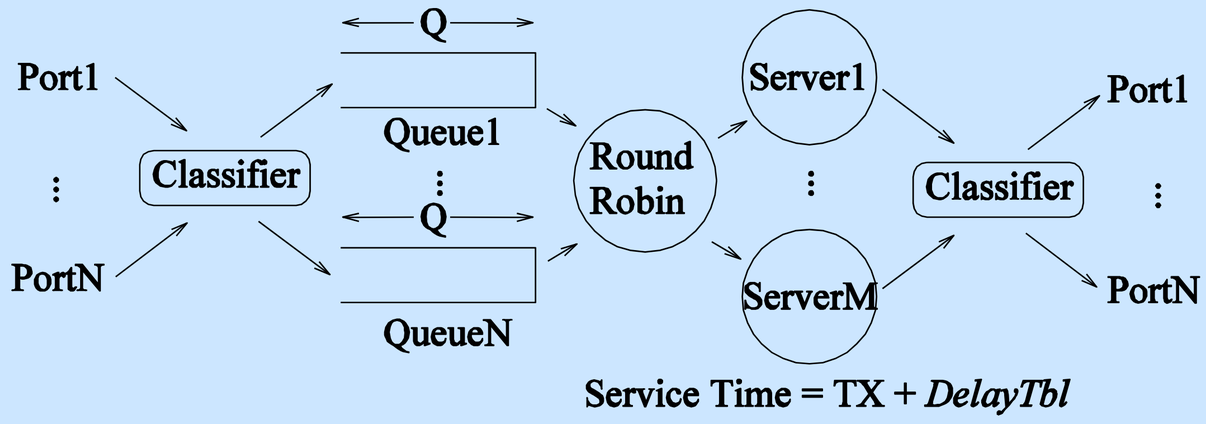
Modeling Forwarding Devices

Sonia Fahmy (Purdue), George Kesidis (PSU), Ness Shroff (OSU) www.cs.purdue.edu/~fahmy/

Replace with a photo of yourself

Large discrepancies between simulated and deployment behaviors have been observed in TCP-targeted denial of service attack experiments. The discrepancies arise because simulators must balance a fidelity-scalability tradeoff, and may thus abstract away important bottlenecks in routers and other forwarding devices.

We develop high-fidelity yet scalable router models that are founded on extensive devise measurements. The structure of our model is device-independent, but has parameters that make it unique for each device.



Our results will allow Internet researchers to understand Internet performance under overload and security attacks.

A new router model enables high-fidelity network security simulations

Approach and Impact

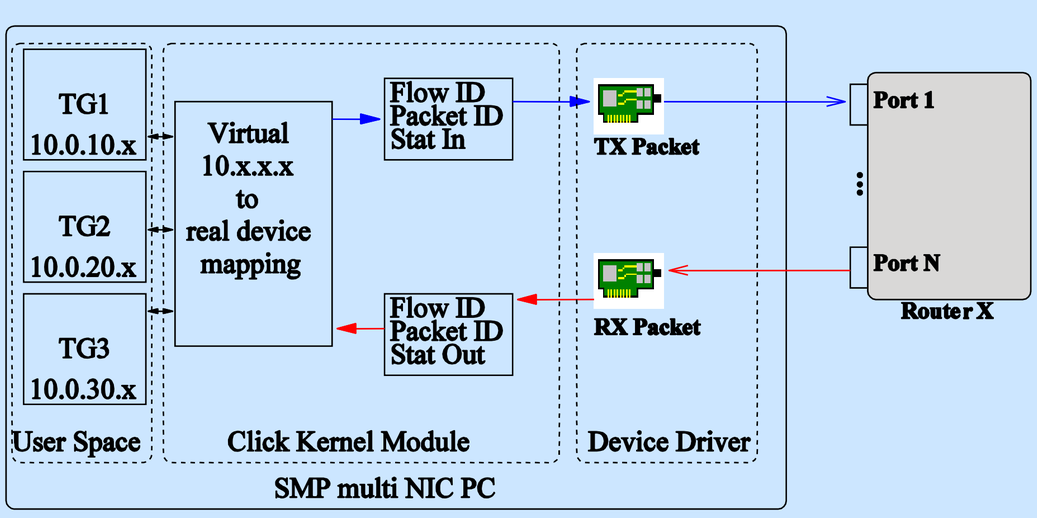
New approach

- Model routers using multiple servers and multiple queues
- Infer number of servers and number of queue slots per packet size

Research Impact

- Enables high-fidelity yet scalable network security experiments
- Facilitates design of network security mechanisms

We have designed and implemented a profiler for routers and other forwarding devices, built on commodity hardware. The profiler measures intra-device latencies and forwarding rates for different packet sizes, and uses these values to infer the servers and queues for each packet size. Our model was validated by comparing it against measurements of Cisco 3660, 7206VXR, and 12410, and Juniper M7i routers.



National Science Foundation
WHERE DISCOVERIES BEGIN

NSF Cyber Trust Principal Investigators Meeting
March 16-18, 2008
New Haven, CT

PURDUE UNIVERSITY
CERIAS