

**Methodology**

**Data Understanding**

We used 2 weeks of DARPA IDS log files for designing our visualization. Each log contains more than hundred thousand rows to parse, so we have to design the system which can do this task effectively. Our system can take any DARPA IDS dataset directly without any pre-processing of the data and renders the visualization. The log files from the dataset contains the multiple attributes like timestamp, duration attack source IP address, attack destination IP address, source and destination port details and the most important attack types and score.

We have to use Microsoft Excel for the understanding of the attributes and data. It gives an idea about the format of the attributes, delimiters and the important fields for the designing our visualization effectively. It also gives a basic understanding of the flow of the data which help to come up with an effective visualization.

**Visual Design**

We have mapped the following visual design with the network attributes to develop our visualization

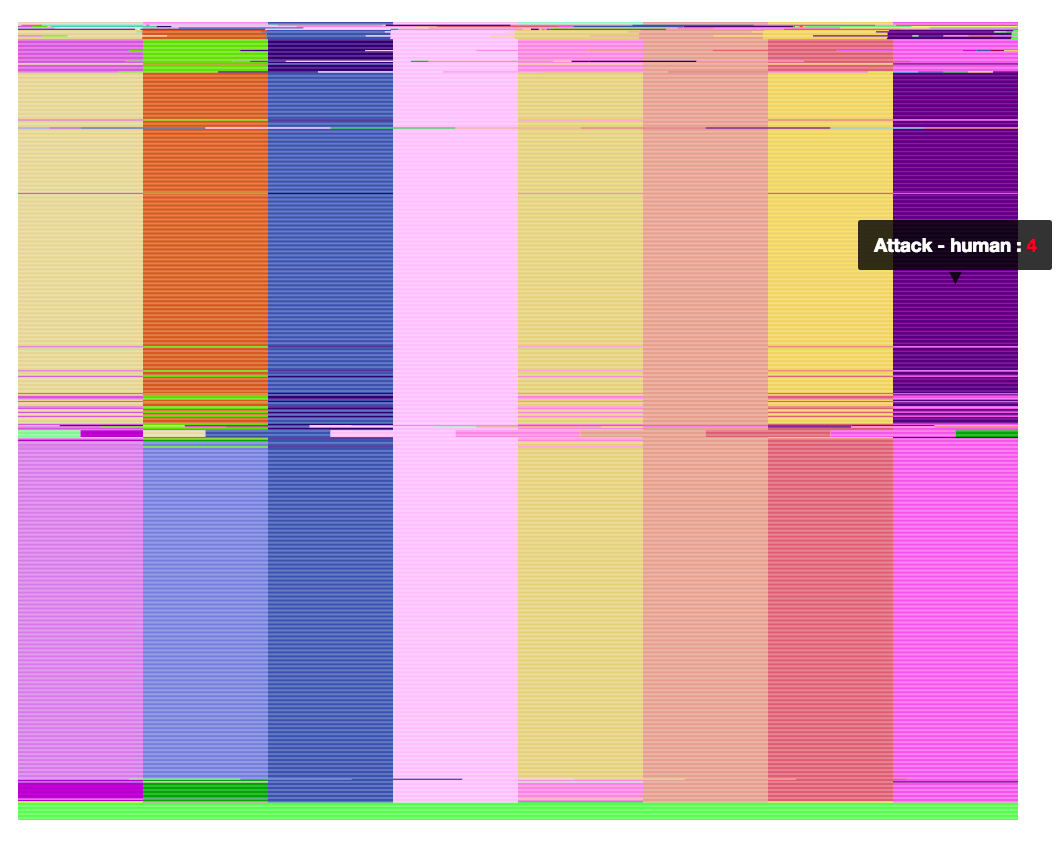
|  |  |
| --- | --- |
| **Visual Design** | **Network** |
| ColorBand | Attack Visualization |
| Force Layout | Network Topology |
| Bubble Chart | Traffic Flow |
| Heat Map | Attack Intensity Per Hour |
| Time Series | Individual attack count on time scale |

**Implementation and Experimentation**

**ColorBand– Attacks visualization**

We came up with the new Visualization Technique for the attack visualization which we named ColorBand to understand different nodes which are under attack. This visualization is made up of multiple horizontal lines where each line further gets divided into multiple lines with different colors representing attack type. This visualization has following features and interactions:

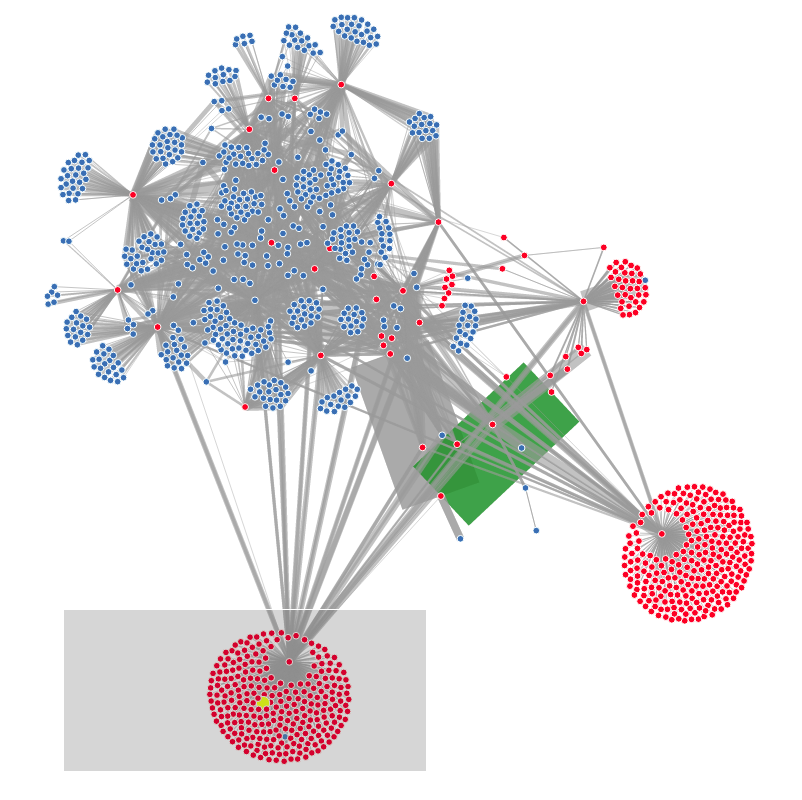
1. On mouse hover this ColorBand zoom hovered node with its IP address (shown at the bottom of the figure).
2. On click the selected node gets highlighted on Force Layout with the yellow color for locating the node in the network topology.
3. Mouse hover on ColorBand also shows the attack type and count of hovered node.

****

****

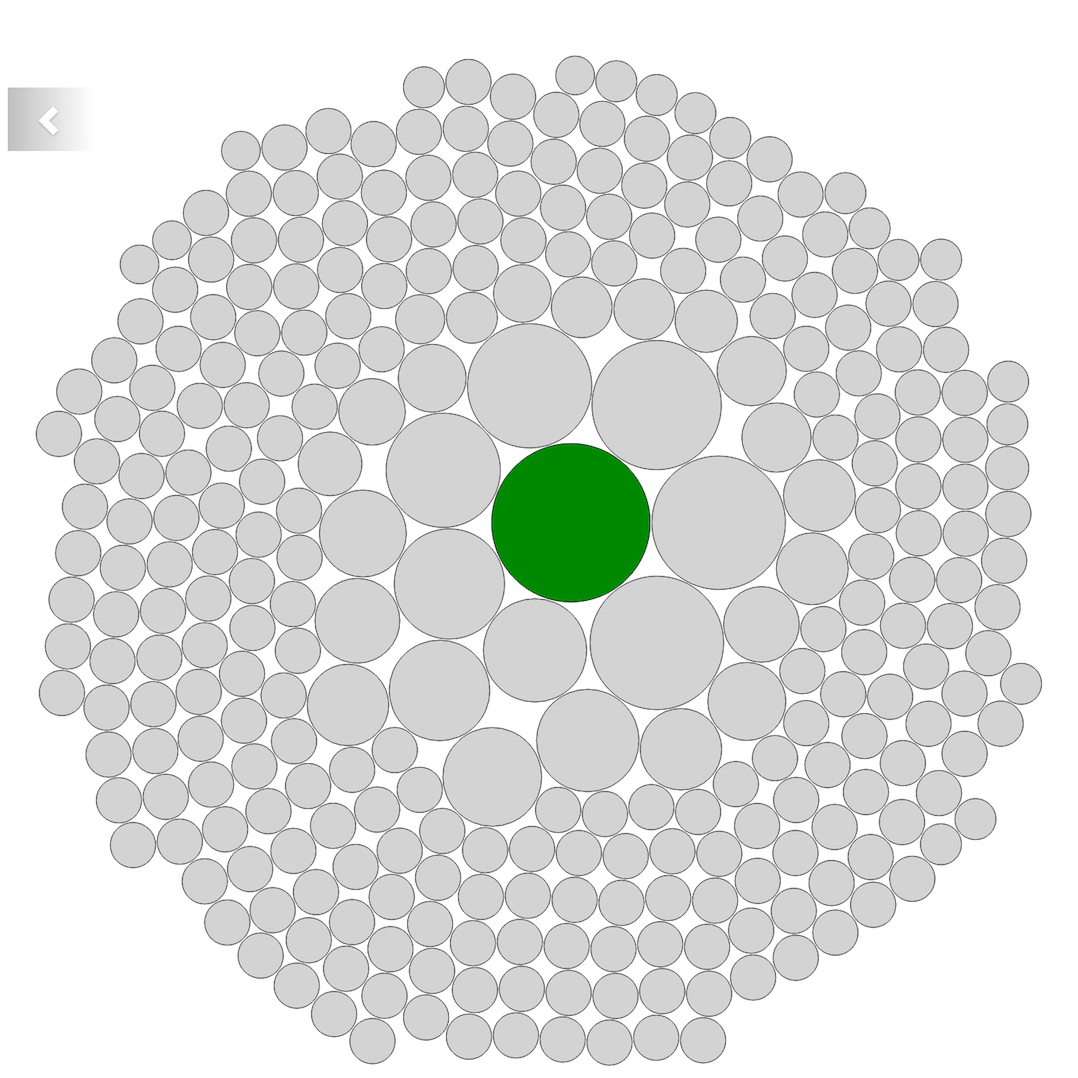
**Figure 1- 1998 Week 1, Friday dataset we have 81 different attacks and to visualize which node is under which kind of attack we have to come up with this new ColorBand technique**.

**Force Layout – Network Topology**

The best way to show any network topology is through Nodes and Links. Applying Force Layout [1] Visualization applied on Nodes and Links its gives an idea about the placement of the components of the network. In Force-Layout, on specifying the force between two elements, it becomes easy to identify clusters in the network topology. We have modified other visual attributes of the diagram which helped to understand the traffic flow and nodes under attack effectively. This visualization has the following features and interaction:

1. Red nodes represent that they are under attack.
2. Width of the links represents the traffic flow and links gets highlighted from the bubble chart click.
3. Yellow node represent the node selected from the ColorBand.
4. In complex formation, nodes can be dragged to understand the topology with other node.
5. Brushing is used to filter the data.

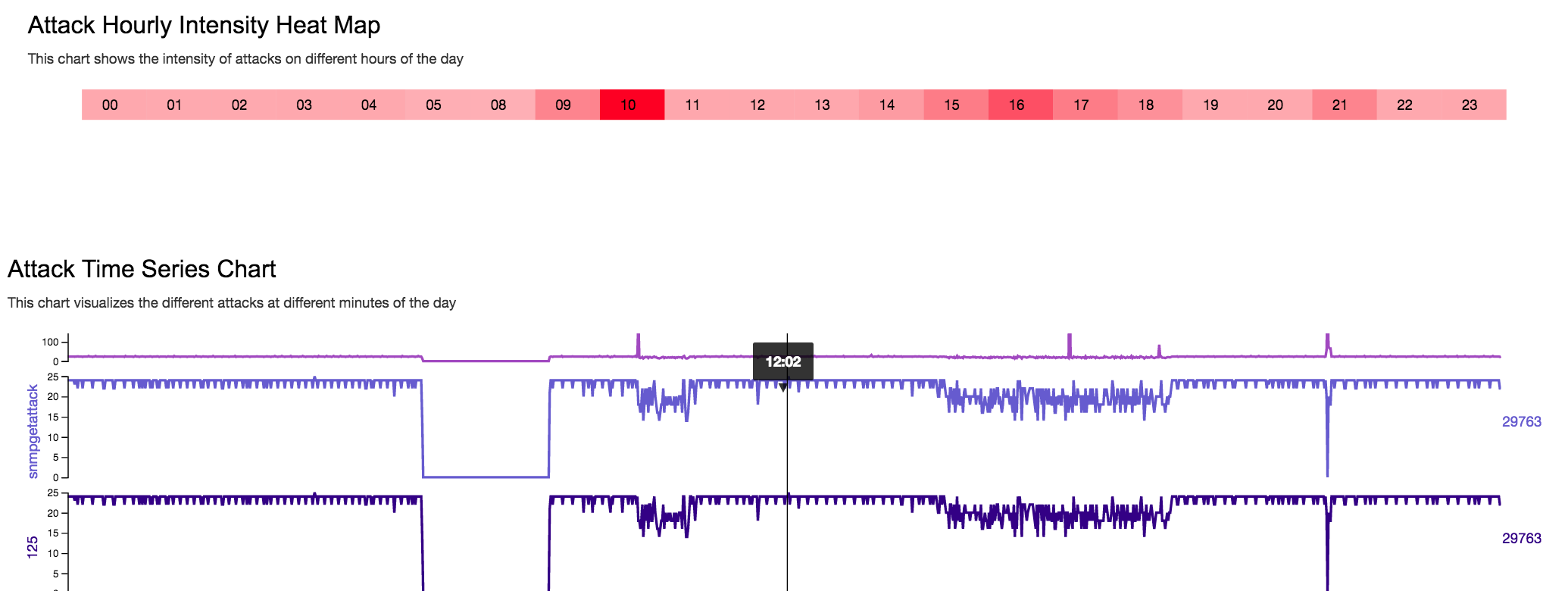
**Bubble Chart – Traffic Flow**

****

Bubble Chart helped us to show the traffic flow between nodes, the larger the size of the circle means greater the traffic, on click of the node particular link the node link diagram gets highlighted with the green color.

**Attack Heat Map and Time Series Chart**

Finally, to understand the attack intensity with respect to time we have implemented attack intensity heat map and line chart for visualizing different attack simultaneously on time scale.

****

Reference:

[1]

<https://github.com/d3/d3-force>

**Attack Visualizer: Towards Detecting Different Network Attacks Effectively**