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.

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

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.

**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.