Scaling Network Security Experiments

Sonia Fahmy, Purdue University

http://www.cs.purdue.edu/~fahmy/software/emist/

- ***Given a cyber-range with a finite amount of resources, design mechanisms to enable accurate large-scale experiments with attacks and defenses***
- Focus on experiments with *high risk/high likelihood* attacks and on security assessment
- Existing solutions, *e.g.*, SHRiNK, TranSim, and DSCALE, introduce artifacts

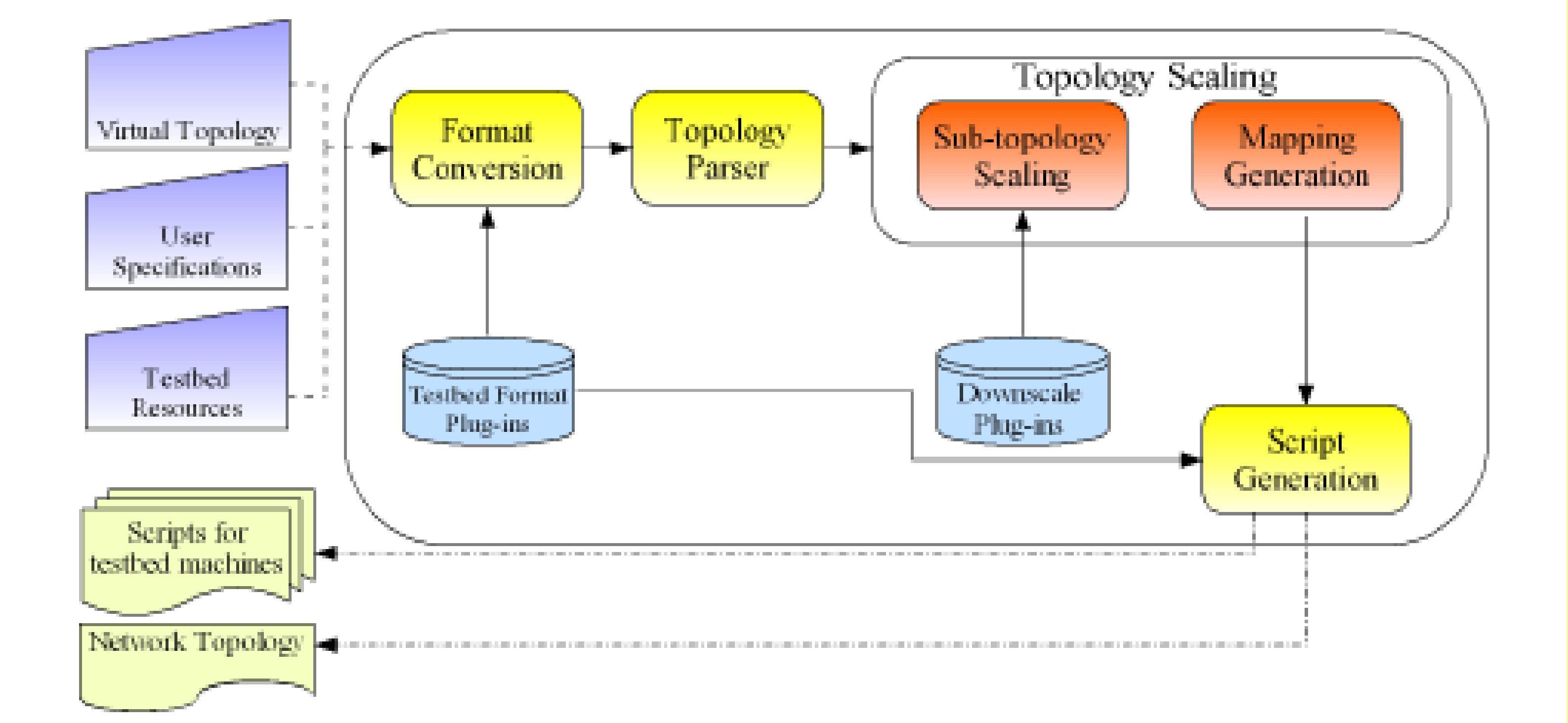
Phase 1:

- Construct a Flow Dependency Graph (FDG)

Phase 2:

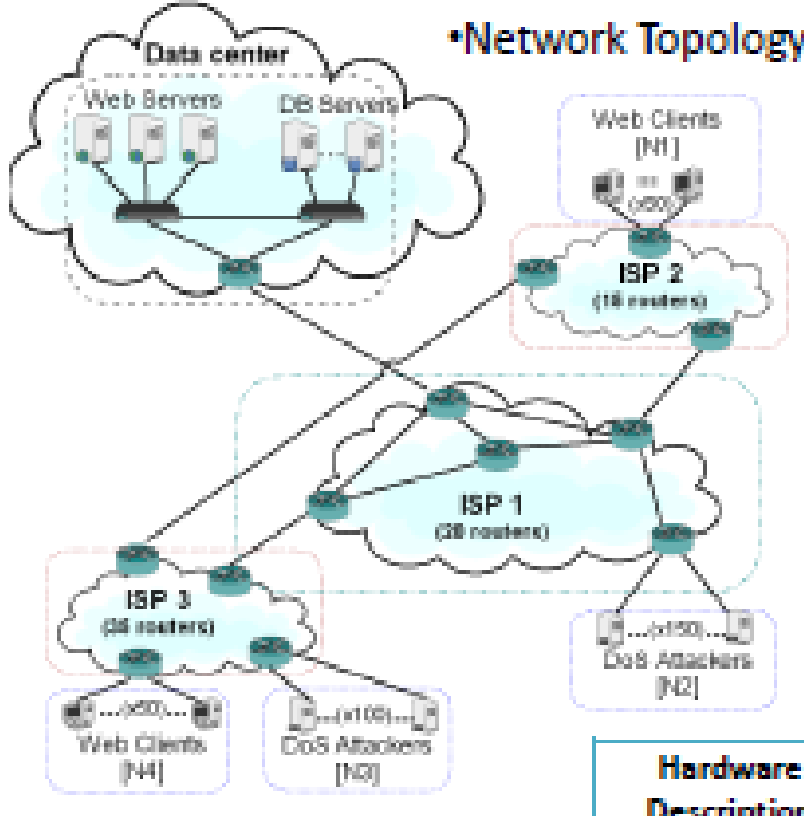
- Conduct sub-scenario experiments independently and iteratively
- Collect traces for dependent flows, if any
- Extract from these traces: application traffic models and network conditions on non-shared links
- Conduct experiments

EasyScale Mapping

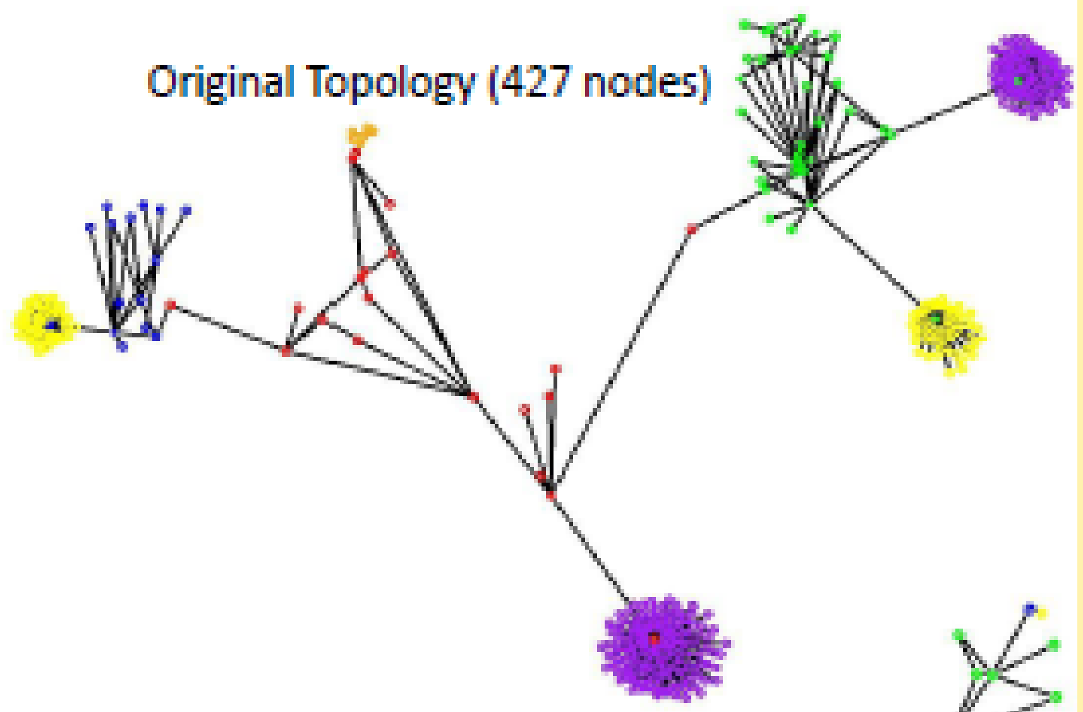


Example:

•Network Topology

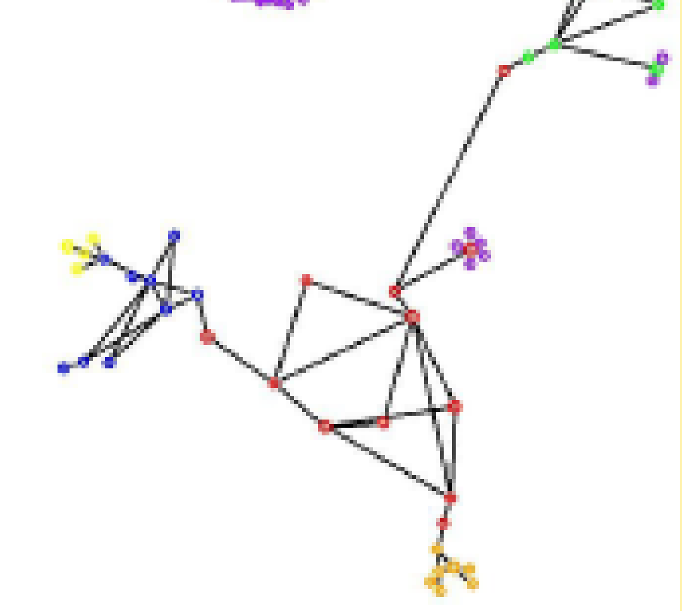


Original Topology (427 nodes)



•Testbed Resources

Hardware Description	Type Notation	Available Machines
High-end Server	Serv	7
Low-end PC	Pc	20
General PC	Pc2	10
General Server	Serv2	10

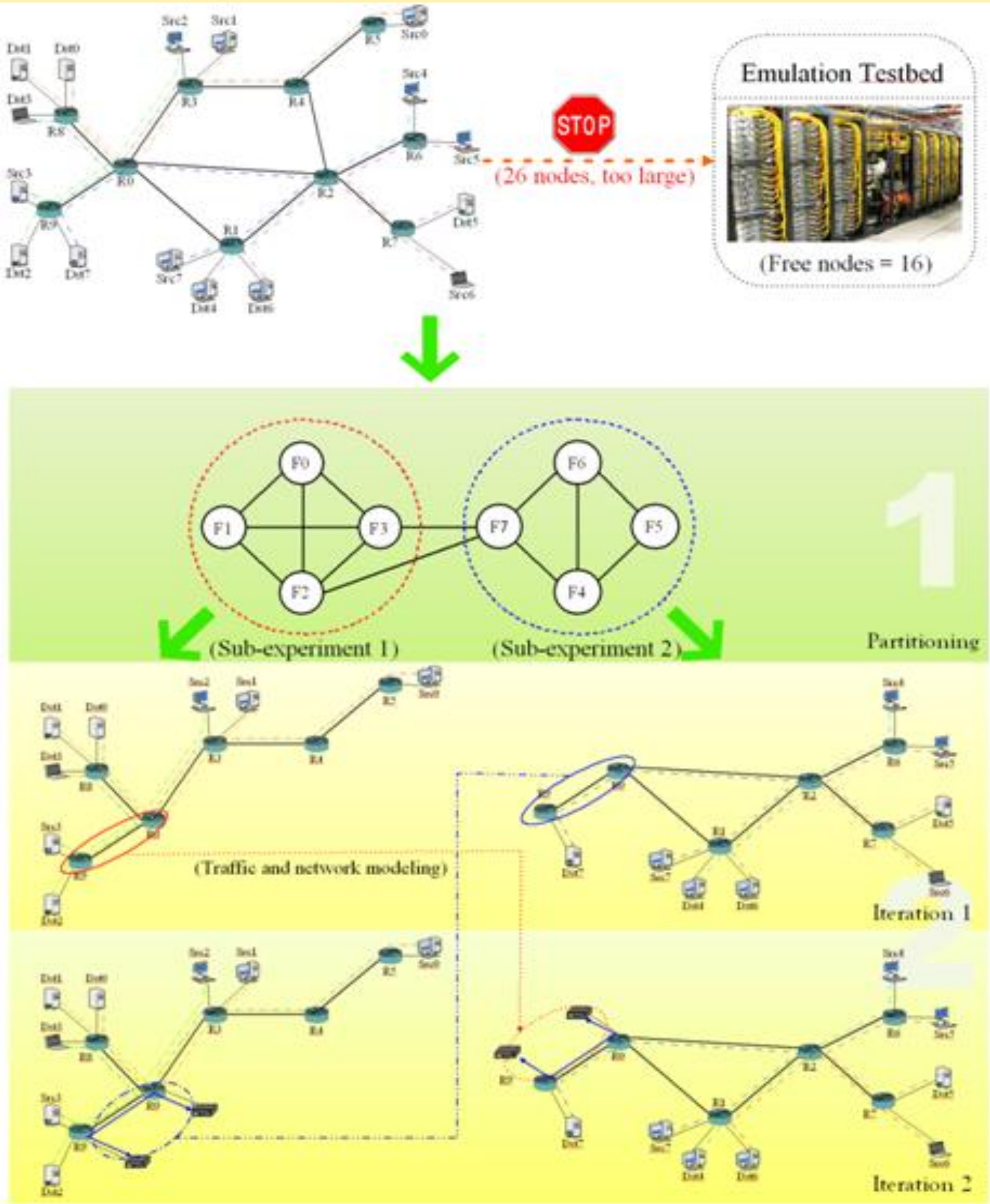


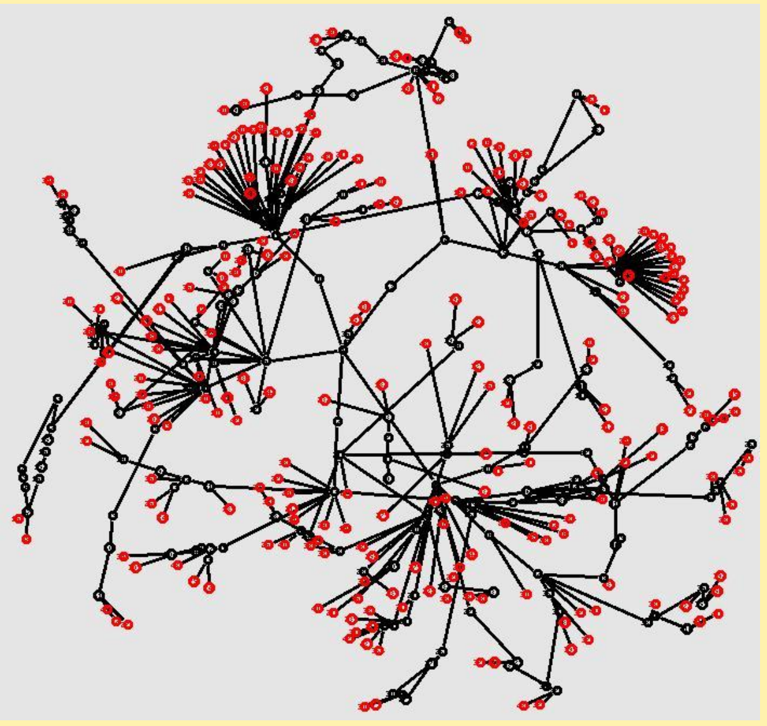
Mapped Topology (47 nodes)

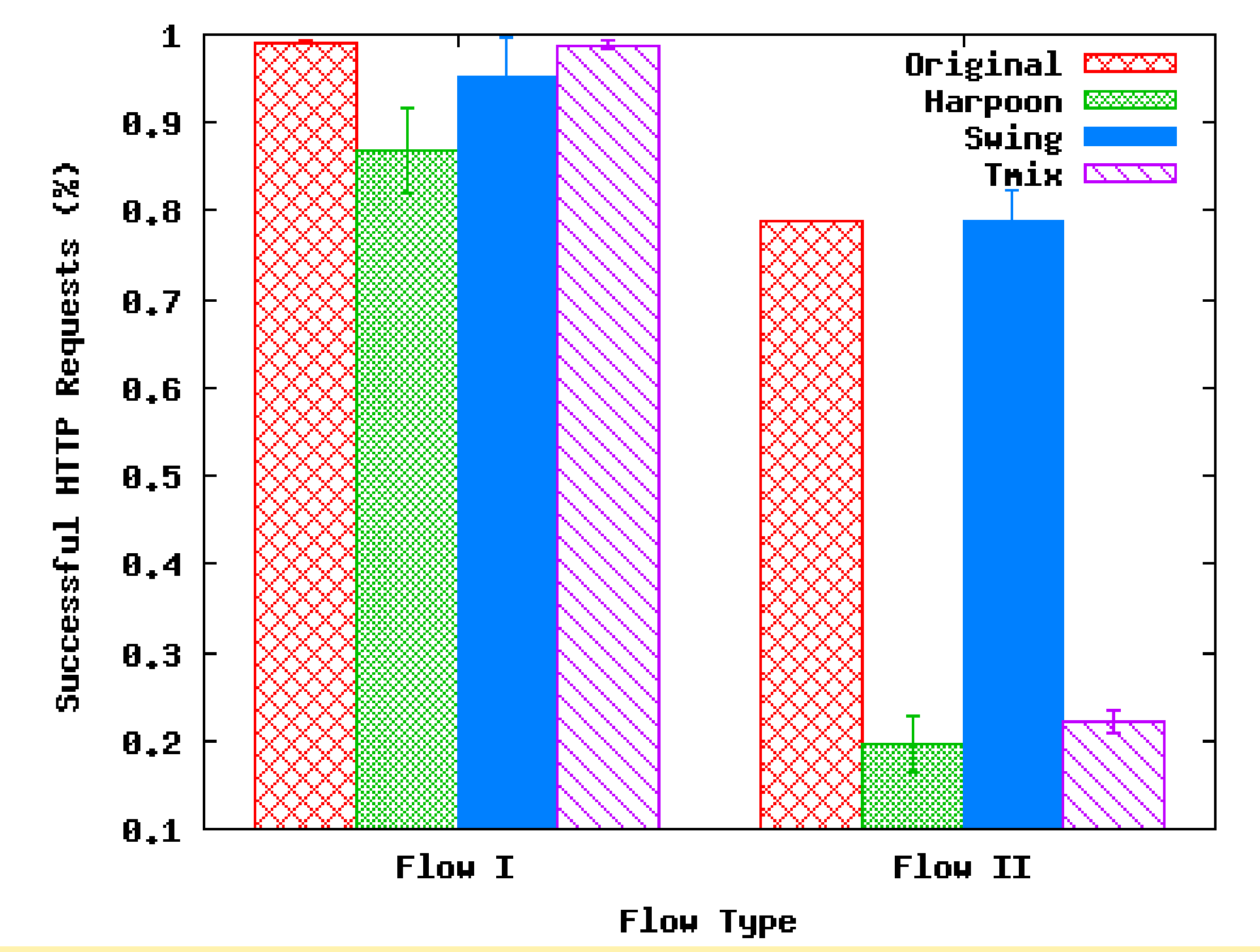
•User-specified Requirements

SubNetwork	ISP 1	ISP 2	ISP 3	N1	N2	N3	N4	Data Center
Nodes	20	15	35	50	150	100	50	7
Fidelity Index	8	5	5	4	3	2	2	Max

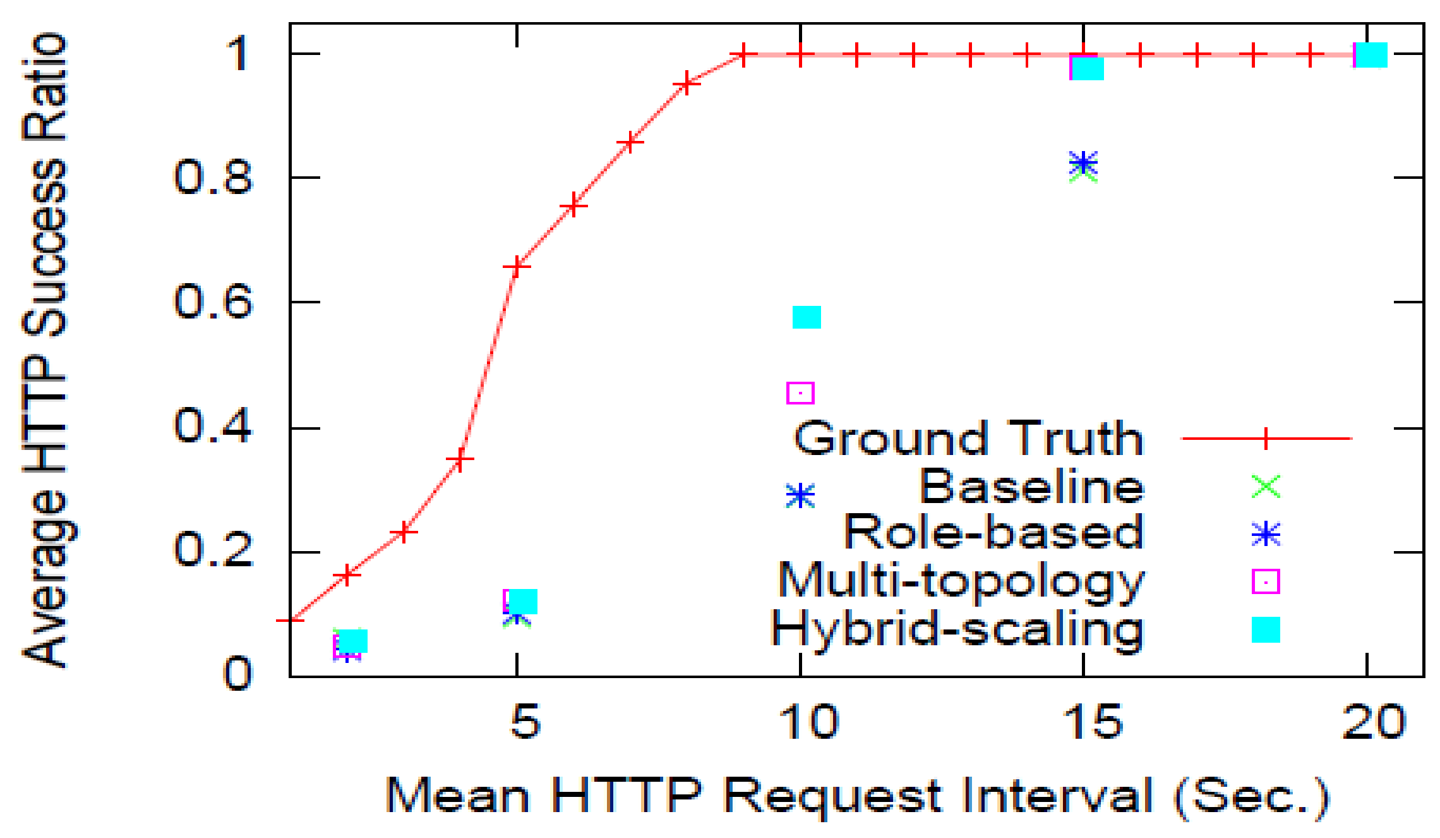
Flow-based Scenario Partitioning







- As the system load increases, the fidelity of the virtualized networks drops
- The fidelity of the virtualized network can be improved when the physical resources are carefully allocated with EasyScale



Interested in meeting the PIs? Attach post-it note below!

NSF Secure and Trustworthy Cyberspace Inaugural Principal Investigator Meeting
Nov. 27 -29th 2012
National Harbor, MD

National Science Foundation
WHERE DISCOVERIES BEGIN

PURDUE
UNIVERSITY