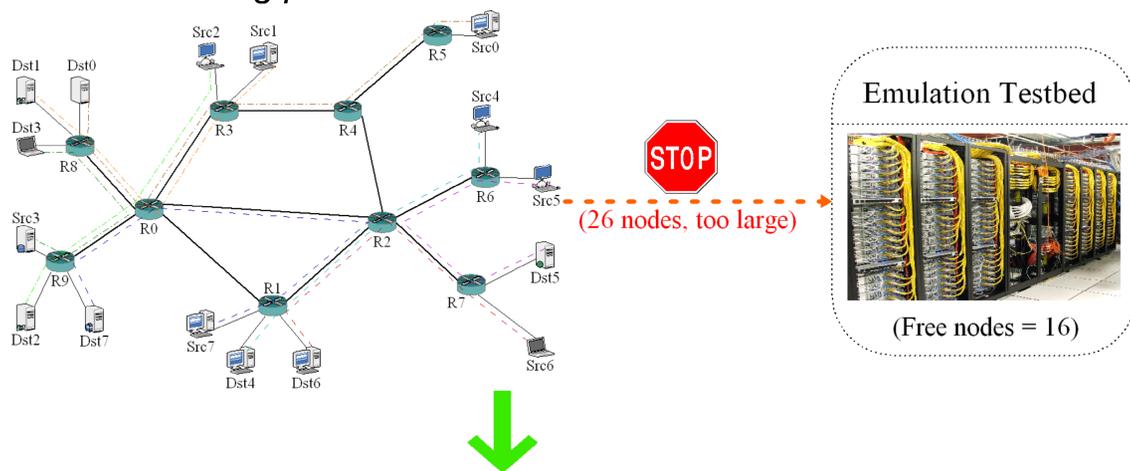# CERIAS

the center for education and research in information assurance and security

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*

STOP

(26 nodes, too large)

Emulation Testbed

(Free nodes = 16)

## 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)**

(Sub-experiment 1)   (Sub-experiment 2)   Partitioning

(Traffic and network modeling)

Iteration 1
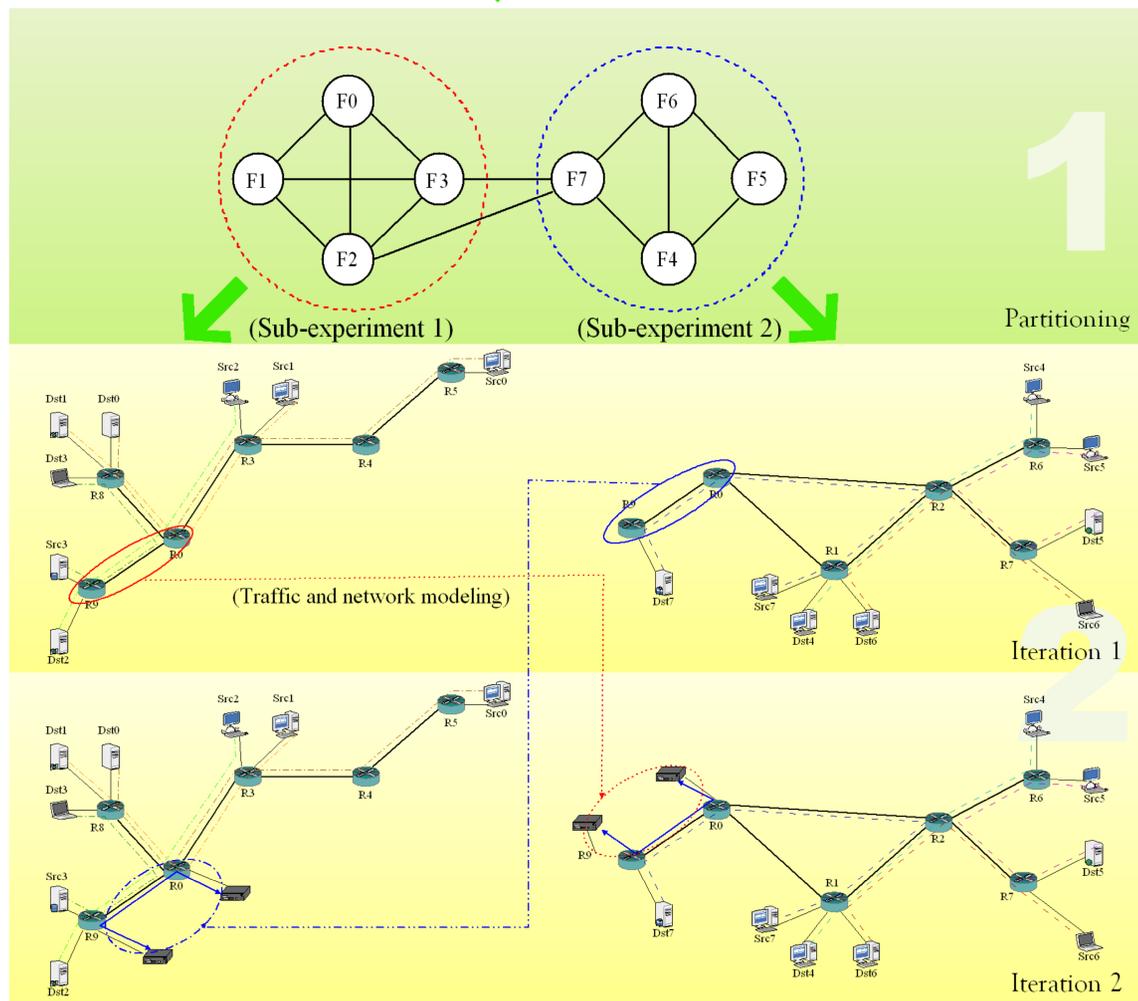
Iteration 2

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*

Ongoing Work:
- *Experiments on DETER testbed*
- *Tradeoff between different traffic generators (Harpoon, Tmix, Swing)*

PURDUE UNIVERSITY

CER IAS

Discovery Park
e-Enterprise Center