Aggregate Congestion Control (ACC)

Ratul Mahajan± Steve Bellovin† Sally Floyd‡ John Ioannidis† Vern Paxson‡ Scott Shenker‡

ACC mechanisms enable the network to protect itself against high bandwidth aggregates generated by DoS attacks and flash crowds

Aggregate

A collection of packets with a common property like destination prefix, ICMP ECHO, TCP SYN, etc.

Motivation

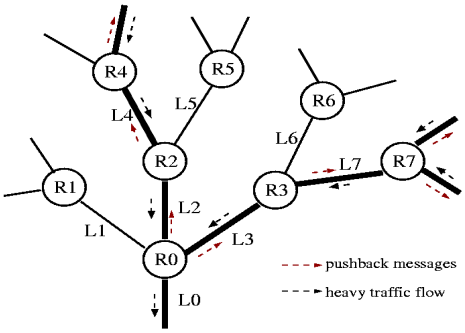
- Internet is vulnerable to high bandwidth aggregates.
- Traditional protection/fairness mechanisms, which work on the granularity of flows, are not useful when the aggregate is composed of many small flows.
- Source filtering and traceback are of limited use.
- Manual intervention takes too much time in both detection and control.

ACC mechanisms

1. Are triggered by **sustained severe congestion**.
2. Use drop history to find responsible aggregate(s). Characterize them by a **congestion signature**.
3. Compute bandwidth limit for the aggregate based on policy and/or desired reduction in drop rate.
4. Rate-limit the aggregate(s) using a light weight mechanism like **virtual queue**.
5. Decide whether to invoke **pushback** based on drop rate within the aggregate and/or external information.
6. Periodically, review situation.

Pushback

Request high sending upstream neighbors to rate-limit aggregate.



- Concentrates rate-limiting on attack traffic.
- Protects innocent traffic in the congestion signature by "spatial" narrowing (protects traffic from L1, L5 and L6 above).
- Improves network throughput by taking dropping upstream.
- Can also be invoked by a swamped server.

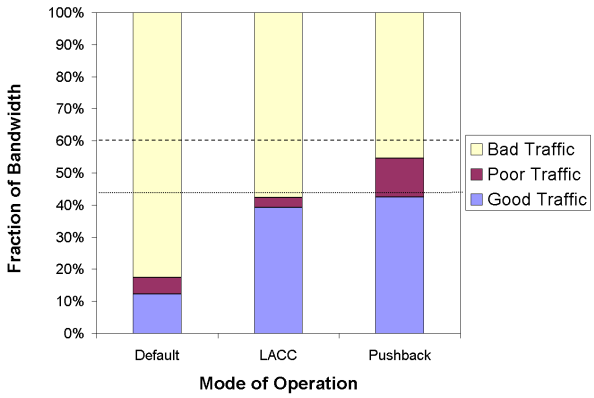
Limitations

- May overcompensate
- Less effective with isotropic attack topologies.

Simulation Results

Topology of 64 hosts and 22 routers.
4 hosts sending "bad" attack traffic.
4 hosts sending "poor" traffic (innocent traffic inside the congestion signature).
10 hosts sending "good" traffic.

The two horizontal lines show the bandwidth of good and poor traffic in absence of bad traffic.



- **Default (no ACC):** bad traffic gets away with most of the bandwidth.
- **LACC (local ACC, no pushback):** protects good traffic but not poor.
- **Pushback:** protects both good and poor traffic. Throughput of good and poor traffic almost same as no bad traffic case.

Open Issues

- How well will it work in practice?
  - Need more data on attack topologies.
  - Packet traces from attacks and flash crowds.
- How often is sustained congestion caused by hardware failures?

± University of Washington †AT&T Research ‡ACIRI

http://www.aciri.org/pushback