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, Scott Shenker (all of ACIRI) and John Ioannidis (of AT&T).

⇒ Graphs from simulations done by Mahajan.

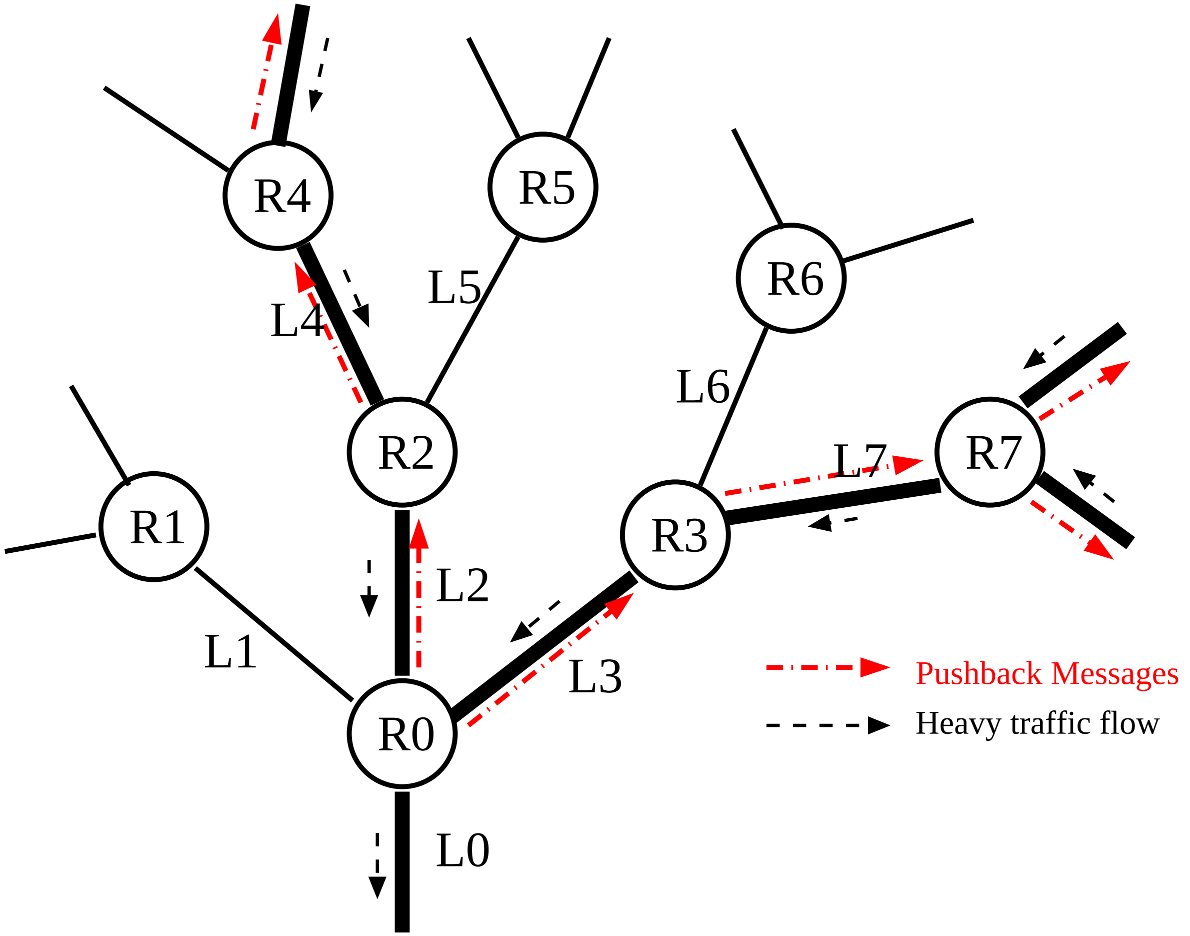
- Based on ideas from informal DDoS research group (Steven M. Bellovin, Matt Blaze, Bill Cheswick, Cory Cohen, Jon David, Jim Duncan, Jim Ellis, Paul Ferguson, John Ioannidis, Marcus Leech, Perry Metzger, Vern Paxson, Robert Stone, Ed Vielmetti, Wietse Venema).

Last Year's Suggestion

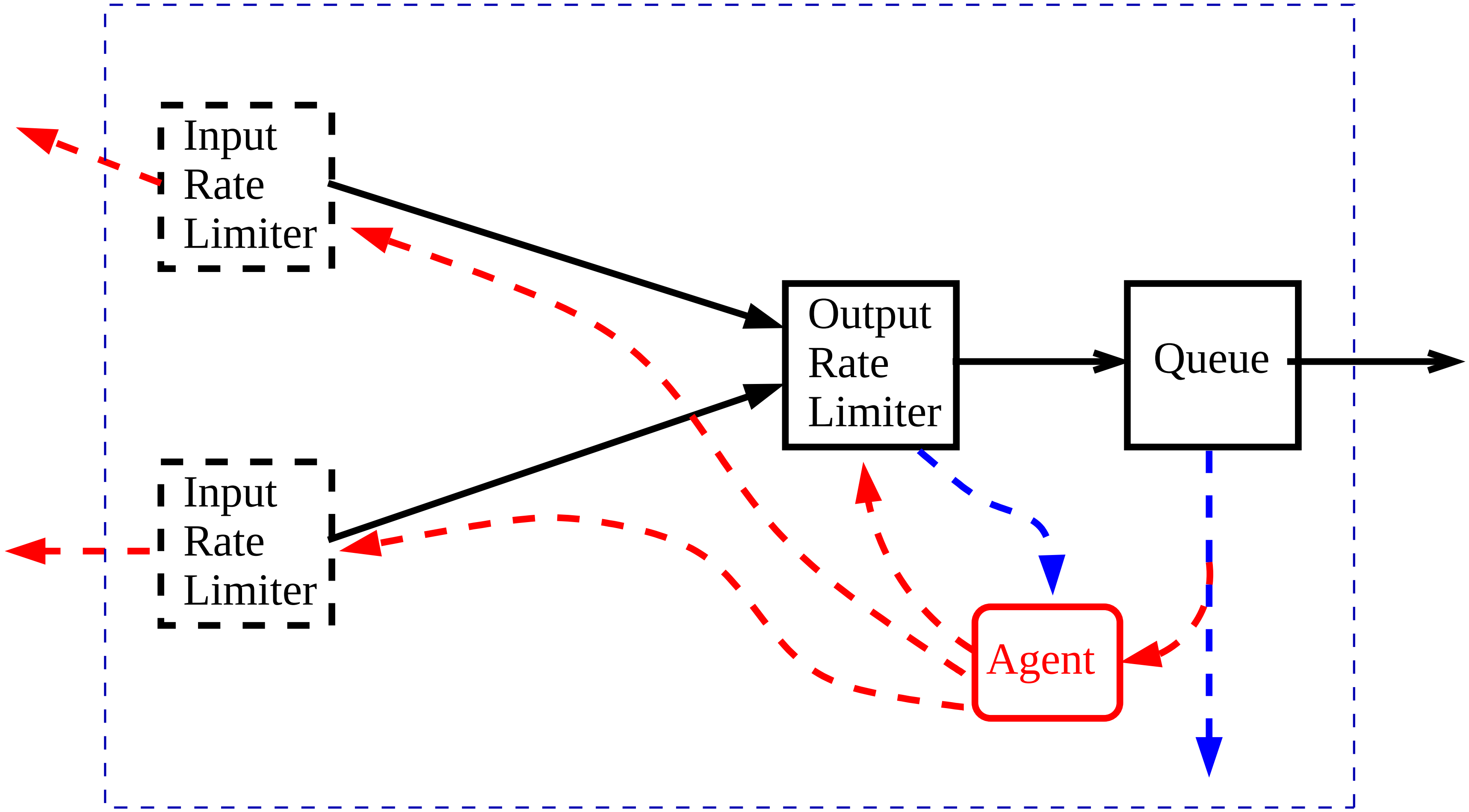
- Define an attack as "too many packet drops on a particular access line".
- Send upstream node a message telling it to drop more packets for this destination.
- Traditional RED+penalty box works on flows; this works on destination alone.
- Issues: authentication, fairness, effect on legitimate traffic, implementability, etc.

We've implemented it under *ns* and measured it, and it seems to work in simulations. But will it work in the real world?

Data Flow


R4
R5
L5
L4
R6
L6
R2
L7
R7
R1
R3
L2
L1
L3
R0
L0
Pushback Messages
Heavy traffic flow

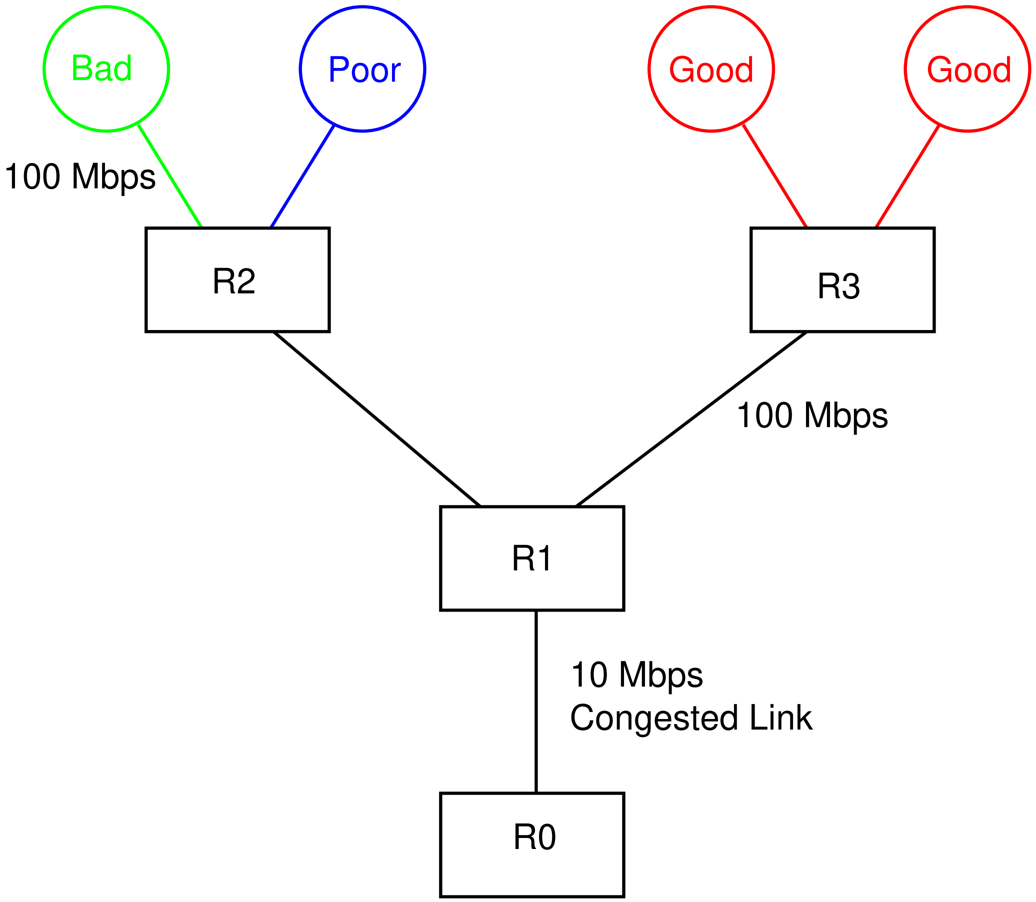
Basic Router Architeture

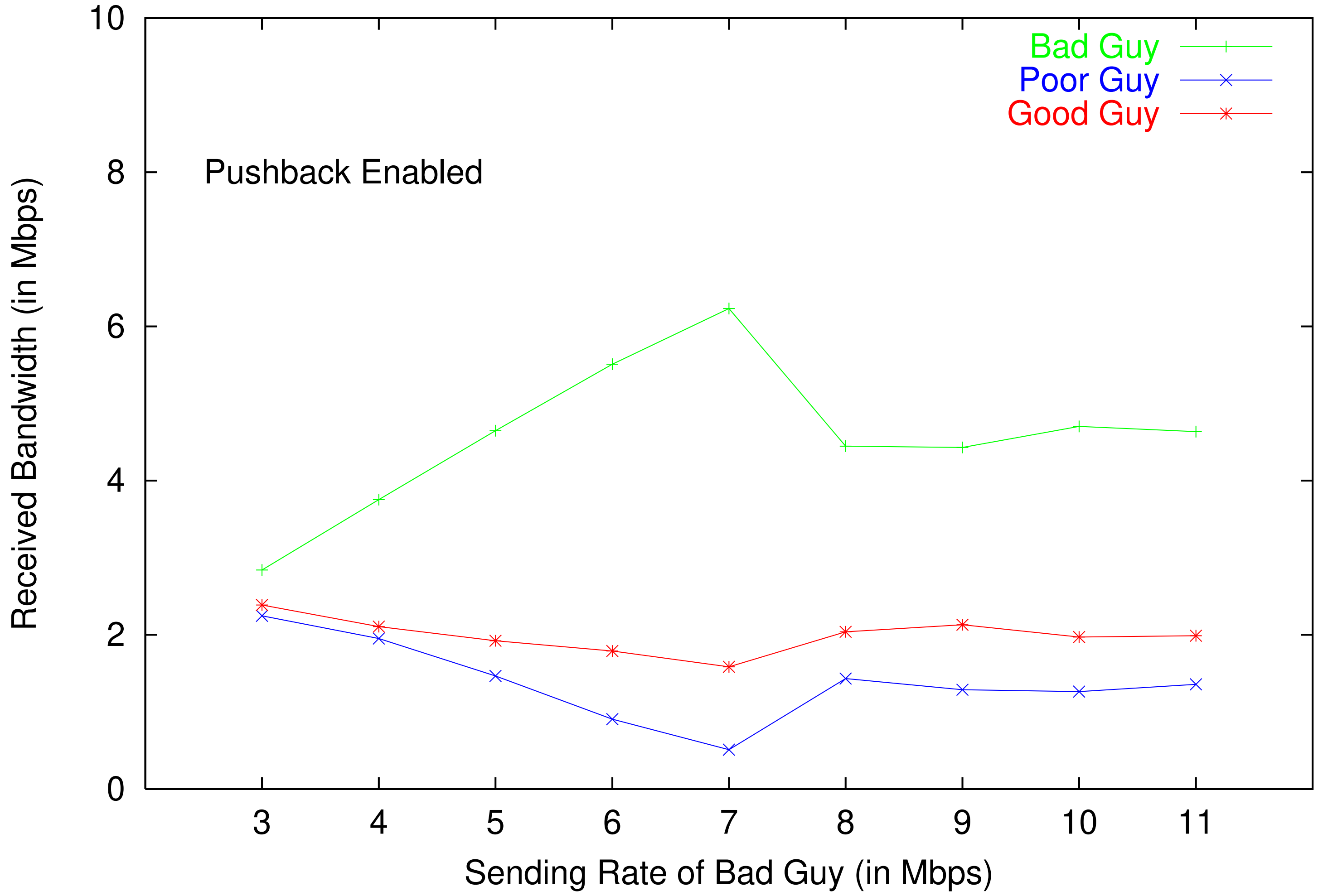


Aggregate Congestion Control

- At times of high congestion, ACC Agent examines queue drops, characterizes problematic "aggregates".
  - May just be destination (prefix).
  - Could contain port numbers, source address, etc.
  - *Not* in packet forwarding path.
- Local ACC: install rate limiter in *this* router.
- Pushback: ask upstream routers (or optional input rate limiter, if upstream peer unsuitable) to control flow.
  $\Rightarrow$Status messages flow downstream.
- Rate-limiter is in forwarding path.

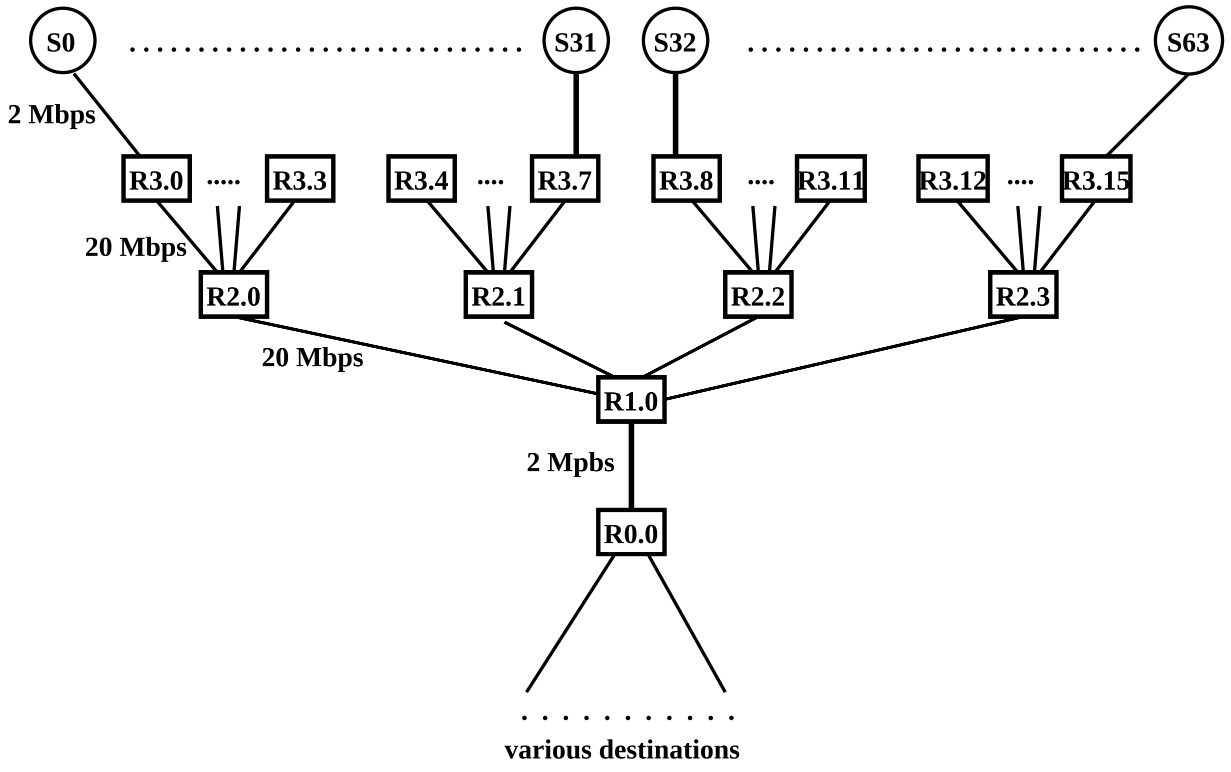
Small Topology





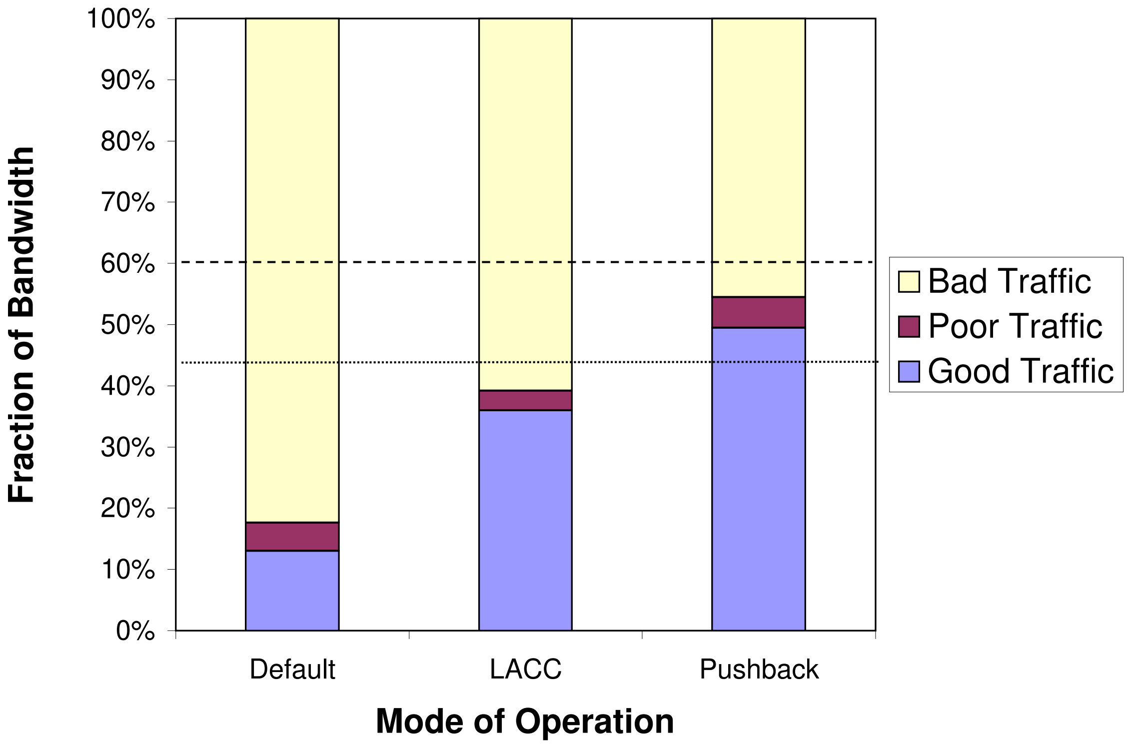
Bad Guy
Poor Guy
Good Guy
Pushback Enabled
Received Bandwidth (in Mbps)
Sending Rate of Bad Guy (in Mbps)
0
2
4
6
8
10
3
4
5
6
7
8
9
10
11

Big Topology, Web-like Behavior

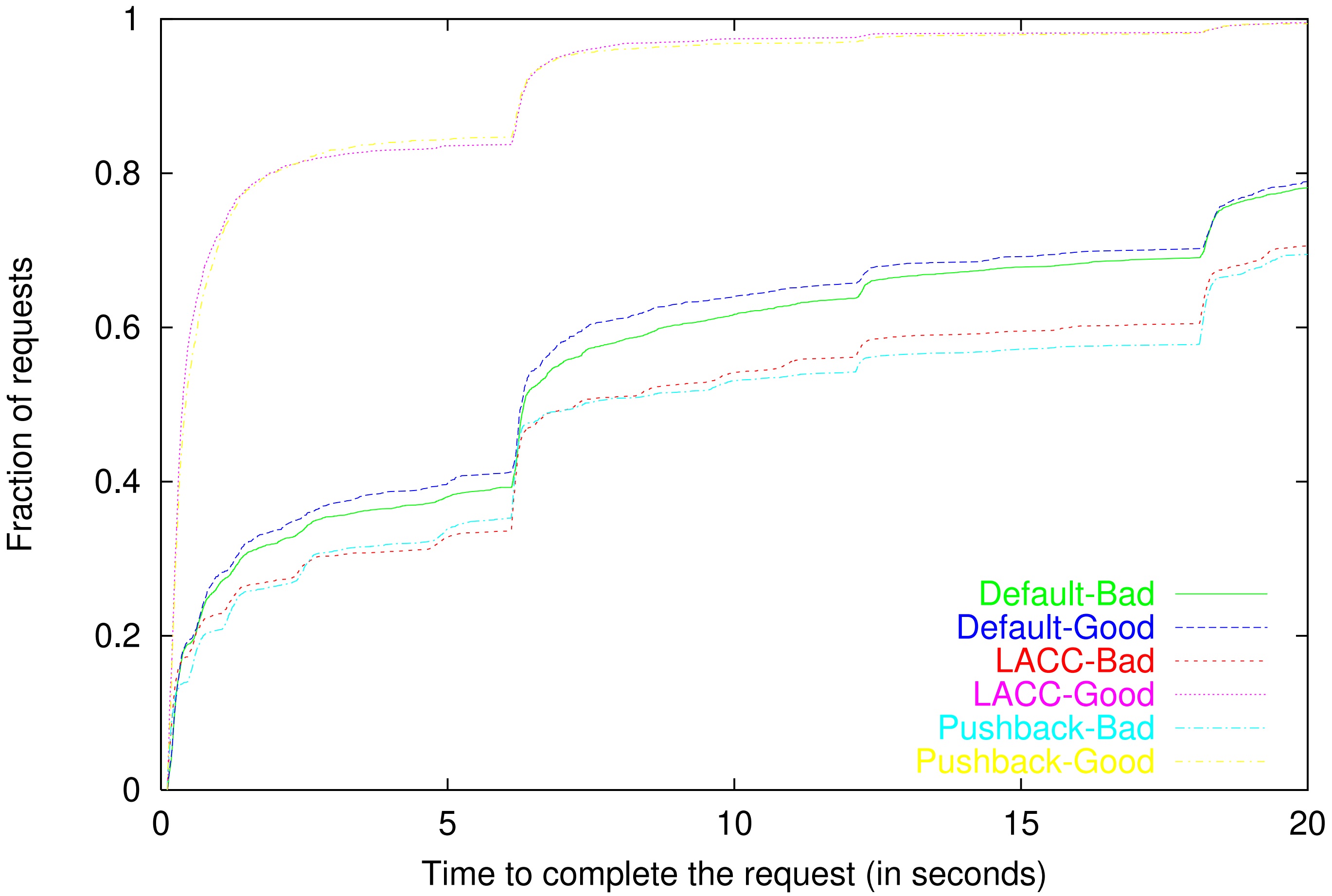


Throughput with 4 Bad Hosts

Throughput with 32 Bad Hosts



Flash Crowd Behavior



Deployability

- Basic design must be deployed in contiguous chunks — is this feasible?
- Use input rate-limiters at edges.
- Perhaps deploy pushback-enabled routers at peering points, and treat intra-ISP backbone as a giant virtual router.

⇒ Can throttle excess traffic from outside, even without full internal deployment.

Can Vendors Build the Boxes?

- Can rate-limiting be done at line speed?
- Can input rate-limiting be done at line speed?
- Do routers know the upstream peer on a per-packet basis? (We can work around that one if necessary.)
- What about layer-2 devices with queues (i.e., ATM)?

Can Operators Use It?

- *Many* policy knobs to twiddle — threshhold, aggregate detection, message timing, etc.
- Can inter-domain pushback requests be trusted?
- What do you do with too many pushback requests?
- Can attackers manipulate pushback to cause worse attacks?
- What should the MIB and/or SNMP traps be?

What Researchers Need

- Feedback on feasibility.
- Better data on topologies.
- Attacker source lists.
- Packet header traces from actual attacks (and other failures).
- More information about sustained periods of congestion:
  - How often do they occur, and for how long?
  - What is the distribution among DDoS attacks, flash crowds, hardware failures, fiber cuts, and plain diffuse congestion?

References

Theory

http://www.research.att.com/˜smb/papers/ddos-lacc.ps

http://www.research.att.com/˜smb/papers/ddos-lacc.pdf

Prototype Implementation

http://www.research.att.com/˜smb/papers/pushback-impl.ps

http://www.research.att.com/˜smb/papers/pushback-impl.pdf