Peer-to-Peer Anonymous Communication using Redundant Structured Topologies
Suman Paul, Indian Institute of Technology, Kharagpur

ADVISOR: Nikita Borisov

**Background**

- The benefits of being connected to, and interacting with, millions of strangers do not outweigh the amount of personal information revealed to those strangers.

- Decentralized nature of p2p systems provides a mechanism to distribute trust among a very large population. Also p2p networks are highly scalable.

- Even the best proposed systems are vulnerable to attacks on anonymity

**Redundant Structured Network**

- A new low latency peer-to-peer anonymous system based on random walk over redundant structured topologies.

- Redundancy is introduced through the concept of shadows that check and certify neighbor information. These certifications enable nodes to perform random walks over the structured topology while avoiding route capture and other attacks.

**Goals**

- Build a simulator for new p2p design

- Compare analytical results to simulation

**Fundamental Questions/Challenges**

- How well does analytical model capture real-world behavior?
  - What are the effects of irregular topologies?
  - Are there hidden correlations not captured in the analysis?

- How to efficiently simulate the system with high fidelity?
  - Simulation performance
  - Parameter choice
  - Error estimation

**Research Plan**

- Chord, a distributed lookup protocol, is used as the structured p2p network. A static chord network consisting of $2^{11} = 2048$ nodes is first simulated in C.

- The predecessor and the successor of a node A in the chord network are its shadows.

- The shadows of A independently maintain copies of the finger table of A.

- The shadows digitally sign the finger table and transmit it to A in order that while a circuit is being built, the fingers need not be contacted.

**Random Walk**

- The initiator I first builds a circuit to a finger A and then queries for a random finger B.

  - A provides signatures about its routing table from the shadows.

  - If all these signatures turn out to be the same, the circuit proceeds to B. A node in such a circuit can be malicious only if the node itself and both its shadows are malicious or if the last node in the circuit is malicious.

**Research Results**

**Related Work**

Prateek Mittal, Nikita Borisov, *Information Leaks in Structured Peer-to-peer Anonymous Communication Systems*, CCS’08
Prateek Mittal, Nikita Borisov, *Peer-to-peer Anonymous Communication using Redundant Structured Topologies*, Manuscript
http://freehaven.net/anonbib/