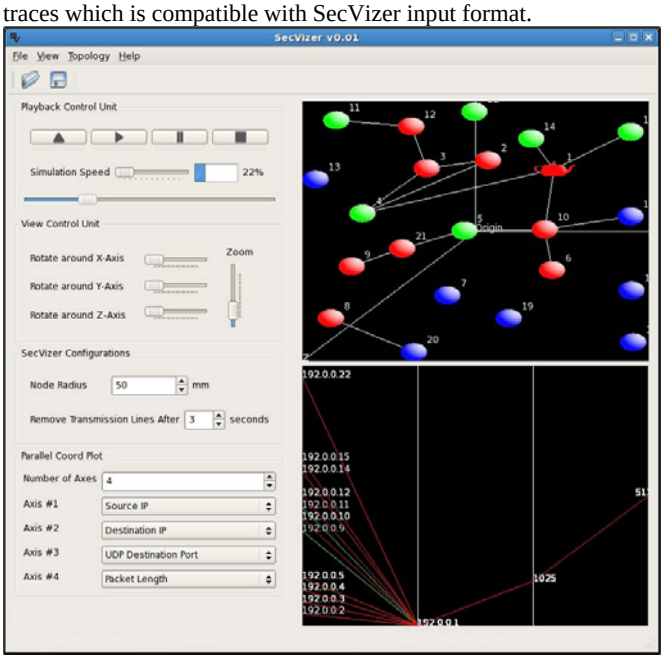
# SecVizer: A Security Visualization Tool for QualNet-Generated Traffic Traces

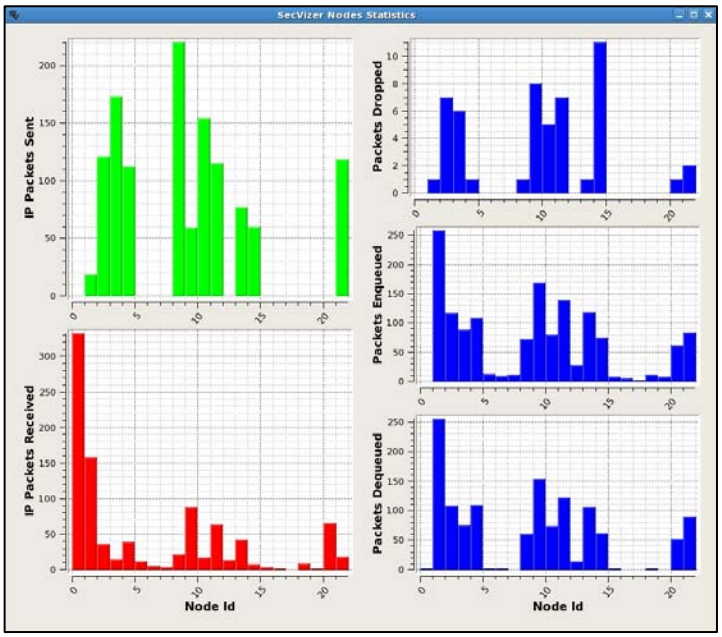
**Giovani Rimon Abuaitah, Bin Wang**
**BMW Lab, Wright State University, Dayton, Ohio**
abuaitah.2@wright.edu, bin.wang@wright.edu

SECVIZER

***Abstract***

Network simulators can produce huge traces of simulated traffic. These traces, usually presented as text, cannot be easily used to detect any malicious activity. Security visualization techniques have been developed over the decades as a result of various research efforts in the industry, academia, and even research carried out by individual hackers. These techniques can be powerful when employed in the field of network security where the visual recognition capability of human eyes can be exploited to allow an early detection of malicious acts. In this research project, we develop a new security visualization tool called "SecVizer". QualNet network simulator is used to simulate various security scenarios and produce traffic traces that would serve as inputs to our developed visualization tool. Employing a combination of techniques, our tool can render a QualNet network topology in 3-D, play animation of the traffic traces, and generate statistics. In particular, it combines both topology visualization in a 3-dimensional perspective and the parallel coordinate plot technique to obtain a faster and more effective identification of network vulnerabilities. By observing image patterns of the parallel coordinate plot, one can identify the different security attacks while at the same time exploring the network traffic volume and the topology being deployed. The tool has shown success in detecting simulated DDoS, port scan and host scan attacks. It was also able to detect real traffic attacks; real-time traffic is converted to QualNet-like traces which is compatible with SecVizer input format.




***SecVizer Current Features***

*3D Rendering of Network Topology:* The tool loads a QualNet topology file and displays it in 3D using OpenGL. Glut is being used to render a sphere representing a typical node, whereas a tea pot is rendered representing a node whose IP address is the intended destination address of the IPv4 packet.

*Parallel Coordinate Plot (PCP):* The user is able to choose up to seven different axes to be shown. The color scheme is as follows: packet sending intent is represented by a green line whereas a red line is being drawn whenever a packet is being received.

*3D Transformations:* Rotating the entire topology around the 3 axes (*x*, *y*, *z*), zooming in and out, and translating the entire topology.

*Display of Node Labels:* Displaying the node ids and IP addresses.

*Trace Visualization:* Sending nodes are green-colored. Receiving nodes are red-colored. A line is drawn from source to destination showing the transmission path.

*Animation controls:* Controlling the simulation animation process (e.g., play, stop, pause and slow down). A progress bar shows the percentage of simulation completion and a simulation slider shows the entire progress.

*Visualization Configuration Control:* Two configurable parameters; the node radius (i.e., how big a node should look like) and the transmission line elimination period (i.e., when should the tool remove the old lines off the display and reset the nodes color).

*Nodes Statistics:* The tool includes a window that presents the collected nodes statistics dynamically during simulation playback using bar graphs. For every node in the network, the graphs show the total number of IP packets sent, the number of IP packets received, the number of packets dropped as well as the number of packets enqueued and dequeued. Nodes' statistics are collected to help better identify the various security attacks. For example, replay attacks can be detected by observing the bar graph of the unexpectedly enqueued packets.