Incentive Mechanisms for Backup Application

Nouha Oualha & Yves Roudier

22 February 2006

Security and Cooperation Mechanisms

Security and safety threats

- Data loss
- Denial of service
- Data disclosure

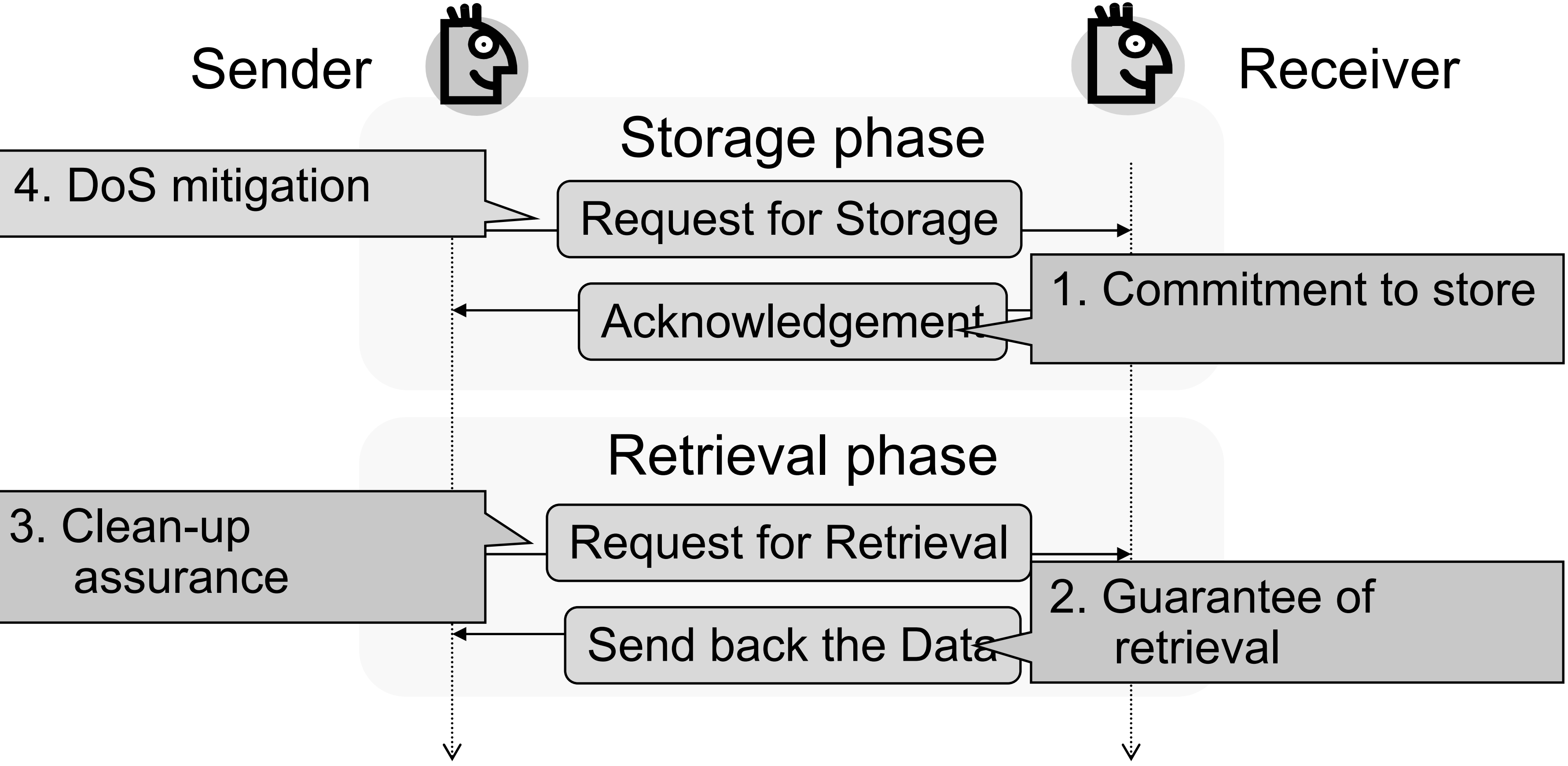
Cooperation enforcement: issues

- No trust authority available when in plain ad-hoc communications
- Separate data storage and retrieval may delay enforcement
- Need self-carried incentives (nearby devices are mostly strangers)

Our experiments:

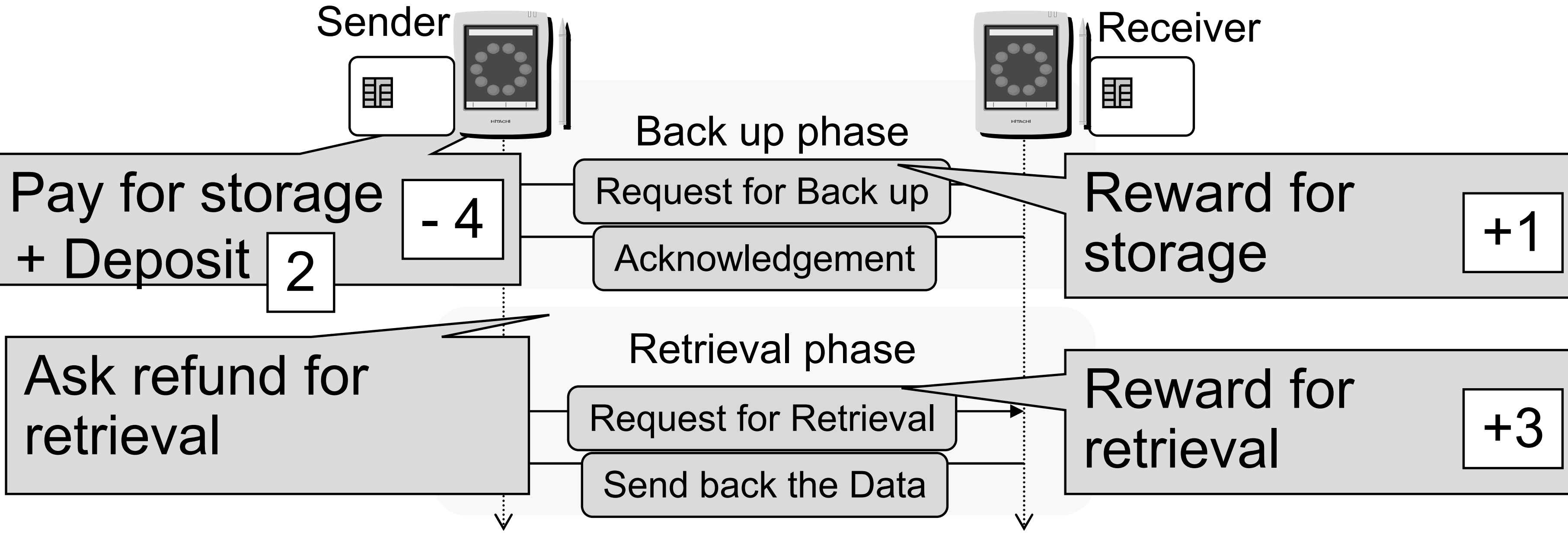
- Payment based approach to cooperation enforcement
  - Promise-based: quality of cooperation evaluated when data retrieved
- Secure *fair exchange* of cooperation incentives
  - Enforced with neutral tamper-resistant hardware (e.g. smart cards)
- Distinguish DoS from communication errors
  - A TTP is required: *optimistic* fair exchange of incentives

Protocol: Overview



Incentive Scheme

Incentives = payment (debit or credit) + deposit



- Credit points managed in smartcards
- System prevents collusion aimed at earning credits

Reputation Scheme: Roadmap

- System Overview
- Reputation Protocol
- Risks & Defenses
- Ongoing Work

System Overview

- Mobile ad hoc network:
  - The system considered is a mobile self-organizing network where physically nearby devices can communicate to each other using single or multi-hop ad hoc connection a priori of small range and all devices can connect intermittently to a fixed infrastructure.

- Trust based on a reputation system on top of TTP based structure:
  - We consider an authority that certifies the reputation values of devices. The non permanent connection to the authority is not annoying because backing up data is a time-consuming application.
  - The authority is constantly connected to the fixed infrastructure. Every time a device has the opportunity to be connected to the fixed infrastructure, it connects to the authority to update its table of reputation and to contribute to the reputation system with its experience.

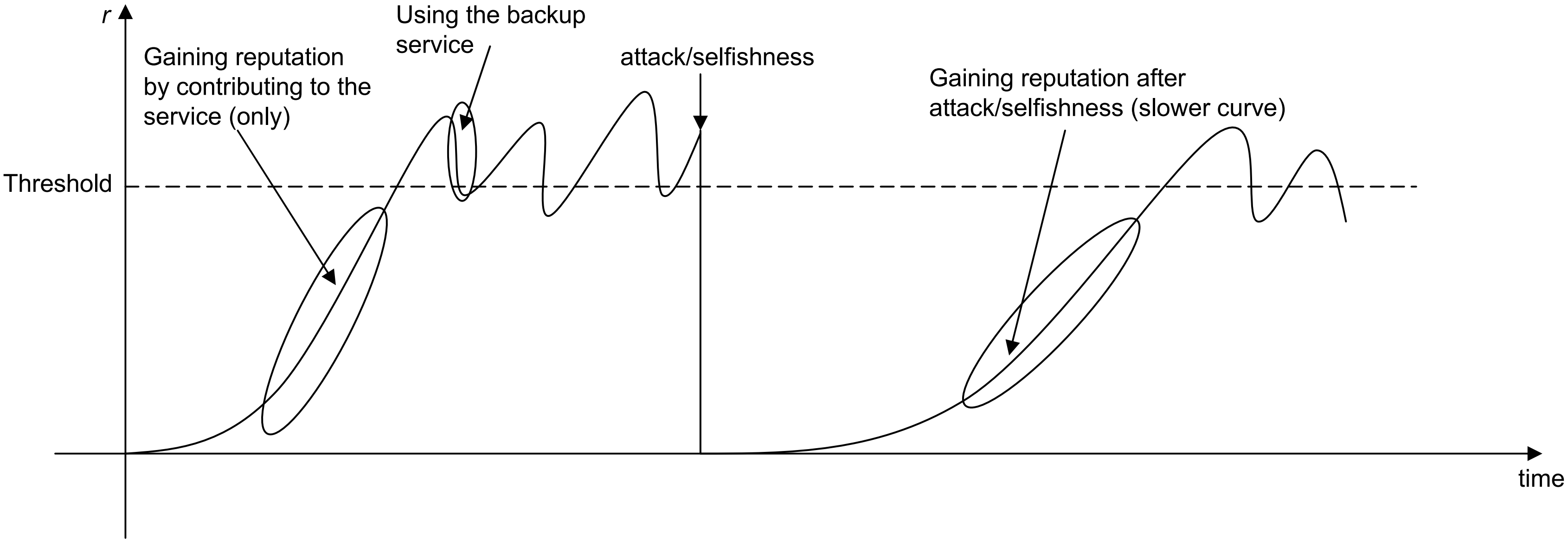
Reputation Protocol (1)

- The reputation of a device i is noted: *R(r,t)*
- Reputation is revalidated by the system authority(ies) on a regular basis
  - *r* is the reputation rating and *t* is the timestamp

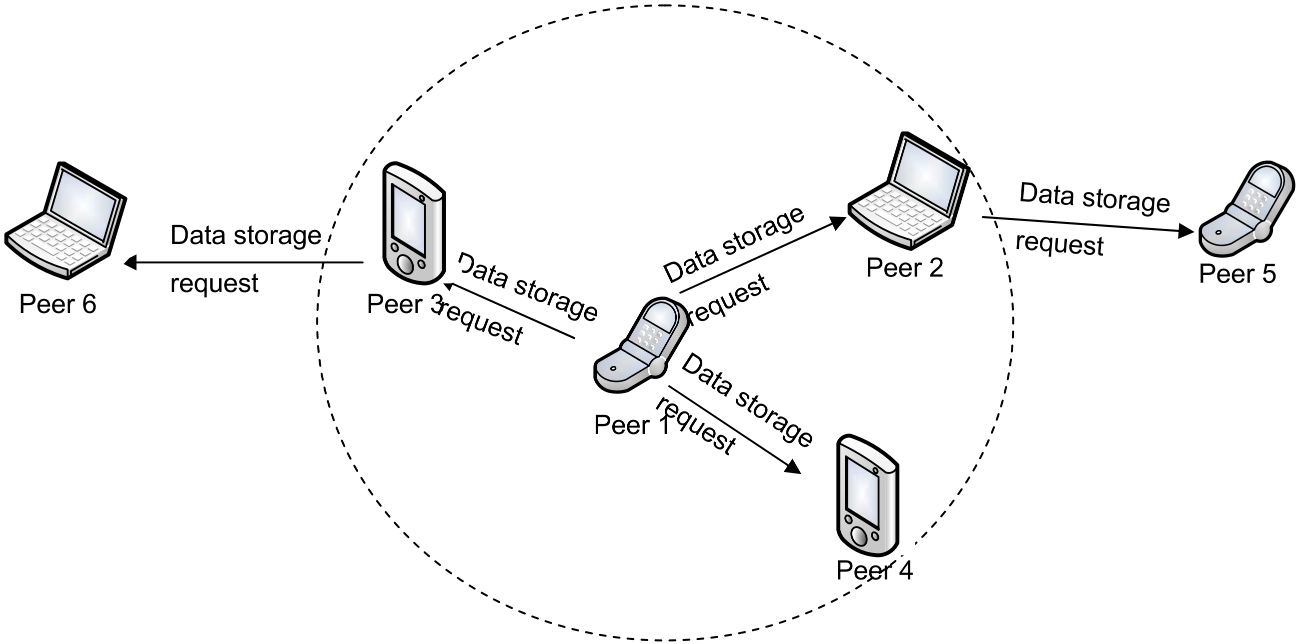
- A peer is authorized to backup its data in the system only if its reputation rating is above a given threshold.
- A newcomer in the system is given the smallest rating.
  - Earns good reputation when performing backups

- A participant who agreed to backup some data must preserve them, otherwise loses a lot of its reputation
  - Addresses reliability estimation concerns (plus maliciousness/selfishness to some point)
- Every time a peer requests a backup, a certain value is deducted from its reputation rating and another one given to the peer holding the data.
  - Addresses selfishness (being able to perform backups requires participating to the infrastructure on a regular basis)
- Advanced features: delegation is encouraged by increasing the reputation rating of peers who delegate. But we have to bear in mind possible attacks on delegation.
  - To be investigated

Reputation evolution

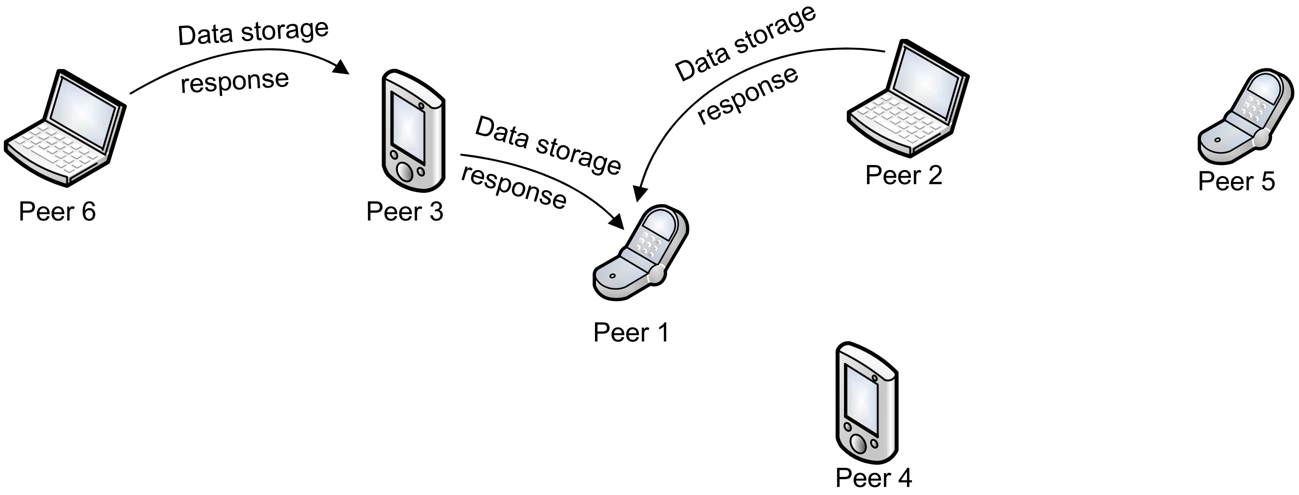


Reputation Protocol (2)
Data Store Search



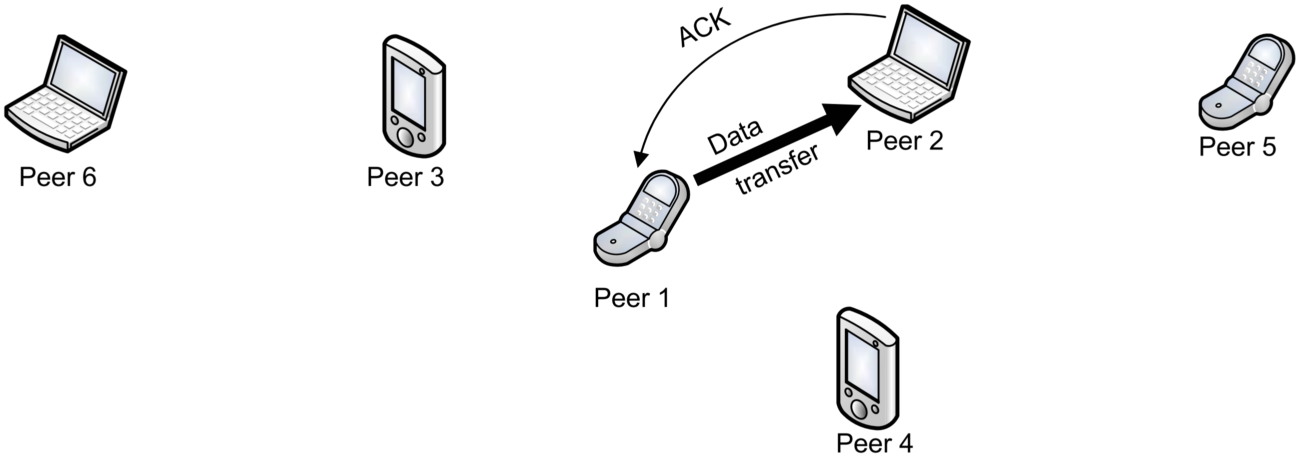
- Peer 1 needs to backup its data into the network and it has the possibility to do that. So it broadcasts a “data storage request” message into the network.
- The message will contain the ID of Peer 1, data size, and an approximate time of storage.

Reputation Protocol (3)
Data Store Selection



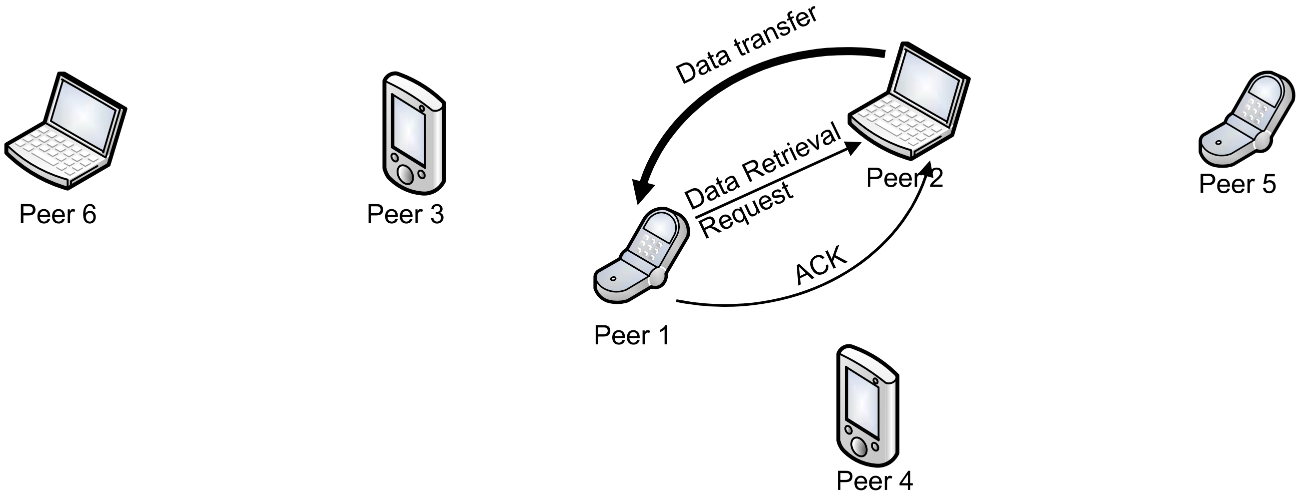
- Peer 2 and peer 5 answers to the request. Answers take into account the reputation of the requestor.
- Peer 1 selects Peer 2 for backup (replication factor is assumed equal to one)
- The selection on the requestor side is as well based on the reputation of Peer 2 and Peer 5.

Reputation Protocol (4) Data Backup



- Peer 1 transfers data to Peer 2. When data is correctly transferred, Peer 2 sends an acknowledgment.
- All peers hearing Peer 1 and Peer 2 will keep account of this operation.

Reputation Protocol (5)
Data Retrieval



- Data retrieval can be achieved by three manners:
  - Push method: When Peer 2 is connected to the infrastructure, it transfers the stored data to a mailbox designed by the data owner Peer 1.
  - Pull method: when Peer 1 is reconnected to the infrastructure, it retrieves the stored data from a data store (may be P2P data store)
  - Ad-hoc pull method: Peer 1 can ask Peer 2 to transfer data back to him with a data retrieval request message (travelling with one's "data cloud")

Risks & Defenses (1)

- Selfishness:
  - A motivation to get into this reputation system is to make use of the backup application.
  - A peer can take advantage of the system only if it has demonstrated its willingness to collaborate by increasing its reputation rating above a threshold. So a peer can take profit of only the amount of storage space it has already contributed with.

- Vulnerability to liars:
  - Information is collected by the authority from all peers which makes this type of attack difficult to launch by one or little number of peers.
  - Intoxication attack is hard to realize because any attacker is severely punished in a way that the attacker will contribute much more storage space than he uses.
  - A victim of colluded liars can detect the attack, then stop cooperating and complain to the authority.

Risks & Defenses (2)

- Identity spoofing:
  - Taking the identity of well reputed peer:
    - With the TTP mechanism, every peer has a pair of keys that authenticate him.
  - Taking a new identity:
    - It is not beneficial since the attacker will have the smallest reputation rating.

- involuntary non cooperation: link breaks, computer crashing, power shortage.
  - Observation should try to distinguish malicious/selfish behavior from involuntary faulty behavior.
    - Observation may no longer be local!
    - Cross-layering may be required
  - Data loss due to faulty behavior can be prevented by data delegation.

Ongoing Work

- Carrying on the specifications of the protocol:
  - Defining $R(r,t)$ and the threshold.
  - The structure of protocol messages exchanged between peers

- Validation:
  - Giving a formal analysis of the performance and fairness of the protocol.
    - Analyzing possible attacks.
  - Simulating scenarios using NS-2 (or Glomosim or self-crafted simulator)