Should the *IETF* do anything about DDoS attacks?

Mark Handley

The Problem

- The Internet architecture was designed to delivery packets to the destination efficiently.
  - Even if the destination does not want them.
- Congestion control and flow control are our mechanisms to match offered load to available capacity.
  - They're transport-level functions.
  - If the sender misbehaves, they're useless.
- An attacker that can compromise thousands of end systems can muster enough firepower to overwhelm most victims.

Should the IETF do anything about DDoS?

- Really two questions:
  - *Can* the IETF do anything about DDoS?
  - Does anyone care enough to *spend money* on solutions?

Can the IETF do anything about DDoS?

- Search Google Scholar for “DDoS”: 7590 hits.
  - No shortage of “solutions”.

- It’s starting to become clear there is no “magic bullet”.
  - No single solution will come along and save us (short of redesigning the Internet from scratch).
- However, DDoS is not like getting compromised.
  - There’s no such thing as a “little bit compromised”.
  - DDoS defense is progressive; it’s a cost/benefit tradeoff.
- Goal should be to *raise the bar* for successful attacks.

Examples of *Raising the Bar*

- Require more firepower for a successful attack
  - Fewer attacks from a fixed bot pool.
  - Make bot herders easier to track down (fewer but larger botnets, so can devote more resources to each).
- Prevent spoofing.
  - Make bots easier to track down.
  - Prevent reflection attacks.
- Enforce congestion control.
  - Bots only get their share.
- Provide automated filtering of flows at the source.
  - If the receiver can tell a host is bad, it can shut down traffic from it.

Goal for IETF?

- Force an attacker to make his traffic indistinguishable from a flash crowd.
  - Essentially, move the attack up the stack.
- Different applications must them tackle the problem using their own application-specific mechanisms.
  - CAPTCHAS, proof-of-work, authorization mechanisms, good application design, etc.
  - Billing for congestion.

Is anyone willing to pay?

- Are the costs of DDoS great enough to merit additional expense?
  - Depends who has to pay.
  - Depends how expensive it is.

Is anyone willing to pay?

For the victims: DDoS is very expensive.

- Direct loss of business.
- Collateral damage for edge ISPs.
  - Often just disconnect the victim.
- Scrubbing solutions work, up to a point, for dumb attacks at lower bandwidths.
  - Victim bears the cost.

For the source ISPs: fairly significant costs.

- Manual cleanup of bots is expensive.
- Many ISPs don't even go looking for bots on their networks.

For transit ISPs: often just more paying packets.

Opportunity costs

- Ever increasing demands are being placed on the Internet.
  - Internet telephone.
  - Internet television.
  - Critical infrastructure.
    - Food supply
    - Banking
    - Utility management.

- Options (pick one):
  1. The Internet gets robust enough to justify these demands.
  2. The demands will be met by parallel networks at increased costs.
  3. A large, well resourced DDoS attack will cause huge economic damage (and perhaps worse) at some point in the next decade.

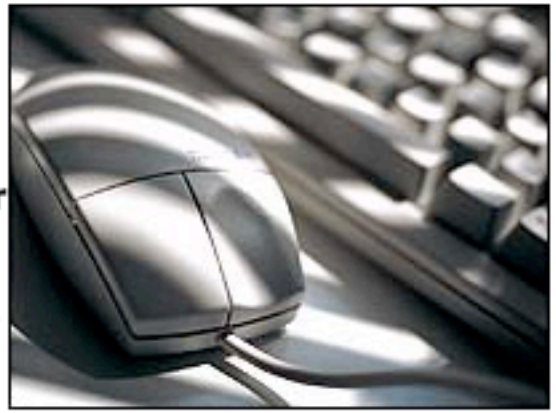
News Front Page
Africa
Americas
Asia-Pacific
Europe
Middle East
South Asia
UK
Business
Health
Science/Nature
Technology
Entertainment
Also in the news
Video and Audio
Have Your Say
In Pictures
Country Profiles
Special Reports
RELATED BBC SITES

Last Updated: Thursday, 17 May 2007, 15:21 GMT 16:21 UK

E-mail this to a friend Printable version

Estonia hit by 'Moscow cyber war'

Estonia says the country's websites have been under heavy attack for the past three weeks, blaming Russia for playing a part in the cyber warfare.



Estonia says many state websites have been affected

Many of the attacks have come from Russia and are being hosted by Russian state computer servers, Tallinn says. Moscow denies any involvement.

Estonia says the attacks began after it moved a Soviet war memorial in Tallinn. The move was condemned by the Kremlin.

A Nato spokesman said the organisation was giving Estonia technical help.

"In the 21st century it's not just about tanks and artillery," Nato spokesman James Appathurai told BBC News.

Legislation

- After the Estonia attacks, governments are starting to wonder if they can legislate solutions.
- Best way to avoid a mess of inconsistent, incompatible, and ill-thought-out legislation is to solve the problem first.

- Need to be very careful the medicine isn't worse than the disease.

Architectural Ossification

- The net is already hard to change in the core.
- IP Options virtually useless for extension.
  - Slow-path processed in fast hardware routers.
- NATs make it hard to deploy many new applications.
- Firewalls make it make to deploy anything new.
  - But the alternative seems to be worse.

- Now consider the effect of DoS mitigation solutions....

The Big Challenges

- How can we mitigate DDoS attacks and other security threats without sacrificing the future?
  - How to enable application innovation?
  - How to provide robust network services in the face of attack?

Extrapolation of current trends does not bode well....

Future: “The Intelligent Network”

- Network “understands” clients, controls “bad” traffic.
  - Network-based application recognition
  - Deep packet inspection
  - Network admission control
  - Packet scrubbing
- Operators them define and control policy for different classes of traffic
  - Security policy
  - QoS policy

Architectural Solutions

- Can we change the Internet architecture in such a way that the low-level easy attacks become hard/impossible?
  - Tilt the balance of power towards the victim?
  - Prevent bandwidth flooding?
  - Prevent spoofing and reflection attacks?
  - Provide safe automated pushback mechanisms?
- Preserve the general-purpose nature of the Internet to allow future innovation.

Two examples.

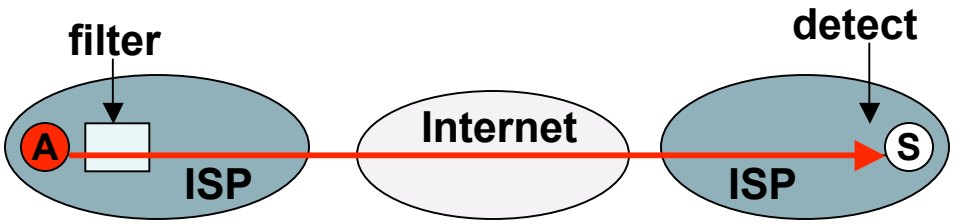
- Automated filtering framework.

  Terminus (Felipe Huici, Mark Handley)
- Improved congestion management framework

  Re-feedback, Re-ECN (Bob Briscoe)

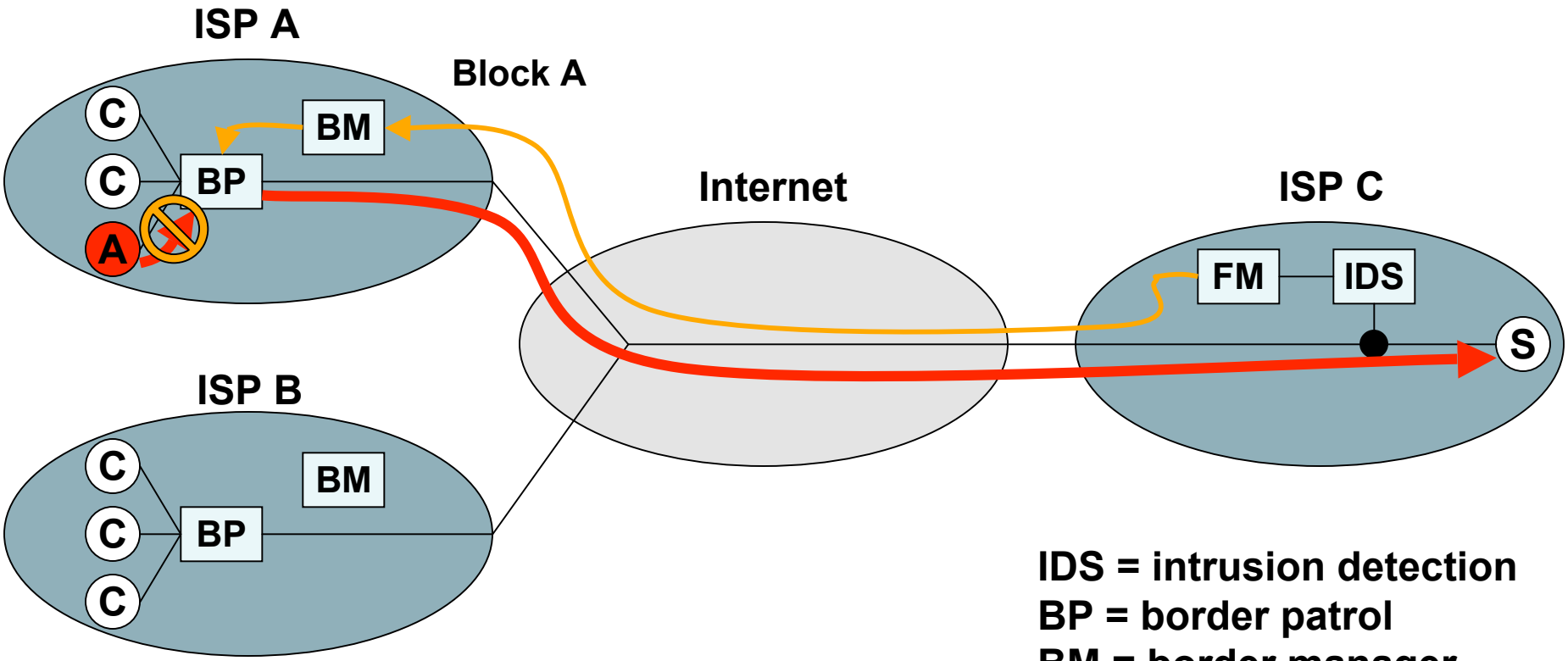
- These are intended as *examples*.
  - I know them well.
  - I think they might be deployable.
  - Others will no doubt have other solutions.

Example 1: *Terminus*



- General idea
  - Identify attack traffic at destination
  - Request that traffic be filtered
  - Block attack traffic at source ISP's filtering box
- Pretty obvious idea…
  - But how to do this robustly and with minimum mechanism?

Terminus Architecture



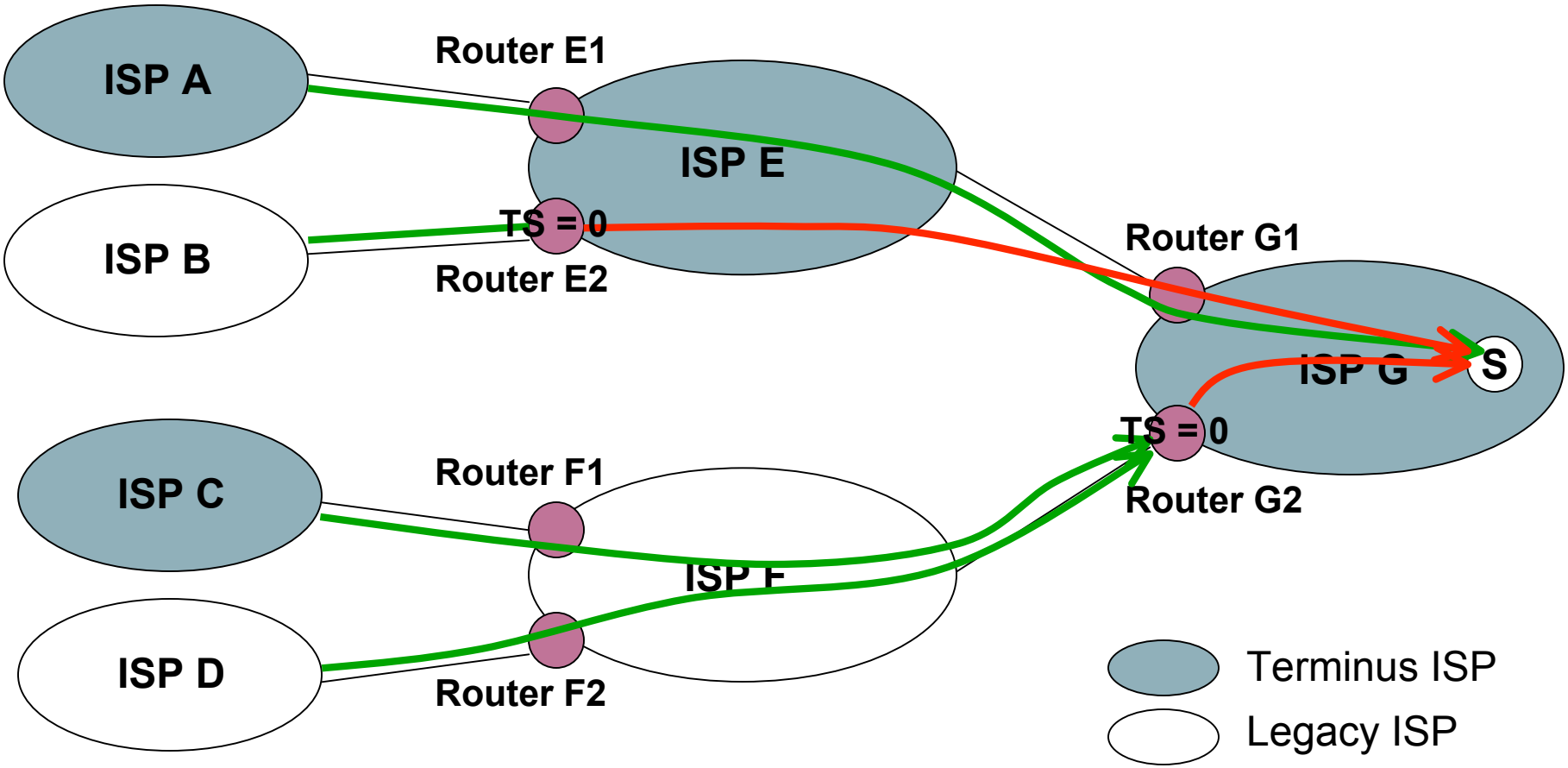
IDS = intrusion detection
BP = border patrol
BM = border manager
FM = filter manager

Preventing spoofing

- Need to know real origin of attack packets
  - Must send filter request to the right place
  - IP source address of attack traffic may be spoofed.
- Dumb idea:
  - Add a “true-source” bit to packets
  - Only Terminus ISPs with ingress filtering can set bit

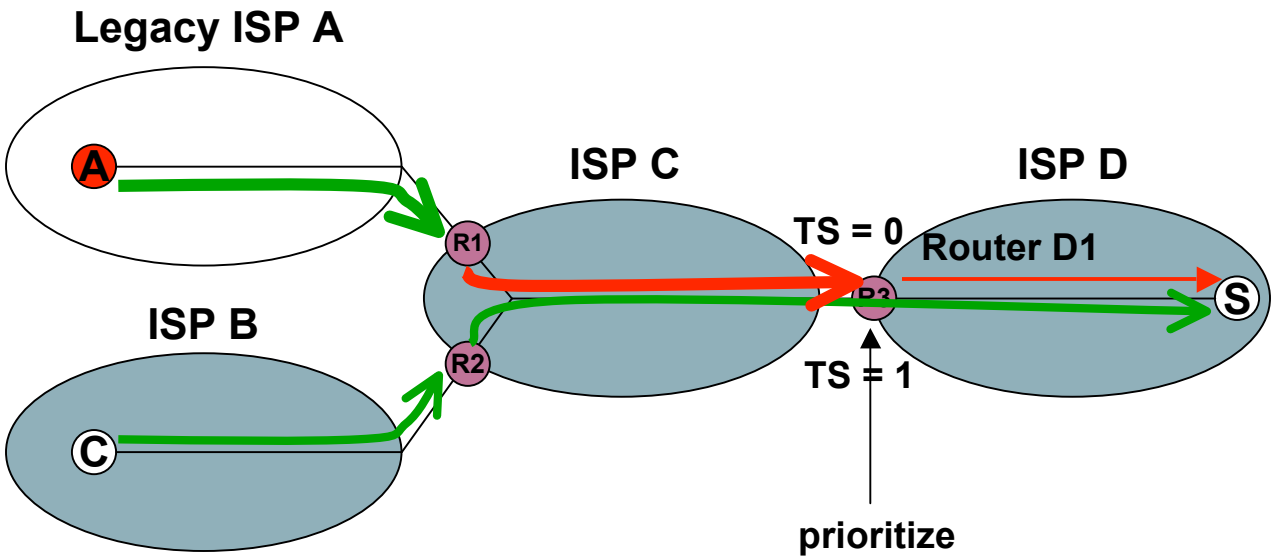
Preventing True-Source Bit Spoofing

- Edge router at Terminus ISP connected to legacy ISP unsets this bit for all packets



Incremental deployment

- During initial stages, legacy ISPs will be the norm
- Use true-source bit to prioritize traffic at the destination ISP's peering routers
  - Implement true-source "bit" as a diffserv code point



Details, details

- Lots of additional details:
  - Where to send filtering requests?
  - How to prevent spoofed traffic shutting down legit traffic?
  - How to preventing spoofed requests?
  - How to avoid reflection attacks from legacy ISPs?

Terminus: god of boundaries

- Details here:

  http://nrg.cs.ucl.ac.uk/mjh/tmp/terminus.pdf

Summary: Terminus is cheap and effective.

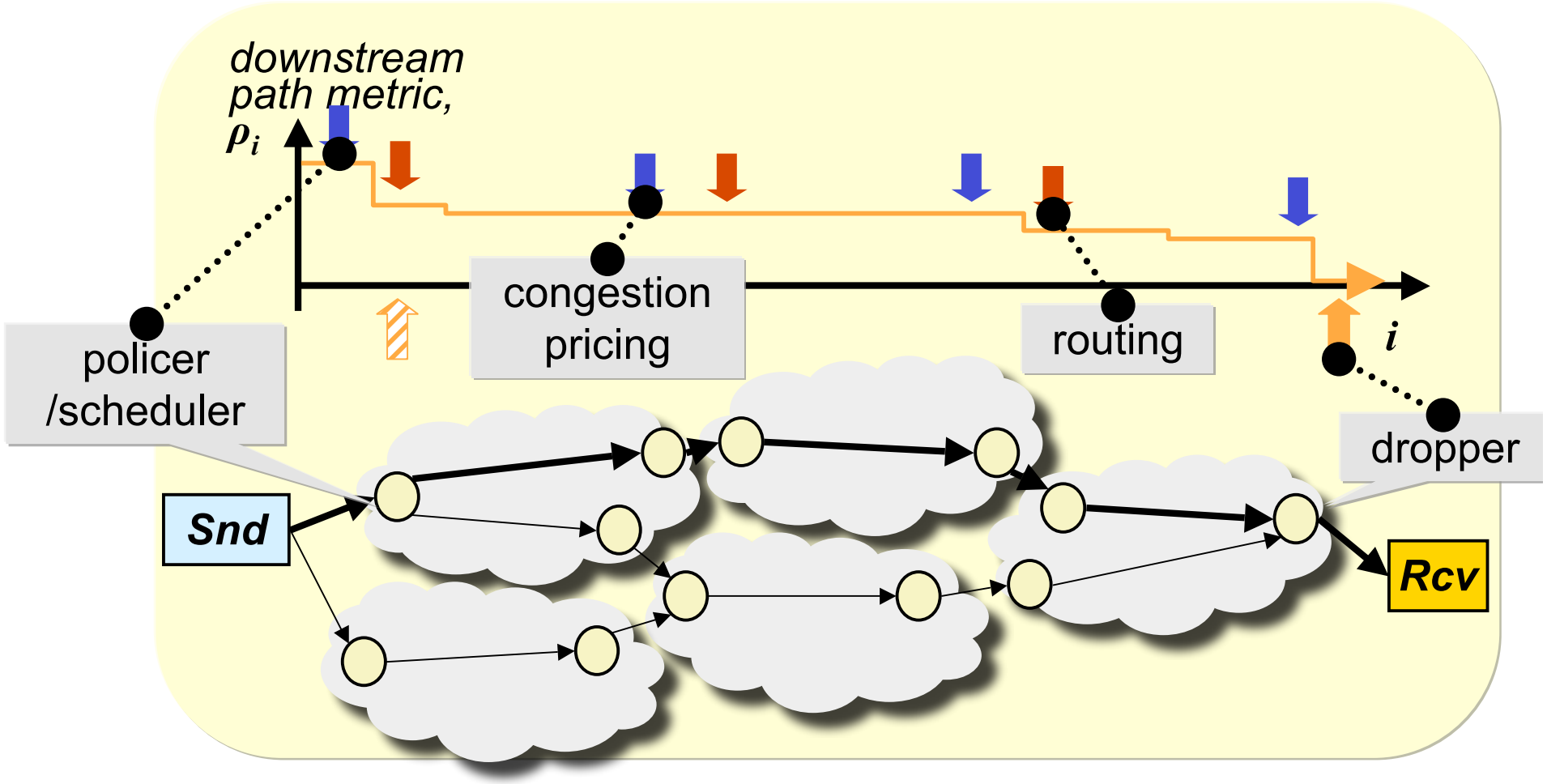
- Only needed at the edges.
  - Can do filtering at more than 1Gb/s with minimum sized packets in cheap off-the-shelf 1u rack-mount servers.
- Should really just be a standard edge-router feature
  - Most have the forwarding plane capability.
  - Just need the control protocol additions.
- Our test implementation can filter a million node botnet in a few tens of seconds.
  - Bottleneck is likely to be how fast you can identify bots.

Re-feedback (Briscoe)

General strategy:

- Tackle flooding attacks as part of a larger incentive framework.
- Routers provide explicit information about congestion levels by decrementing a congestion field in packets.
  - Feedback explicit information about downstream congestion to the data sender.
  - Data sender-reinserts this feedback information into the packets.
  - Goal is for the sender to set the field correctly so the remaining value is zero at the receiver.
- Policy at ingress and egress to provide incentive for sender to send at the correct rate for the network congestion level.

Incentive framework



Summary: re-feedback

- Long-term approach to re-architecting the congestion-control framework for the Internet.
  - Nice alignment of incentive with mechanism
  - Pushes the costs for misbehaviour towards the origin network of the malicious traffic, but provides the mechanism to throttle it.

- Incremental deployment should be possible, though longer term than Terminus.
  - See proposals on Re-ECN.
  - Re-ECN bar-BOF here (Weds, 1pm, Red Lacquer room).

Should the IETF do anything about DDoS?

- Who else will?
- *Effective* solutions requires protocol changes.
  - That's our business.
- Doing nothing:
  - Hurts everyone through deployment of changes that harm innovation.
  - Costs real money in both mitigation and workarounds.
  - Risks legislated solutions.

The enemy of the good is the perfect

- Voltaire

- We can *raise the bar* for DDoS attackers.
- There are general *technical solutions* that would help.
- Some seem *economically feasible*.
  - The only way to find out is to try.