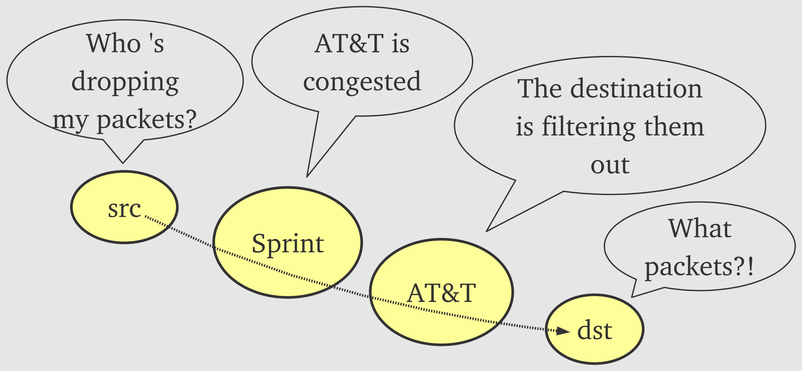
An Accountability Interface for the Internet

Olga Irzak and **Ashish Subramanian** (EPFL) with **Katerina Argyraki**, **Petros Maniatis** and **Scott Shenker** (EPFL) (Intel Research) (UC Berkeley)

1. End-system view of Internet failure



▸ ***Can't determine who is accountable for losing/delaying its packets***

- Cannot adapt to failure
- Cannot evaluate ISP performance

▸ ***Without accountability, no competition, innovation in the Internet*** [Laskowski06]

2. State-of-the-art approach: probing

- Traceroute, network tomography, ...
- Reveal fate of probes, not actual data
- ISPs can treat probes preferentially

▸ ***Less than end systems want to know***

- Can reveal ISP internal structure, policy
- Expose security vulnerabilities

▸ ***More than ISPs want to reveal***

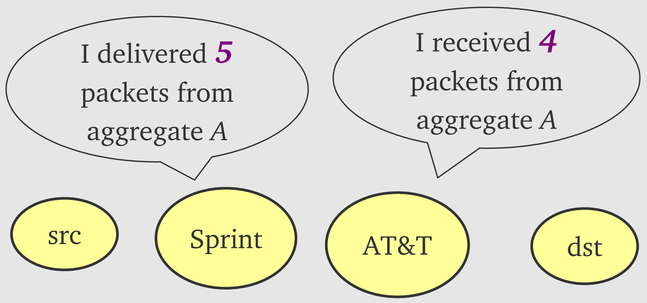
3. Our approach: ISP feedback

- For each traffic aggregate, ISP records:
  - how many packets entered/exited
  - average entry/exit time
  - previous and next ISP
- ISP periodically sends collected statistics to the corresponding source networks

▸ ***End systems learn the loss/average delay incurred by their traffic within each ISP***

▸ ***No prying into ISP internals***

4. What about lying ISPs?



- Lying = blaming failure on peering ISP
- Implicated ISPs produce conflicting feedback

▸ ***Each lie leads to a feedback inconsistency***

- Src notifies the ISPs of their inconsistency

▸ ***Lying ISP is exposed to the peer it implicated***

5. Overhead evaluation

- Implementation for TCP flows
- Bandwidth overhead < 2%
  - assuming avg 5K bytes/flow
  - 4 reporting ISPs per path
- 1 GB of short-term state
  - enough for millions of flows
- 150 GB of long-term state
  - enough to keep 5-hour history
  - assuming 1 trillion flows/hour

6. Summary

▸ ***Accountability interface***
- ISPs report on their own performance

▸ ***Resistant to lying***
- lies manifest as feedback inconsistencies

▸ ***Reasonable bandwidth overhead***
- small % of forwarded traffic

7. Coming up + future work

- Click-based prototype
- Enhanced threat model
  - e.g., malicious feedback modification
- Different aggregate types
  - UDP flows, sampled flows