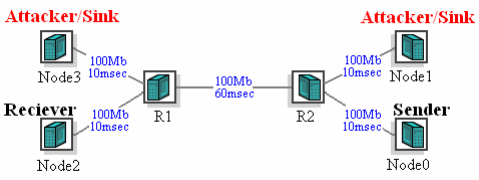
Evaluation Methodologies for Internet Security Technology (EMIST)

Sonia Fahmy, Ness Shroff, Eugene Spafford
Students: Roman Chertov, James Early, Abdallah Khreishah, Pankaj Kumar

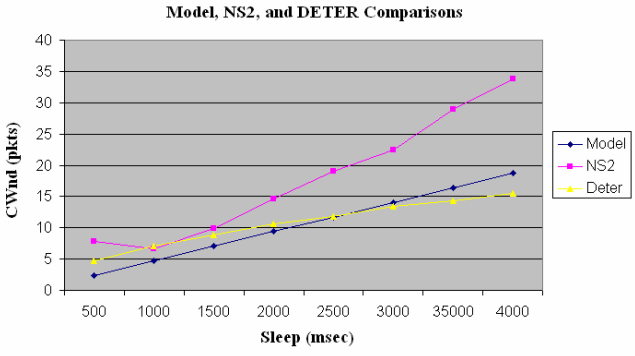
What is EMIST?

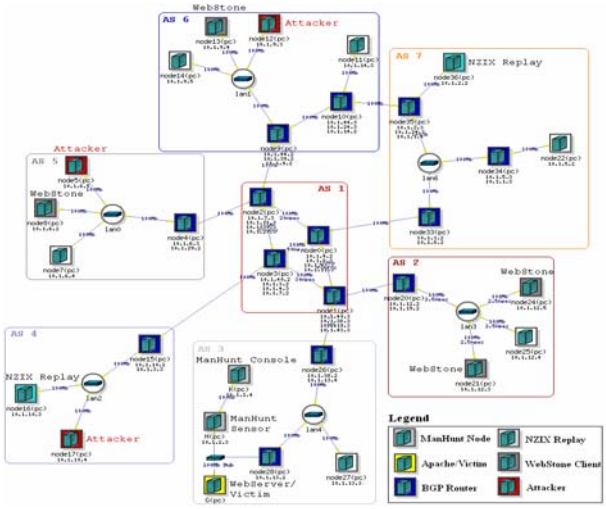
- A multi-institution project to develop rigorous testing methodologies, tools, and benchmarks for important classes of Internet attacks and defenses
- A companion project to DETER: a remotely accessible experimental testbed, based on Utah Emulab, that allows researchers to evaluate Internet cyber security technologies in a *realistic*, but *quarantined* environment



Our Objectives

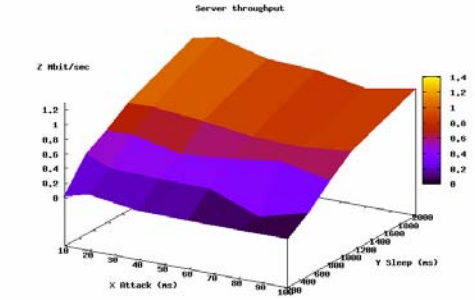
- Identify limitations of analytical, simulation and emulation models
- Quantify the impact of attacks against congestion control (TCP) and routing (BGP/OSPF) and their defenses
- Design scale-down techniques for experimental scenarios, without loss of fidelity





Our Accomplishments

- Designed and implemented:
  - A scriptable event system for experiment control and automation
  - Instrumentation and experimental data processing tools
  - A software-based link monitor
- Modeled, simulated, and emulated attacks against congestion control



Lessons Learned

- Simulation models do not capture the intricacies of real systems
- Small differences in emulation testbed capabilities have a significant impact on results
- Attacks may have unforeseen interactions with protocols, e.g., BGP routing

Funded by:

Partner organizations:

PURDUE UNIVERSITY

CERIAS

Discovery Park e-Enterprise Center