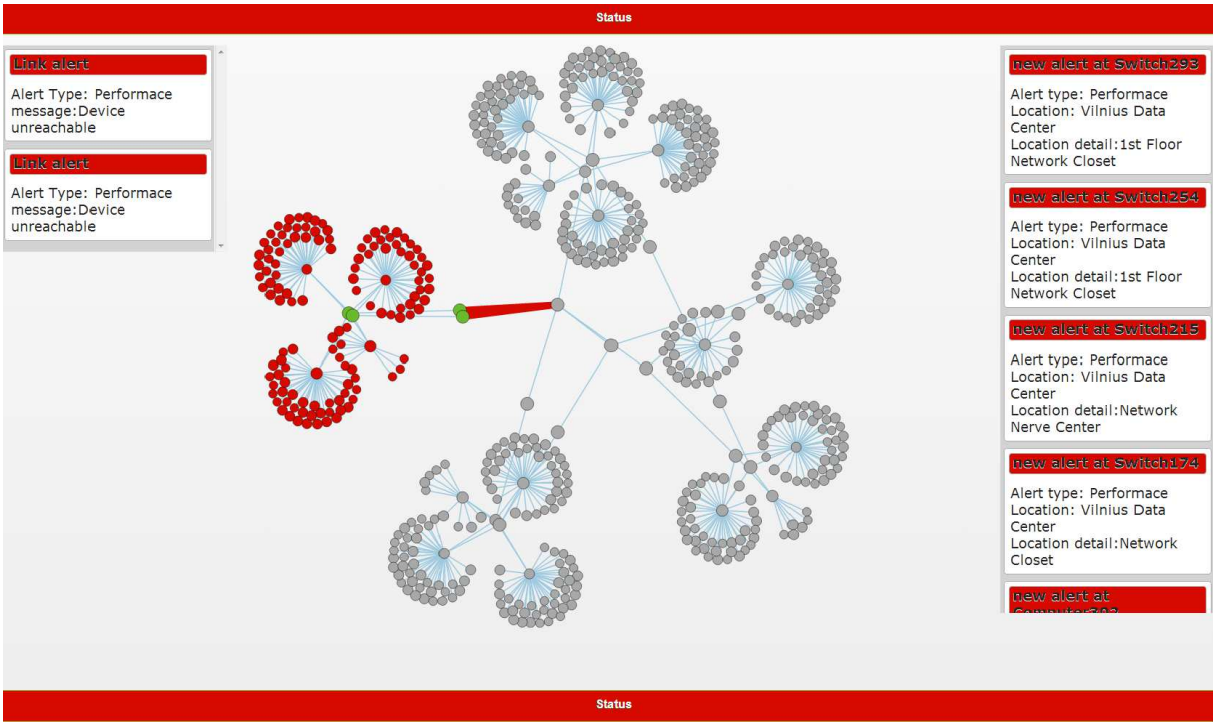

Fig. 1. Network visualization display module.

Abstract—This project is an attempt at the VAST 2013 Mini-challenge 2. We present our design for visualizing a large-scale network status and events. The main focus is our display module which enables situational awareness for Network Operations staff.

1 Introduction

The VAST 2013 Mini-challenge 2 presents a largely open-ended design challenge for innovative graphical designs to support situational awareness for large-scale computer networks. The ultimate goal is to design a single integrated visualization that will enable situational awareness of the entire network.

Our project looks at common practices in network visualizations, adopts a non-interactive approach to enable optimal reporting and awareness of network status.

In the following sections we will discuss Related Work, including current network visualization techniques and software; Data, including the challenge requirements; Tools; Approach, including our design decisions and how they work to meet the requirements; Conclusion; and Final Thoughts.

- *Mohan Krishna Kodali, Old Dominion University, Norfolk, VA 23508. mkoda001@odu.edu*
- *Ujwal Manjunath, Old Dominion University, Norfolk, VA 23508. umanj001@odu.edu*
- *Andrew A. Schaefer, Old Dominion University, Norfolk, VA 23508. aschaefe@cs.odu.edu*

Manuscript received 31 March 2013; accepted 1 August 2013; posted online 13 October 2013; mailed on 27 September 2013.
For information on obtaining reprints of this article, please send e-mail to: tvcg@computer.org.

2 Related Work

2.1 BANKSAFE

A visual situational awareness tool for Large-scale computer networks This was one of the VAST mini challenge of 2012. It is a situational awareness application for large scale computer networks. To enhance security and provide situational awareness for large scale computer networks Banksafe uses a combination of multiple visual representations. [1]

2.2 zenoss

This is one more situation awareness display for a large-scale network. It consists of a dashboard that shows system information resources and webpages, important error-level device events, Geographical high-level view, troubled devices. Navigation menu lets you access major system features which is divided into events, infrastructure, reports and advanced. The main content of the Dashboard comprises portlets, which provide information about the system and infrastructure (Device Issues, Google Maps, Zenoss Issues, Production States, Site Window, Top Level (Root) Organizers, Messages, Object Watch List)[1]

[1] http://www.zenoss.com/

2.3 Flowing Data

There are lots of interesting things about display of large networks in flowingdata.com. It is a large repository of examples of different kinds of visualizations. Two recent examples are shown in Fig. 2 [2] [3].

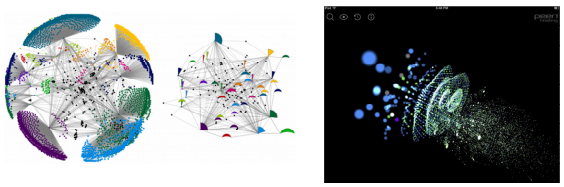

Fig. 2. Network visualizations from flowingdata.com

3 Data

Due to the open-endedness of this challenge, there was no dataset provided. Instead, a thorough description of the requirements and desired elements were discussed, as well as a background of the current environment.

3.1 Challenge Background

The challenge is provided by the fictitious company Big Enterprise, they have a global network consisting of several hundred thousand computers, which is expected to grow over time. Big Enterprise has commissioned this challenge to design a new Network Awareness Display for their Network Operations Center (NOC). In addition to the NOC, there are offices worldwide, each with their own computers that will connect and disconnect without coordinating through the NOC. The network operations manager has expressed concerns with their current system including, multiple displays required, wasted time digging through information, information cues and unclear and inconsistent, and important connections between events are not obvious.

3.2 Challenge Requirements

The major goal in designing the visualization is to provide a means for the NOC staff to asses the network status and enable situational awareness. This should allow for answering questions such as:

- Is everything normal?
- If not, how serious are the deviations?
- Will important components fail within the next few minutes? hours?
- Are key components broken or failing?
- Is there significance of any particular failure or trend?

At a minimum the display should:
1. Provide an accurate portrayal of the network.
2. Communicate information and knowledge about the current situation in the context of the network. This information should be accurate, clear, and useful.

The display should assess the status of network across three categories:

- Health: Are all the computers behaving as expected?
- Security: Are there any attacks that might affect the Enterprise?
- Performance: Are there data transfer issues affecting network speed?

The assessment of incidents within these categories should be further categorized according to severity:

- Normal Activity: everything is operating as expected
- Routine Issue: common problems with a well-known solution
- Non-routine Issue: new or infrequent problem
- Crisis: severe and/or multiple issues occuring simultaneously

4 Tools

The display was created in Javascript using the d3 toolkit, using CSS for styling. We also made use of php scripts to simulate polling and event occurrence. We made extensive use of JSON for passing network structure and event information. Additionally we utilized C and python for JSON creation and testing.

5 Approach

Our approach to this challenge was to focus first and foremost on the display design and work backwards as time permitted. In this vein, we identified three major segments to the overall system shown in Fig. 3:
1. The network and associated monitoring software
2. The event aggregator
3. The visual display

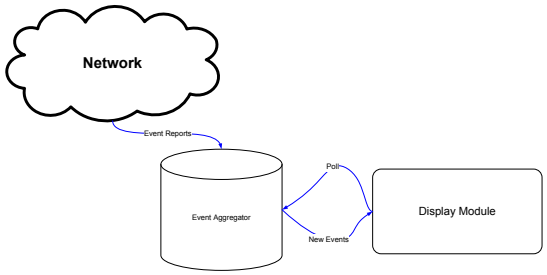

Fig. 3. Overview of entire system

Throughout this section we will discuss the assumptions we made for our design, important design decisions and features, as well as how these decisions and features meet the requirements of the challenge.

5.1 Assumptions made

In focusing on the display we made the following assumptions with regards to the other aspects of the system. The network and computers will have the appropriate monitoring software, virus-detection, load reporting, etc. This software will be configured to detect events of interest and upon detection will create and submit an event report to the event aggregator. The display module will poll the event aggregator for new events periodically and update the display accordingly.

Ultimately, we make the assumption that the monitoring software and event aggregator are responsible for analyzing events and determining their classification across the two categories: class (Health, Security, or Performance) and Severity (Normal, Routine, Non-Routine, Crisis). The display module is solely responsibly for displaying the event information it receives and should not make any changes to that information.

5.2 Design Motivation

We drew our initial motivation from looking at a myriad of existing network visualizations and tools. In collecting these visualization we analyzed them to assess what aspects where beneficial and which were confusing or unhelpful.

5.3 Design Decisions

Our guiding design decision was to make our display non-interactive. Because the display is supposed to be a large heads up display for the entire NOC staff, we wanted to minimize the interference of point-and-click features that could only be utilized by one person at a time. Instead we decided our display should provide as much information as possible and be able to quickly guide staff to the important events and allow individuals to utilize desktop tools to explore the situation further as needed.

Our second major design decision was to display the network topology rather than attempt to capture the geographic layout. Knowing where a device is geographically is not a vital as knowing where it is in the topology and how critical it is to the overall operation of the network. As events occur, the geographic data will be displayed in the sidebar with all the supporting information.

In our design we took the four severity statuses and assigned them the standard red-orange-yellow-green color coding, red indicating a crisis event, and green a normal condition.

5.4 Design Features

Our Display module consists of 3 main components. Fig. 4 shows our prototype mockup. The components are the Status Indicator Bars (one on top and one on bottom), the Event Details pane, and the main Network Display.

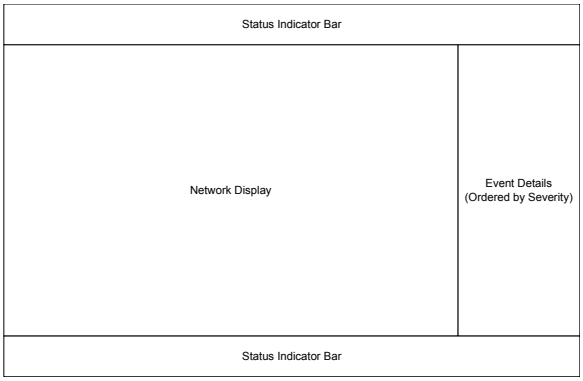

Fig. 4. Display Prototype

The Network Display contains the network topology being monitored, each monitored device is represented by a node, and monitored connections are represented by edges. The node size varies slightly for each device, determined by a criticalness value. A key device will have a high criticalness and will receive a larger node, where a regular device will have a smaller node size. Under normal conditions all edges are colored grey and edges are colored blue. As events are reported for a node or edge, the coloring changes to indicate the severity of the event. Once resolve the node/edge will turn green for a short time before returning to its neutral color.

The Status Indicator Bar is designed to be a one-glance indicator of the situation. It will be colored green during normal conditions when there are no issues. As events occur, it will flash briefly and update color to indicate the severity of the events. It is designed to flash to attract attention as the condition of the network is changing. It will remain the color of the most severe event until resolution, at which time it will downgrade to the next most severe event, until all issues are resolved and will return to green.

Finally, the Event Details pane, will display the details of all ongoing events sorted by severity. When new events occur the will be added to this pane in the appropriate order. Events are color coded as well, to maintain consistency throughout the display. This is designed to provide the supporting information to assess the situation and determine where to go and which additional tools to use to address the issues and resolve. This is the area where the geographic details will be displayed as well as device names/identifiers to allow for thorough troubleshooting by NOC staff.

5.5 Meeting the Requirements

Here we will discuss how our display design meets the requirements of the challenge.

5.5.1 Network Size

We use d3's force layout as the basis for displaying our graph, this will accomodate any number of nodes and edges. The nodes and edges are reported by the event aggregator upon initialization.

5.5.2 Network Growth

Our display accepts updates to the network structure and adds nodes and edges dynamically. It will accommodate any amount of growth.

5.5.3 Normal Operation

Staff will easily be able to identify normal operation conditions through the one-glance Status Indicator Bar, if it is green, then there are no outstanding issues and normal operation can be assumed.

5.5.4 Severity of issues

When there are issues, the status indicator will be a non-green color. The color will be determined by the severity of the events reported. This will allow quick assessment of how critical the situation is. Additionally, staff will be able to scan the Event Details pane for further information.

5.5.5 Key Components

While the network topology should assist staff in determining the status of key components based on where they lie in the network, we have also added a size variance to the displayed nodes. Larger nodes represent more critical devices.

6 Future Work

Given additional time, our next steps would entail work on the event aggregator and possibly the monitoring software. For the event aggregator we would like to design a database to store events and an interface for the display module to query for new events to display.

For the monitoring software, we would like to create a module to create event reports that would submit to the event aggregator. It is feasible this module could be created as an add-on to existing anti-virus software or similar security software

It would be our goal to allow these components to be fully customizable, to allow for adjusting thresholds for triggering various events, and the ability to add new events over time.

Additional work could be done to make a more robust layout algorithm, including adapting to various network sizes.

7 Conclusion

In this project we present an initial approach to the VAST 2013 Mini-challenge 2. We focus on the display aspect, and present a functioning display that polls for events and updates the display accordingly. It is designed to meet the requirements of the challenge, while provide accurate, clear, and useful information.

We outline our design of the full system, and briefly discuss the future work required to fully flesh out the design.

8 Final Thoughts

8.1 Problems Faced

The major difficulties we faced were for the data and coming up with a design. Being a real time display for a network, there was no data available and we had to create our own data files which took us some time.

The other difficulty we faced was getting an idea on the initial design of the project. There were lot of thoughts running about which type of visualization to use, for example: a world map or using a dashboard with different events, etc.

We also faced few minor problems during the time of visualization like managing the display within the boundaries of the dashboard, handling time delay when simulating the events, etc.

8.2 Lessons Learned

Beyond the cursory expansion of knowledge of Javascript and d3 for visualization. We spent a lot of time working with JSON's. We exclusively use JSONs as the data structure returned to the display upon polling for events and structure.

8.3 Contribution of each group member

Mohan Krishna Kodali Creating JSONs, scheduled group meetings and sent out updates and worked on project report and PowerPoint.

Ujwal Manjunath Lead development of the visualization and also contributed to project PowerPoint.

Andrew Schaefer Creating JSONs, visualization, worked on Project report and PowerPoint.

References

[1] F. Fischer, J. Fuchs, F. Mansmann, and D. A. Keim. Banksafe: A visual situational awareness tool for large-scale computer networks: Vast 2012 challenge award: Outstanding comprehensive submission, including multiple vizes. In *Visual Analytics Science and Technology (VAST), 2012 IEEE Conference on*, pages 257–258. IEEE, 2012.

[2] K. Rees. Network diagrams simplified, May 2012.

[3] N. Yau. App shows what the internet looks like, Mar. 2013.