# Enabling Practical Traffic Analysis Resistance

PI: David Choffnes, Northeastern University

https://anonymity.ccs.neu.edu

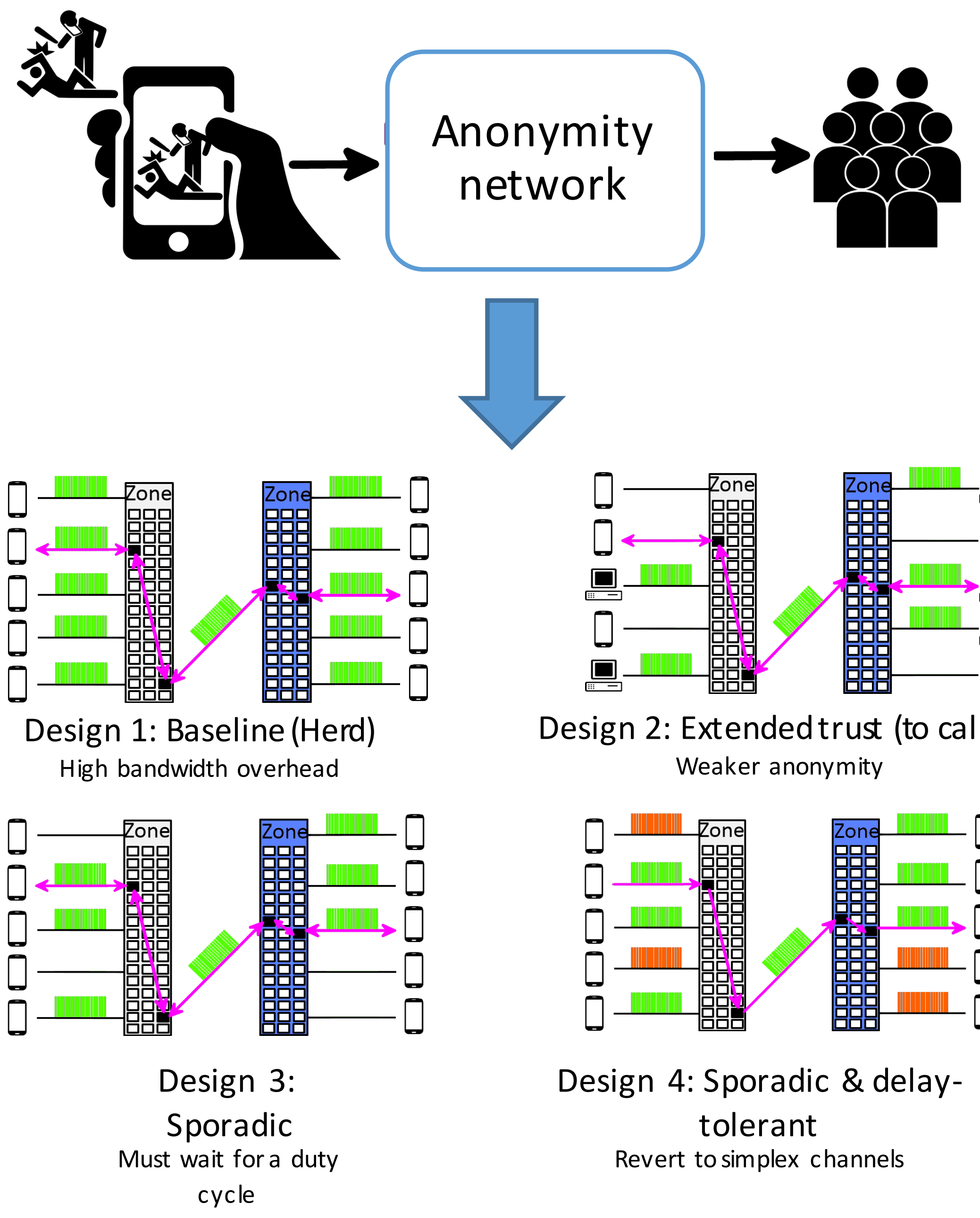
## Strong anonymity despite state-level adversaries

**Our goal** is to provide **high-performance, strongly anonymous communication** over fixed line and mobile networks---even in the face of today's powerful adversaries

### Motivation

Existing anonymity networks face several **shortcomings** that make them **impractical**

- Vulnerable to traffic analysis
- Offer unsuitable (medium/high) latency
- Do not address mobile platforms


Anonymity network
Zone
Design 1: Baseline (Herd)
High bandwidth overhead
Design 2: Extended trust (to callee)
Weaker anonymity
Design 3: Sporadic
Must wait for a duty cycle
Design 4: Sporadic & delay-tolerant
Revert to simplex channels

### Key Challenges

- Resilience to traffic analysis
- Low latency (for VoIP/video)
- Scalability to millions of users

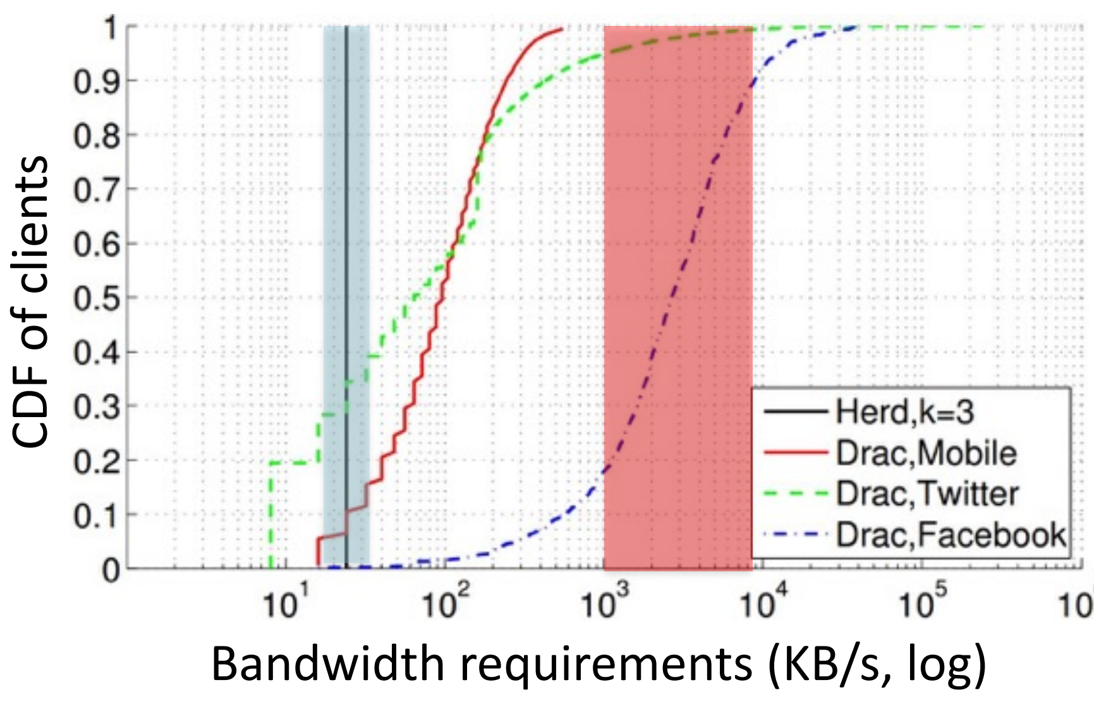
is essential for wide adoption

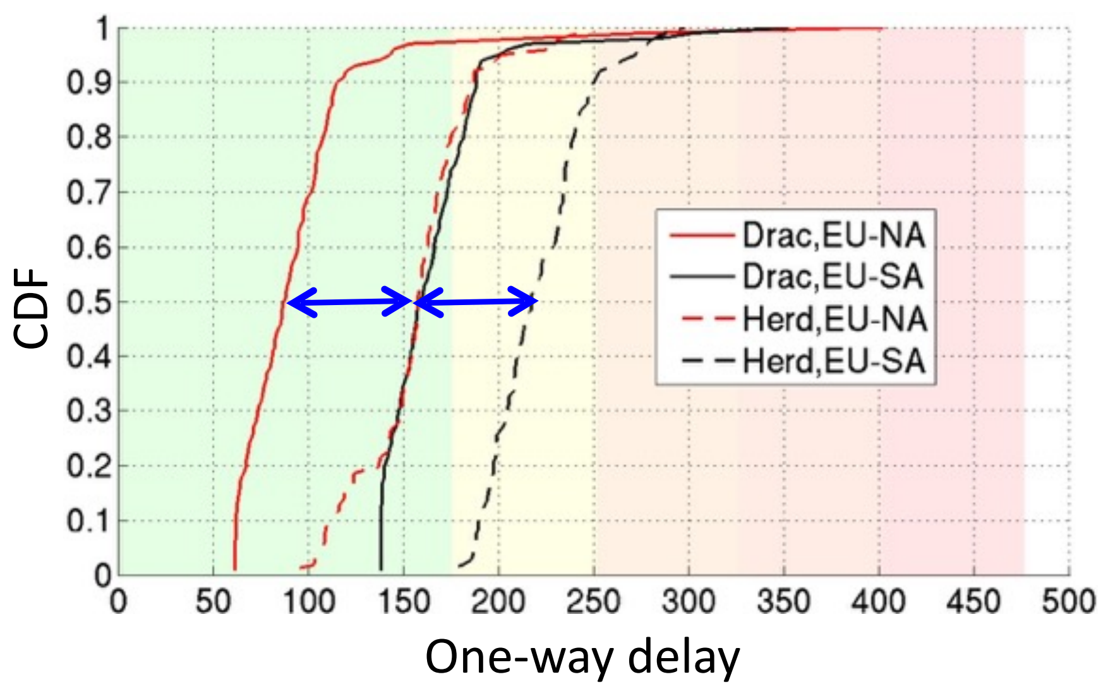
### Approach

- Trust zones: a set of data centers in a jurisdiction
  - Client's anonymity depends on their choice of trust zone only
  - No single adversary has access to all parts of the Internet
  - There is likely a jurisdiction that is friendly or indifferent
- Low latency due to fully connected zone mixes
- Traffic-analysis resistance from continuous chaff at rate proportional to VoIP

### Herd: Support for fixed-line clients

- Large anonymity sets
- Scalable bandwidth
- Low latency (50-100ms)
- Reasonable cost per user





### Transitioning to Mobile

- Variable last-mile latency (cell tower or WiFi AP)
- Limited or costly traffic volume on mobile network
- Limited energy available & high energy consumption on 3G
- Impact of mobility across networks (3G/LTE/WiFi)
- Good cross-platform implementation (Android & iOS) is necessary for wide adoption

### Future challenges

- Enable anonymous, group communications
- Compose designs to federate applications with different requirements
- Enhance private VoIP/messaging applications (e.g., Signal) with anonymity
- Prevent abuse of bandwidth and storage

National Science Foundation
WHERE DISCOVERIES BEGIN