Structured Peer-to-Peer Overlays for Mobile Networks

Farida Chowdhury
Computing Science

Supervisor: Dr. Mario Kolberg
Research Goal

- Feasibility of extending P2P in mobile networks
- Experimentation the performance of various P2P overlays under high churn and bandwidth consumption
- To make sure that every node can participate in a P2P network whether it is behind a Network Address Translation (NAT) or not, we must solve the NAT traversal problem
- A general approach of NAT traversal for ring based overlays without the use of a single server
- An adaptable routing protocol that utilises both recursive and iterative routing in terms of the level of node churn and NAT connectivity
P2P in Mobile

• P2P networks are highly popular among users that have stationary computers with high-bandwidth Internet connections
• The use of mobile devices on cellular networks has dramatically changed over the last few years and moved strongly towards smarter and more powerful devices
• Providing P2P services in mobile networks will allow a user to harness the potential of P2P service while on the move
• Individual users as well as (mobile) operators and service providers
Major Challenges

- Energy Consumption
- High Churn Rate
- NAT and Firewall Traversal
Experimentations

• Distributed Hash Table (DHT) based Structured P2P overlays
• Identify features which are suitable for use on cellular networks
• The performance of various P2P overlays
Experimentations

Lookup Success Ratio under a very high churn environment

Bandwidth Consumption under a very high churn environment
NAT Traversal

- NAT is used to share a single public IP address among several end systems on a private network thereby allowing many computers in the network to access the Internet using the single IP address.
NAT Traversal in OverSim

• NAT traversal is a huge issue for any P2P
• Increasingly problematic with router manufacturers
• Integrated a NAT traversal approach in the working P2P simulator – OverSim
• Proposed a NAT traversing approach without the use of single server components
UDP Hole Punching without a Server

• A relatively straightforward procedure
• A third party peer with a public IP address, assisting the peers with private IP addresses about to connect by informing them of each others’ public addresses
• When the peers are aware of the addresses they begin sending UDP packets to one another
• This causes mappings to be formed in the intermediate NATs
• Once outbound packets have passed the NATs, inbound packets are translated using these mappings
Case 1: Peers behind a common NAT
Case 1: Peers behind a common NAT

1) Request to connect to B
Case 1: Peers behind a common NAT

2) Forward B’s endpoints to A
2) Forward A’s endpoints to B
Case 1: Peers behind a common NAT

3) Connection established
Case 2: Peers behind different NATs
Peers behind different NATs

1) Request to connect to D
Case 2: Peers behind different NATs

2) Exchange A and Ds information between P1 and P2
Case 2: Peers behind different NATs

3) Forward D’s endpoints to A

3) Forward A’s endpoints to D
Case 2: Peers behind different NATs

4) Connection established
Work in Progress

• Churn and NAT aware Routing Protocol
• NATed nodes will initially utilise the recursive routing. In cases when these nodes sense high churn in the environment, they will use the iterative routing scheme
• Non-NATed nodes will utilise the iterative routing first. If they sense moderate/low level of churn they will switch to recursive routing
• Started writing my thesis