NetKarma Provenance for Packet Throughput and Packet Loss

NetKarma, which captures and visualizes the provenance of network experiments, has recently been extended to harvest NS2 experiment trace and topology files to capture the provenance of packet transfers and infer the provenance of packets dropped. This provenance is then visualizable at different levels of granularity.

In this example we capture and visualize the provenance of experiments based on research done at Clemson University on WiMAX distributed denial of service (DDoS) attacks. Their experiment, running on NS2, has 100 subscribers and analyzes varied configurations.

Figure 1: Zoomed in visualization showing packet and node details.

NetKarma's provenance filters and visualization extensions to Cytoscape enable side-by-side performance comparison of different configurations. In this visualization subscribers are laid out based on the network topology and surrounded by the packets dropped (red) and/or received (blue).

Run id	Frame duration	number of attackers	attack backoff start	attack request retry	bw backoff start	bw request retry
1	0.004	20/80	1	2	1	2
244	0.01	20/80	1	2	1	2
487	0.02	20/80	1	2	1	2

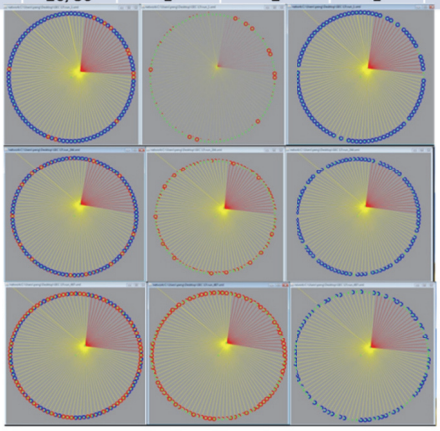

Figure 2(a) packets dropped increases as frame_duration increases from 0.01s to 0.02s.

Run id	Frame duration	number of attackers	attack backoff start	attack request retry	bw backoff start	bw request retry
406	0.01	80/20	1	2	1	2
407	0.01	80/20	1	2	1	6
408	0.01	80/20	1	2	1	10

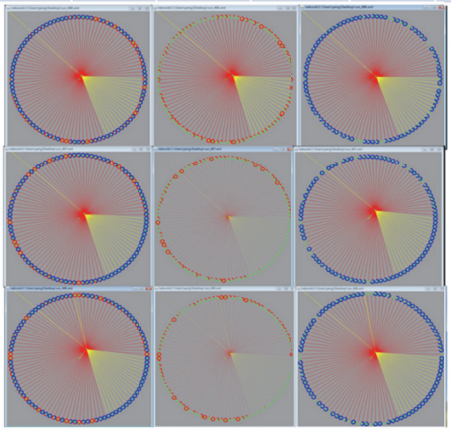

Figure 2(b) packets dropped decreases as bw_request_retry increases from 2 to 6.

On-Going Research: We are extending NetKarma to capture the provenance of WiMAX on ORBIT and also working with researchers at Indiana University and the University of Delaware to capture the provenance of experiments using the eXtensible Session Protocol (XSP) for data transfers.

Visit NetKarma at the Data to Insight Center's Web Site:

http://d2i.indiana.edu/provenance_netkarma

DATA TO INSIGHT CENTER
INDIANA UNIVERSITY
Pervasive Technology Institute