The Design of A Distributed Rating Scheme for Peer-to-peer Systems

Debojyoti Dutta[1], Ashish Goel[2], Ramesh Govindan[1], Hui Zhang[1]

[1]University of Southern California

[2]Stanford University

Outline

- Research motivations
- Basic design issues in P2P rating schemes
- A distributed rating scheme to incentivize cooperation in P2P file-sharing systems
- Dealing with collusion and malice
- Conclusion & future work

Research motivations

- Object: P2P file-sharing systems
  - ❑ Open social communities.
  - ❑ An explicit reputation layer was ignored in the original design.
- Goal: Build reputation in such systems
  - ❑ Incentive for user participation
    - free-riding phenomenon [Adar et al. 2000][Saroiu et al. 2001]
  - ❑ Isolation of malicious users
    - distribution of inauthentic files
    - propagation of virus or worms [VBS.Gnutella][Fizzer.Kazza]

P2P rating: basic design issues

- "Distributed" rating
  - following P2P design philosophy.
- "Efficient" rating
  - low cost to run and maintain this reputation system.
- "Collusion-proof" rating
  - Effectiveness.

A distributed rating scheme

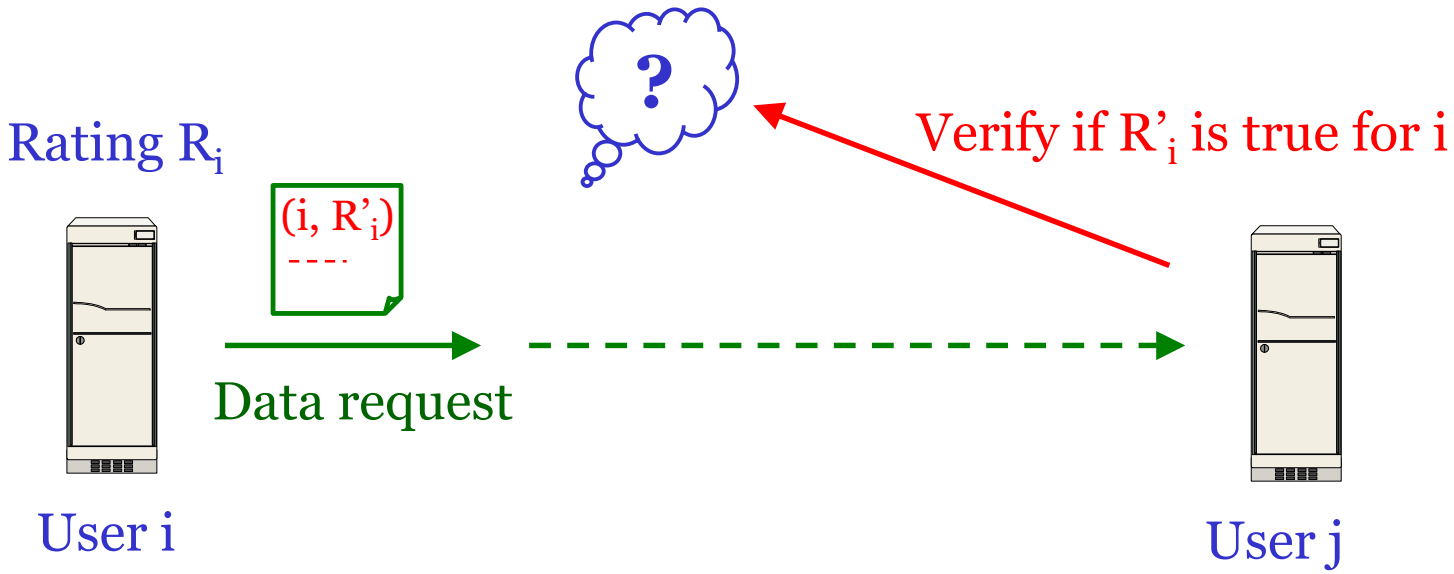
- To incentivize cooperation in P2P file-sharing systems

- Main components
  - Positive rating
  - Rating verification scheme

Positive rating

- The recognized service done to the community
  - R_i of user i: non-decreasing with the number of successful requests that it has satisfied within some sliding time window.
  - The higher R_i user i has, the better service it gets from the network.

Verification-based rating scheme



Two verification schemes

- Structured verification scheme (SVS)
  - Each user has a set of designated supervisors which keep its up-to-date reputation information.
  - The supervisors are responsible for the verification.

lightweight

L

- Unstructured verification scheme (UVS)
  - A user j queries some of user i's claimed customers for the verification, and believes i when the majority of the probed users reply with a "yes".

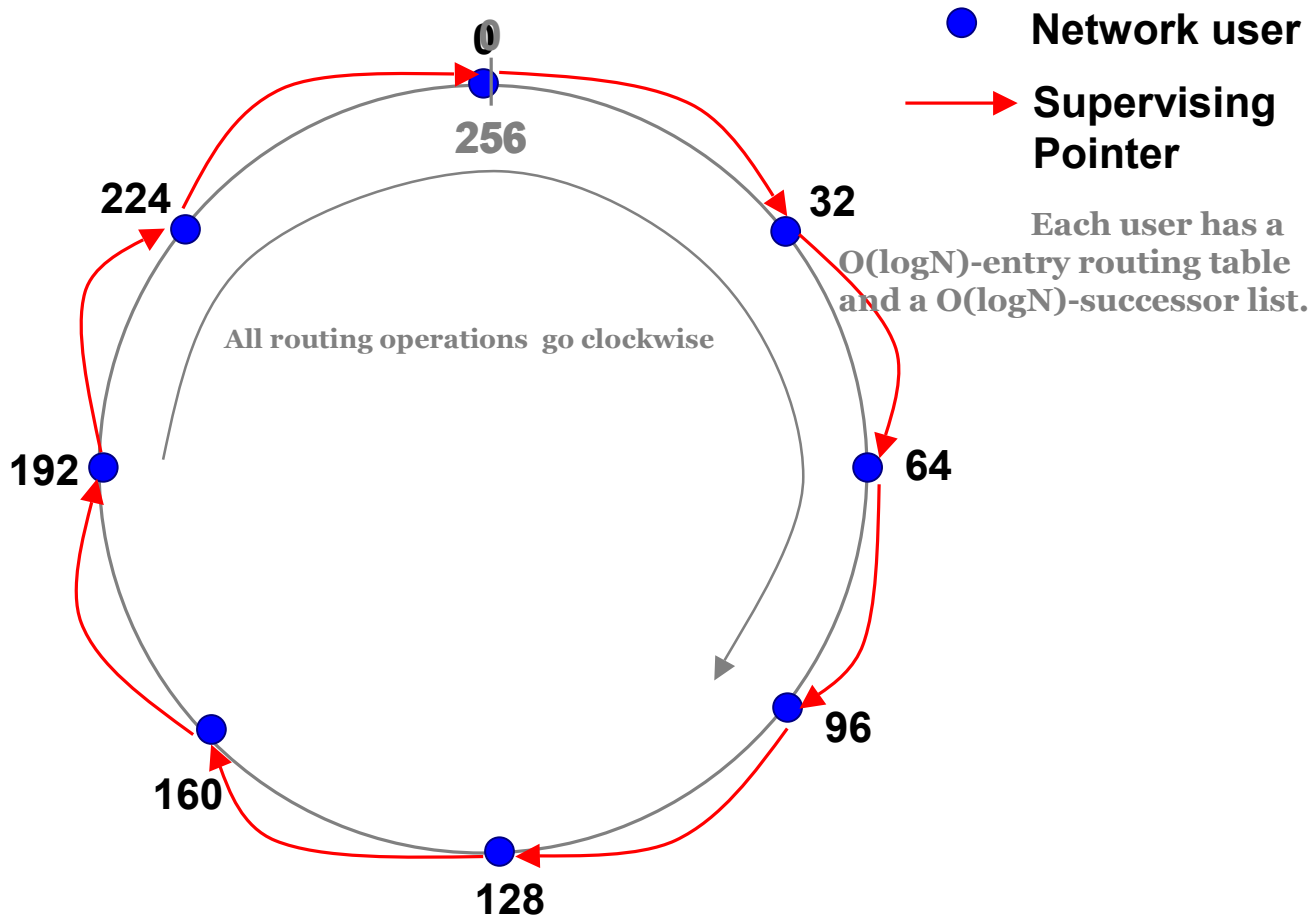
Assumption

- Users are distinguished by their IP addresses.
  - At a given time, one IP address corresponds to an unique user.

SVS – the supervising topology

- In the supervisory directed graph
  - Any user is random to its supervisors.
  - No small supervising loop exists.
  - There is a fast *reactive* approach for any user j to deliver a message to any other user i's supervisors, and the path never includes i.

A Chord[stoica2001] supervising overlay

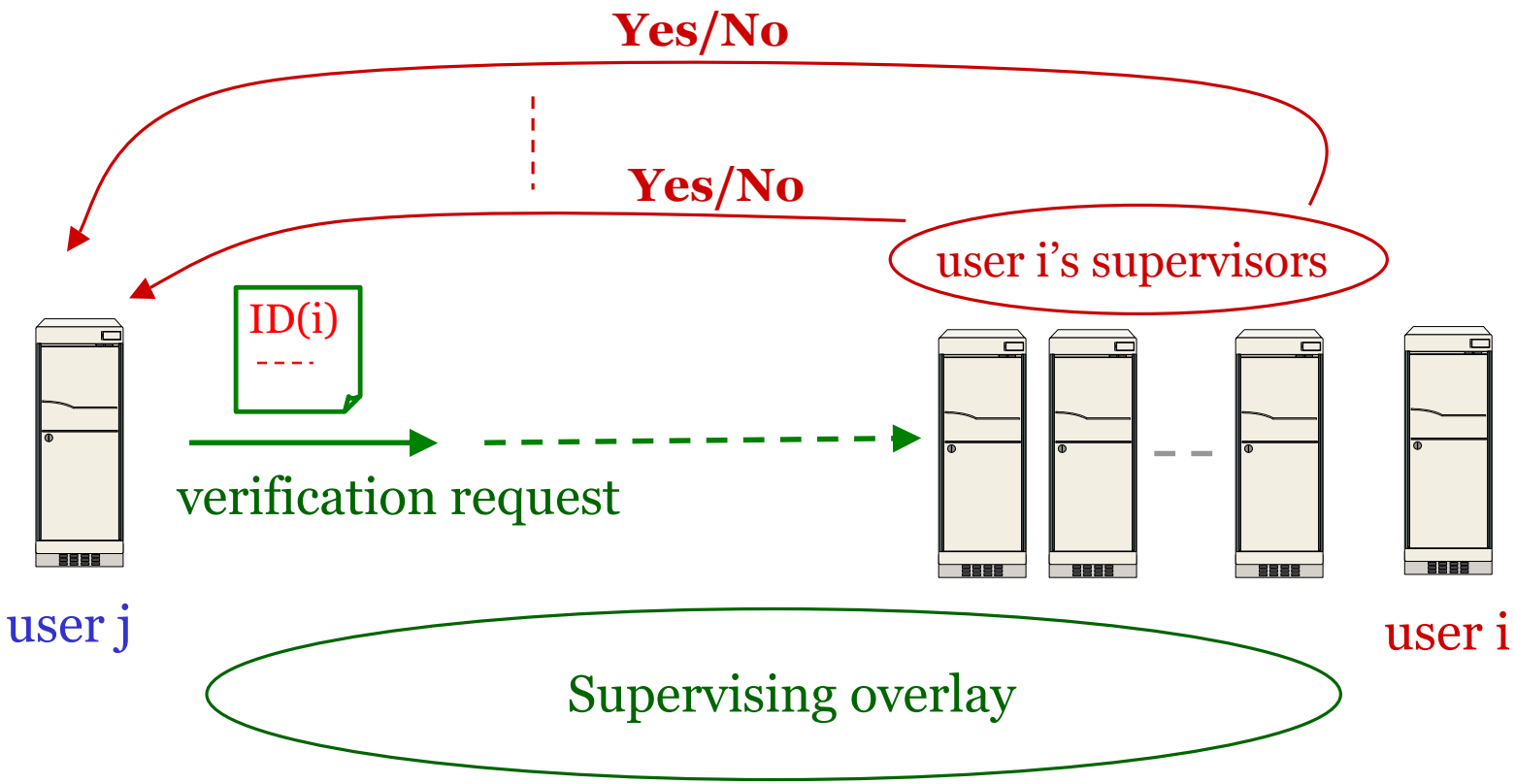


A Chord network with 8 users and 8-bit key space

SVS – the supervising topology

- In the supervisory directed graph
  - Any user is random to its supervisors.
  - No small supervising loop exists.
  - There is a fast *reactive* approach for any user j to deliver a message to any other user i's supervisors, and the path never includes i.

Rating verification in SVS



Structured verification scheme

- "Distributed" rating ✓
- "Collusion-proof" rating ✓
- "Efficient" rating ?
  - Extra cost to maintain a supervisory overlay when the underlying network is not DHT-based.
  - Repetitive actions when there are multiple supervisors.

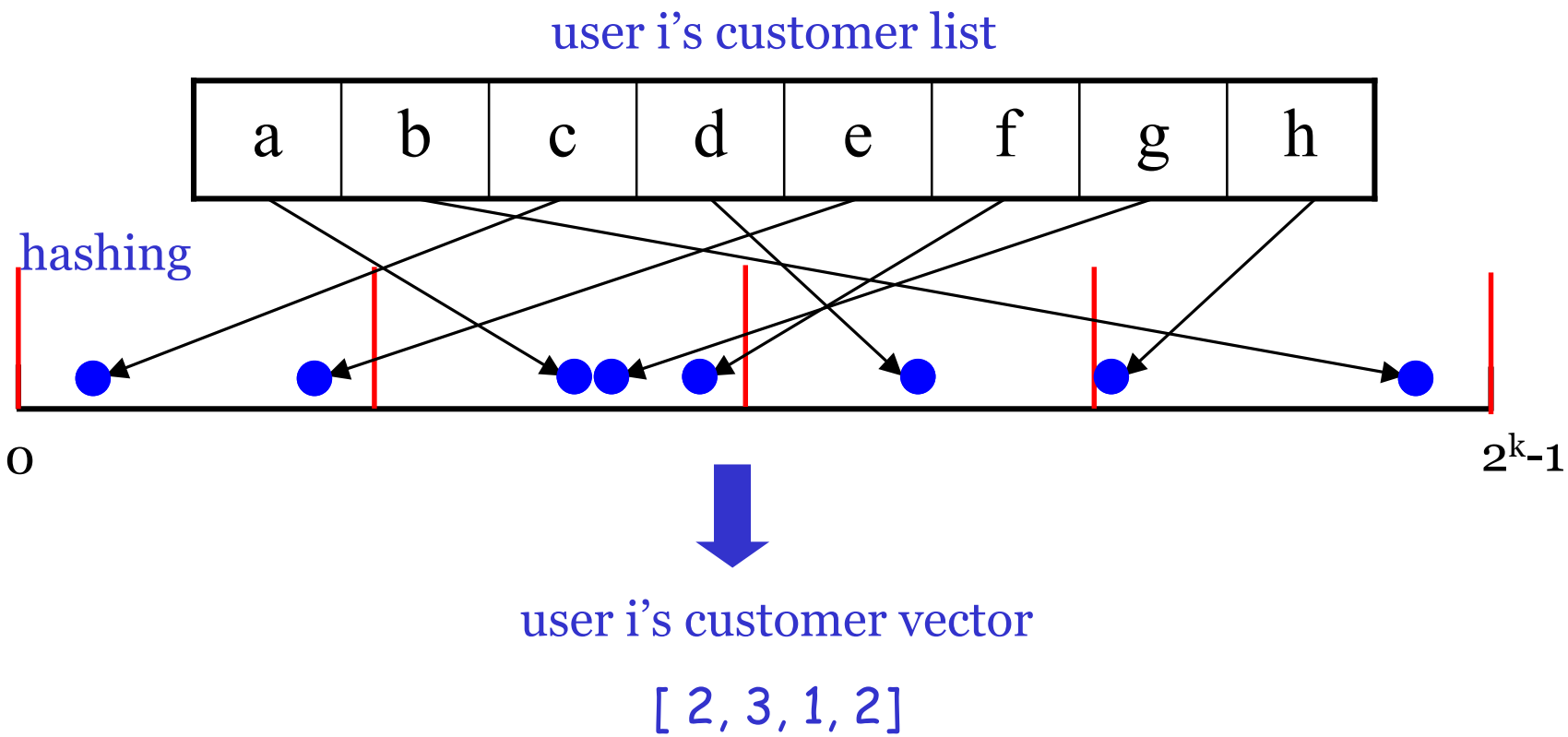
Unstructured verification scheme

1. When user j decides to verify user i's rating, it gets a portion of i's customer list, and asks the users on the list if i did the claimed service to them.

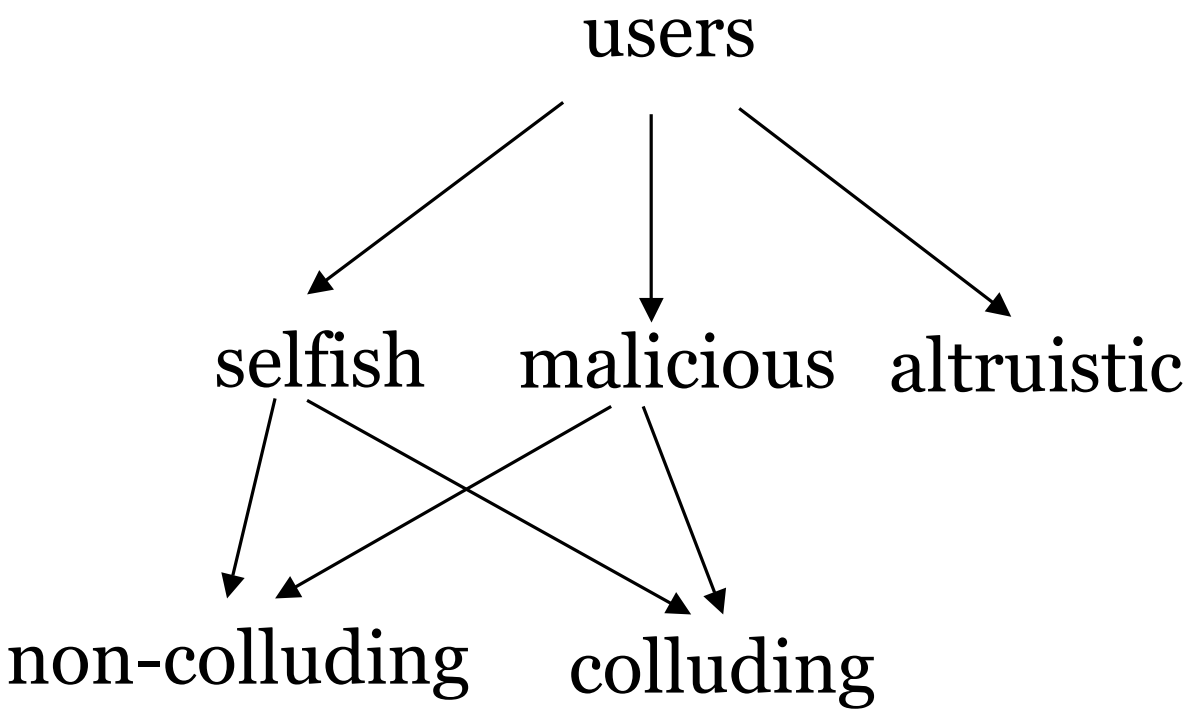
   - The customer samples should be random on the full customer list of node i.
   - Disclosure of full customer list could raise privacy concern, and incur high communication cost.

2. When the majority of the probed users reply with a "yes", j is convinced that R'_i is R_i.

Randomly sampling without the complete customer list



P2P users


users
selfish
malicious
altruistic
non-colluding
colluding

Colluding selfish users

- Possible solution 1: discrete rating
  - Grade★ : if a user has served no more than 10 users.
  - Grade★ ★ : if a user has served between 10 and 100 users.
  - Grade★ ★ ★ : if a user has served more than 1000 users.

- Possible solution 2: rating as virtual currency
  - A user has to pay (reduce its rating) for the service it claims to have received.
  - SVS: asks the requestor's supervisors for a payment.
  - LUVS: future work.

Colluding malicious users

- One possible strategy
  1. A user i quickly earns a high rating by faking transactions with other colluding users.
  2. User i then does bad things until earns bad-enough reputation.
  3. User i quits the network to clear its history,
  4. User i rejoins the network and repeats the above actions.

Conclusion & future work

- A simple distributed rating scheme to incentivize cooperation in P2P file-sharing systems.
  - Two distinct verification schemes
- Refine LUVS scheme to handle colluding selfish users.
- Refine our rating scheme to be collusion-proof.