The Center for Cyber Defenders

Expanding computer security knowledge

Firewheel

Matthew Ghormley (NMT); Sneha Venkatesan (UCLA);
Nick Hilbert (MS&T); Ethan Sterk (CU)

Project Mentors: Kasimir Gabert & Todd Jones, Org. 5638

Usability Project

Problem Statement:

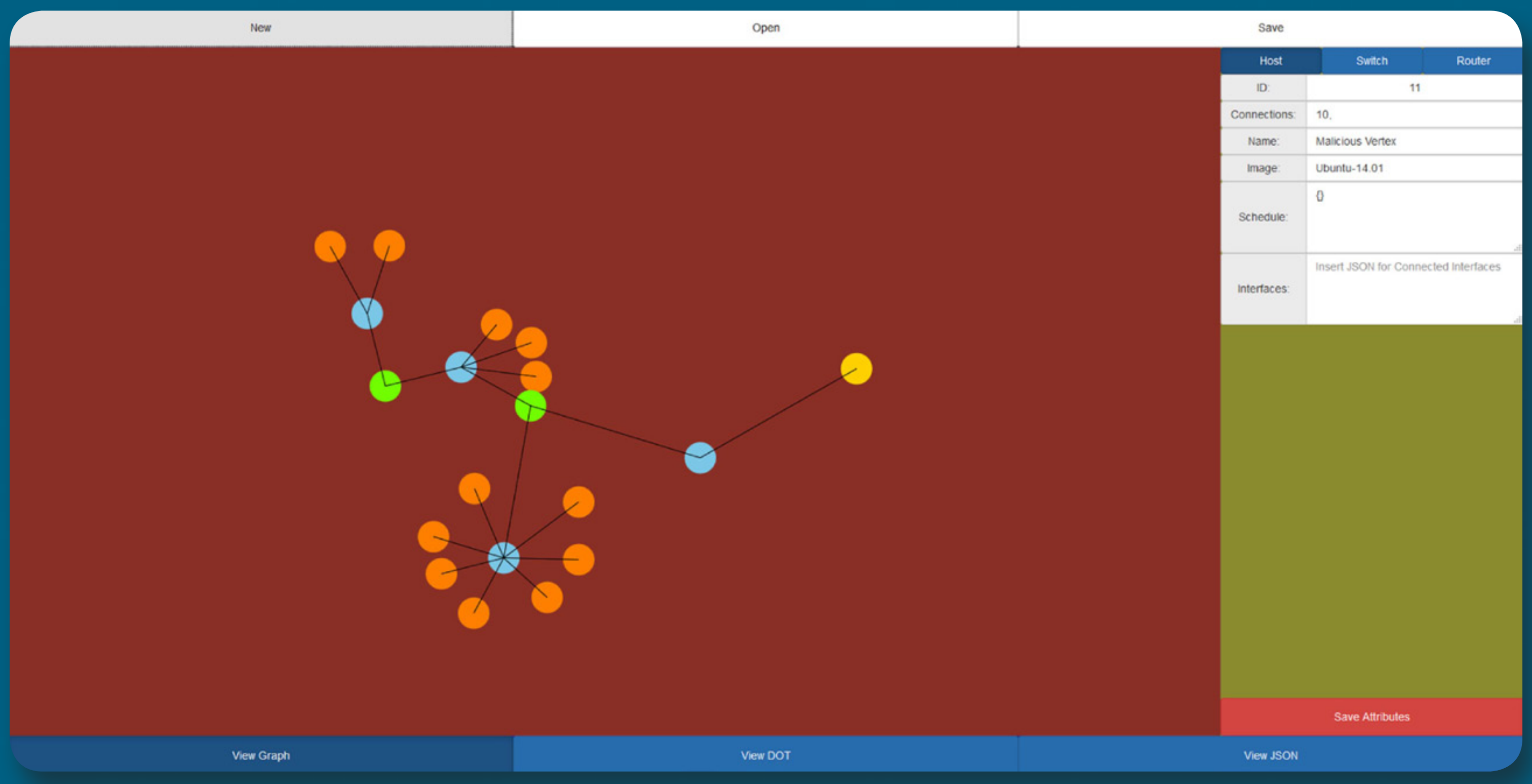
Over the past 10 years, Sandia has been researching and developing a platform for emulating and analyzing large complex information systems. From the ashes of past Emulytics® tools, a new flame for large scale system emulation has emerged – Firewheel.

Objective and Approach:

Since Firewheel can be used for emulating many different types of systems, it needs to be robust to account for different changes per network. Thus, improving user experience with Firewheel is the main goal of this project. The improvement chosen was to implement a GUI so system creation would be streamlined. This web application would be used to allows users to visually lay out and examine what a network would resemble before running the experiment in Firewheel.

- Users will then be able to create more elaborate networks using the knowledge gained from each vertices' attributes

Results:



ID: 11
Connections: 10,
Name: Malicious Vertex
Image: Ubuntu-14.01
Schedule: {}
Interfaces: Insert JSON for Connected Interfaces

GUI showing an example network

This web application provides users with the ability to see a network being created before running the emulation in Firewheel. Instead of needing to change a python script, the user can instead select a node (or nodes) and change the details with a click of a button. As vertices in the graph are updated, a separate JSON file is updated in real-time to account for these changes.

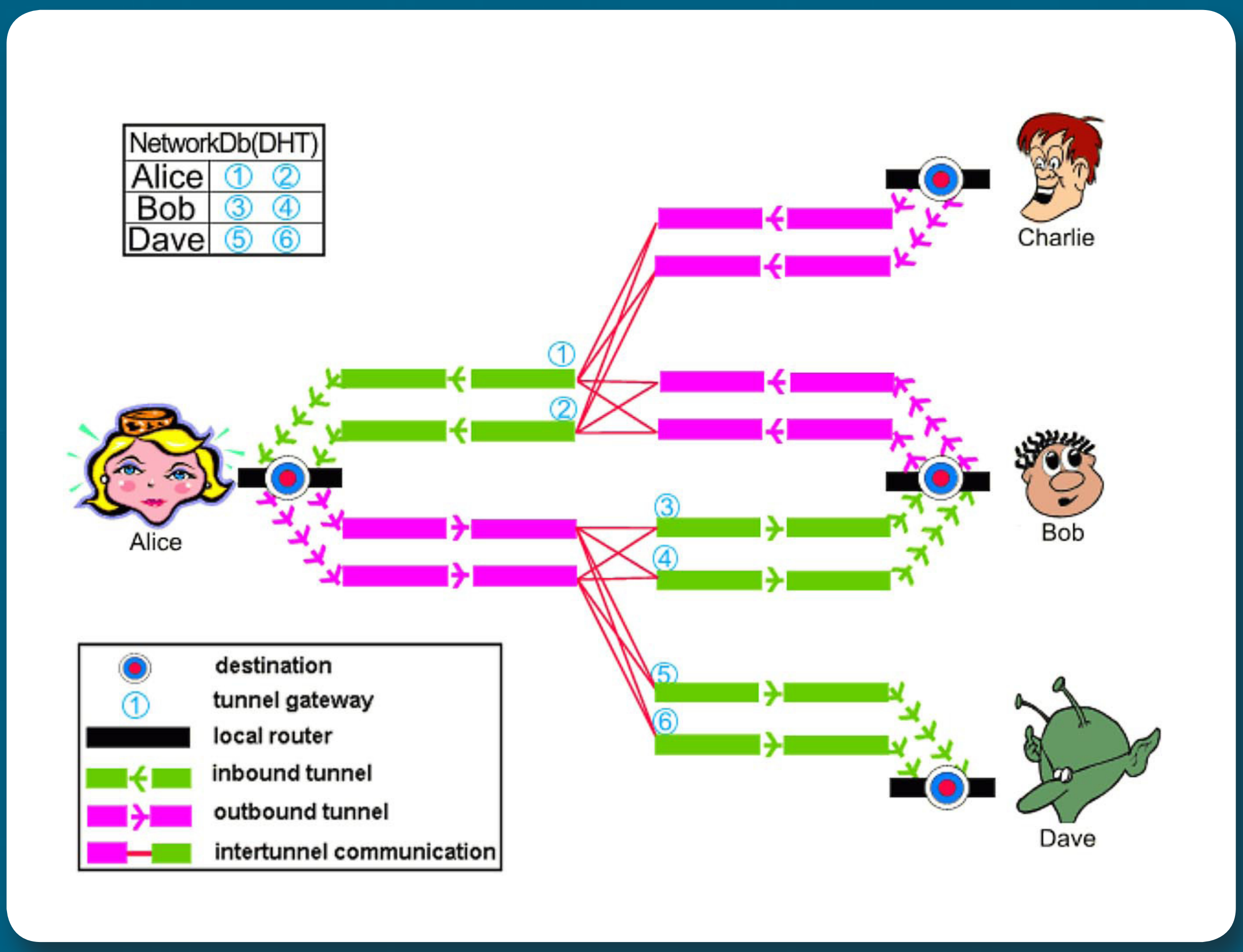
Future Work:

1. The next step to improving the GUI is to create an option that allows for direct JSON manipulation which updates the graph concurrently.
2. The graph will also have the option to show a DOT file created in real time that can be used to view the graph in Gephi (or a similar application).

I2P Project

Problem Statement:

The Invisible Internet Project (I2P) is an overlay network commonly used for anonymous file transfers, chatting, blogging, and other internet applications. Furthermore, I2P is optimized for hiding services and provides fewer out-proxies to the web. Similar to Tor, I2P implements a unique routing protocol which encrypts many messages together called garlic routing. At each router, encryptions are either added or removed so that any singly router only knows about the preceding and following routers along a tunnel.



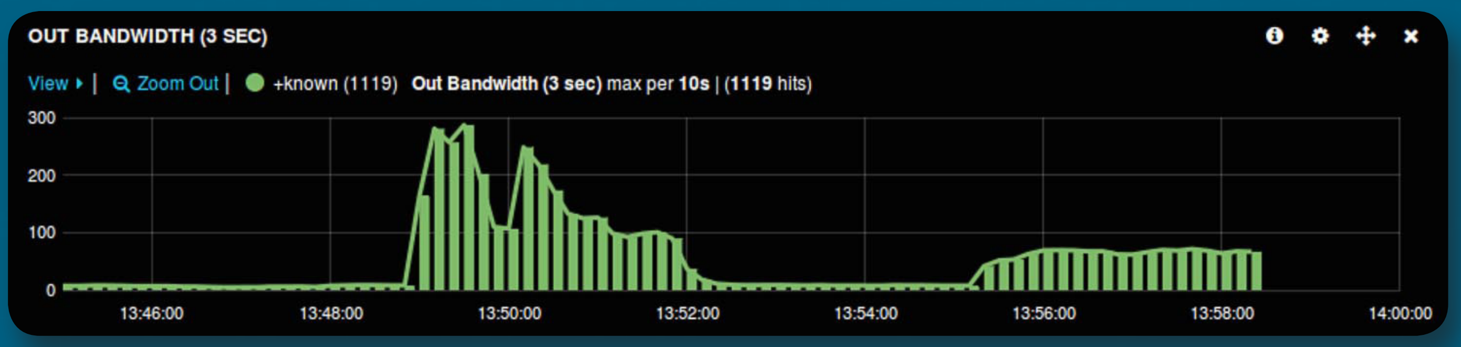
I2P network example

Objective and Approach:

Create an emulation of the I2P network that can be used to study and make predictions about the real I2P network. This emulation makes it possible to test applications before running them on the real I2P network.

- For example, an application that estimates the number of clients involved in the network can be tested by running it on the emulation, where the number of clients is not hidden. Then running the application on the real I2P can verify the results.

Results:



Out-bandwidth during an I2P emulation when traffic is set to download a large file every 5 minutes.

The results gathered from our emulation demonstrate that changing levels of traffic has a direct effect on variables like bandwidth. By developing an agent to simulate background traffic dependent on adjustable parameters, it's possible to create an emulation almost identical to the real I2P network.

Future Work:

1. Future work would involve analyzing the data from the real I2P network and comparing it against the data from the emulation.

Sandia National Laboratories

LOCKHEED MARTIN

Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000. SAND2016-XXXXC.

U.S. DEPARTMENT OF ENERGY

NNSA National Nuclear Security Administration