How I2P Works

- An I2P client is downloaded onto a person's PC
- When the client starts, it picks out flood router information from a given seed URL, using this as the basis for directory services
- Each time a new service connects to I2P, it creates a new set of tunnels
- Tunnels are added to a pool of routes for redundancy and fault-tolerance
- Each connection must first query the netDb to get the address information for the destination user's inbound tunnel
Hypothesis

I hypothesize that as the rate of nodes leaving a Kademlia network (as in used by I2P) increases, node lookup time will increase.
Paper 1: Performance Analysis of Anonymous Communication Channels Provided by Tor

- Overview of what Tor is
  - Onion routing
  - Circuit switched network
- Overview of common usage habits with Tor
  - Users will generally only tolerate up to four seconds of latency
- Tests two Tor clients
  - The original Tor client
  - The OnionCoffee Tor client
  - Experiments on both public and private networks
Experiments on a private network

- Throughput under load on private network:
  - Node tested to see how well circuits are established
  - Steady decline in throughput up to fourteen nodes
  - Differences in OnionCoffee and Tor

- Circuit Establishment
  - Time for a client to establish a full circuit
  - Declined as number of penetrators increased
Experiments on the public network

- Circuit establishment
  - Circuit establishment is slower in general
  - Repeated with variable hop-sizes
- RTT
  - Mean RTT is 1.6s
  - Tor/OnionCoffee use probabilities to select nodes
    - Based on self-reporting of bandwidth
  - Improvement: latency based path selection
Paper 2: Kademlia: A peer-to-peer information system based on the XOR metric

- DHT using an XOR metric to determine the distance between keys in the key-space
  - XOR is used because it is symmetric
  - Information automatically spread throughout network via lookups

Diagram from Maymounkov and Mazieres, pg. 3
Paper 2: Kademlia: A peer-to-peer information system based on the XOR metric

Diagram from Maymounkov and Mazieres, pg. 3
Paper 2: Kademlia: A peer-to-peer information system based on the XOR metric

- Nodes store contact information
  - Tuples of (IP address, UDP port, Node ID)
- $0 \leq i < 160$ k-buckets
  - Bucket stores node information $[2^i, 2^{(i+1)}]$
  - Updated on receipt of any message
  - $k$ is a system-wide parameter
Paper 2: Kademlia: A peer-to-peer information system based on the XOR metric

- Routing table is a binary tree
  - Initially contains one k-bucket
  - Nodes split the k-bucket based on their own node id as the k-buckets fill

Diagram from Maymounkov and Mazieres, pg. 8
Paper 3: I2P Data Communication System

- Peer to peer "garlic" routing protocol for anonymous Internet access
- Utilizes multiple connections in parallel
- Uses one-way tunnels
  - Refreshed at regular intervals
- Use case different from Tor
  - Only users already on I2P can communicate securely
Paper 3: I2P Data Communication System

● **Strengths:**
  ○ Distributed/Decentralized
  ○ Supports many different protocols

● **Weaknesses**
  ○ Susceptible to partitioning attacks
    ■ Malicious nodes can simulate benign ones
  ○ Vulnerable to intersection attacks
    ■ Watches target and number of nodes in the system
References

