Partitioning Network Experiments for the Cyber-Range

Wei-Min Yao, Sonia Fahmy

Why perform large-scale network experiments?
- Study network attacks (DoS, Worms)
- Verify defense mechanisms
- New routing protocols

How to perform large-scale network experiments?
- Emulation testbeds provide high fidelity but have limited capacity
- Simulators and mathematical models sacrifice fidelity for scalability
- Need an accurate platform for large-scale experiments

Can we divide a large-scale experiment into a sequence of experiments on a testbed?
- Not all flows are related
- Fine-grained metrics are not always required
- Flow-based scenario partitioning (FSP)

Methodology:
Phase 1
- Map flows in the experiment to a dependency graph
- Partition the graph to minimize weight of cut and generate sub-experiments

Phase 2
- Conduct sub-experiments independently and iteratively on a testbed
- Collect packet traces on all shared links
- After the first iteration, model interacting sub-experiments on shared links based on the collected traces
- 2 iterations are sufficient for most cases

Results:
- The network topology of a Botnet experiment with 438 nodes.
- Percentage of successful HTTP/1.0 sessions in the Botnet experiment. The maximum number of nodes in a FSP partition is 100.
- The comparison among three different traffic modeling tools.
- A comparison between FSP and the TranSim downscaling technique.

This research is funded in part by Northrop Grumman Corporation and the National Science Foundation.