4 Security & reputation ~~repudia~~ in P2P

Attacks

DDOS (use botnet)

- Pushing / requsting
  - minimize cost of loosing peer
  - important peers hard to find
  - Caching
  - Protect data vs overwrite

Malicious peers

- reroute, claim peers down, poisen routing, create high churn
  - Use multiple paths
  - verify peers and data

Sybil attacks

- Subvert or spy on traffic
  - ensure use different subnets
  - make join expensive

Eclipse attacks

- sourround peers, can remove peers from network
  - Cannot freely choose persition in network
  - Several paths

Tarzan

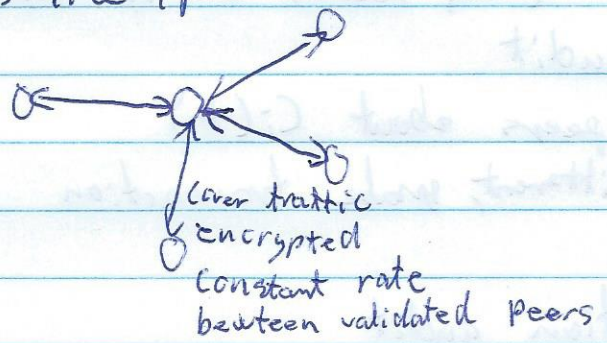
P2P mix network

÷ blocking

÷ traffic analysis

K neighbours

API - looks like ip



Joining

Contact known peer, get peer list

Contact new peer to get peer list

Continue until satisfied

Malicius peer

- Sybil attack most likely on same subnet
  - Tarzan selects many different subnets when routing.

Routing

- Built iteratively - generates synchronous encryption key
- Always under mimics

ARA - A robust Audit

- Credit
- transactions

  <Id_j, Id_i, C_i, bytes, direction, period, interested peers>

~~Signed by~~ Created and signed by i, j individually

- Periods (keep records for m periods)

Credit audit

- Ask peers about $C_i(t)$
- If different, make transaction audit

Transaction audit

- Check consistency
- If different, then proof round (signed by i)

Interested peer list audit

- Check if one self is on list of others
- Can always check j, since he must be there