A Systematic Simulation-based Study of Adverse Impact of Short-lived TCP Flows on Long-lived TCP Flows[1]

Shirin Ebrahimi-Taghizadeh
University of Southern California
sebrahim@usc.edu

Ahmed Helmy
University of Southern California
helmy@usc.edu

Sandeep Gupta
University of Southern California
sandeep@poisson.usc.edu

http://www-scf.usc.edu/~sebrahim/sigcomm04-poster.html

ABSTRACT

Best effort applications over non-TCP protocols, e.g., UDP, can be used in attacks that capture unfairly large share of bandwidth compared to TCP flows. While earlier studies may have pointed out that short-lived TCP flows (mice) may hurt long-lived TCP flows (elephants) in the long term, no insight was given as to developing scenarios leading to drastic decrease in throughputs of long-lived TCP flows. We have systematically developed TCP attack scenarios that differ from all prior research in that we use short-lived TCP flows to attack long-lived TCP flows. Our attacks are interesting since, (a) they are more difficult to detect, and (b) they point out the increased vulnerabilities of recently proposed scheduling, AQM and routing techniques that further favor short-lived flows.

We systematically exploit the ability of TCP flows in slow-start to rapidly secure greater proportion of bandwidth compared to long-lived TCP flows in congestion avoidance phase, to a point where they drive long-lived TCP flows into timeout. We use simulations, analysis, and experiments to systematically study the dependence of the severity of impact on long-lived TCP flows on key parameters of short-lived TCP flows – including their locations, durations, and number, as well as the intervals between consecutive flows. We derive the ideal durations of, as well as the ideal intervals between, attacking short-lived TCP flows. We show that targeting bottleneck links does not always cause maximal performance degradation for the long-lived flows. In particular, our approach illustrates the interactions between TCP flows and multiple bottleneck links and their sensitivities to correlated losses in the absence of 'non-TCP friendly' flows and paves the way for a systematic synthesis of worst-case congestion scenarios. Table 1 shows the percentage reduction in throughput of long-lived flows when attacked by UDP flows [3]. The table also shows that an attack by a carefully selected sequence of short-lived TCP flows (Figure 1) achieves nearly equal reduction in throughput.

Randomly generated scenarios (where the numbers, durations, and locations of, as well as the intervals between, short-lived flows are all selected randomly) cause less than 10% reduction in the throughput of long-lived flows. In contrast, the scenarios generated using our heuristic approach based on the above results provide greater than 85% reduction in throughput. Figure 2 depicts the frequency response of the long-lived TCP flows under such attacks. Similar scenarios achieve similar reductions for several TCP variants (Tahoe, Reno, New Reno, Sack), and for different packet drop policies (DropTail and RED). Our results demonstrate that even TCP friendly-flows, if carefully orchestrated, can severely degrade throughput of long-lived flows. They also demonstrate that scheduling, AQM and routing techniques and TCP variants designed to give higher preference to short-lived flows will make long-lived flows even more vulnerable to such attacks.

Table 1: Comparing UDP and TCP attacks

Type of malicious flows	Long-lived TCP flows throughput degradation
UDP constant bit rate flows	Up to 100%
UDP short bursts with P=1 sec	More than 90% [7]
Random mix of TCP short-lived and long-lived flows	Up to 10%
Specific pattern of TCP short-lived flows with P=1	>85%

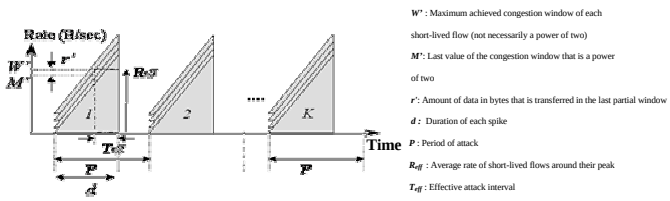

Figure 1: Effective stream of short-lived flows

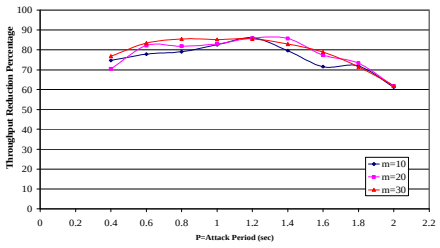

Figure 2: Frequency response of the long-lived TCP flows for *m* concurrent short-lived flows per attack interval

REFERENCES

[1] L. Guo and I. Matta , "The War between Mice and Elephants," Proc. of ICNP'2001, November 2001.

[2] A. Kantawala and J. Turner, "Queue Management for Short-Lived TCP Flows in Backbone Routers," Proc. of High-Speed Symposium, Globecom 2002.

[3] A. Kuzmanovic and E. Knightly, "Low-Rate TCP-Targeted Denial of Service Attacks," Proc. of SIGCOMM August 2003.

[1] This work was supported by grants from DARPA, NSF and NASA.