A Credit Mechanism Based on Automatic Audit in P2P File Sharing Systems

Ruixuan Li, Cuihua Zuo, Yuntian He, Zhengding Lu

College of Computer Science and Technology
Huazhong University of Science and Technology

P2P applications booming

- P2P file sharing has become an important application
- Problems in P2P file sharing systems
  - Free-riding phenomenon
  - Malicious acts
    - Juggling and collusion
    - Slandering and exaggerating
    - White-washing attack

Solutions and challenges

- Solutions in P2P file sharing systems
  - Trust management mechanism
- Challenges in trust management
  - Rely on the centralized servers
    - Potential risk of single failure
  - Manual intervention to trust or reputation value

Our contributions

- A credit mechanism based on automatic audit in pure P2P network
- No man-made intervention
- Without centralized servers or super peers

Related work

- Reputation-based trust management technology
  - Most of reputation systems only use positive (credible) or negative (not credible) information
- Reputation scheme based on local recommendation
  - E.g. P2Prep
- Reputation scheme based on other peers' evaluation
  - E.g. PRIDE and NICE

Related work (contd.)

- Incentive mechanisms in P2P network
  - Faster download speeds or higher priority access
  - Promote cooperation among peers
- Differentiated service scheme based on reputation system

Outline

- Introduction
- Credit model
- Automatic audit mechanism
- Performance evaluation
- Conclusion

Design issues

- Basic idea:
  - Micro-pay economic transaction
  - Automatic audit
  - Peer restriction
- Initial presuppositions:
  - Pure P2P file sharing network
  - Each peer has a unique and unchangeable identifier
  - Peers can query resources each other
  - Most of the peers are selfish

Basic credit model

- Credit value of peer *i* in a period time *t*: $C_i(t)$

$$C_i(t) = \sum_{u=0}^{t-1} (B_{Oi}(u) - B_{Ii}(u))$$

  - $B_{Ii}(u)$ denotes the whole downloads of peer *i* from other peers in a period time *u*
  - $B_{Oi}(u)$ *means the whole uploads from peer i in a period time u*

Issues in basic credit model

- Need an unpredicted huge amount of space to store the transaction information of peers

Amended credit model

- Use the latest *m* periods to calculate $C_i(t)$

$$C_i(t) = \sum_{u=t-m}^{t-1} (B_{Oi}(u) - B_{Ii}(u))$$

Service threshold

- Service threshold *LIM* is a positive constant and the lowest limitation of service provision
- When the credit value of a peer is less than the threshold *LIM*, request from the peer will be refused

Problems in threshold

- System deadlock
  - E.g. at the beginning, all peers' credit value is zero which is lower than the threshold of *LIM*
- *System "hunger"*
  - *If only few peers has enough credit value to bear their consumption, the system is still in a state of "hunger"*

Valid service threshold

- The valid service threshold LIM_e of service provider *p*

$$LIM_e = \min(LIM, k_{LIM} \cdot \max(C_p, 0)) \quad 0 < k_{LIM} < 1$$

  - C_p: *p*'s credit value; k_{LIM}: coefficient parameter
  - Peer *i* can obtain the service from peer *p* if its credit value C_i is no less than the valid service threshold *LIMe* of service provider *p* , even though the credit value of peer *i* is lower than *LIM*

Improved credit model

- The improved credit model of peer *i* in the period *t*

$$C_i(t) = \sum_{u=t-m}^{t-1}(B_{Oi}(u) - B_{Ii}(u)) + \min(k_C \cdot LIM, k_O \cdot \sum_{u=t-m}^{t-1} B_{Oi}(u))$$

$$k_C > 1, \quad k_O > 0$$

Advantages of the design

- Resist the acts of free-riding
- Restrain the white-washing attack
- Encourage sharing resources in P2P network

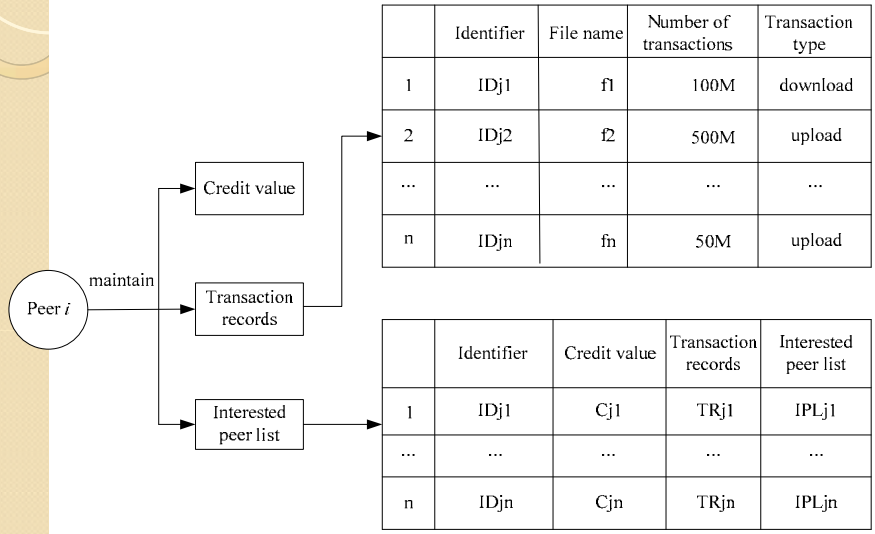
Outline

- Introduction
- Credit model
- Automatic audit mechanism
- Performance evaluation
- Conclusion

Peer's information

- Each peer maintains a credit table including three kinds of dynamic information:
  - credit value
  - transaction records
  - interested peer list

Peer's information



	Identifier	File name	Number of transactions	Transaction type
1	IDj1	f1	100M	download
2	IDj2	f2	500M	upload
…	…	…	…	…
n	IDjn	fn	50M	upload

	Identifier	Credit value	Transaction records	Interested peer list
1	IDj1	Cj1	TRj1	IPLj1
…	…	…	…	…
n	IDjn	Cjn	TRjn	IPLjn

Synchronization strategies

- At each period time *t* of peer *i*,
  - peer *i* adds timestamp into its credit value, transaction records and interested peer list
  - issues this information to its interested peers who are online

Synchronization strategies

- When peer *i* and peer *j* have a transaction,
  - peer *i* updates its credit value in the local credit table and creates a new transaction record
  - issues this information to its interested peers who are online

Synchronization strategies

- When peer *i* gets online,
  - E.g. peer *i* wants to update the information of its interested peer *j*
  - peer *i* issues update request to all online peers in peer *j*'s interested peer list
  - gets the information with the latest timestamp to update peer *j*'s credit table information

Audit strategies

- Audit the credit value
- Audit the transaction records
- Audit the interested peer list

Example for audit strategy

- The interested peer *j* of peer *i* initiates the audit of peer *i*'s credit value
- It selects some online peer *k* in the interested peer list of peer *i* with the probability P_C and asks peer *i*'s credit value and compares it to peer *i*'s credit value *Ci*(*t*)
- If they are inconsistent, peer *j* asks peer *k* to send him the credit value *Ci*(*t*) signed by *i* as the evidence of malicious acts of peer *i*

Outline

- Introduction
- Credit model
- Automatic audit mechanism
- Performance evaluation
- Conclusion

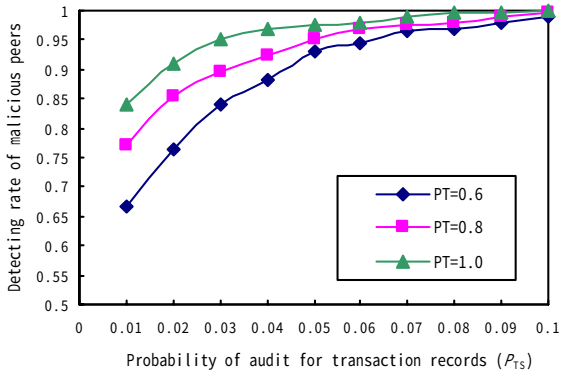
Experimental settings

- JXTA platform
- The period of time *t* is set to 10 minutes
- The number of latest records *m* is 12 and *LIM* is 10
- The running time is 20 periods
- The number *n* of interested peers for each peer is 50

Experimental methods

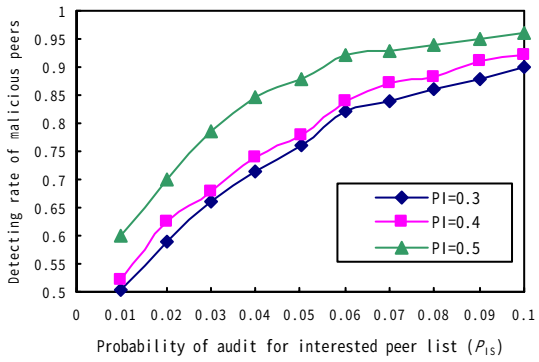
- Through observing the simulation experiment in a certain time period, we get the relationship between detecting rate of malicious peers and the probability of audit.

Experimental results



- When P_{TS} achieves at 0.05, its corresponding detecting rate will be up to larger than 0.9. That is, 90 percent malicious actions can be found in the P2P network.

Experimental results



- When P_{IS} reaches at 0.06, its corresponding detecting rate will be up to larger than 0.8. That is, 80 percent malicious actions can be detected in the network.

Outline

- Introduction
- Credit model
- Automatic audit mechanism
- Performance evaluation
- Conclusion

Conclusion

- Analyze the characteristic and shortage of existing algorithms
- Design a credit model
- Design automatic audit mechanism
- Restrict malicious actions

Thank you!

http://idc.hust.edu.cn