Emulation versus Simulation: A Case Study of TCP-Targeted Denial of Service Attacks

by R. Chertov, S. Fahmy, N. B. Shroff
Center for Education and Research
Information Assurance and Security
Purdue University, West Lafayette, IN 47907-2086

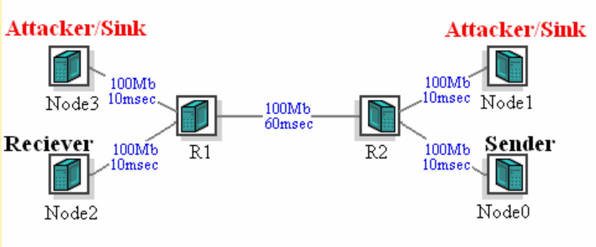
Emulation vs. Simulation: A Case Study with DoS Attacks

PIs: Sonia Fahmy, Ness B. Shroff, Eugene H. Spafford Student: Roman Chertov

http://www.cs.purdue.edu/~fahmy/software/emist/

A lot of research is done on simulators such as ns-2 and SSFNet. Simulators, however, cannot execute real applications, and only approximate various appliances. Emulation provides a way to use real appliances and applications, but is constrained by the number of nodes, types of appliances, and difficulty in configuration. Therefore, it is imperative to accurately compare the two, so that the strengths of both approaches can be harnessed.

The goal of the EMIST project is to develop rigorous testing methodologies, tools, and benchmarks for important classes of Internet attacks and defenses. It is crucial to understand the effectiveness of defense mechanisms on *real* networks. Results obtained on an emulation testbed can be used to develop more accurate simulation models.



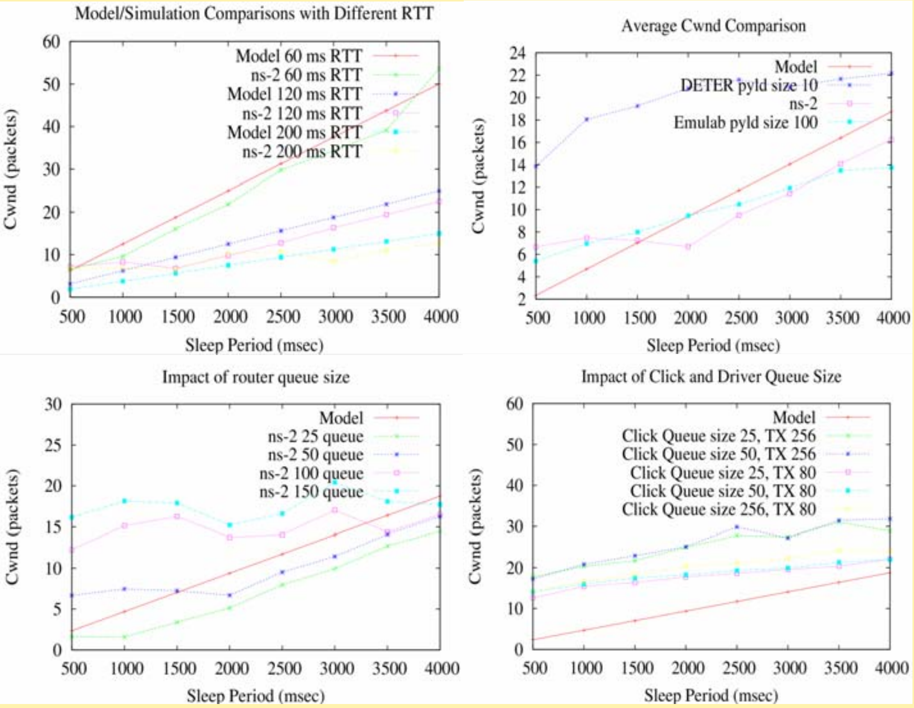
A simple topology for simulating and emulating a TCP-targeted low-rate attack. The attacker sends short pulses at a fixed frequency to exploit the TCP congestion control mechanism.

Our results indicate that an attack pulse length of one RTT is the most effective, and our analytical and simulation results match.

Large queue sizes can effectively dampen the attack when the TCP flow has not reached its full transfer rate.

Discrepancies between DETER and Emulab testbed results are attributed to differences in the underlying hardware and system software.

Click experiments demonstrate the importance of device driver settings.


Model/Simulation Comparisons with Different RTT

Average Cwnd Comparison

Impact of router queue size

Impact of Click and Driver Queue Size

Model Overview

α is the Cwnd growth during a sleep period

t time between two loss events

$$W_S = \lim_{i\to\infty}\left(2^{-i}W_N + \alpha\left(\sum_{j=0}^{i-1}2^{-j}\right)\right) = \alpha\left(\sum_{j=0}^{i-1}2^{-j}\right) = 2\alpha$$

$$W_{avg} = \frac{3t}{4rtt}$$

NSF Cyber Trust Annual Principal Investigator Meeting
Sept. 25 -27th 2005
Newport Beach California