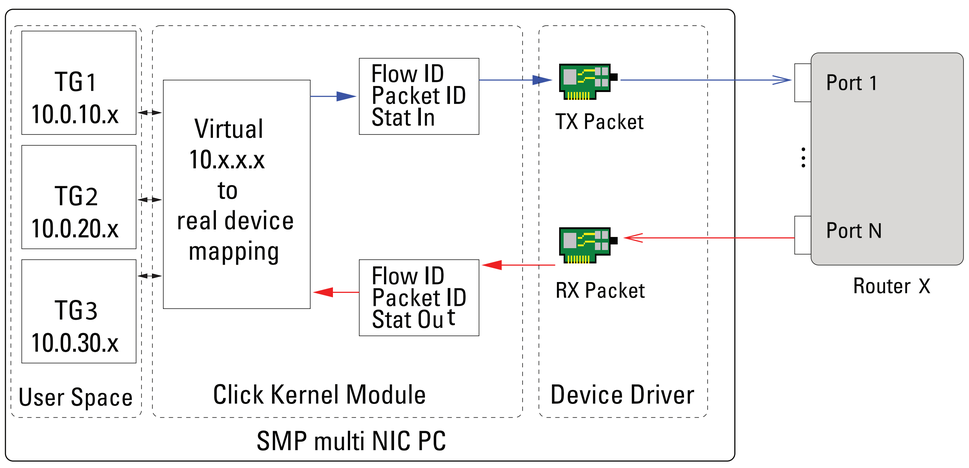
CERIAS
the center for education and research in information assurance and security

High - Fidelity DoS Simulation and Emulation Experiments

Roman Chertov, Sonia Fahmy, and Ness B. Shroff

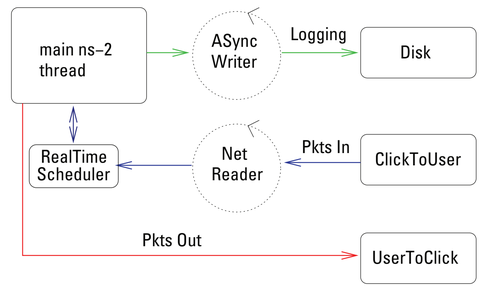
A high-bandwidth Denial of Service (DoS) attack can produce very different impacts on the different platforms, even if the experimental scenario is supposedly identical. This is because many popular simulation and emulation environments fail to account for realistic commercial router behaviors, and incorrect results have been reported based on experiments conducted in these environments. In this work we describe the architecture of a black-box router profiling (BBP) tool which can allow us to create high-fidelity network simulation/emulation models that are not computationally prohibitive.

Layout of the BBP system



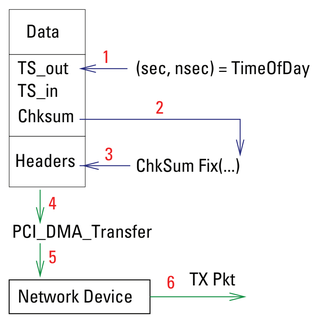
Userspace traffic generator (ns-2 simulator) is connected to physical network devices via an emulator. Traffic from multiple "subnets" traverses the router.

Async I/O



Every packet leaving and entering the system is logged to disk. Threads are used to avoid blocking the main simulation thread.

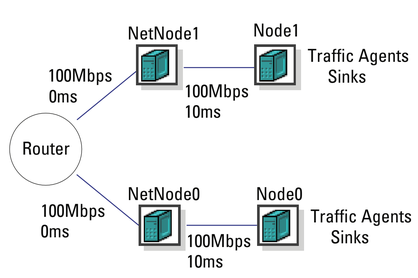
Timestamping



Packets get timestamped in the device driver just before a transmit and just after a receive. Partial checksums are used to fix the packet checksum without doing the entire calculation from scratch.

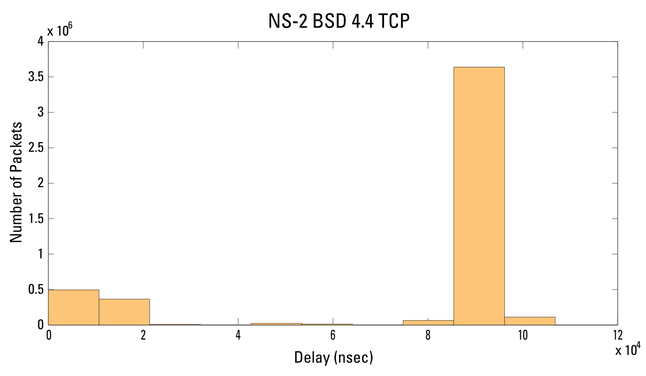
Experiment

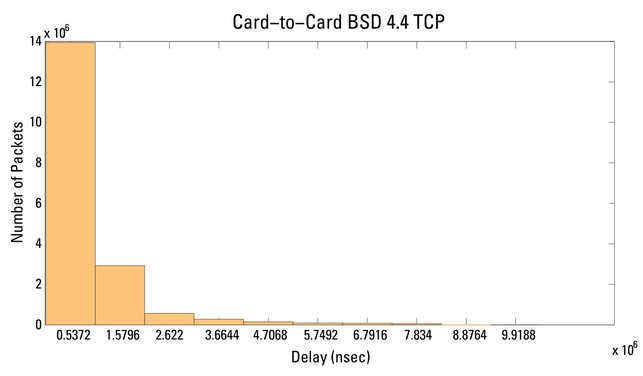
Setup

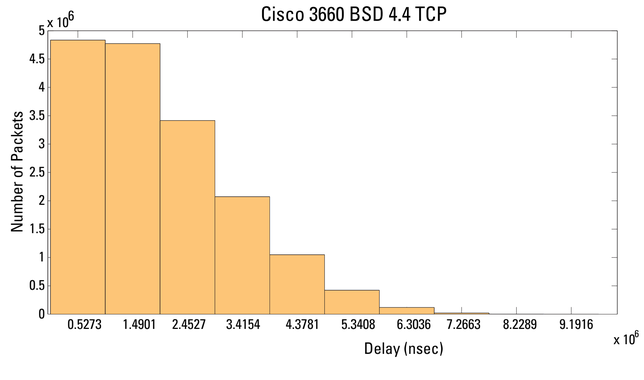


NetNodes and *Nodes* are logical nodes on the same PC with BBP, while *Router* is either a cross-over cable or a Cisco 3660 router. In the ns-2 simulation, nodes have 50 slot queues. There are 100 TCP flows with unique IPs, 50 per *Node0* and 50 per *Node1*.

Results







Conclusion

The delay distribution for ns-2 simulation is quite different from a distribution of a real router. The large difference between calibration and real router results indicates that it is possible to separate the two and create a high-fidelity model of the router.