

DDoS for Zombies

John "JI" Ioannidis
AT&T Labs - Research
ji@research.att.com

Security Attacks

- Ordinary security attacks:
 - Exploit target vulnerabilities.
 - Give resources to attacker.
 - Fixing vulnerability solves the problem.
- Denial-of-service attacks:
 - Prevent others from using the targetted system.
 - Attacker gets indirect benefits.
 - Some DoS attacks exploit vulnerabilities.
 - Most just eat up resources.

Attacks I: Target is end node.

- CPU attack.
 - Application-level attacks.
 - Cause unnecessary processing to happen.
- Memory attack.
 - Buffer overruns (most frequent source).
 - Bug exploits (e.g., ping of death)
 - Memory exhaustion (e.g., SYN attacks)

Easier to mitigate:

- Proper host security.
- Proper protocol design (e.g., cookies).

Attacks II: Target is network link

- By target link:
 - Usually access link (core network over-provisioned).
 - Slow border links (to distant lands).
- By source of attack:
 - Trin00/TFN style: master/slaves.
 - Reflector attacks.
- By packet contents:
 - Random (just bandwidth).
 - Calculated (SYN, directed broadcasts).
- By cause:
 - Deliberate attack.
 - Flash crowd.

DOCTOR FUN

11 Apr 2000



Copyright © 2000 David Farley, d-farley@metalab.unc.edu
<http://metalab.unc.edu/Dave/drfun.html>

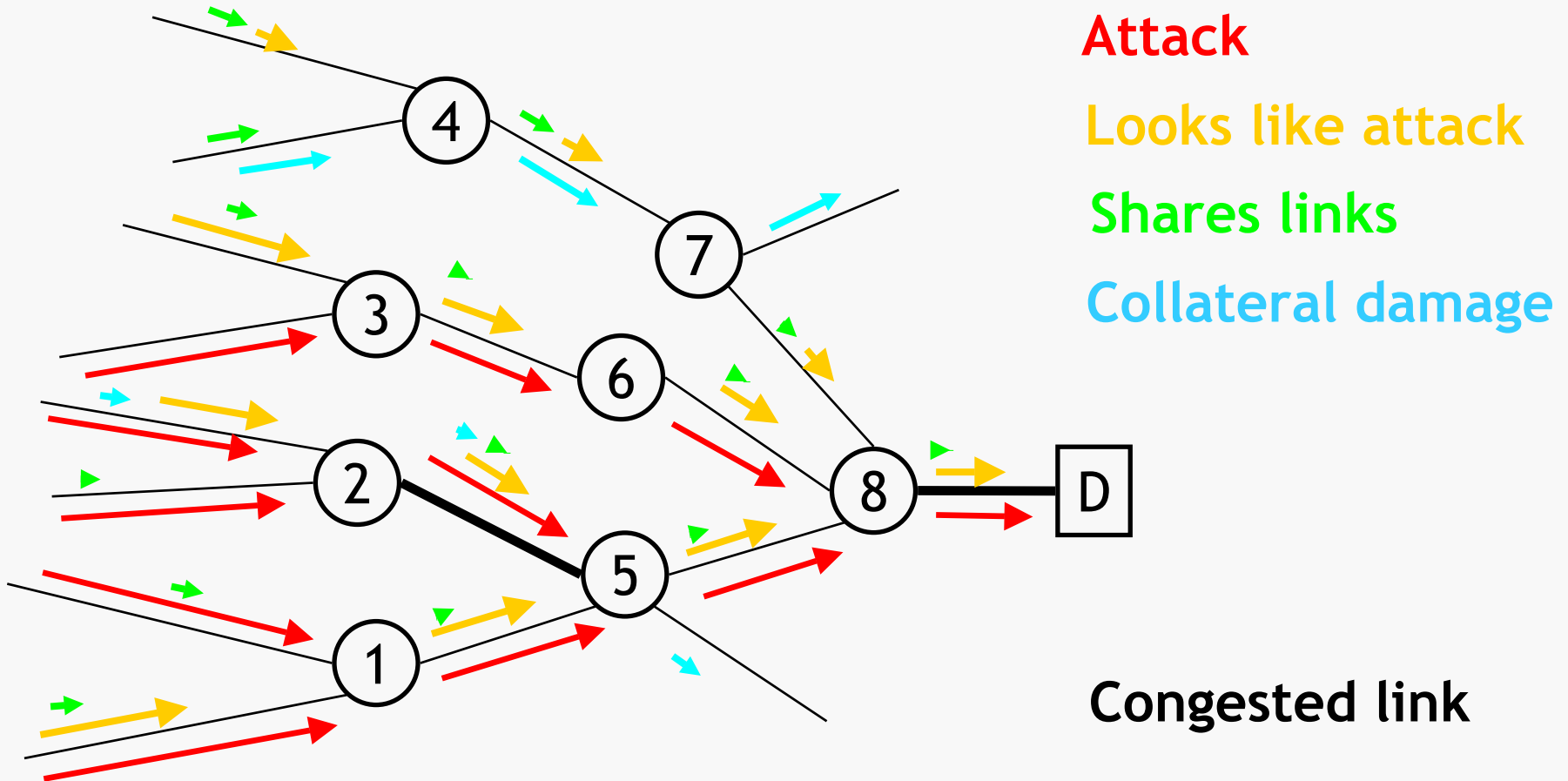
This cartoon is made available on the Internet for personal viewing only. Opinions expressed herein are solely those of the author.

The Enterprise suffers another distributed tribble flood attack.

DDoS: Distributed Denial of Service

- Network attacks aim at flooding the victim's link.
 - Strong attacker against weak victim.
- Distributed attacks use multiple sources.
 - Lots of weak attackers against strong victim.
- Usual implementation:
 - Multiple compromised machines with *zombies*.
 - Masters direct zombies to attack victim.
 - Victim overwhelmed.

An Attack in Progress



Why are DDoS Attacks Hard to Defend Against?

- Nothing victims can do to protect themselves:
 - Usually, attack is on *connectivity*.
 - Better overall host security *would* help.
 - As would source address filtering.
- Bandwidth management not applicable.
 - End-to-end congestion control not applicable.
 - Source does not obey E2E CC.
 - Active Queue Management not applicable.
 - 'Flows' very short-lived.
- Diffserv/Intserv do not help with best-effort traffic reqs.

Characteristics of Current Attacks

- Several small-scale attacks a day.
- Fairly crude.
 - Captured code is of abysmal quality.
 - Have recently started pairing up with virus writers.
 - Aggressive viruses also result in congested links.
- Anisotropic.
 - Locality of penetrated machines.
 - Internet too large to design an isotropic attack.
- Purpose used to be just ego gratification.
 - IRC turf wars/vandalism.
- Spammers are now paying for DDoS services.
- We worry about tactical uses.

Design of a Perfect Attack

- Looks like legitimate traffic.
 - Flash crowd.
- Isotropic/topology aware.
 - Uses network mapping information.
- Adaptive.
 - Responds to our attempts to quench it.
- Automatic propagation.
 - Viruses or other software flaws.

Why is the network still running?

Probably because the attackers don't want to lose their playground.

Defense I: Detection

- Traffic monitoring.
 - Content.
 - Shape/characteristics.
- Link/interface monitoring.
 - Drop rates
 - NetFlow
- Traffic marking.
 - ICMP TRACEBACK
 - Packet marking (many variants).
 - Only useful if source IP addresses are faked.

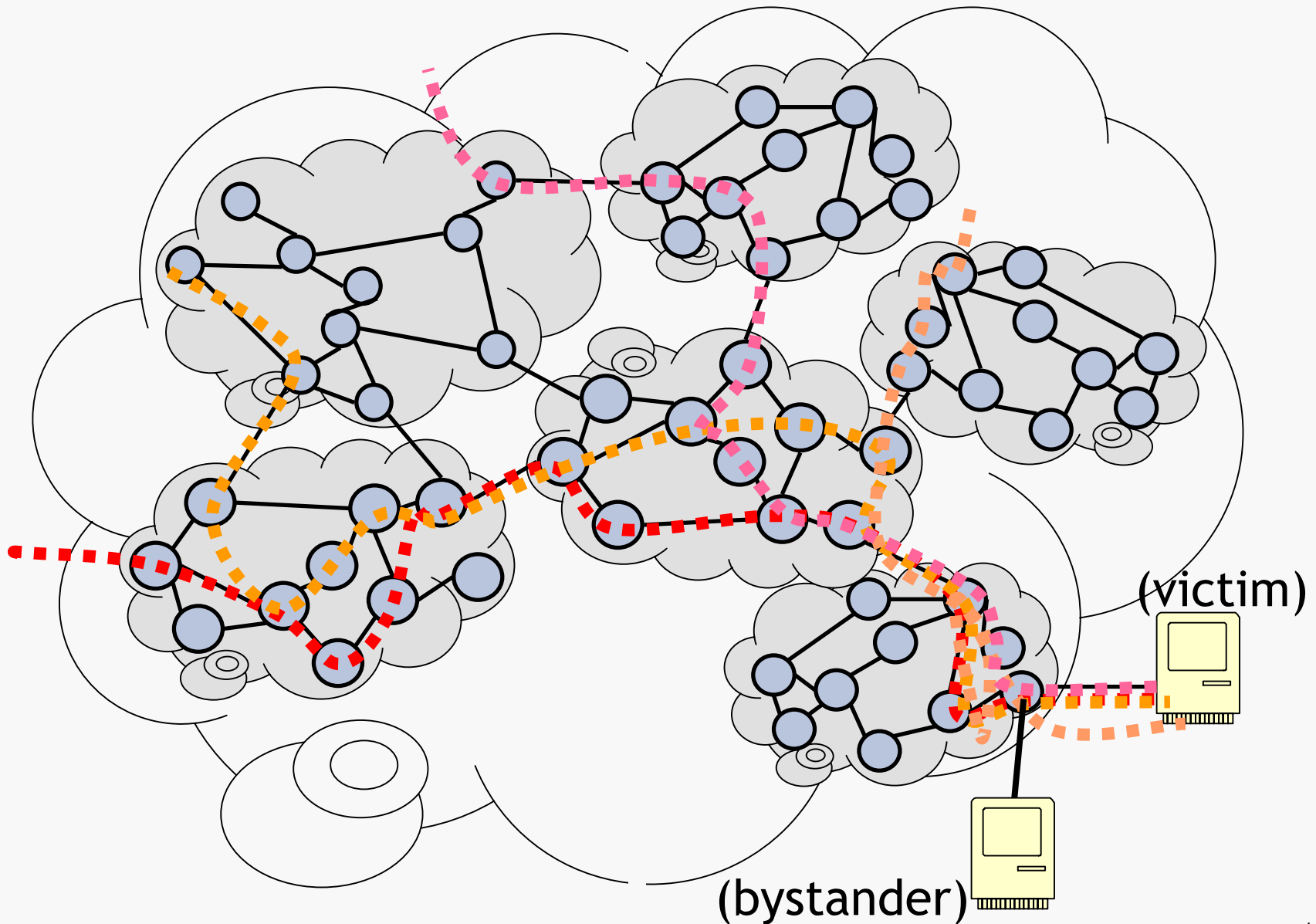
Defense II: Response

- Traffic management:
 - Rate limiting.
 - Filtering.
 - Redirection.
- Distribution:
 - At specific points (*e.g.*, border routers)
 - Along attack path.
- Scope:
 - Within an administrative domain (intra-ISP).
 - Across administrative domains (requires collaboration).

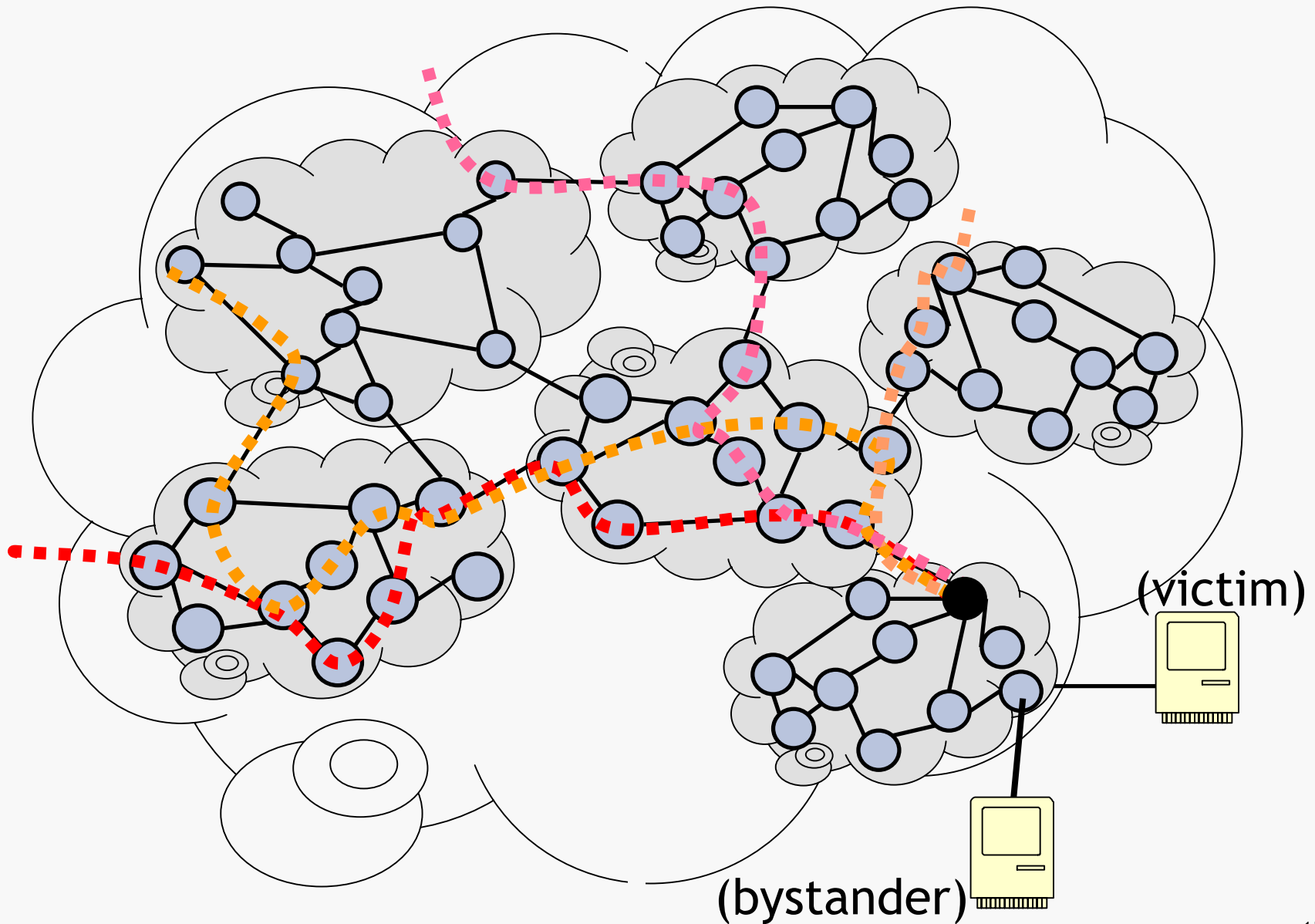
Defense II: Response, cont'd

- Cost/benefit:
 - Innocent traffic.
 - Level of service.
 - Vulnerabilities introduced?
- Identification of attacker?
 - Just mitigating effects.
 - Finding attacker and/or zombies.
 - Punishing.
 - Fixing!

Blackholing



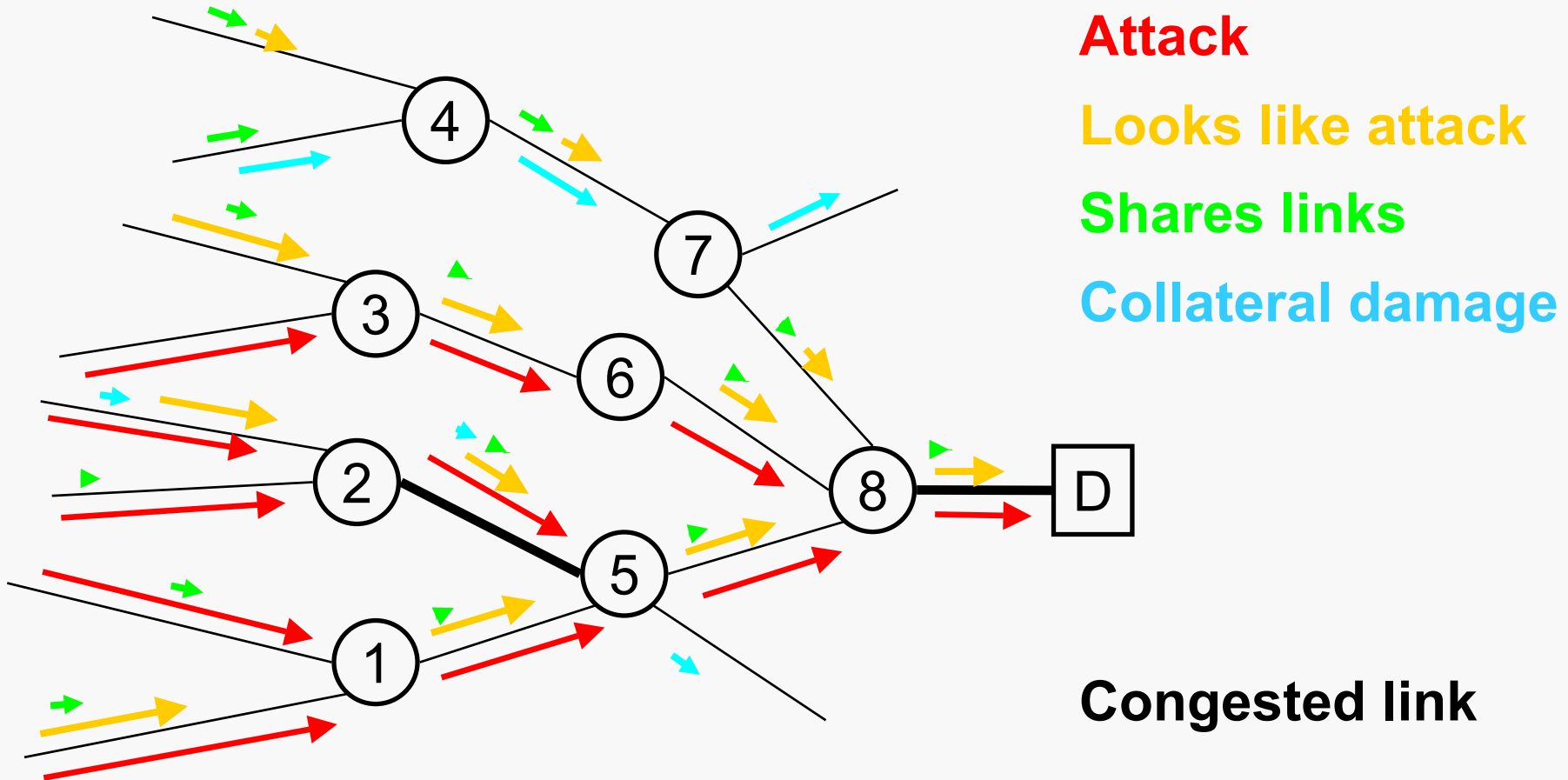
Blackholing



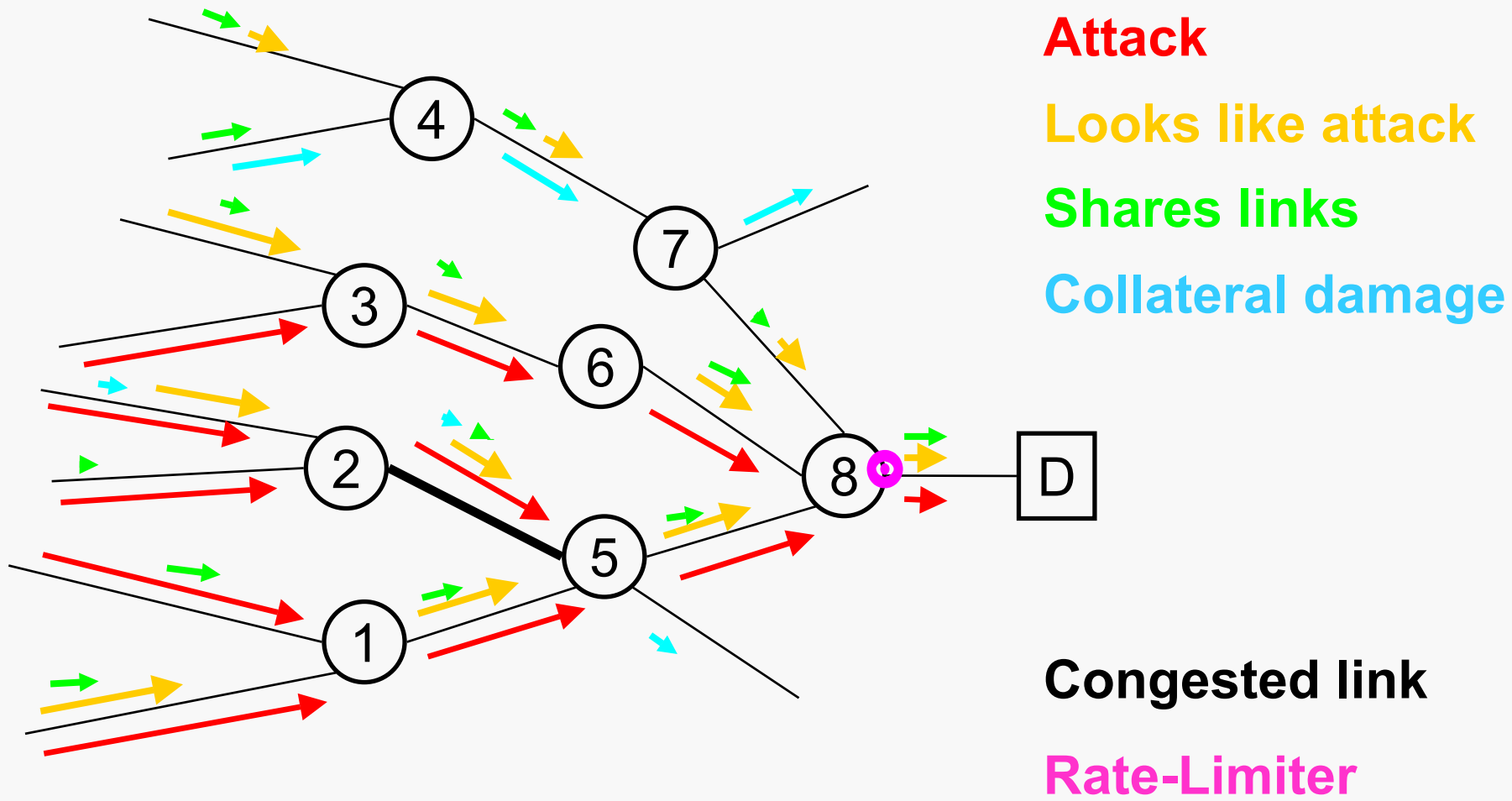
Pushback

- Router-based solution against bandwidth attacks.
- Attack: too many packet drops on a particular link.
- Aggregate: set of packets with a common feature.
- Find the most common aggregate in the drop set.
- Aggregate-based Congestion Control (ACC).

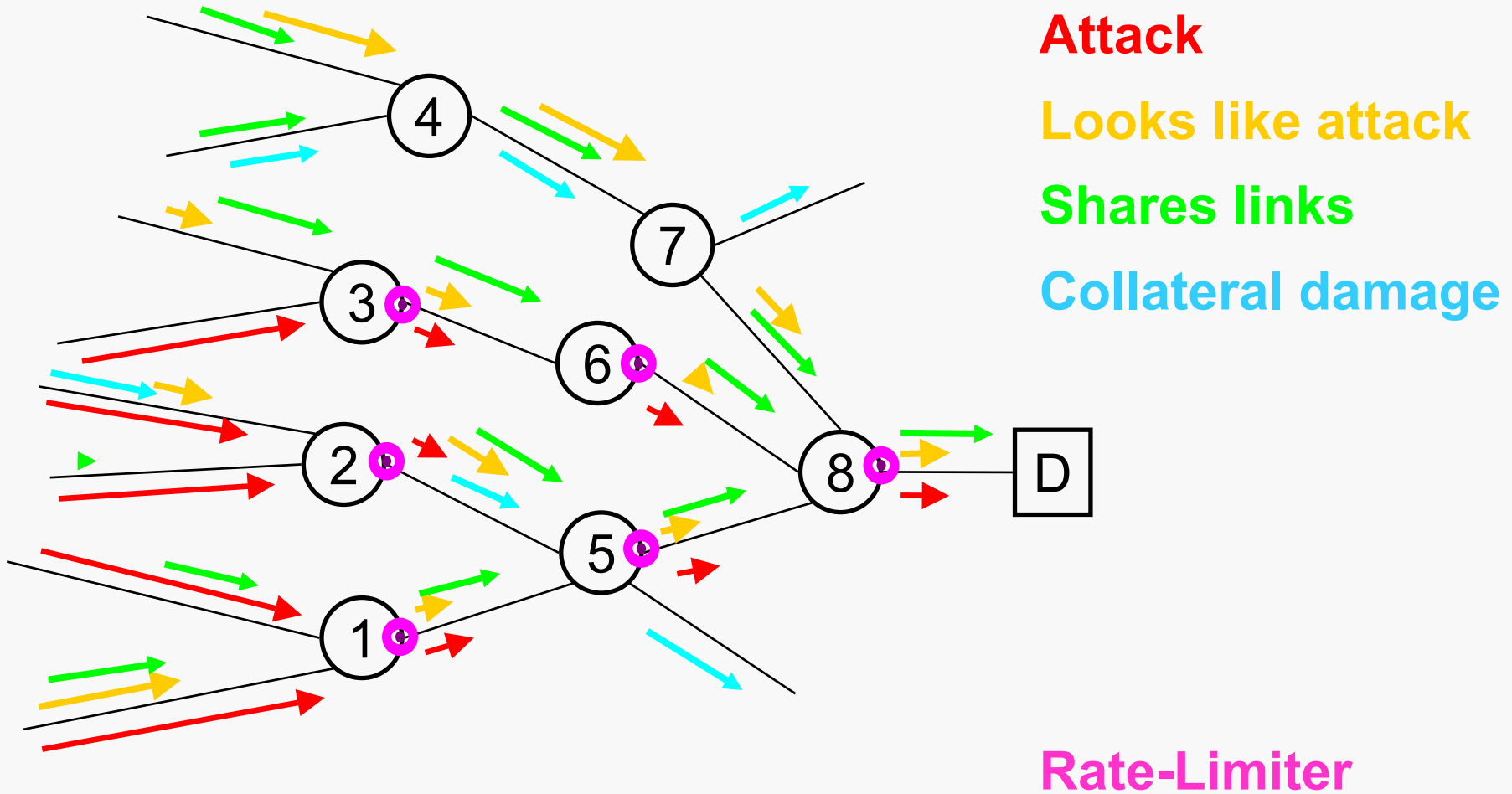
An Attack in Progress (again)



Local Rate-limiting



Pushback



Limits

- Flash crowds.
- Accurately characterizing attack traffic.
- Unexplored dimensions?
 - Legal/social.
 - Radically change Internet architecture.
 - Per-packet payment?
 - Back to virtual circuits?
 - Active networks?

My Questions

- Size distribution of botnets?
 - A: 100K+ zombie botnets are available for the asking.
- Distribution of classes of attacks?
 - Esp. application vs. network level attacks
 - A: we see all kinds.
- Forged vs. real IP addresses?
 - A: they seem to be mostly real IP addresses. This may change if we aggressively punish the sources. Not everybody is actually doing source address filtering and/or uRPF.

... questions ...

- Visible in peering routers?
 - A: yes, esp. in mid-level ISPs. Definitely visible in access routers.
- Repeat attacks?
 - A: yes, many.
- Geographical distribution?
- AS distribution?
- Economics?
 - A: spammers seem to be paying for attacks.
- Sociology?
- How long before a coordinated attack on the routing infrastructure?

Reasons not to give up hope