DDoS Attacks and Pushback

Steven M. Bellovin

smb@research.att.com

http://www.research.att.com/~ smb

+1 973-360-8656

AT&T Labs Research

Florham Park, NJ 07932

Joint Work

- Joint work with Ratul Mahajan (U. of Washington), Vern Paxson, Sally Floyd, and Scott Shenker (all of ACIRI).

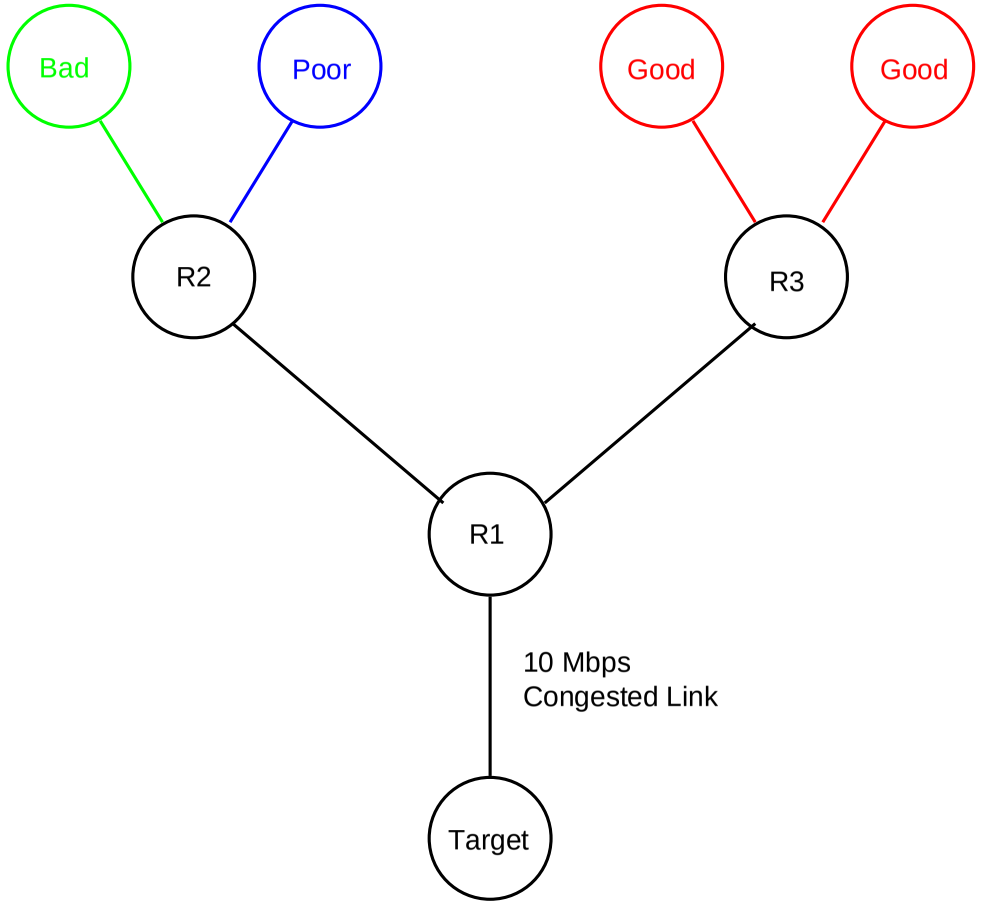
⇒ Graphs from simulations done by Mahajan.

- Based on ideas from informal DDoS research group (Steven M. Bellovin, Matt Blaze, Bill Cheswick, Cory Cohen, Jon David, Jim Duncan, Jim Ellis, Paul Ferguson, John Ioannidis, Marcus Leech, Perry Metzger, Robert Stone, Vern Paxson, Ed Vielmetti, Wietse Venema).

Basic Idea

- DDoS attacks result in massive, sustained congestion at some link.
- Router ends up discarding many packets, throwing away the good with the bad.
- Statistically, most discarded packets are from attackers.
- When many packets from a given upstream link are discarded, ask that router to discard the packets instead.
- Apply process recursively.

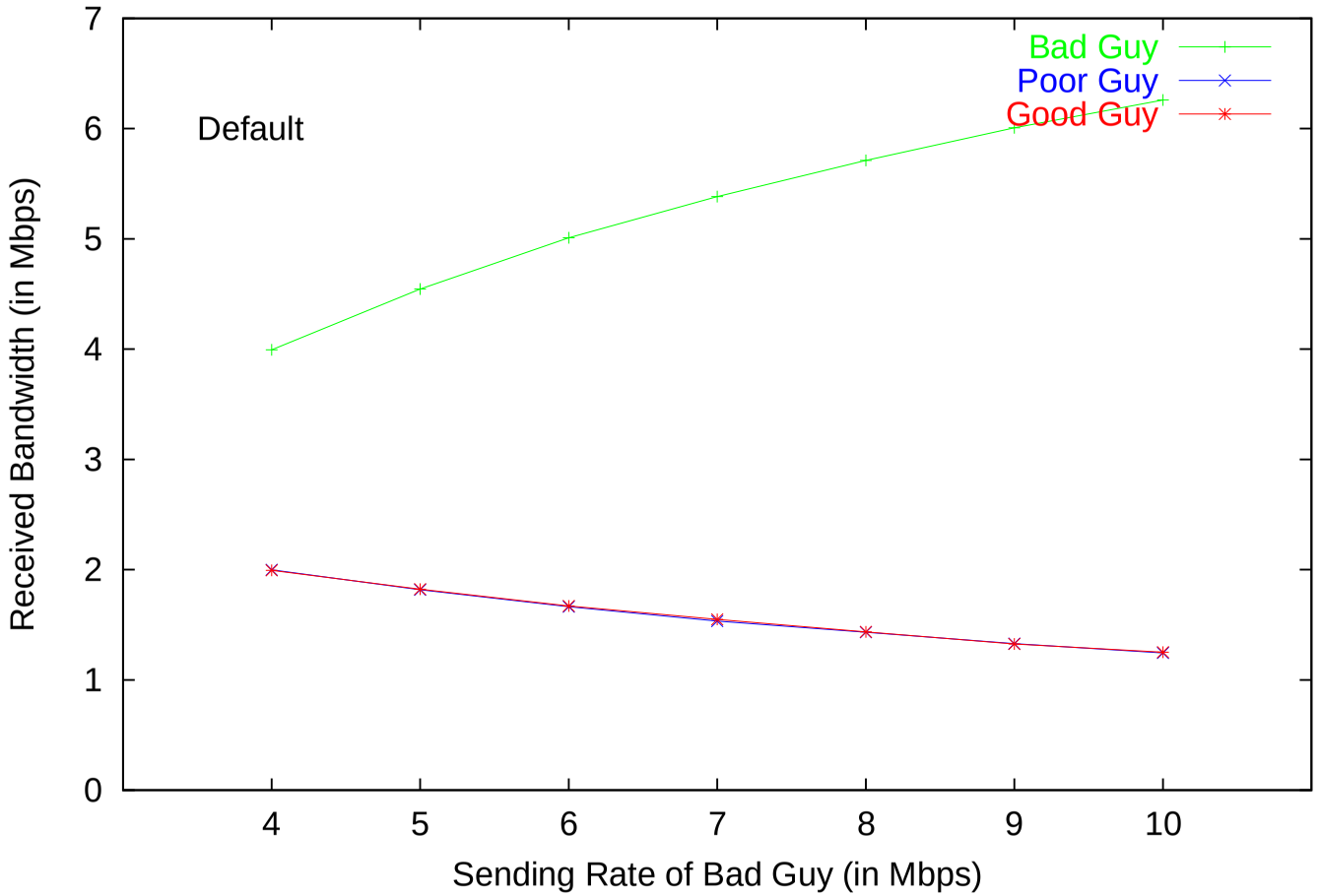
Test Topology



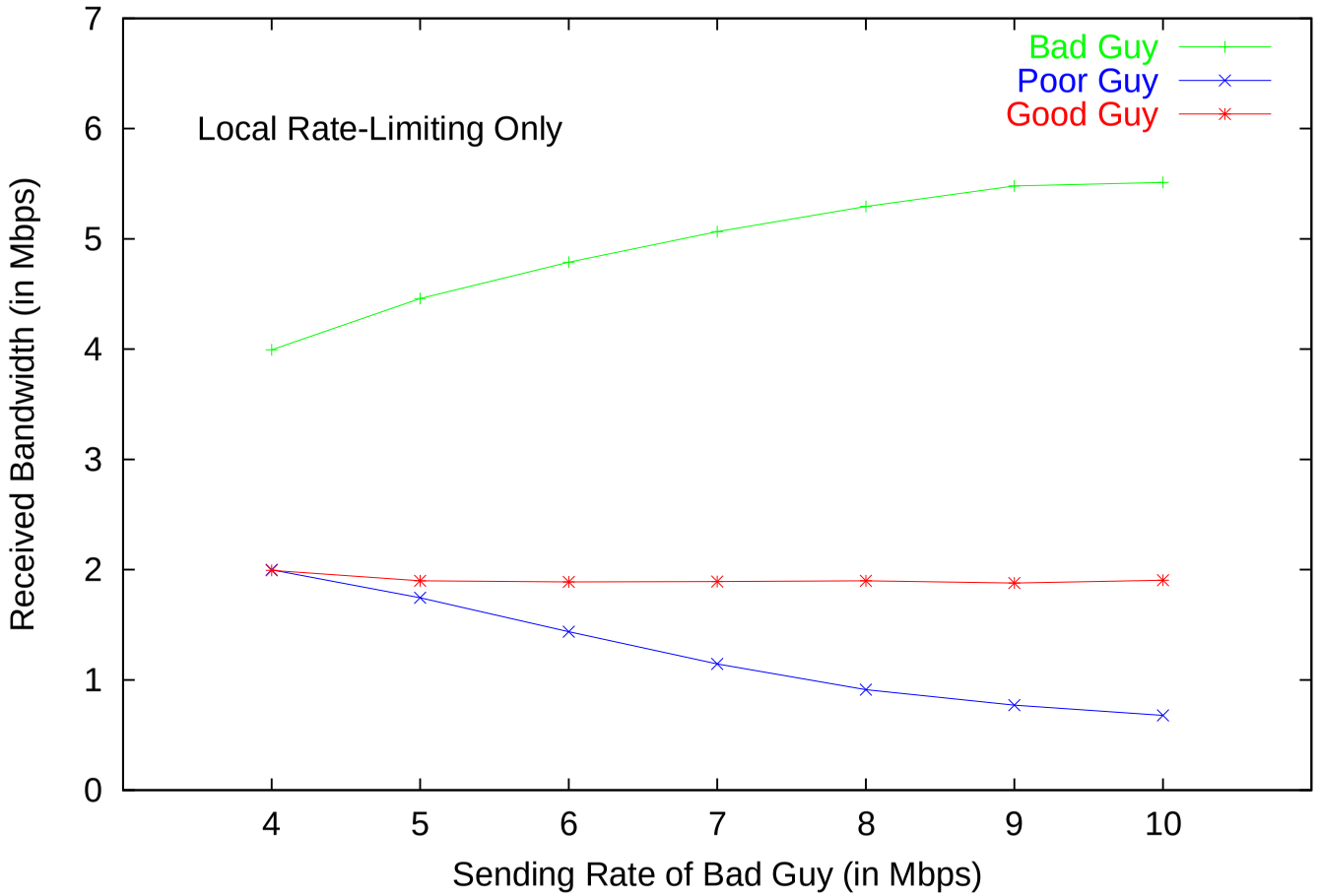
Test Topology

- ”Good” and ”Poor” are legitimate, well-behaved users of ”Target”.
  $\Rightarrow$”Well-behaved” connections throttle back sending rate during congestion.
- But ”Poor” happens to share a router with the attacker, ”Bad”.
- The link from R1 to Target is the bottleneck.

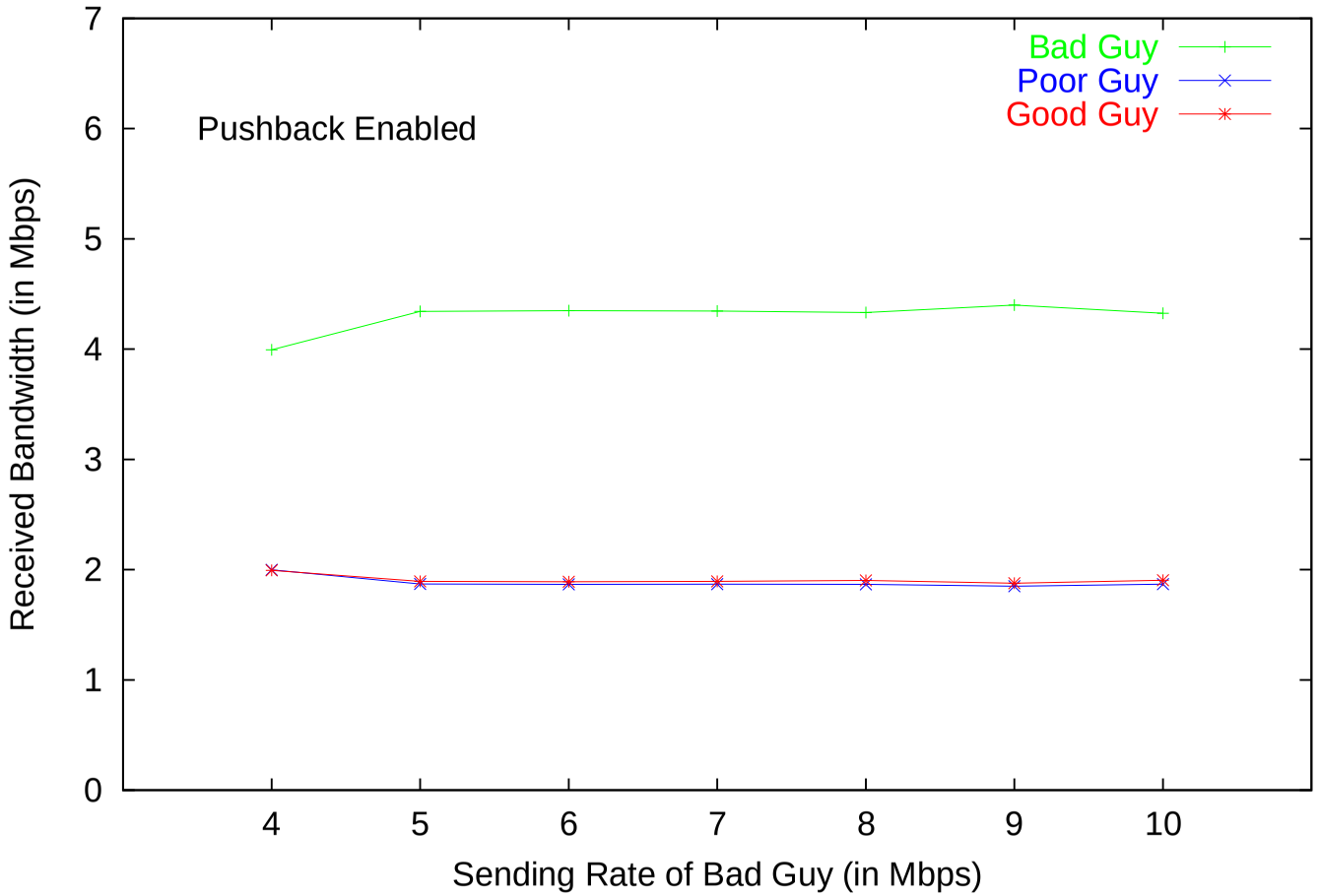
Legitimate Users at 2 Mbps



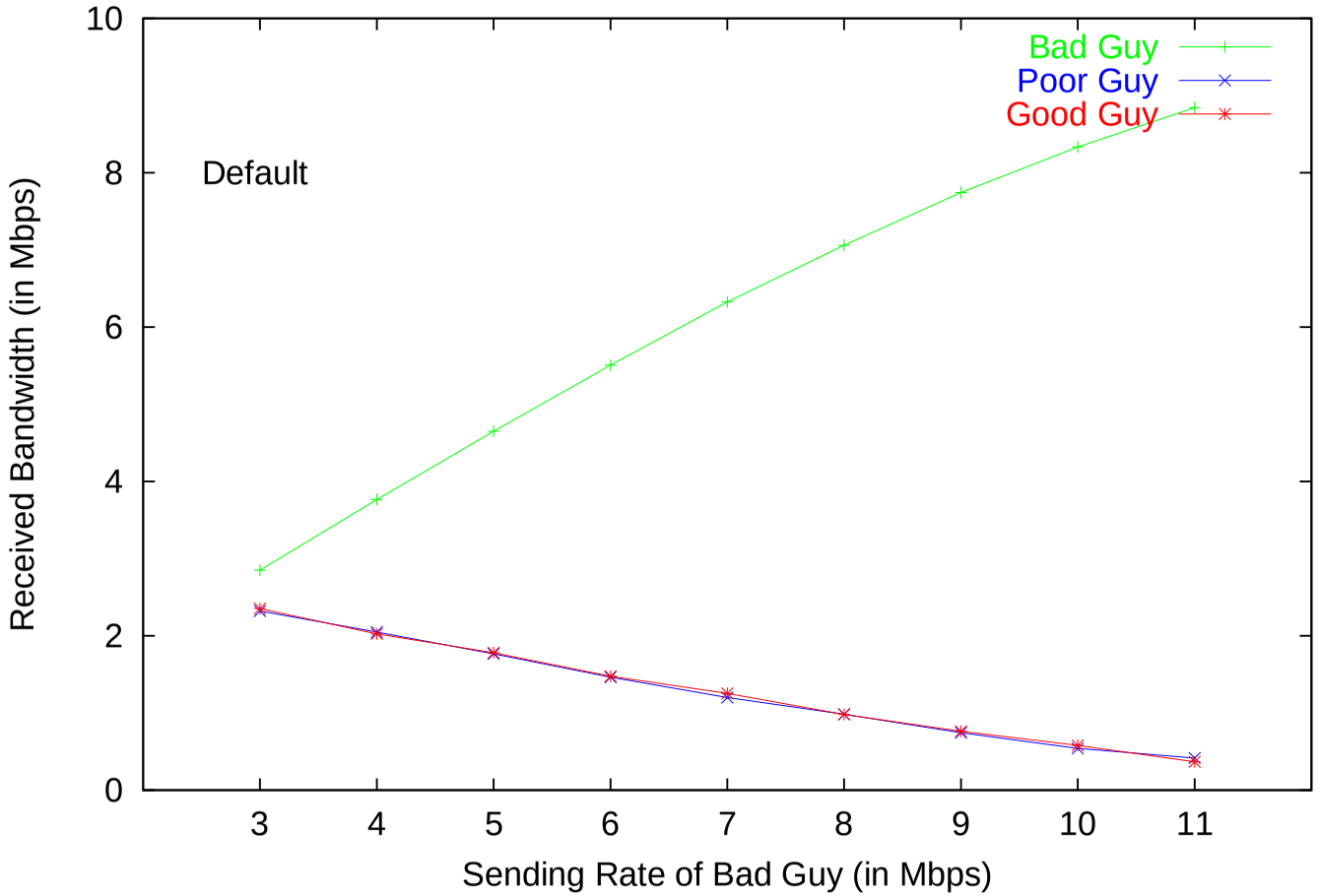
Legitimate Users at 2 Mbps: Local Control



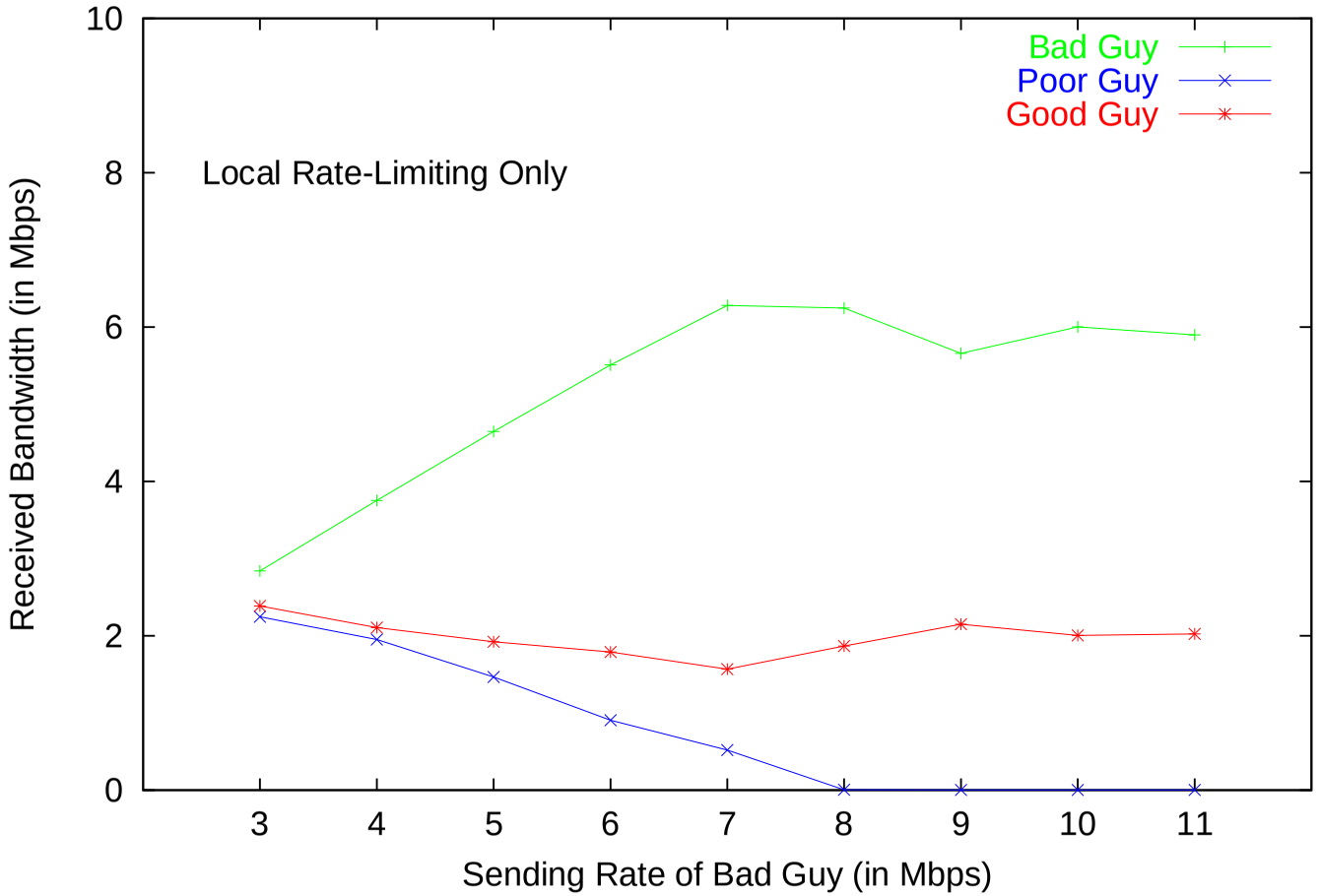
Legitimate Users at 2 Mbps: Pushback



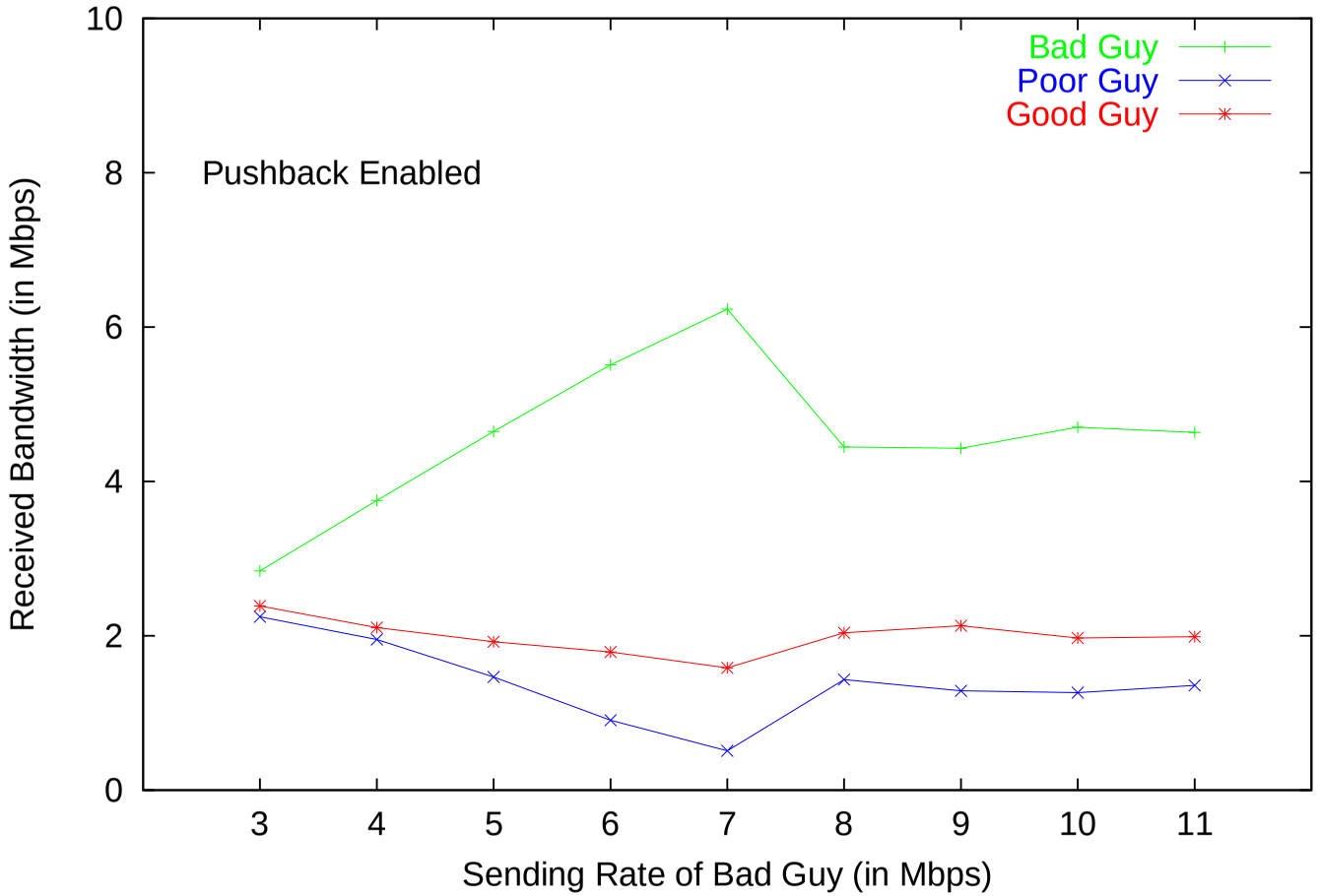
Legitimate Users of TCP



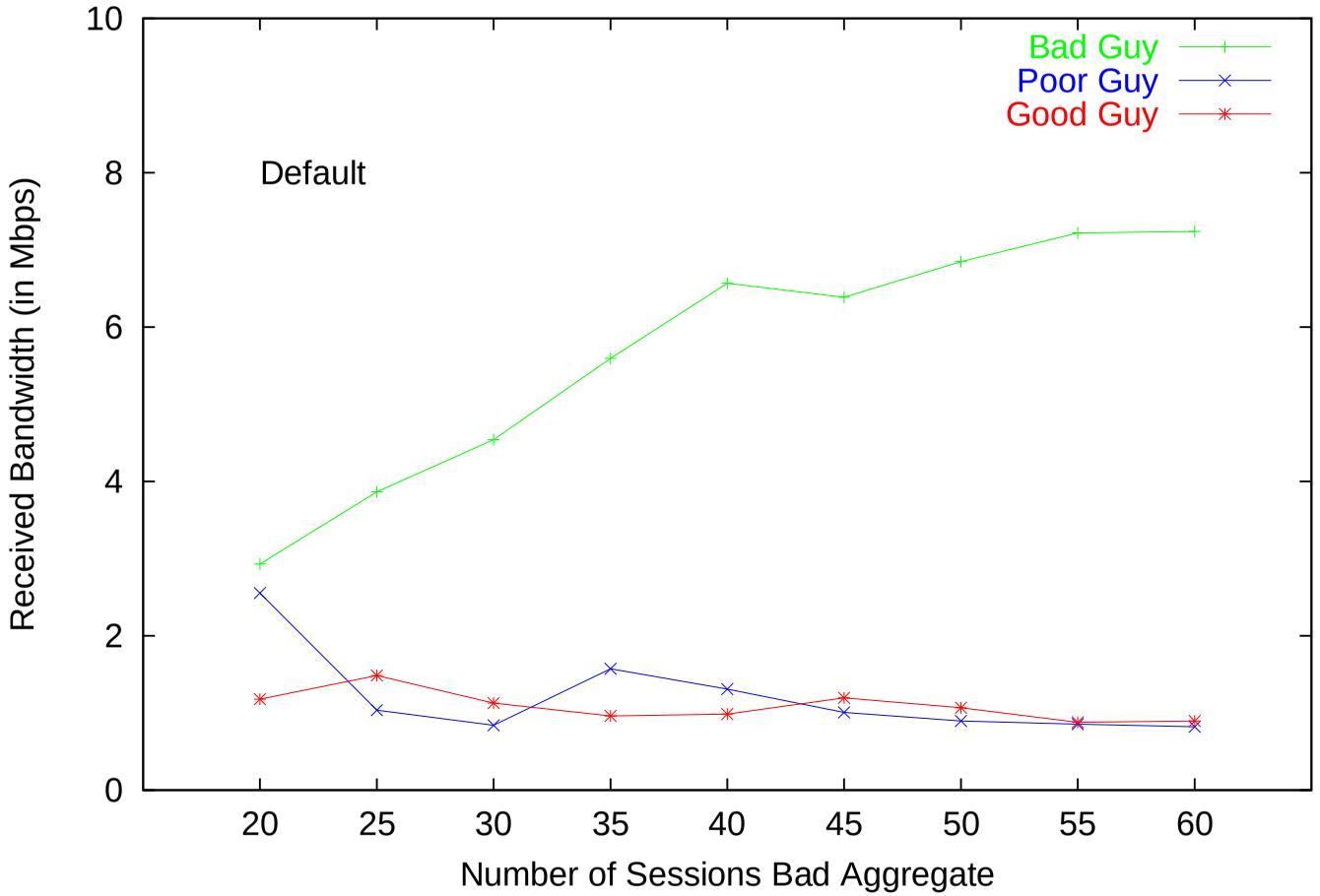
Legitimate Users of TCP: Local Control



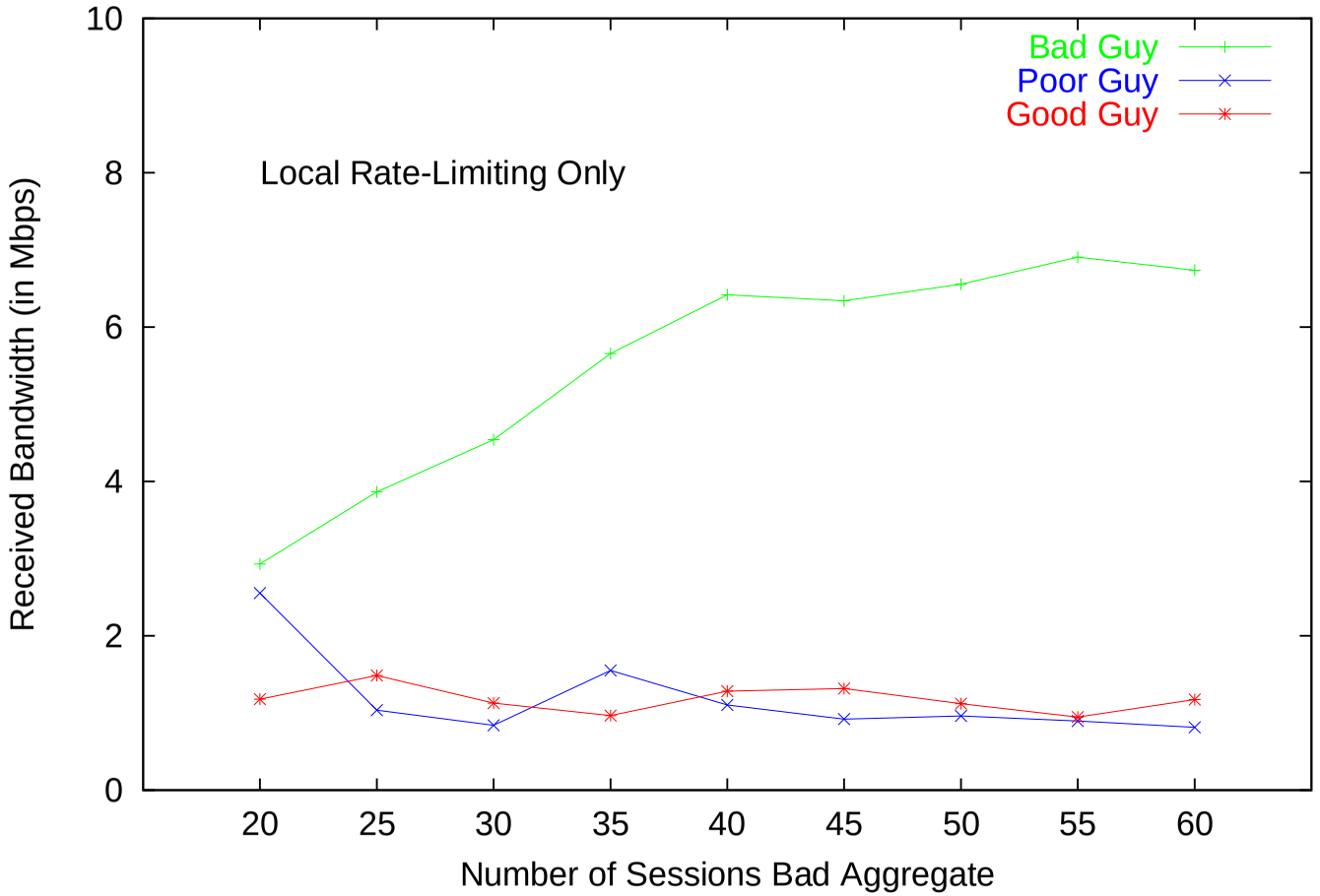
Legitimate Users of TCP: Pushback



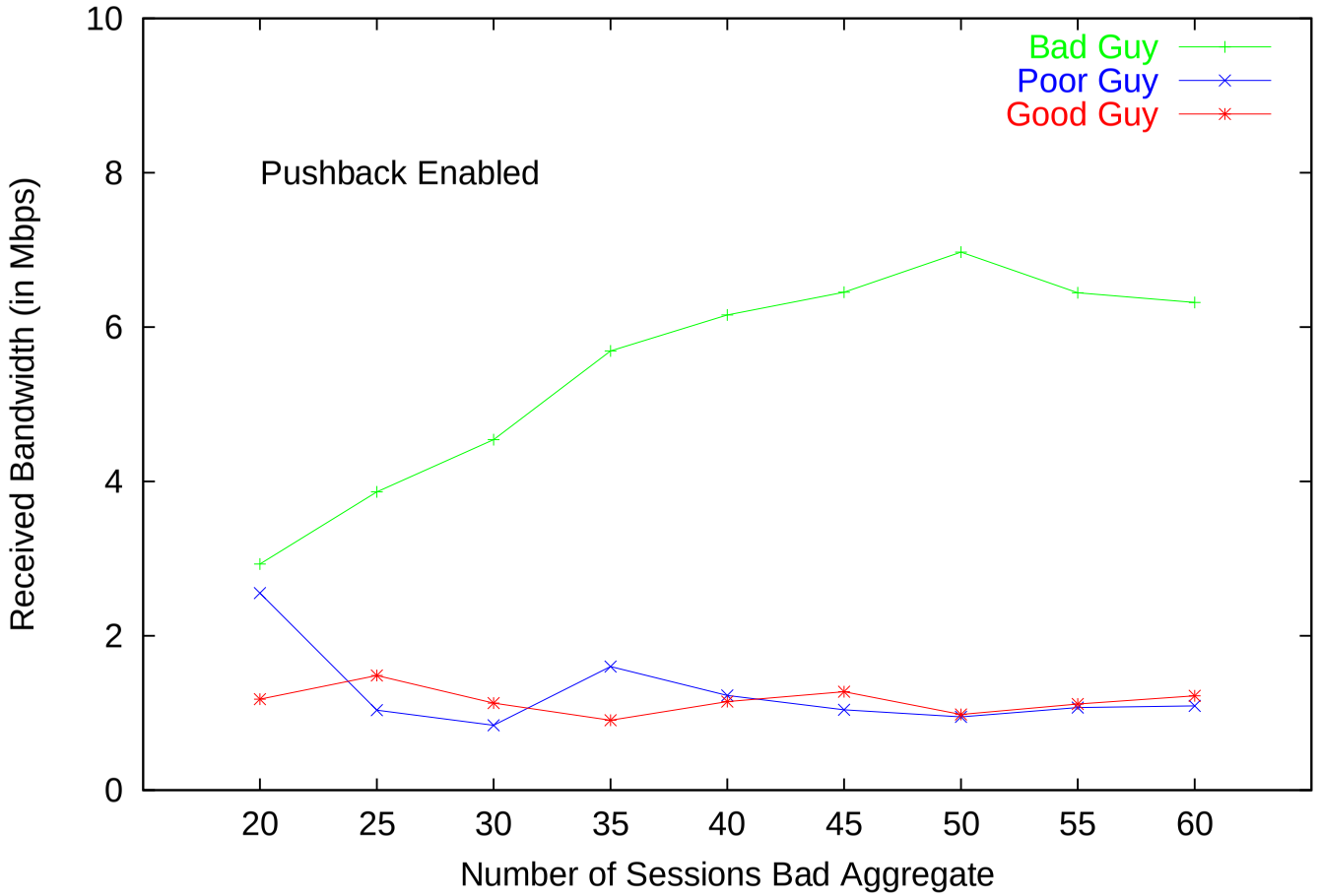
Web-like Traffic



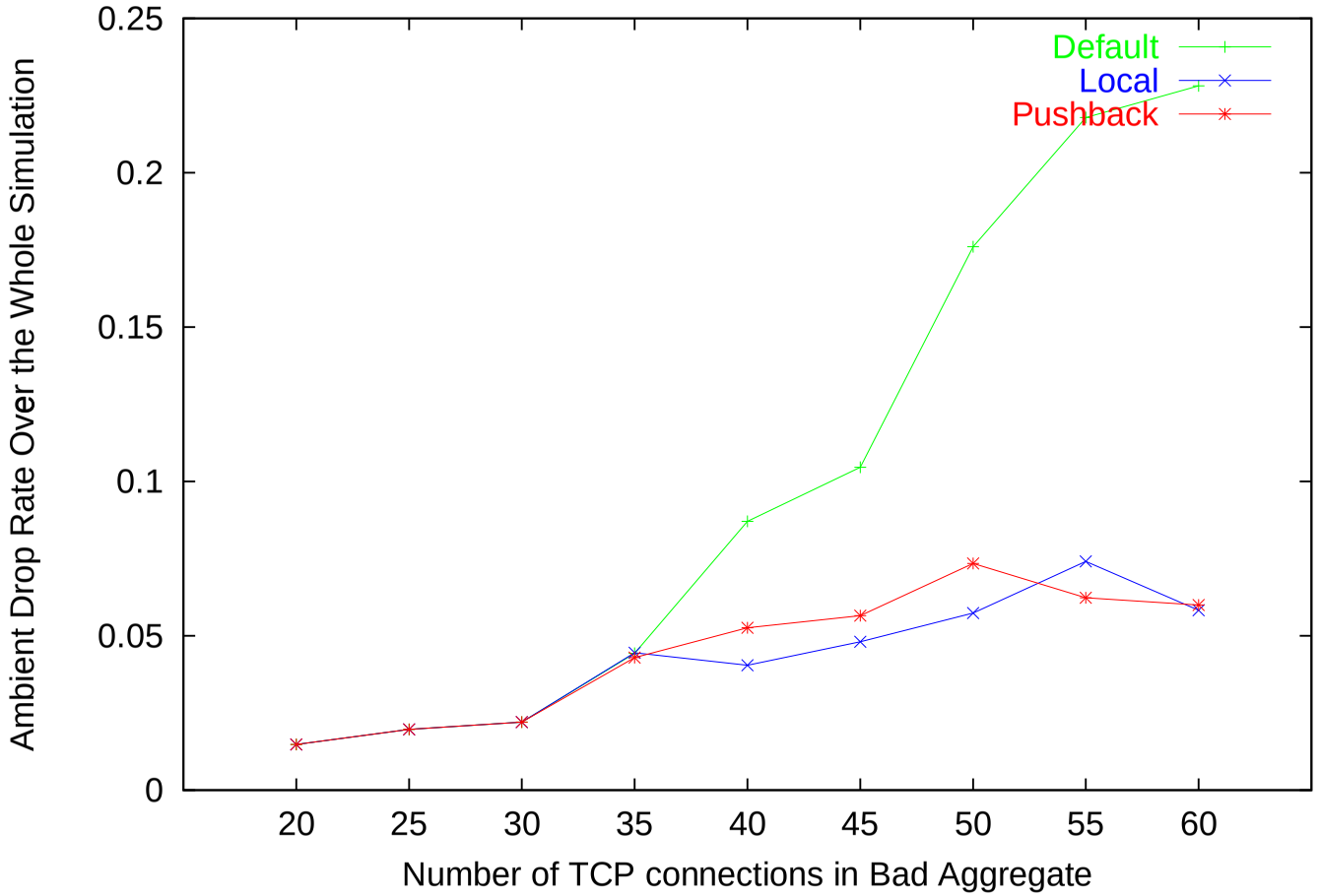
Web-like Traffic: Local Control



Web-like Traffic: Pushback



Web-like Traffic: Packet Drop Rate



Design Details

- Pushback implemented as rate limit before output queue — anything below that rate simply goes in output queue with everything else.
- “RED”-initiated packet discards are used to find the the traffic from a “flash crowd” or DDoS attack.
- Upstream routers report their behavior to their downstream neighbors.
- Pushback requests are “soft state” — requesting router must refresh the requests.

Open Issues

- What are the proper time and drop rate constants?
- Can we easily detect likely attack aggregates?
- How diffuse an attack can this handle?
- Is this useful as a more general traffic management technique?

Status

- Simulations and other theoretical studies continuing.
  (Should have draft paper in a couple of months.)
- Trial implementation (based on FreeBSD) being built by John Ioannidis.
- Still a research area; *not* yet ready for implementation by router vendors.