Incentives to relay

- 1) Incentives to relay traffic
- 2) Incentives to do it well
- 3) Incentives to allow exits.
- Naïve tit-for-tat probably not so smart. But maybe something like it?

“Run two servers and wait”

- Over time, Alice will choose your nodes as entry and exit.
- Guard nodes.
- What's the right way to do guard nodes in the presence of churn?

Location diversity

- When many nodes are at a single ISP, and many paths are observable by a single ISP, what **local** algorithms can Alice use to improve (maximize?) her safety?

Non-clique topology

- Right now we assume all nodes can reach all other nodes. We're fine as long as that's mostly true.
- What about Internet splits?
- What about nodes in China – or entire Tor networks in China?
- One answer is Geoff Goodell's "Blossom" project at Harvard.

Mid-latency

- How much latency do you need to add to start seeing end-to-end defense?

Asymmetric bandwidth on servers

- Servers on cablemodem pull down bytes easily, but can't send them out again.
- Need to rate limit reading so we do our own push-back?

Does it mix?

- Does low-latency traffic provide cover (“mix”) with mid/high-latency traffic?

Website fingerprinting

- Do these attacks work against Tor?
- Does cell size change things?
- Does variable delay change things?
- What about a little bit of padding, e.g. long-range dummies?

Fragmenting streams

- Should we fragment streams across multiple paths?

Congestion attacks

- Can you “measure” Alice by ICMP pings even if she doesn't relay traffic for you?
- (Cf Murdoch/Danezis Oakland05 paper)

Pseudonyms/profiles

- Logging into your gmail account and then posting to Indymedia is bad.
- But a new circuit for every request is also bad.
- What's the right compromise/strategy?

Puzzles to manage load?

- If each server demands that Alice solves a puzzle, can we make the puzzle proportional to load?
- Alice's delay reveals which node she's solving a puzzle for?

Transporting UDP and IP

- Need IP-level packet normalization library.
- Application-level streams still need scrubbing (e.g. privoxy).
- DNS requests to your local nameserver still leak information.
- DTLS exists now, but we still need a new Tor protocol that handles tagging attacks, drops, resends, etc.
- Exit policies for arbitrary IP packets mean building a secure IDS.
- The Tor-internal name spaces (.onion, .exit) must be redesigned.