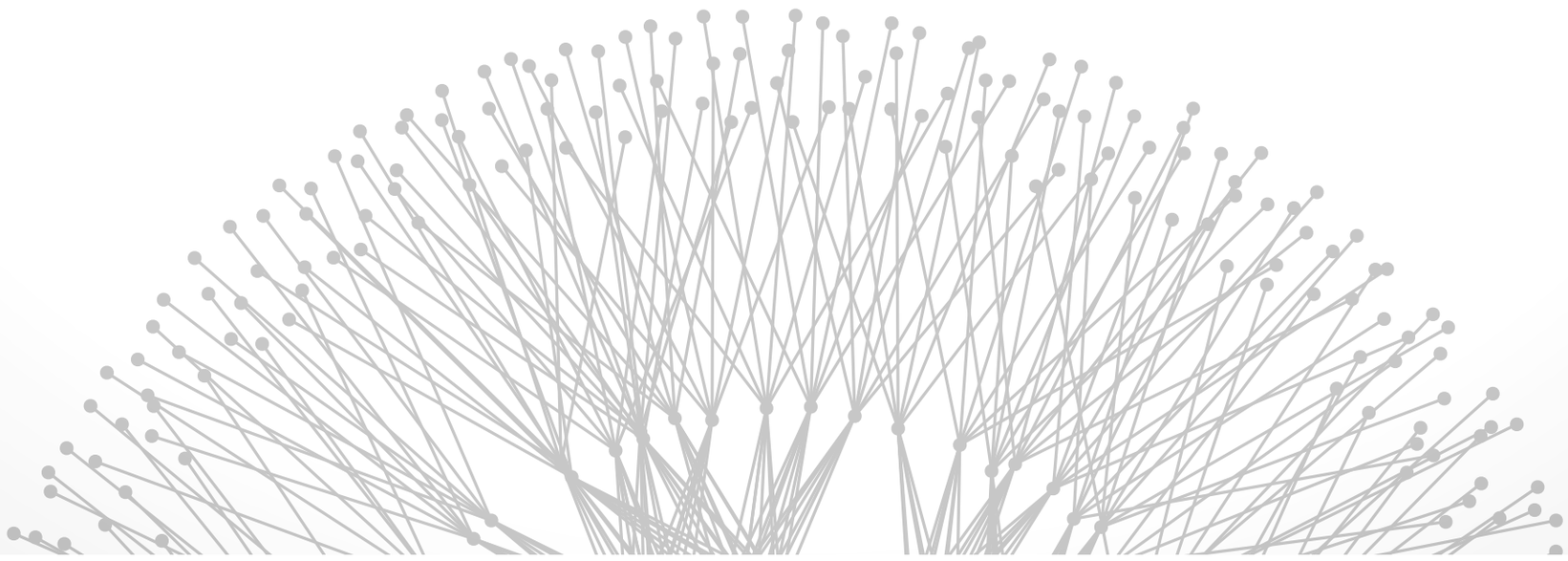
Future Internet Architectures

Brighten Godfrey

CS 538 May 1 2017



Internet Architecture challenges

Security & accountability

Privacy

Mobility

Reliability

Performance

Evolvability of the architecture itself

"Tussle" between stakeholders

Not as challenging…

- Scalability
- Content-awareness

"Tussle in Cyberspace"

[Clark, Wroclawski, Sollens, Braden, ToN'05]

Tussle: process of "contention among parties with conflicting interests"

What tussles have we studied this semester?

"Tussle in Cyberspace"


SECTIONS

The New York Times

In Europe's Election Season, Tech Vies to Fight Fake News

In France's Poor Suburbs, Angry Voters May Skip Big Election

WATCH HERE

Exiled Iranian TV Executive Is Assassinated in Istanbul

EUROPE

Turkey Purges 4,000 More Officials, and Blocks Wikipedia

By PATRICK KINGSLEY APRIL 30, 2017

What tussles have we studied?

- Content access: countries & ISPs censor & block for security; users circumvent with Tor
- Congestion: selfish user behavior; ISPs block apps; etc.
- Routing policy: conflicting preferences cause divergence
- ...

Key point: Design of protocols shapes how tussles play out in the running system

Example 1:
Naming & Addressing

Naming & addressing

Originally "just" technical problems...

- Address: indicates location, convenient for routing
- Name: location-independent, convenient for human

...all wrapped up in tussle

- Names tied to trademarks
- Addresses difficult to change (and now scarce for IPv4!)

How would you fix this?

Modularize to protect the system

Principle: Modularize along tussle boundaries

- Separate task of location independent identification of endpoints (hosts/services) from tussle spaces

Possible implementation: flat names

- Endpoint identifier (EID): Just a bag of bits
- Human-readable name maps to location-indep. EID
- Location-independent EID maps to address

Or, can we route directly on flat names?

- VRR, ROFL [Caesar et al, SIGCOMM'06]
- Disco [Singla et al, CoNEXT'10]

Example 2:
Control of routes

Choice in routing

Current Internet: routes fixed within the network

- Each router makes part of the route choice
- Picks one route per destination & advertises that one

Technical problems

- Single offered path may be broken, congested, insecure
- Decision-makers (in the network) lack end-to-end path quality measurements

Tussle problems

- Parties disagree on what is a "good" path
- Lack of choice discourages competition

Choice in routing

Architecture exacerbates tussle: no way to enable choice even if involved parties want it

- In IP, typically just get to specify destination
- No infrastructure for exposing extant choices

One solution: separate routing from the network by letting sender specify a route in packet

- Switch quickly in response to end-to-end failures
- Use multiple routes simultaneously
- Better load balance, more efficient use of capacity
- Competition among providers

Pathlet routing

[Godfrey, Ganichev, Shenker Stoica, SIGCOMM '09]

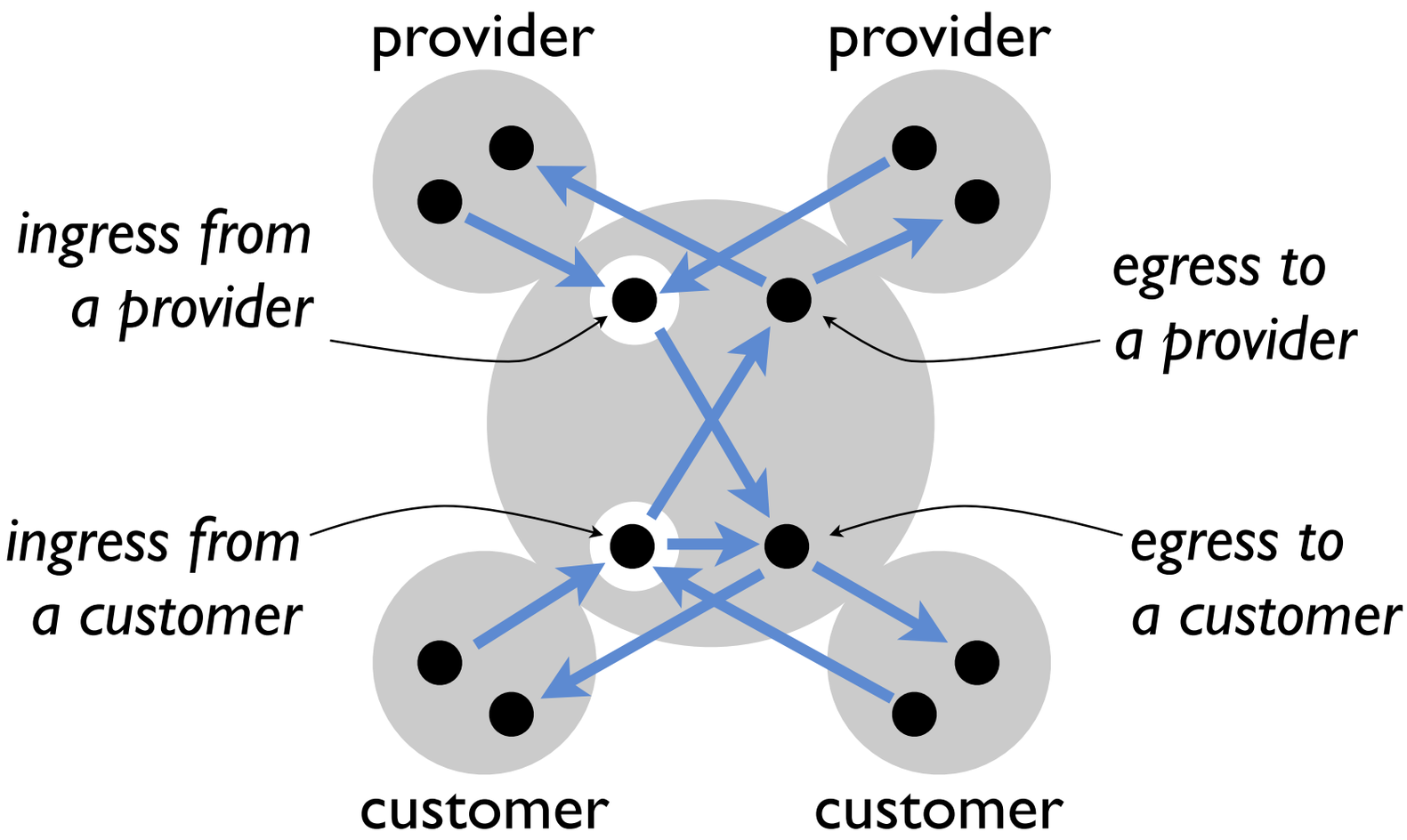
Idea: separate route computation from the network

Refined idea: route in a virtual topology which can flexibly represent policy constraints

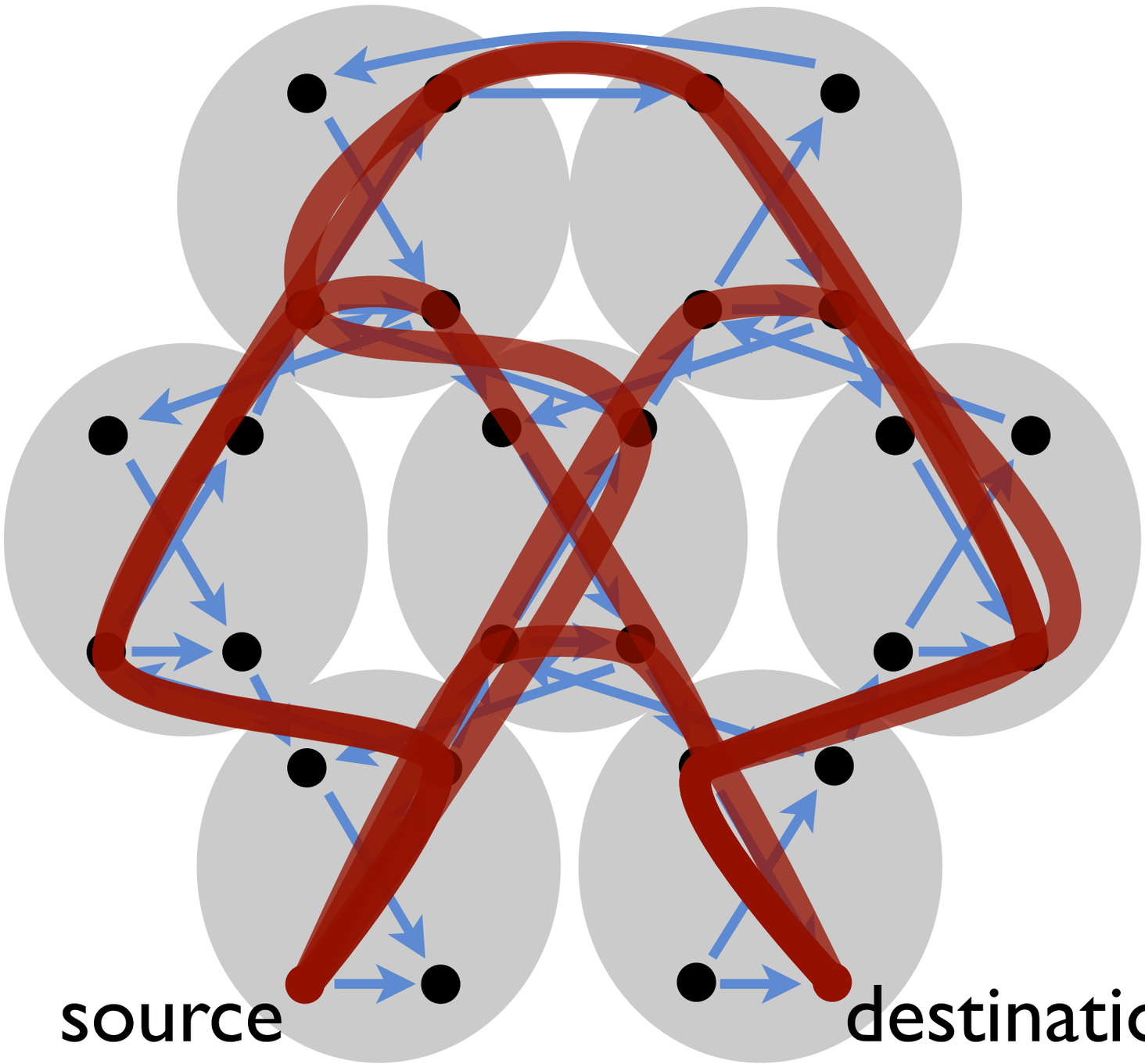
- For network owners: flexibility to define how the network can be used, via what virtual links (pathlets) are advertised
- For users: flexibility to choose paths or services defined by any concatenated sequence of advertised pathlets

Pathlet routing example

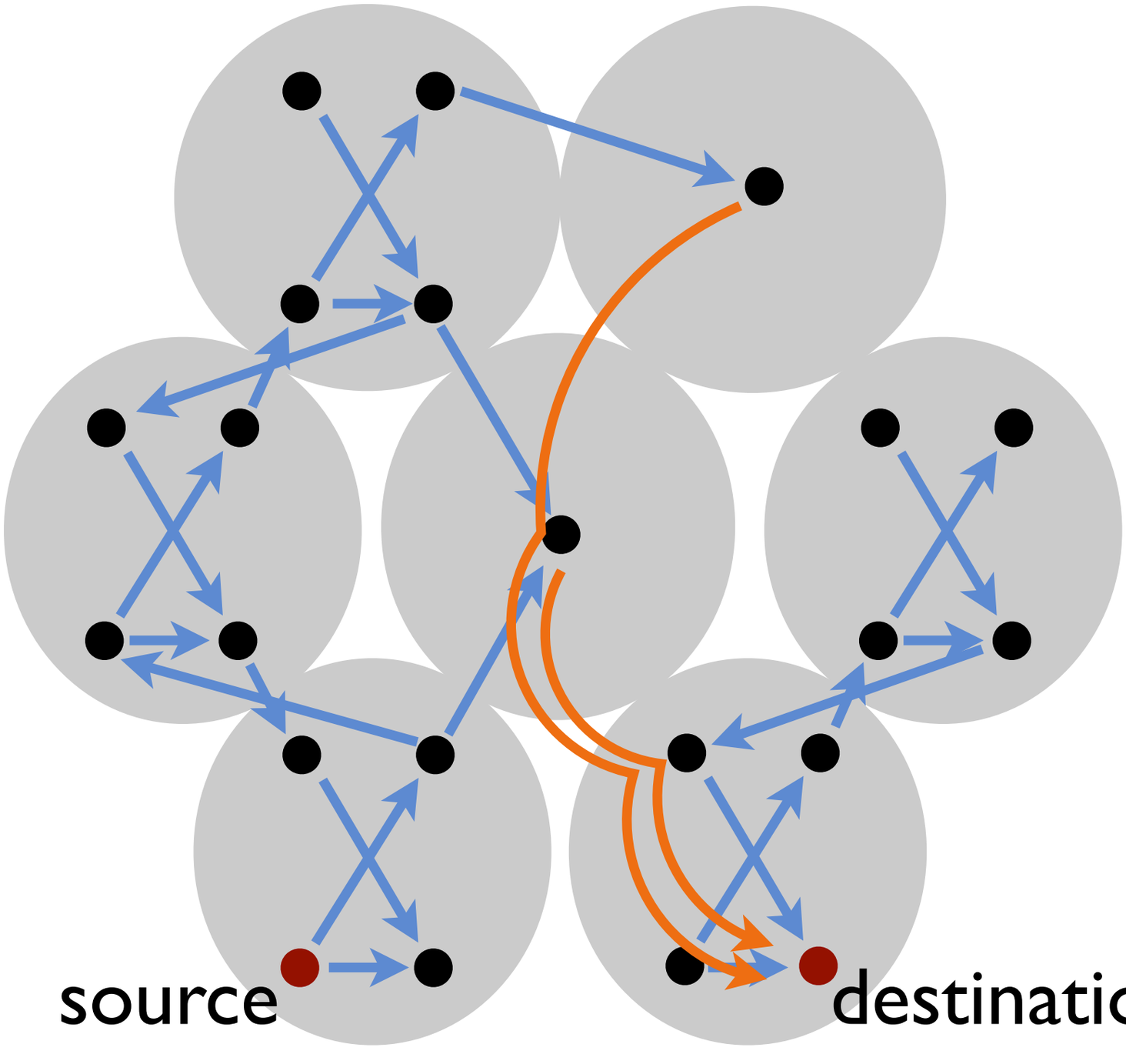
e.g., all valley free routes
("customers can go anywhere;
anyone can route to customer")



Pathlet routing example



Pathlet routing example 2



Design for variation

> *Design for variation in outcome*, *so that the outcome can be different in different places, and the tussle takes place within the design, not by distorting or violating it.*

— Clark, Wroclawski, Sollins & Braden

Balancing Accountability and Privacy in the Network

[Naylor, Mukerjee, Steenkiste, SIGCOMM 2014]

Terms & concepts

Egress filtering

- Drops packets that do not pass security check as they try to exit the network
- e.g. "source address should always be in one of this network's IP prefixes"

Unicast reverse path forwarding (uRPF)

- Strict: router accepts packets only on interface it would send a reply
- Loose: router accepts packets only when source address exists in routing table

Terms & concepts

Self-certifying identifier

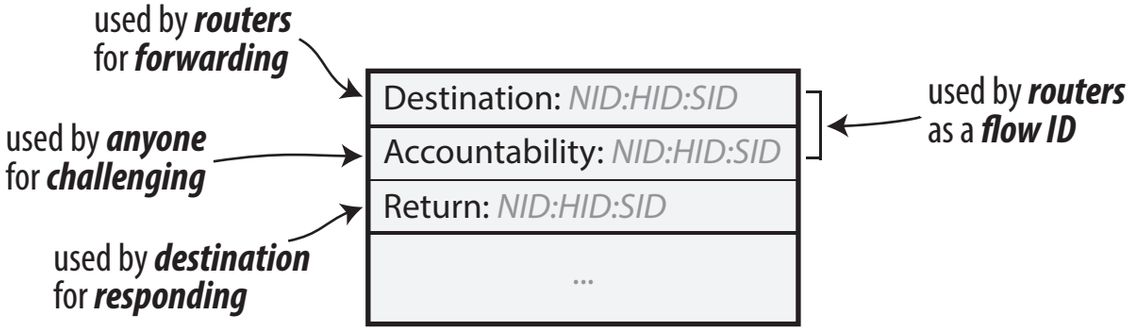
- Principal's identifier is its public key (or hash thereof)
- No need for trusted authority to prove ownership of ID

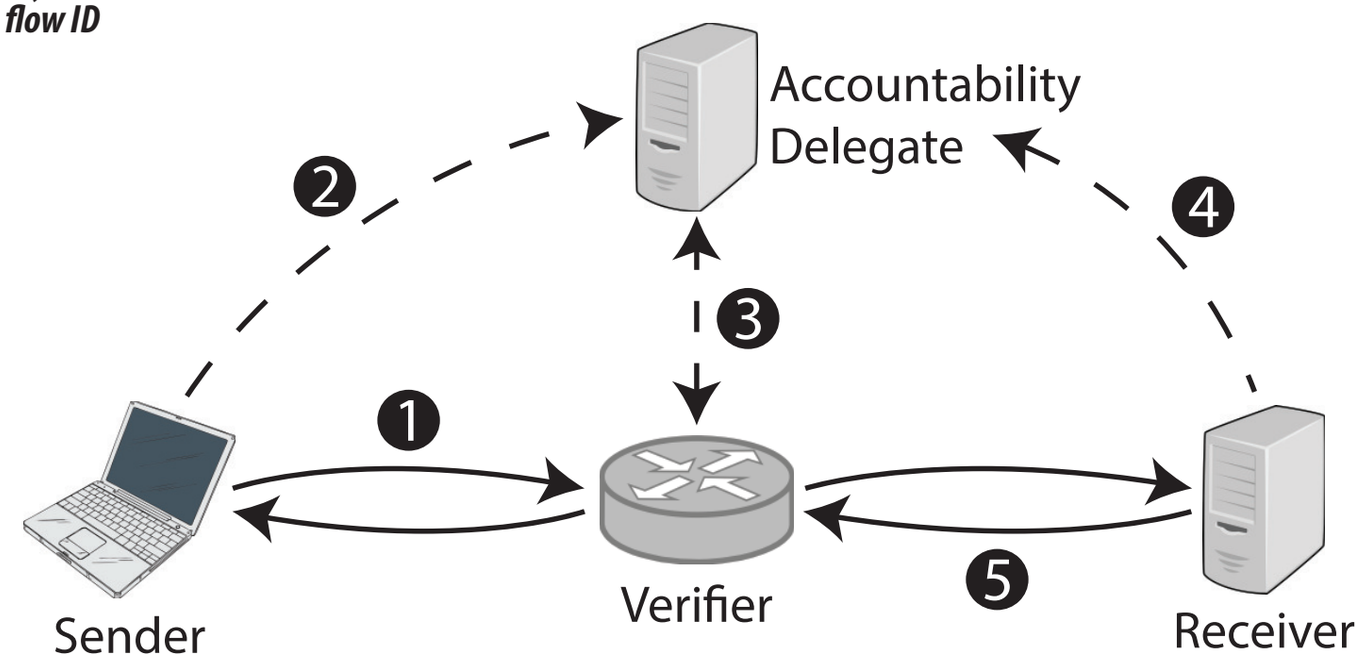
- Another interesting example
  - ID = address or hash of address
  - Used by some distributed hash tables
  - Why is this self-certifying?

Key points in paper

Decouple accountability and return addresses

- Source address has at least 5 different roles today!
- Might not need return address in every packet!





[Figures from Naylor et al.]

Discussion

Who do you pick as your accountability delegate? Your ISP?

- + No need to send briefs
- + Already have a relationship with them
- – Implicitly reveals information about your location

Brief-flooding: why would a host flood its own delegate?

Discussion

In AIP [Anderson et al, SIGCOMM'08], receivers could send shutoff requests directly to attackers (handled by NIC).

- Sound crazy? Could it work?

Announcements

Final lecture Wednesday

- Discuss project presentation format & requirements
- Course wrap-up
- ICES survey

Final Project Presentations

- Tue May 9, 11am - 2:00 pm
- 3403 SC