CERIAS

The Center for Education and Research in Information Assurance and Security

PURDUE UNIVERSITY

# Resource Mapping on Hybrid Testbeds

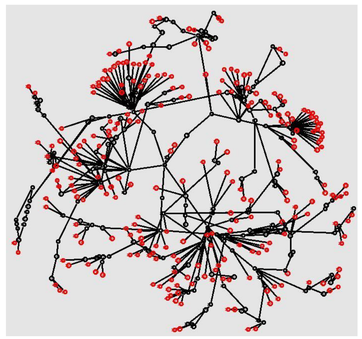
Wei-Min Yao, Jiahong Zhu, Sonia Fahmy

**Problem Statement:**

*Given a cyber-range with a finite amount of resources, design mechanisms to enable accurate large-scale experiments with attacks and defenses.*

**Why perform large-scale network experiments?**

- Study network attacks (DoS, Worms)
- Verify defense mechanisms
- New routing protocols



➔Emulation testbeds provide high fidelity but have limited capacity.

**Mapping Large Experiments:**

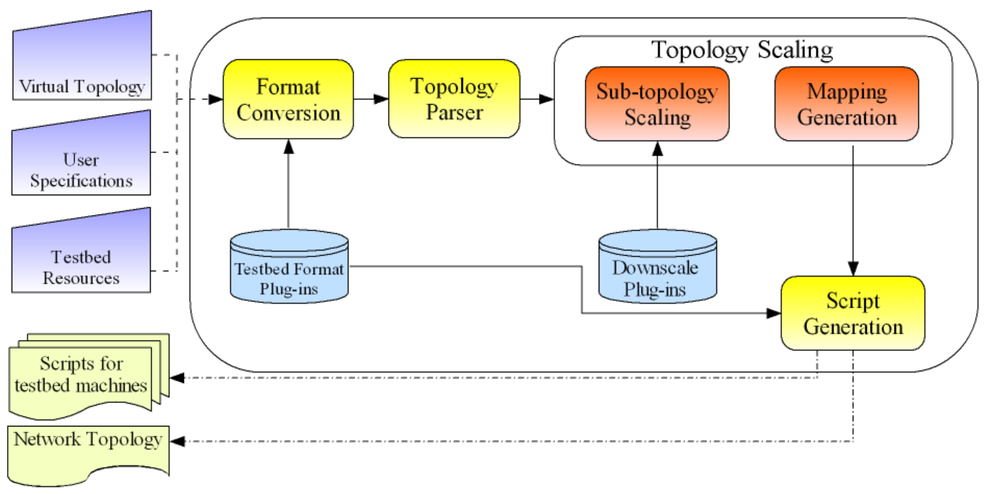
- Testbeds can scale via intelligent resource mapping mechanisms.
- Scenario partitioning across platforms/virtual machines is currently *user-specified.*

➔We need to ***automate the mapping procedure*** to support large-scale experiments on testbeds.

**Methodology:**

- Utilize the fact that not all parts of an experiment require highest fidelity
- Allow users to define "important" parts in an experiment and automatically map a large experiment to different *scaling techniques*
- This can support dynamic routing and various testbed architectures
- Partitioning results indicate how virtualization techniques can be utilized in large-scale experiments on the cyber-range according to user's requirements

**Procedure:**

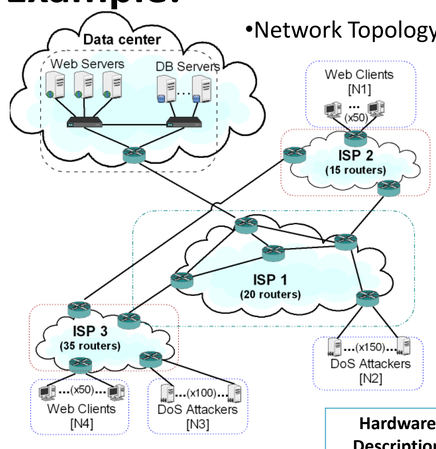



**Popular Virtualization Techniques on Testbeds:**

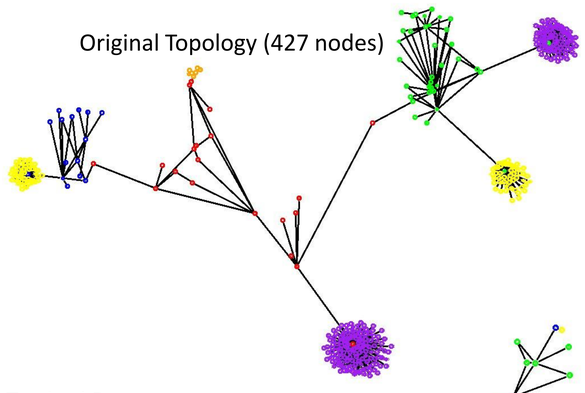
| Method | Scalability | Fidelity | Existing solutions | Limitations |
|---|---|---|---|---|
| Full virtualization (Hardware virtualization) | Small | High | Virtualbox, Vmware, KVM | High overhead (especially without hardware support). |
| Paravirtualization | Small | High | Xen | Can only install modified Guest OS. |
| OS-level virtualization | Medium+ | Medium | LXC (Linux), OpenVz (Linux), Jail (FreeBSD) | Native performance, but cannot install Guest OS. |
| Real-time simulator | Large | Low | ns-3, PRIME | Low fidelity. Hard to interact with real systems (e.g., real routers). |

**Example:**

•Network Topology




Original Topology (427 nodes)

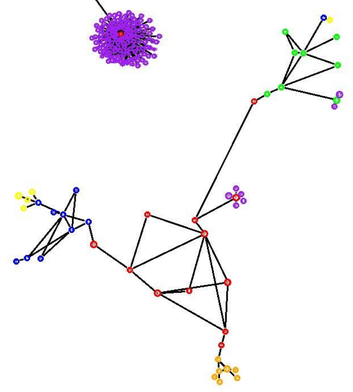


•Testbed Resources

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

•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 |



Mapped Topology (47 nodes)

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

CERIAS®

Discovery Park e-Enterprise Center