Web Of Trust Simulation

Rumor spreading in simulated PGP trust networks

Why and how use PGP ?

- **Electronic based communications (e-mail,...)**
  - Ensure the privacy of communications
  - Ensure the identity of the sender
- **How ?**
  - Using public key cryptography
    - Each user has a key pair
    - The public key is (hopefully) widely distributed to everybody
- **Problem: how can a key be trusted ?**

Web Of Trust

- **A trust network**
  - Use one's own key to sign valid keys
  - The more signatures a key has, the more trustworthy it is
- **How to build it ?**
  - People meeting in real life can surely identify each other
    - Organize large meetings to help the key spreading (signing parties)
  - Sign keys according to who already signed those
    - Importance of the trust in each signer

Agent based modeling

- **Agents**
  - Key
  - ID
  - List of signatures on the key
  - Keyring: trust levels and keys signed by the agent
- **Scheduler**
  - Organizes the meetings between agents
  - Periodic signing parties

Agent behaviour

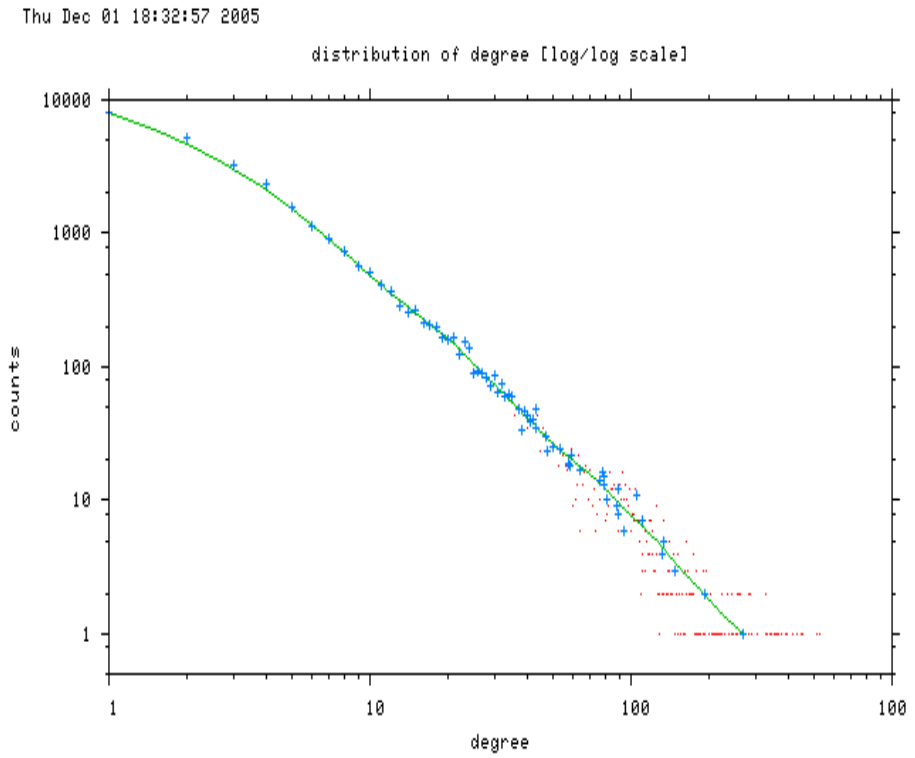
- **3 local trust levels**: Full, Marginal, Unknown
- **3 behaviour schemes**:
  - Strict: only signs in real life meetings
  - Laxist: signs whichever encountered key
  - Prudent: trusts the Web Of Trust
- **Fake keys**:
  - uses others' ID
  - introduced by real agents signing them

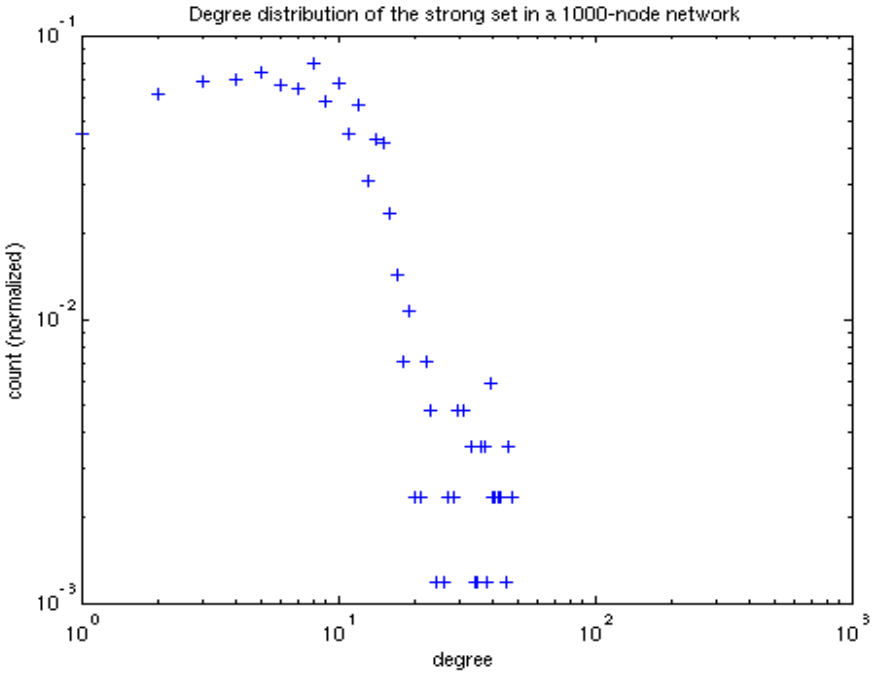
Scheduler

- **“Regular” key signing**
  - A random agent is proposed a random key to sign according
- **Single meetings**
  - Two random agents sign each other's key
- **Signing parties**
  - A random group of agents meet in real life
- **Random selection**
  - Roulette wheel

Model validity

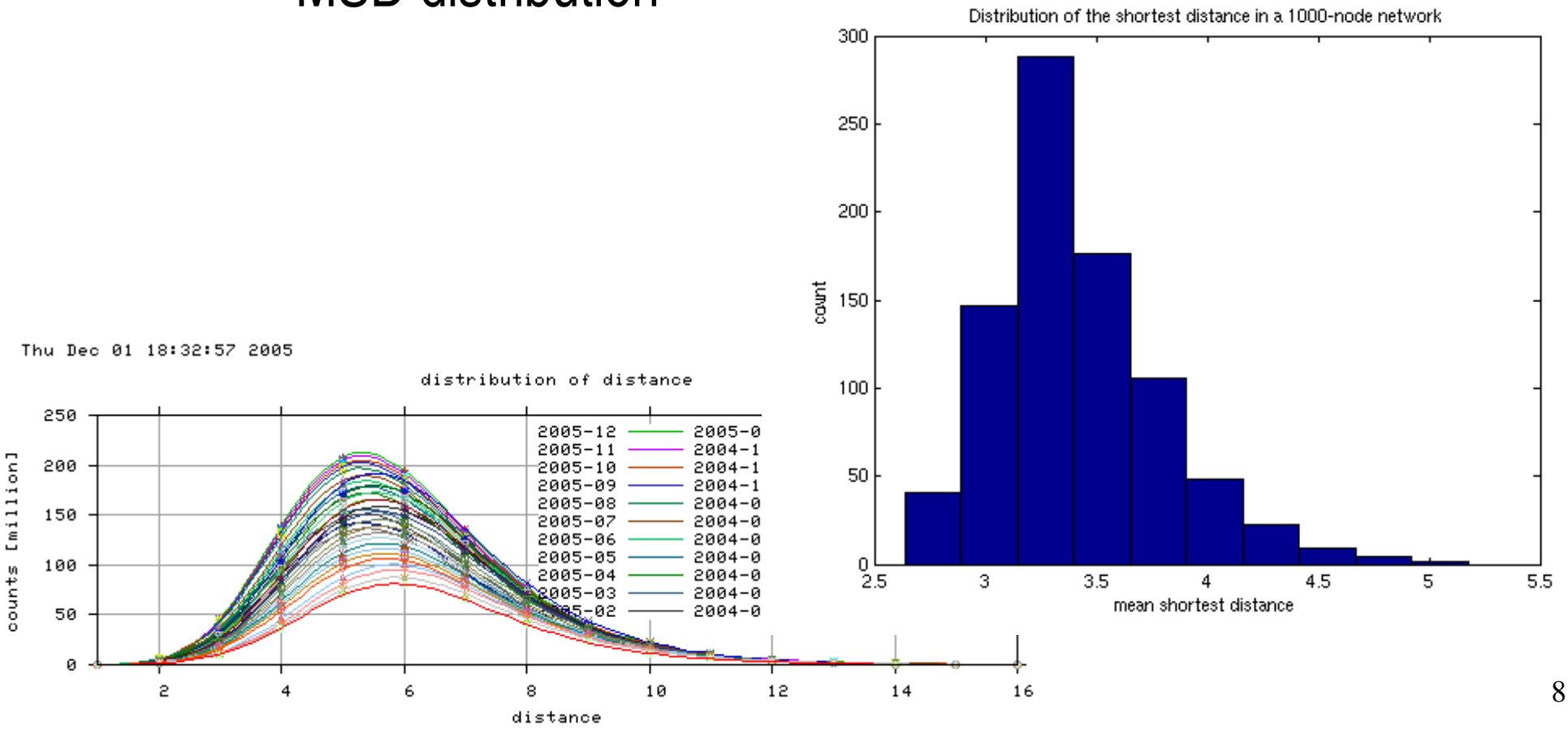
- **Scale Free network behavior**





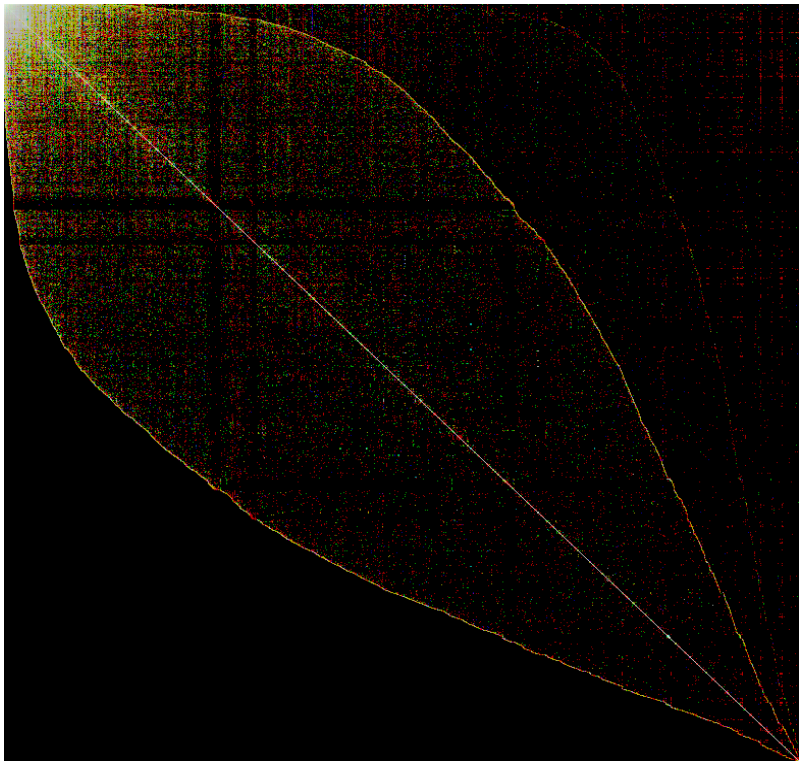
Model validity

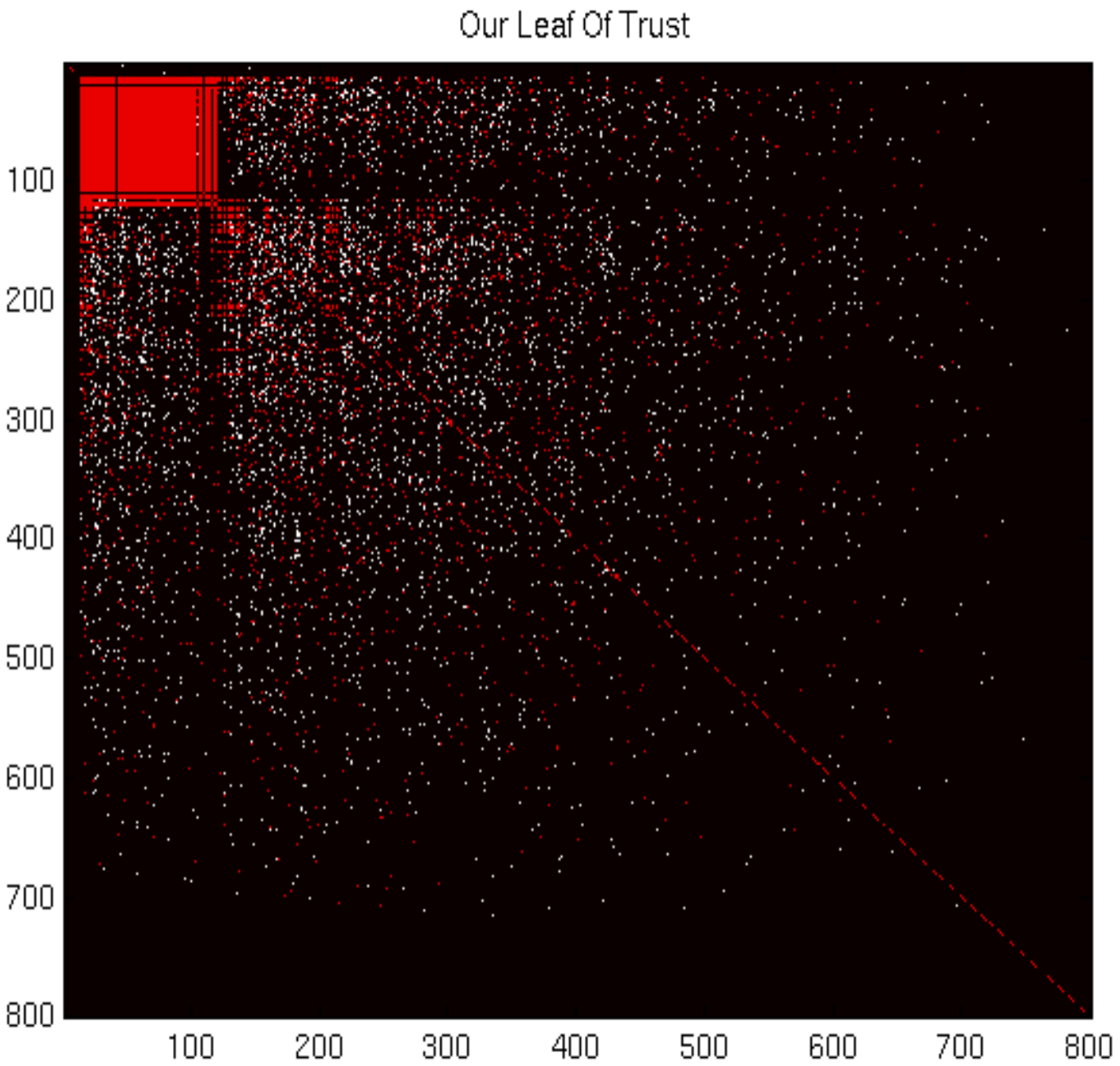
- **Scale Free network behavior**
  - whole average path length
  - MSD distribution

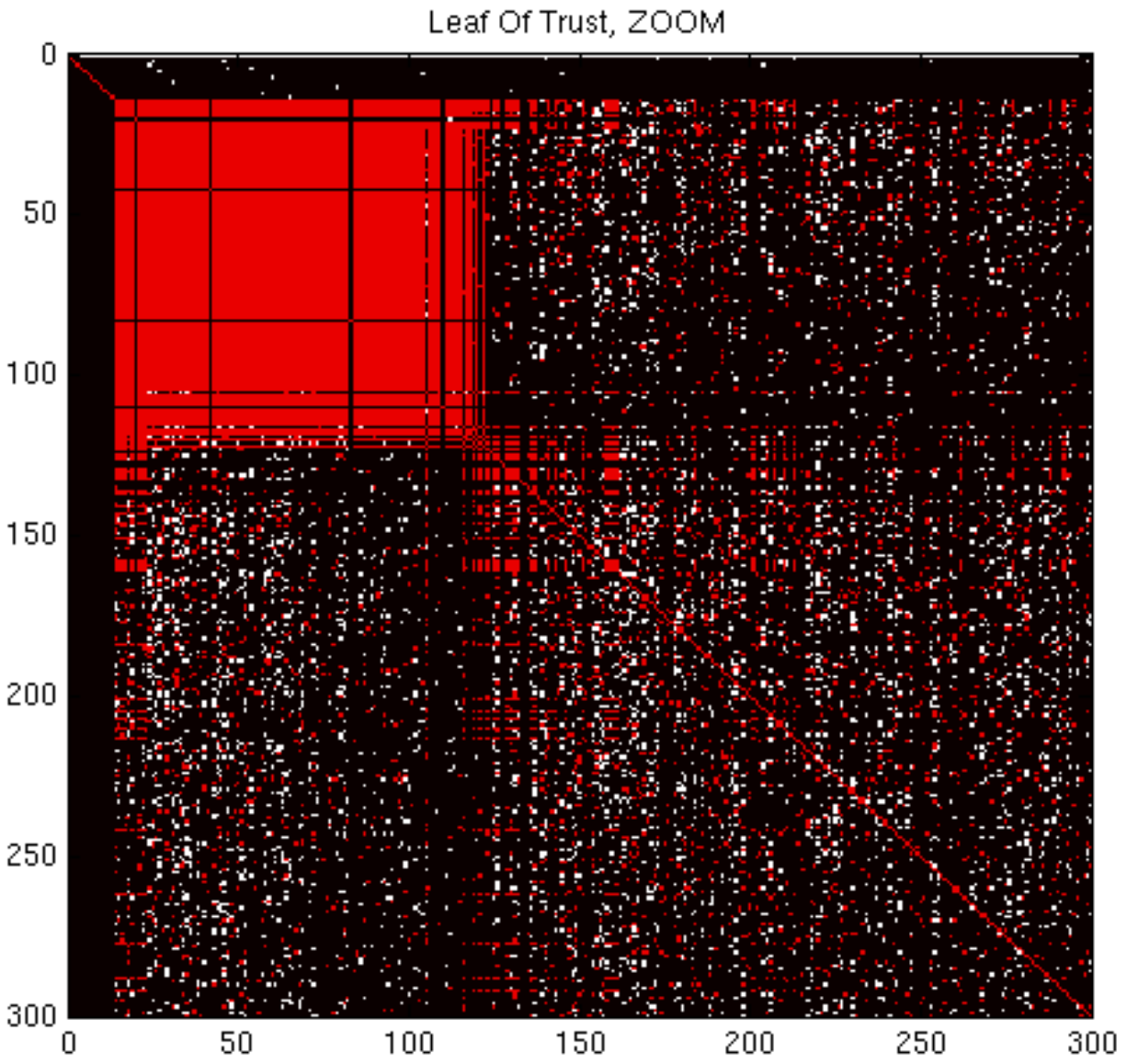


Model validity

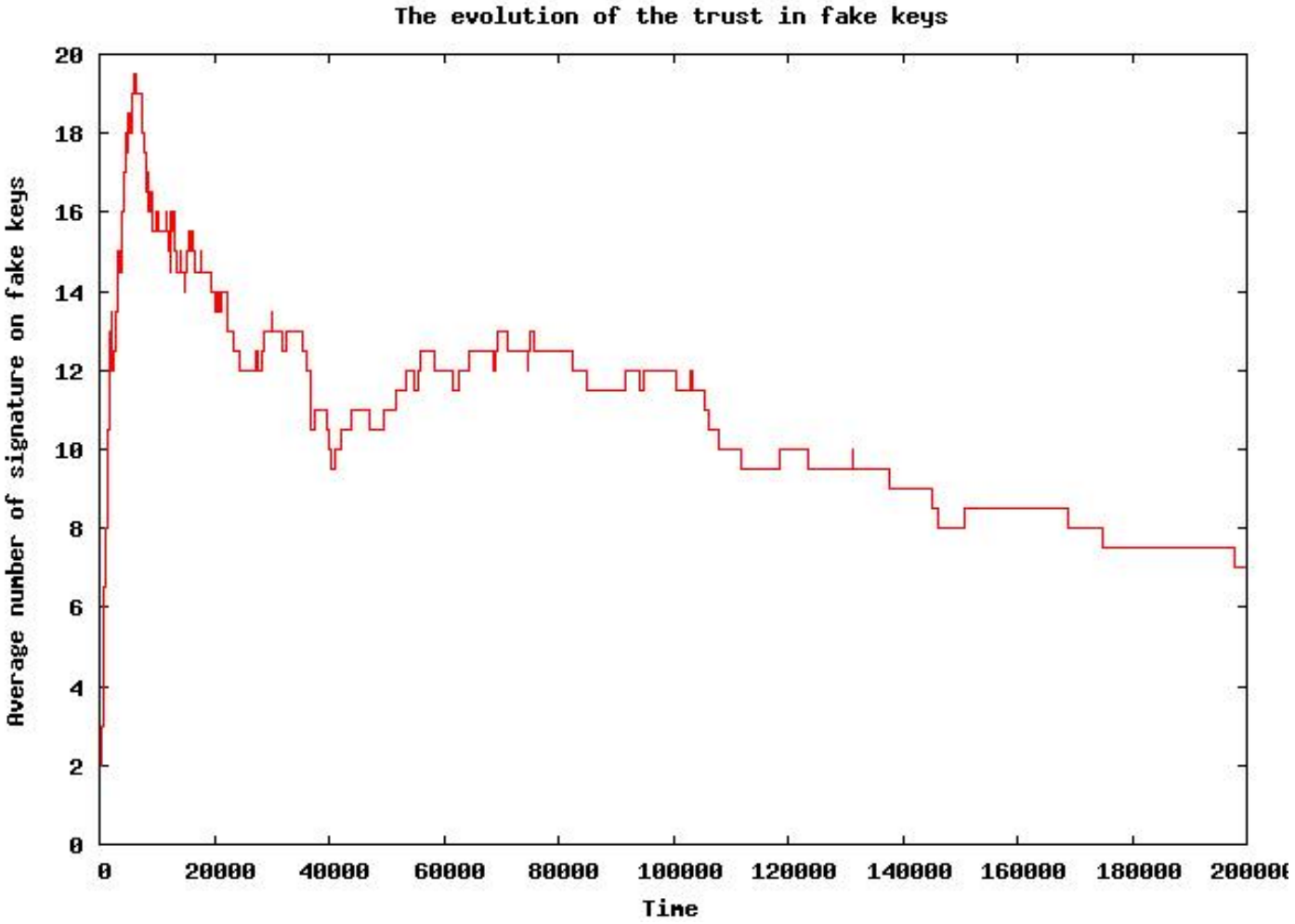
- **Leaf Of Trust**
  - Graph sorted by MSD




Our Leaf Of Trust
100
200
300
400
500
600
700
800
100
200
300
400
500
600
700
800


Leaf Of Trust, ZOOM
0
50
100
150
200
250
300
0
50
100
150
200
250
300

Rumor Spreading



Rapid growth in the trust in false keys at first

- Influence of the laxists agents
- Influence of the initial signature

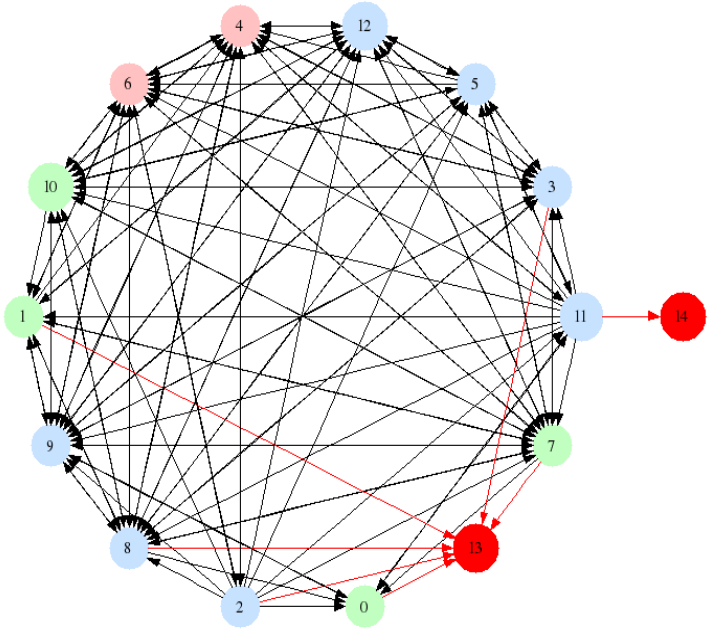
•Signing party effect

- Real agents are known

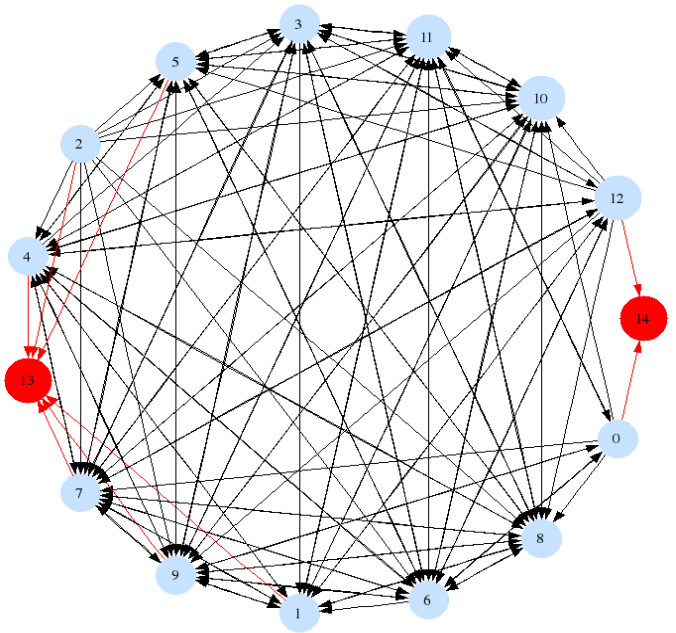
•Time

- More and more agents tend to meet the real one

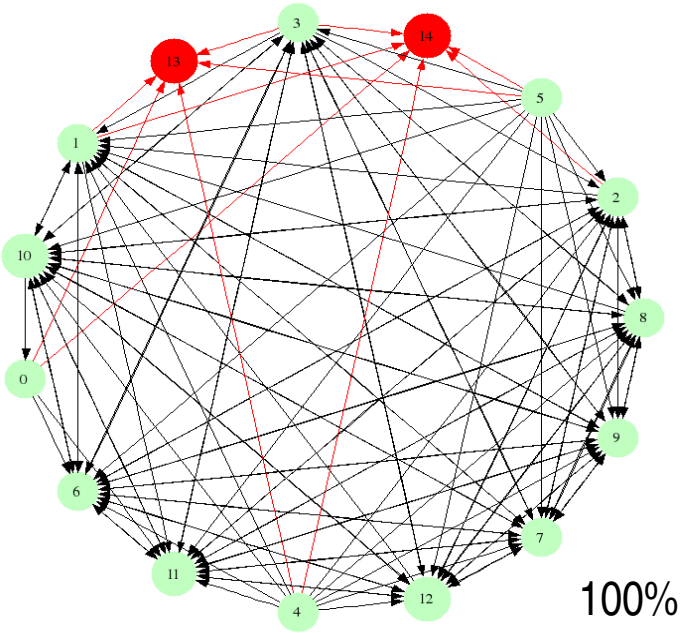
Some small networks



1/3 each



100% prudent



100% laxist

References

- **Analysis of the strong set in the PGP web of trust**
  - Henk P. Penning
  - http://www.cs.uu.nl/people/henkp/henkp/pgp/pathfinder/plot/
- **Dissecting the leaf of trust**
  - Jörgen Cederlöf
  - http://www.lysator.liu.se/~jc/wotsap/leafoftrust.html

Questions ?