Low-Latency Dissent

Daniel Jackowitz, Eleanor Cawthon*, David Isaac Wolinsky, Lining Wang, Bryan Ford
Yale University *Pomona College

Motivation

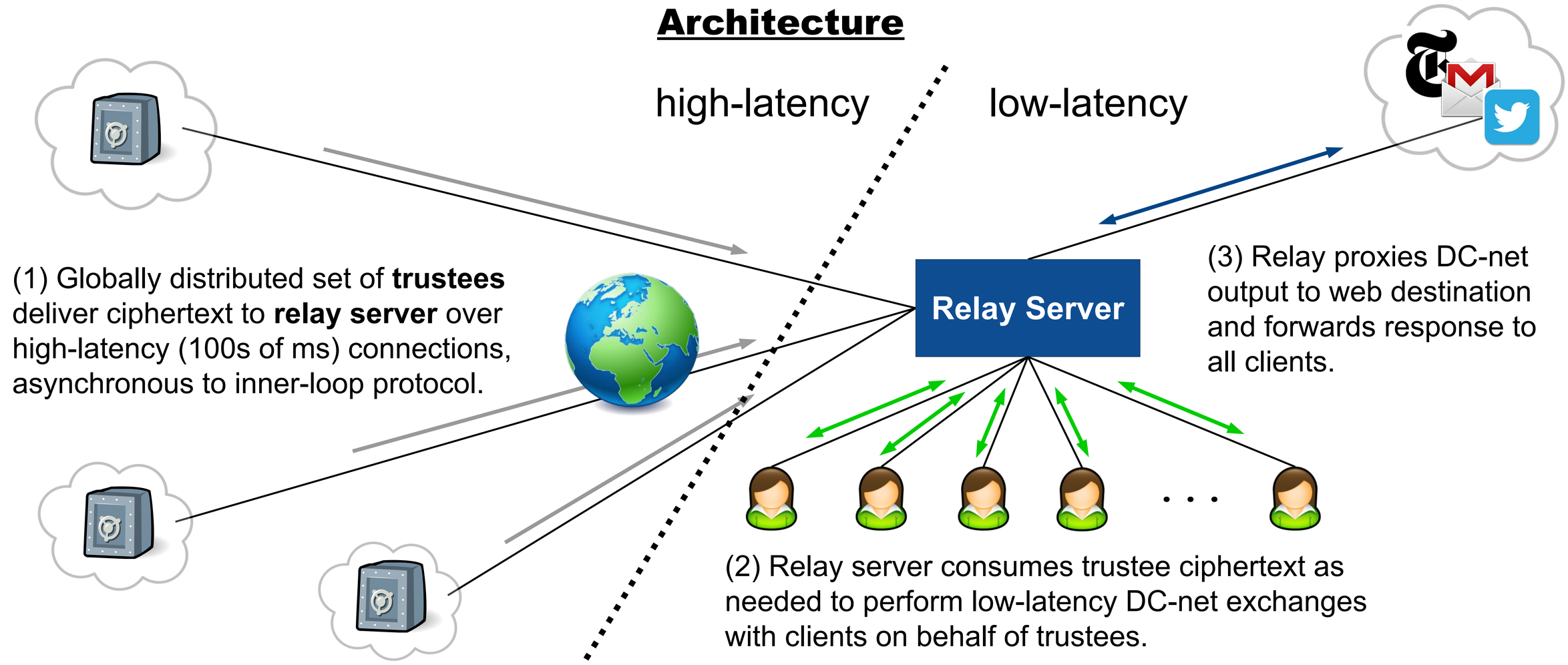
Anonymous communication systems often place low-latencies at odds with trust distribution

- Geographically and administratively diverse entities more robust against collusion and compromise
- System limited by slowest path

Our Goals

➔ **One-hop proxy latencies**
➔ **Strong anonymity guarantees**
➔ **Internet-scale trust distribution**

Architecture



Why this is hard... (Technical Challenges)

1) Trustees must agree on set of online clients
   ➔Trustee-to-trustee communication (high latency)
2) Trustees must enforce accountability
   ➔Trustee-to-trustee communication (high latency)
3) Clients must certify consistent output before proceeding
   ➔Extra client-to-relay round-trip

...and how we do it

1) Trustees update client set at regularly occurring configuration events. In typical case, can pipeline production of configurations.

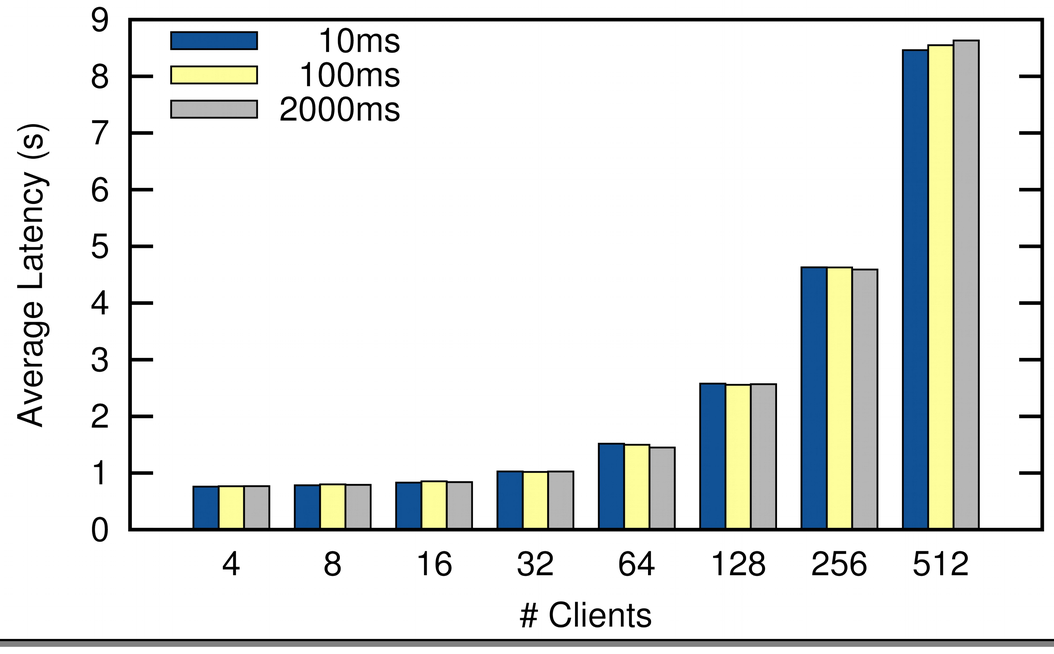
2) Trustees use signed message transcripts from relay to identify disruptors outside of main protocol loop.

3) Clients proceed immediately, encrypting next round's ciphertext as a function of prior rounds' output; inconsistent encryptions yield indecipherable cleartext.

(Non-)Effects of Trustee Distribution

Relay as SOCKS5 proxy, 128KB HTTP GET

Varied trustee-to-relay delay



Background: DC-nets