Extending Trust in Peer-to-Peer Networks

Stephen Clarke
Bruce Christianson
Hannan Xiao

TR4Web - Riga, Latvia
7th Sept 2009
University of Hertfordshire

Motivation

- We often need to do business with strangers.
- Reputation systems don't sufficiently reduce the perceived risk.
  - We don't know the people leaving the ratings.
  - Even if we did, trust isn't necessarily transitive.

Assumption

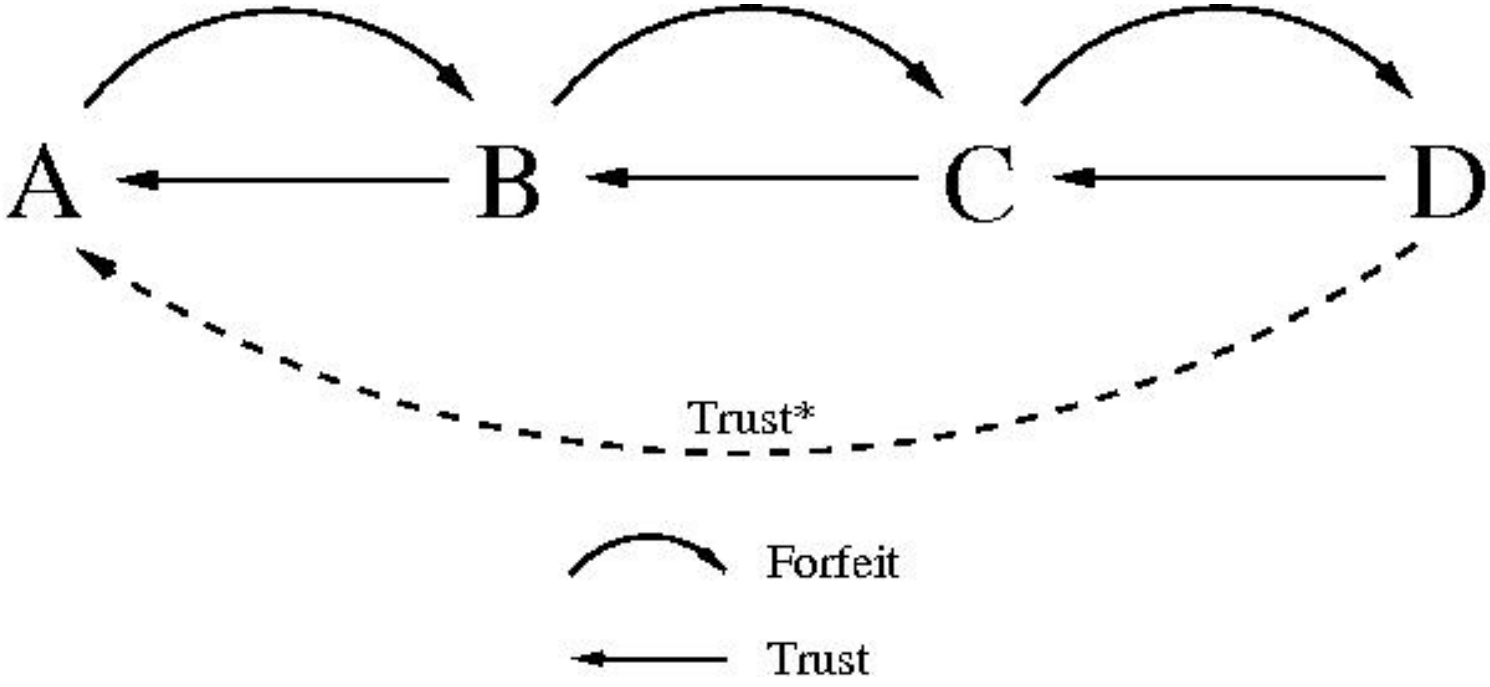
- Local trust management works.
  - Users rating people they do regular business with.
  - They do this by maintaining policies stating whom they trust and the scope to which it applies.
  - We do not prescribe the choice of mechanism used. However, we used KeyNote.
  - This method is better than trusting a centralised service.

A Real World Motivation

- Third-party guarantees.

- Carol still doesn't trust Alice but now can act as if she does.
- Bob's incentive could be to take a commission.
- All trust relationships remain local and are updated independently.
- This can be extended to multiple hops.

The Trust* Concept



- All trust relationships and forfeit payments are local.
- Bob believes that Alice will *either* provide the service *or* pay the forfeit.

Applying Trust* to P2P

- Trust* aims to provide missing assurances when file-sharing with unknown peers.
  - Is the file a good copy? E.g. untampered with, not corrupt, original, etc
- Reputation systems exist to isolate “bad” peers.
- However, trust* can be used to reduce the risk involved when transitively trusting others.

Turtle P2P Client

- Popescu *et al* designed a P2P client that enables file-sharing to take place between friends.
- These “friends” are people that a peer knows and has existing trust relations with in the real world.
- Search queries and file transfers will only be relayed via these locally trusted peers. But sharing is transitive, friendship isn’t.
- The authors of Turtle aimed to provide a client to protect the privacy of its users (or the files they might share).
- Our aim is to provide assurance of the correctness of copyright free content.

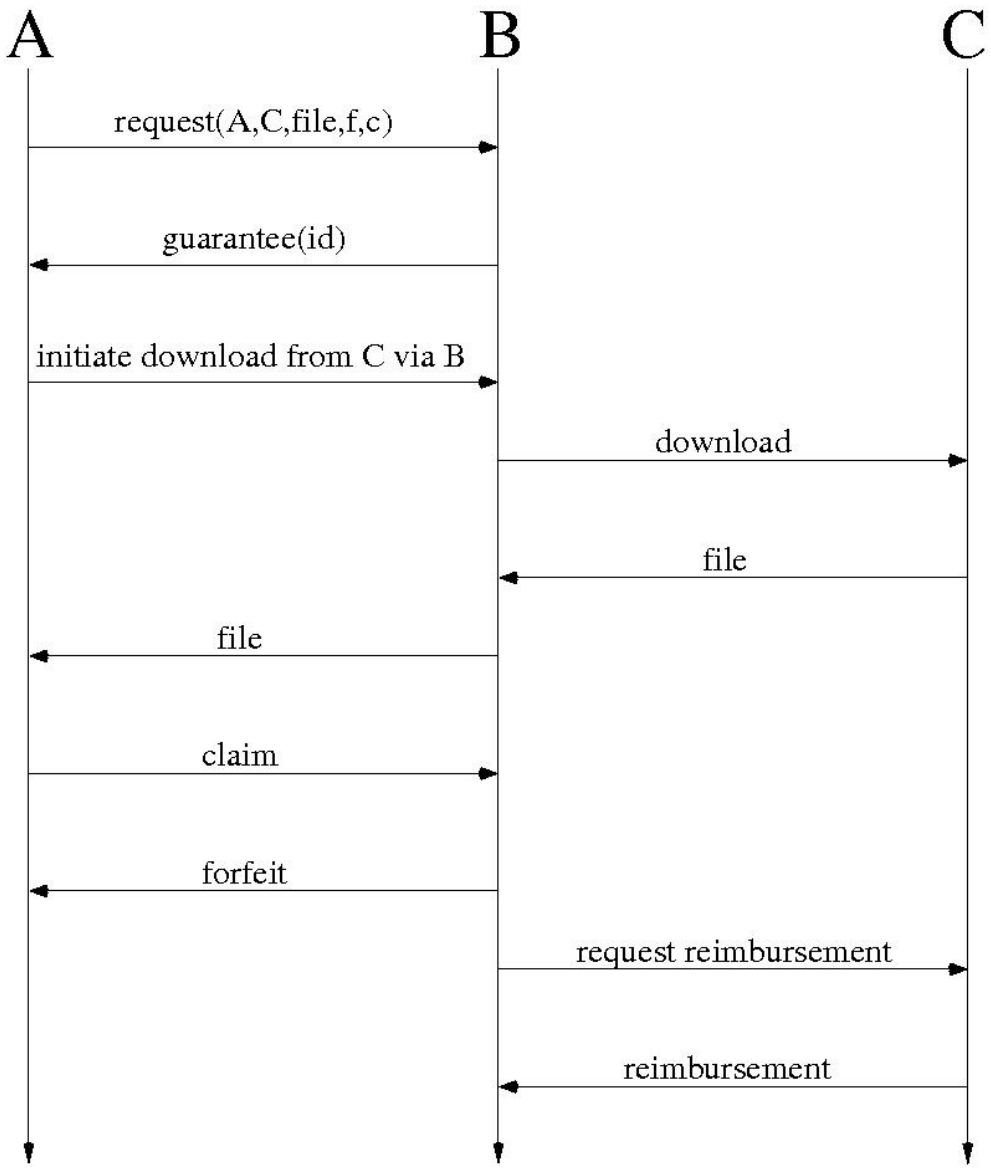
Economic Models

- In their paper, Popescu *et al* suggest extending the client with an economic model to encourage cooperation and fairness.
- We propose that the economic model is used to provision guarantees to “clean-up” a P2P network.
- For example, in combination with an economic model whereby credit is calculated on an upload/download basis, the trust* forfeit/commission payments could be the resources themselves.

Commissions or Forfeits?

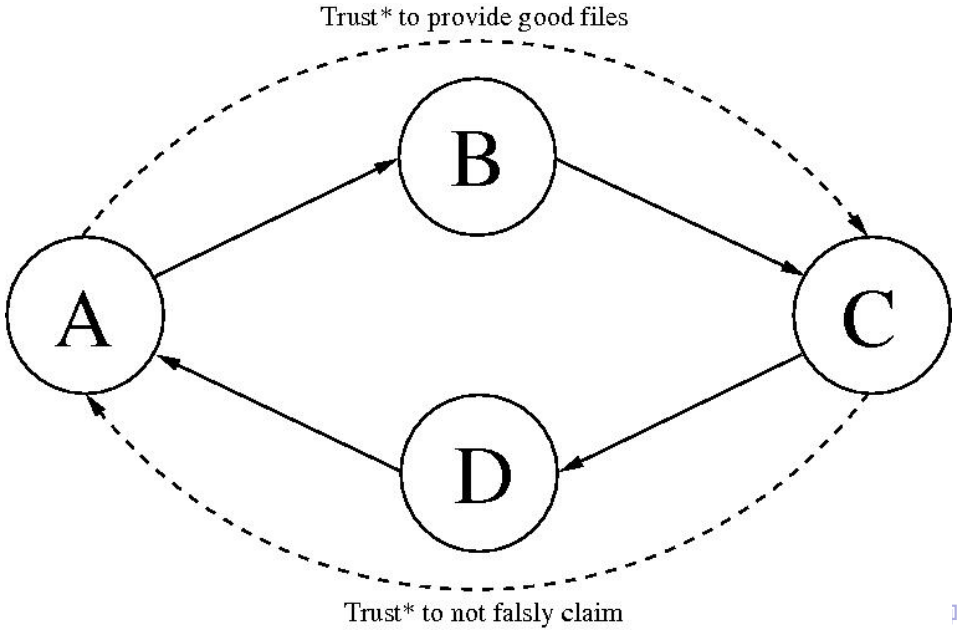
- There is a trade-off between trust and commission/forfeit rates.
- Purpose differs – (a) compensate client (b) deter server.
- Risk perception differs – Alice must assess: (a) will Carol default? (b) will Bob pay up?
- If Bob gets fed-up of paying forfeits to Carol, he will simply stop providing guarantees to Alice.
- If Bob becomes worried about his potential liability, he could apply back-pressure by increasing his commission requirement from Alice.

An Example Protocol



Route Finding

- Route finding can be provided by Turtle but is really just a networking problem. Multiple routes might be possible via different friends but at different costs.
- Also, the trust* route could be different to the file transfer route.
- Trust isn't symmetric but many service agreements need to be. Cycles of trust* can be used to provide assurances in the opposite direction.



Trust* Simulation

- The trust* model has been simulated using the Repast agent modeling toolkit.
- The protocol was repeatedly invoked until all available guarantors are exhausted.
- Different variables affected the behaviour of the agents involved. E.g. truthfulness, chance of defaulting.
- The results show that using trust is more effective and cheaper if agents behave responsibly.
- Agents who misbehave will be held accountable and their usage of trust* will be extremely short-lived.

Summary

- Trust* lowers the perceived risk for the trust*er and shifts it towards the trust*ee.
- The trust*er can act as if they trust the trust*ee directly. Even though trust* is transitive, the guarantees aren't. So, either the service will be provided or the forfeit will be paid.
- For example, the landlord will always get his rent whether it be from the tenant or the tenants guarantor.

Future Work

- Although the trust* model has been prototyped using KeyNote and various application scenarios have been simulated, any further issues might not become evident until it is deployed in a real application.
- Therefore, the next stage of this work is to implement a usable system which could be plugged-in to P2P clients such as Turtle.
- Currently, an MSc student at UH is working on providing a trust* mechanism on top of PGP's web of trust.

Thank-you for listening.

s.w.1.clarke@herts.ac.uk
homepages.feis.herts.ac.uk/~comqswc