UNIVERSITY of CALIFORNIA • IRVINE

ANDāNA

Anonymous Named Data Networking Application

Steve DiBenedetto[1], Paolo Gasti[2]
Gene Tsudik[2], Ersin Uzun[3]

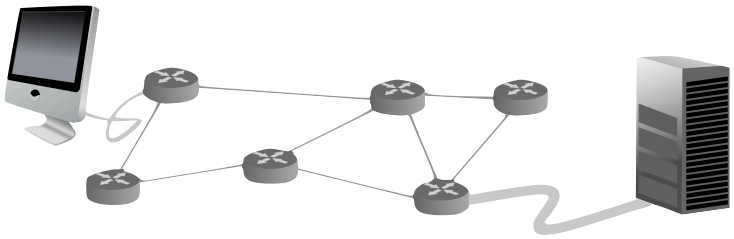
[1]Colorado State University
[2]University of California, Irvine
[3]Palo Alto Research Center

Agenda

- NDN Overview
- Privacy in NDN
- ANDāNA
  - Design
  - Security
  - Performance and comparison with Tor

1876

- IP enables any host to talk to any other host
  - It names "boxes"
  - End-to-end communication
  - Datagram delivery

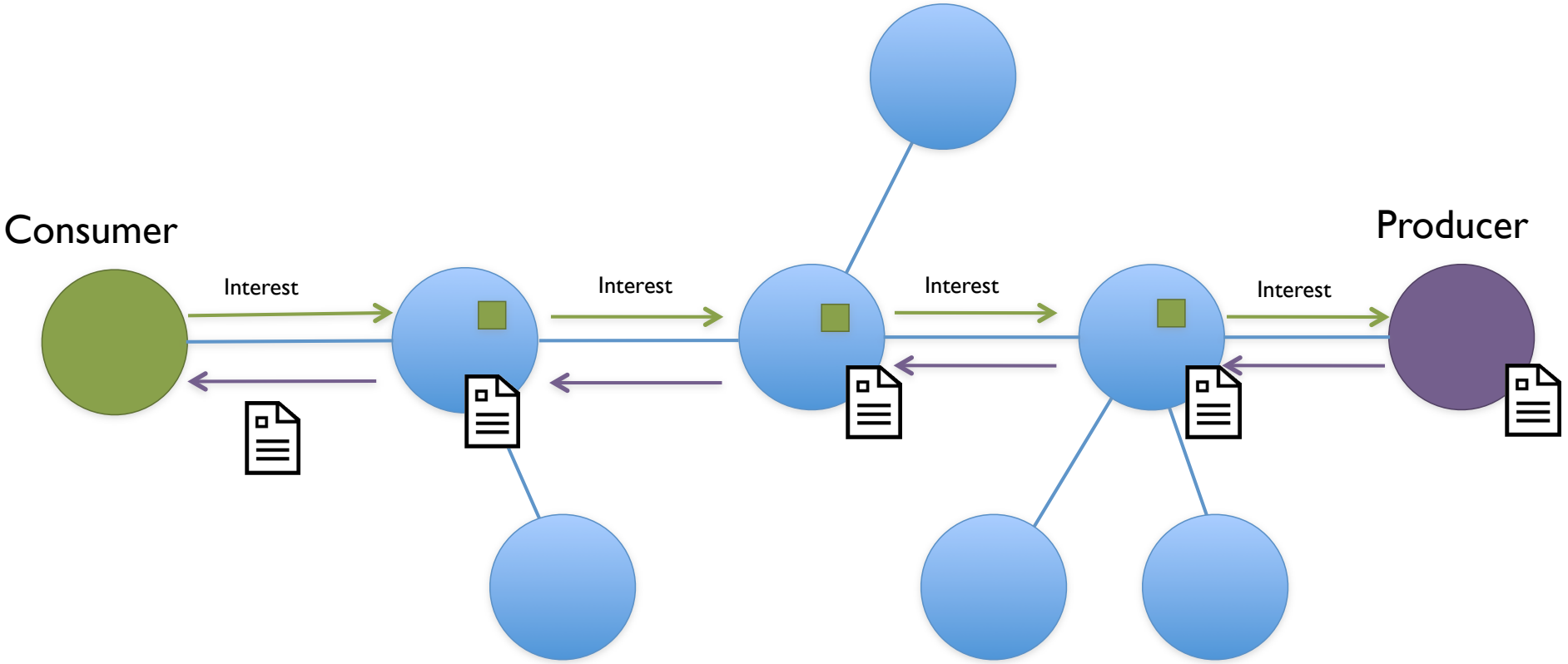


1977-2012

Content-centric Networking

Name "boxes"	→	Name content
Communication	→	Content distribution
Emulate wire	→	Retrieve content
Mobility difficult	→	Mobility easy
Secure process	→	Secure content
Memory invisible	→	Memory explicit

NDN Overview



NDN

- Closely spaced interests can be aggregated
- Content can be retrieved from caches
- All content objects are signed

NDN: Privacy Challenges

- Name privacy
  - /wikipedia/STDs
- Content privacy
  - Retrieved content is mp3 file
- Cache privacy
  - Detectable hit/miss
- Signature privacy
  - Leaked publisher identity

NDN: Privacy benefit

- Interests lack "source address"
  - Data can be routed back without knowing consumer identity/position
- One interest may correspond to multiple consumers
- Caches reduce effectiveness of observers close to producers

ANDāNA

- Onion routing architecture
  - Any router/host can be an *anonymizing router*
- "Ephemeral" circuits
  - Only carry one or a few data packets

ANDāNA Goals

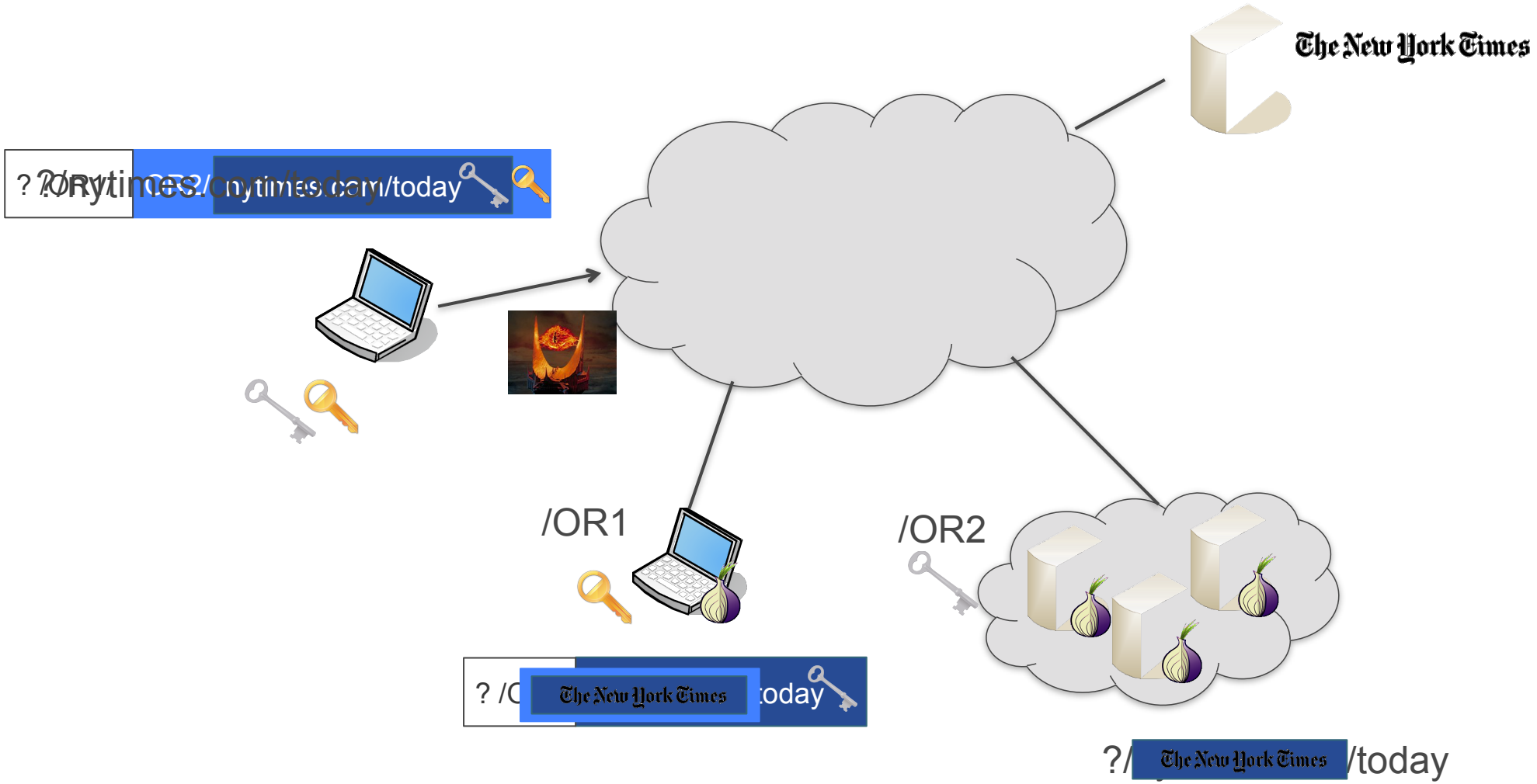
- Small/medium-size, interactive communication
  - Web browsing, IM, VoIP, etc.
- "Beyond suspicion" degree of anonymity
- Realistic (non-global) adversary
- Producers may not be aware of ANDāNA (or willing to collaborate)

ANDāNA Design

- Circuits are composed of two routers
  - Entry router
  - Exit router
- Security comparable with Tor (with three routers)

Why Two Routers?

- NDN itself provides limited anonymity
  - Lack of source address in interests
  - Anonymizing routers do not learn origin of traffic


The New York Times
/OR1
/OR2
/today

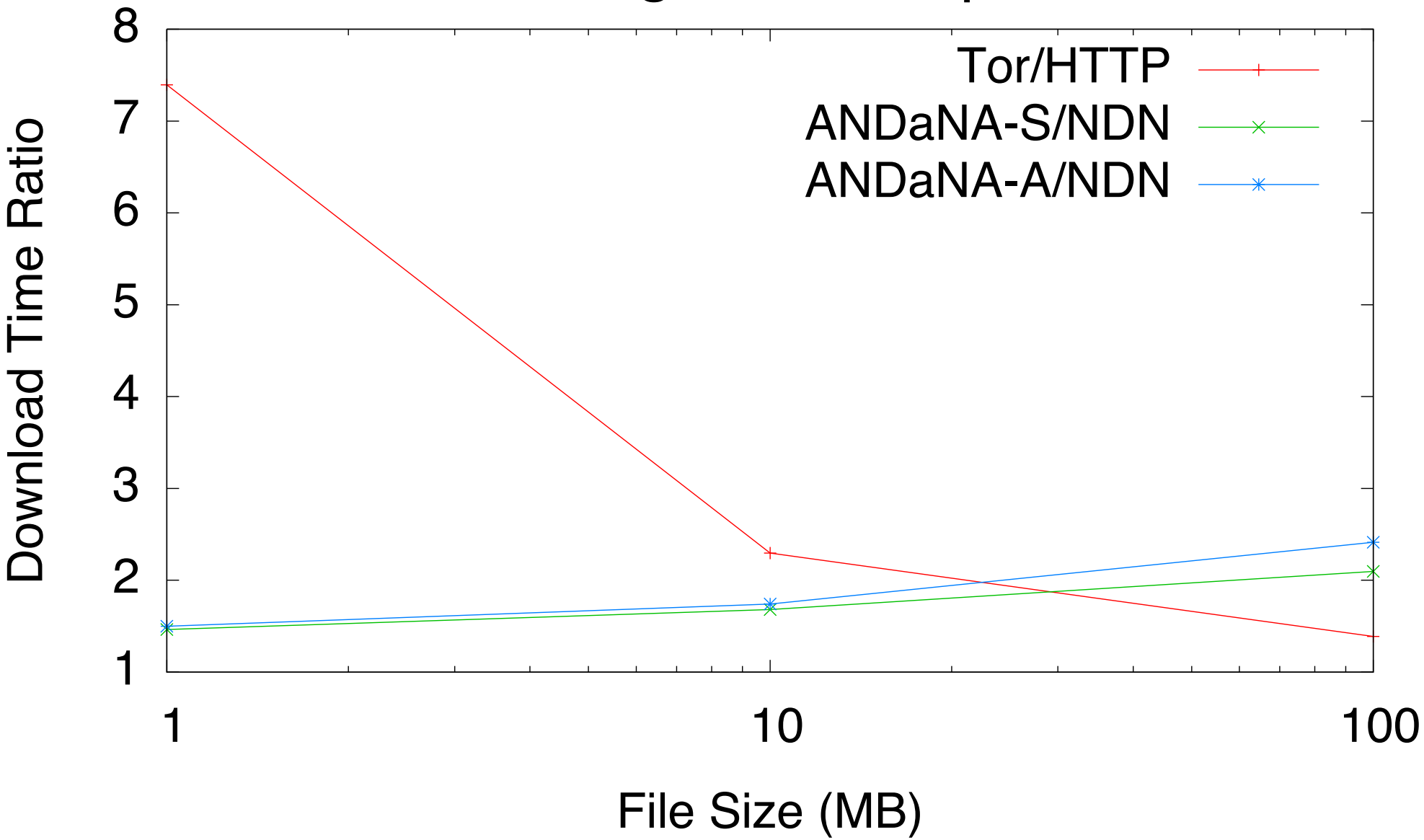
ANDāNA Design

- Asymmetric
  - One ephemeral circuit per content object
  - No circuit setup required
- Session-based
  - Lower cryptographic overhead
  - Cheaper circuit setup compared to Tor
  - Multiple packets use same ephemeral circuit

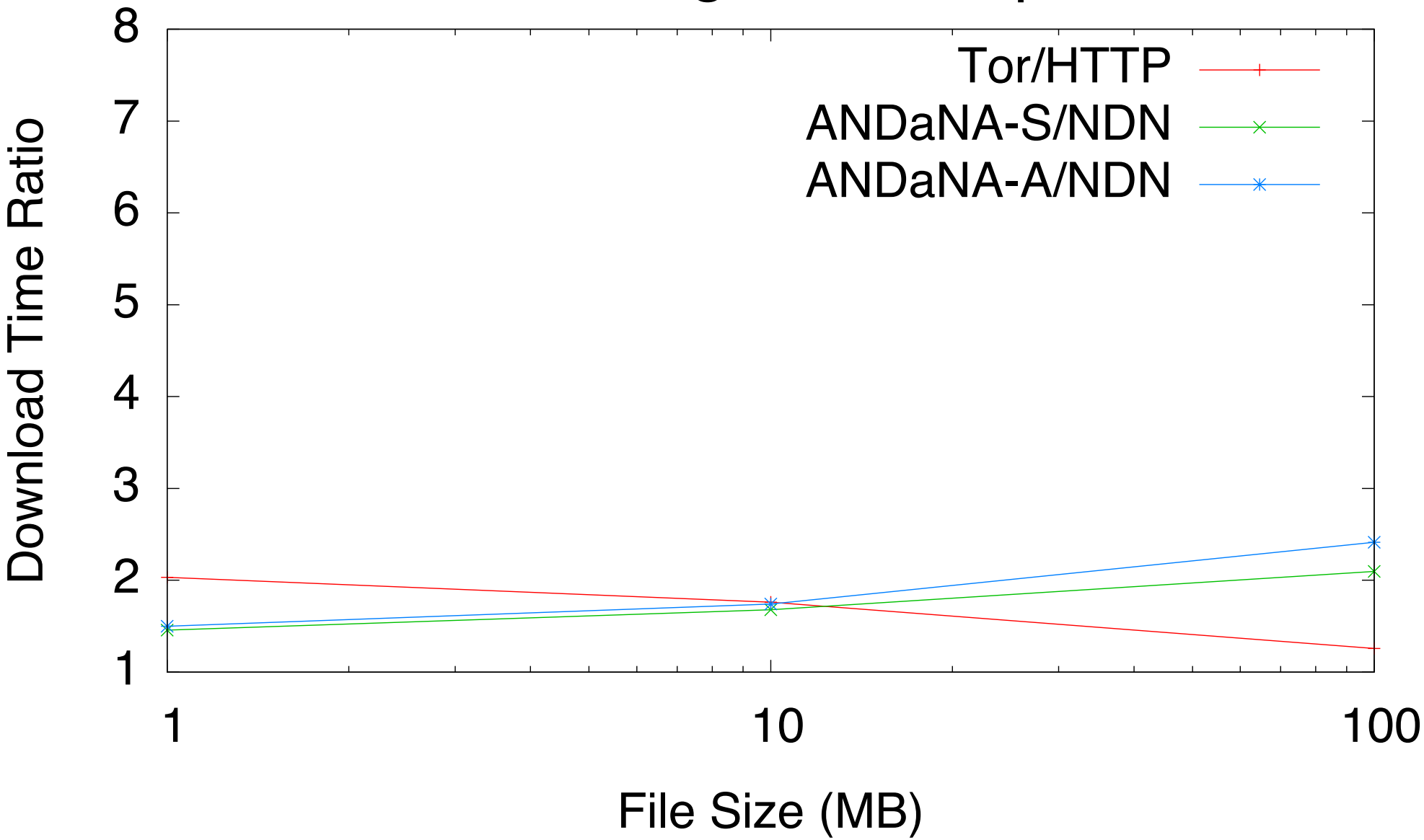
Performance

- WUSTL's Open Network Laboratory (ONL)
- Compared against Tor with same privacy
  - ANDāNA vs. NDN
  - Tor + HTTP vs. plain HTTP

Including circuit setup



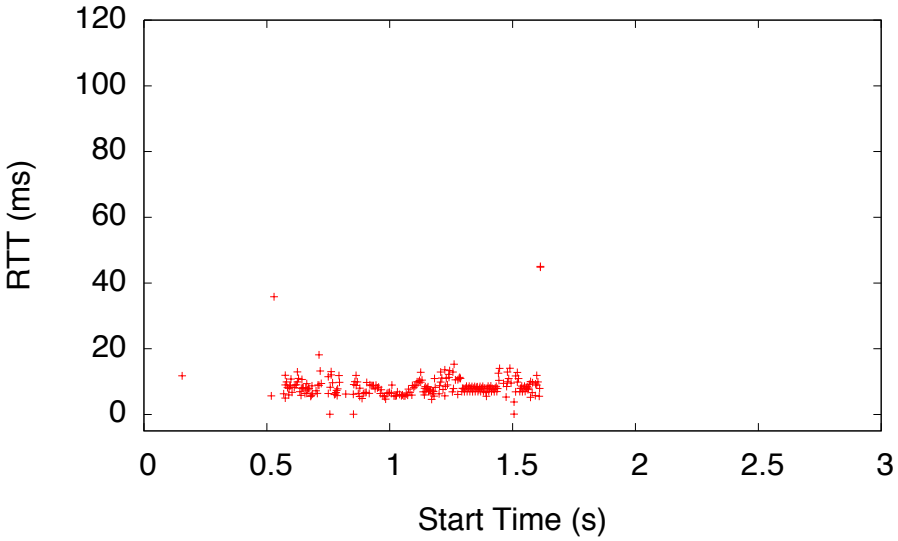
Not including circuit setup

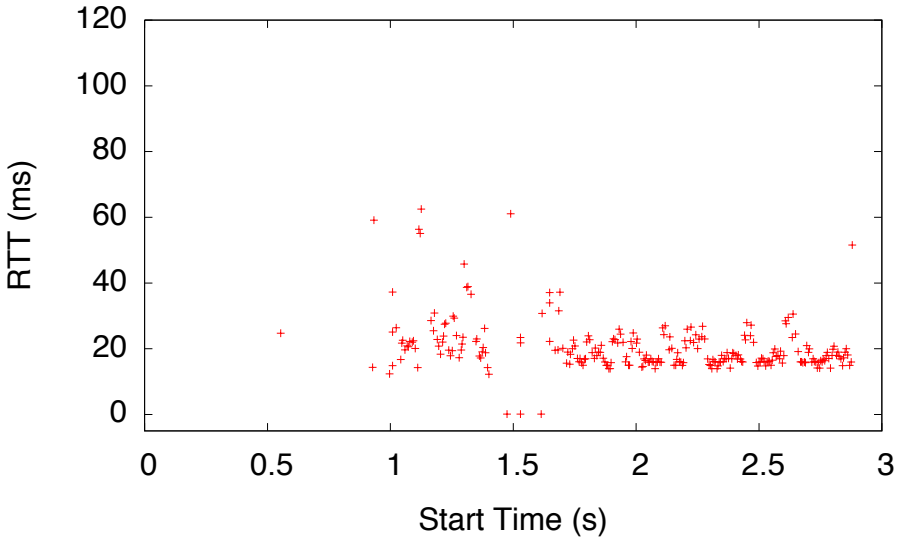


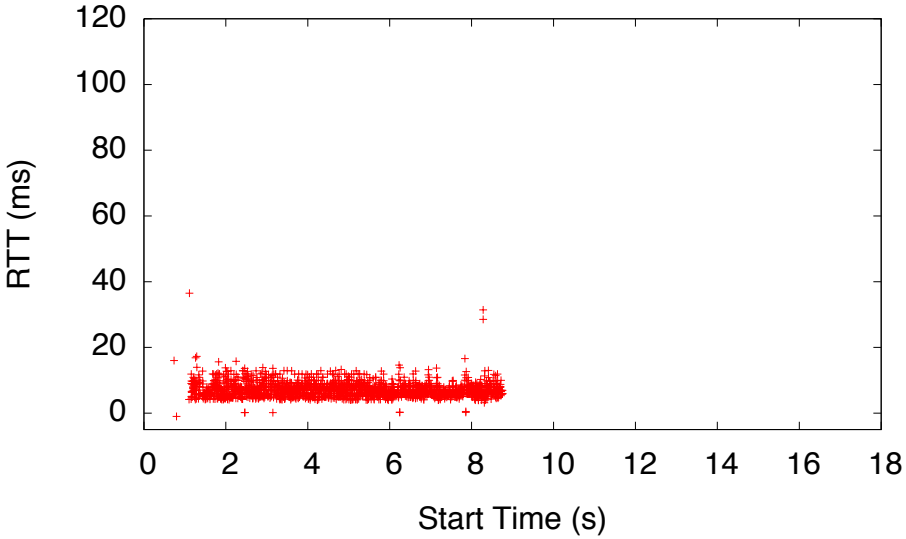
Conclusion

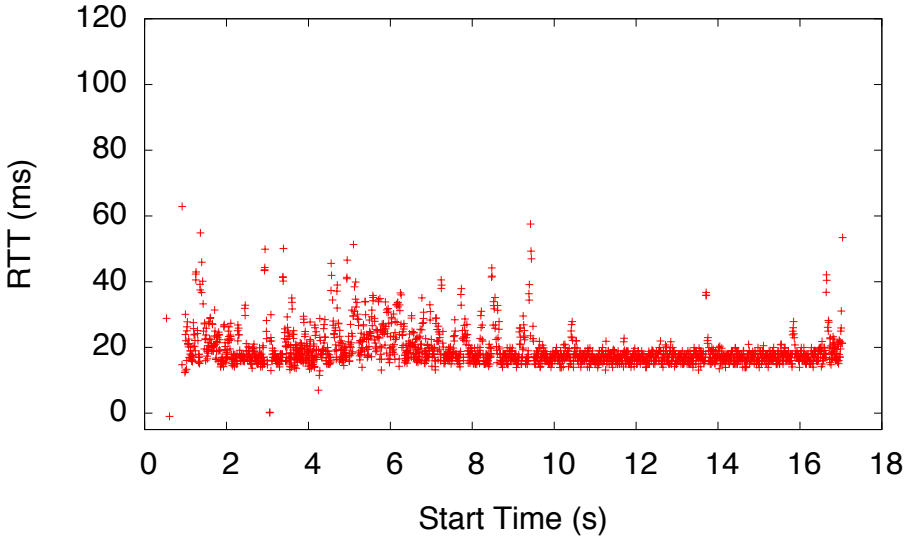
- NDN introduces interesting privacy challenges
- ANDāNA: initial attempt to provide strong anonymity
- Two routers are equivalent to Tor's three
- Performance overhead lower than Tor for small content

- Questions?


RTT (ms)
Start Time (s)
0
20
40
60
80
100
120
0
0.5
1
1.5
2
2.5
3


RTT (ms)
Start Time (s)
0
20
40
60
80
100
120
0
0.5
1
1.5
2
2.5
3


RTT (ms)
Start Time (s)
0
20
40
60
80
100
120
0
2
4
6
8
10
12
14
16
18


RTT (ms)
Start Time (s)
0
20
40
60
80
100
120
0
2
4
6
8
10
12
14
16
18