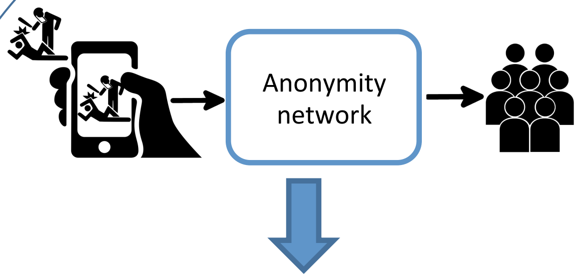
Enabling Practical Traffic Analysis Resistance for Anonymous Communication Systems

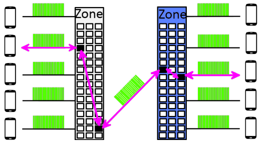
Challenges:

- Shortcomings of existing anonymity networks
  - Traffic analysis
  - Medium/high latency
  - Mobile platforms
- Real time communication needs
  - Low latency
  - Scalability
  - Resistance to strong attacker

Solution:

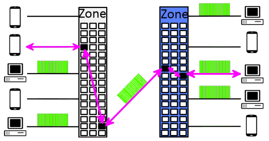
- *Trust zones*: data centers in a jurisdiction
  - Anonymity depends on client trust zone
  - No adversary has access entire Internet
  - At least one jurisdiction that is friendly or indifferent
- Low latency due to fully connected zone mixes
- Traffic-analysis resistance due to continuous chaff traffic at (multiple of) VoIP rate





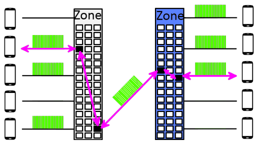
Design 1: Baseline (Herd)

High bandwidth overhead



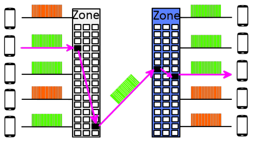
Design 2: Extended trust (to callee)

Weaker anonymity



Design 3: Sporadic

Must wait for a duty cycle



Design 4: Sporadic & delay-tolerant

Revert to simplex channels

Scientific Impact:

- Project will lead to new communication models and systems designs to protect online freedom of speech
- The project will make observations from empirical analysis of services and communication patterns available to the research community to improve the effectiveness of solutions.

Broader Impact:

- The project will help improve freedom of speech by enabling effective anonymity
- We will release our source code publicly and develop working systems to support vulnerable populations
- We will develop courseware, whitepapers, and tutorials based on our research

Award #1618955
PI: David Choffnes, Northeastern Univ.
choffnes@ccs.neu.edu