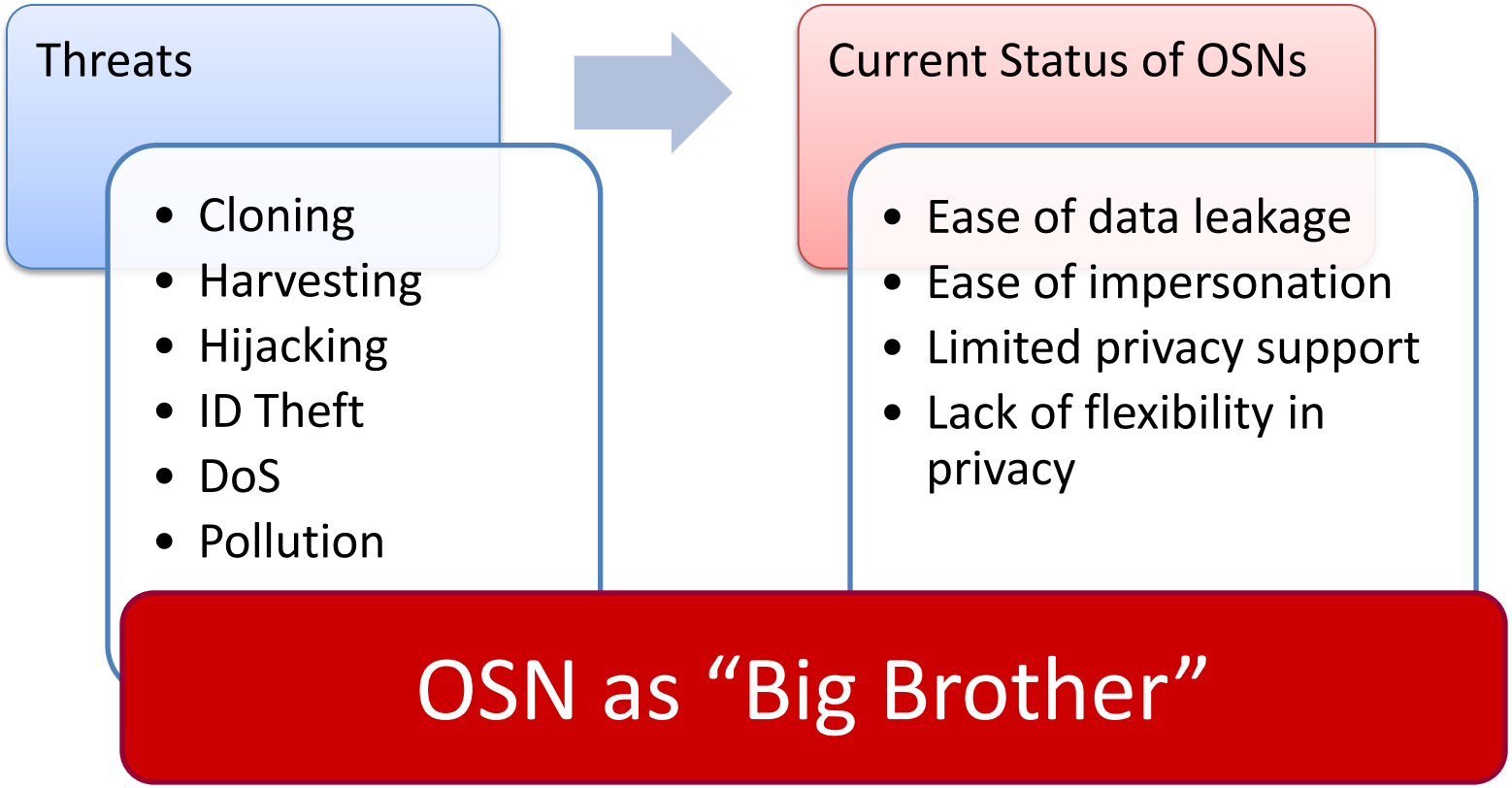
Leveraging Social Links for Trust and Privacy

Antonio Cutillo, Refik Molva, Melek Önen, Thorsten Strufe
EURECOM
Sophia Antipolis
refik.molva@eurecom.fr

Security and privacy issues in OSNs



The “Big Brother” problem with OSN

- Privacy protection against
  - Intruders
  - Crawlers
  - Third parties

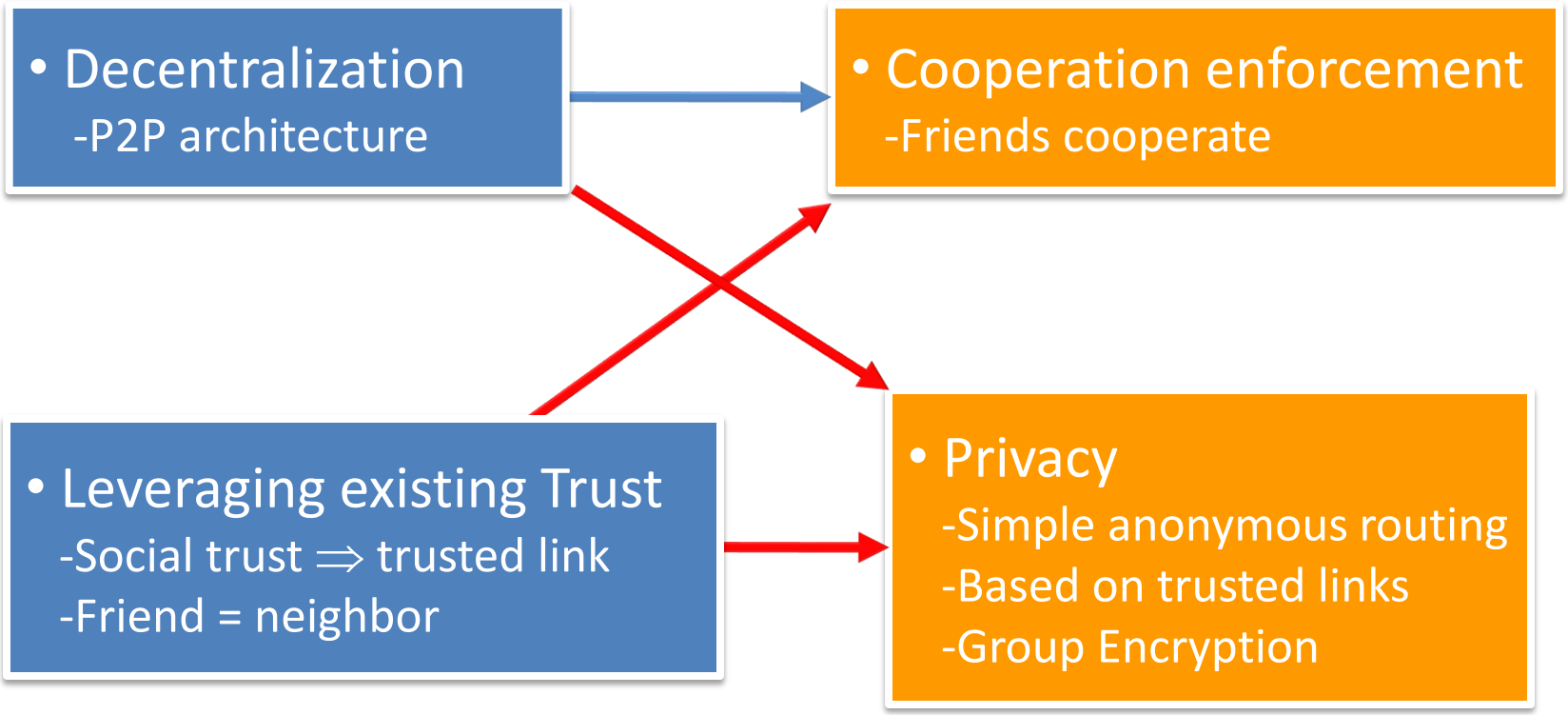
Does not prevent Application Server from disclosing/exploiting your data

All existing OSN suffer from it!

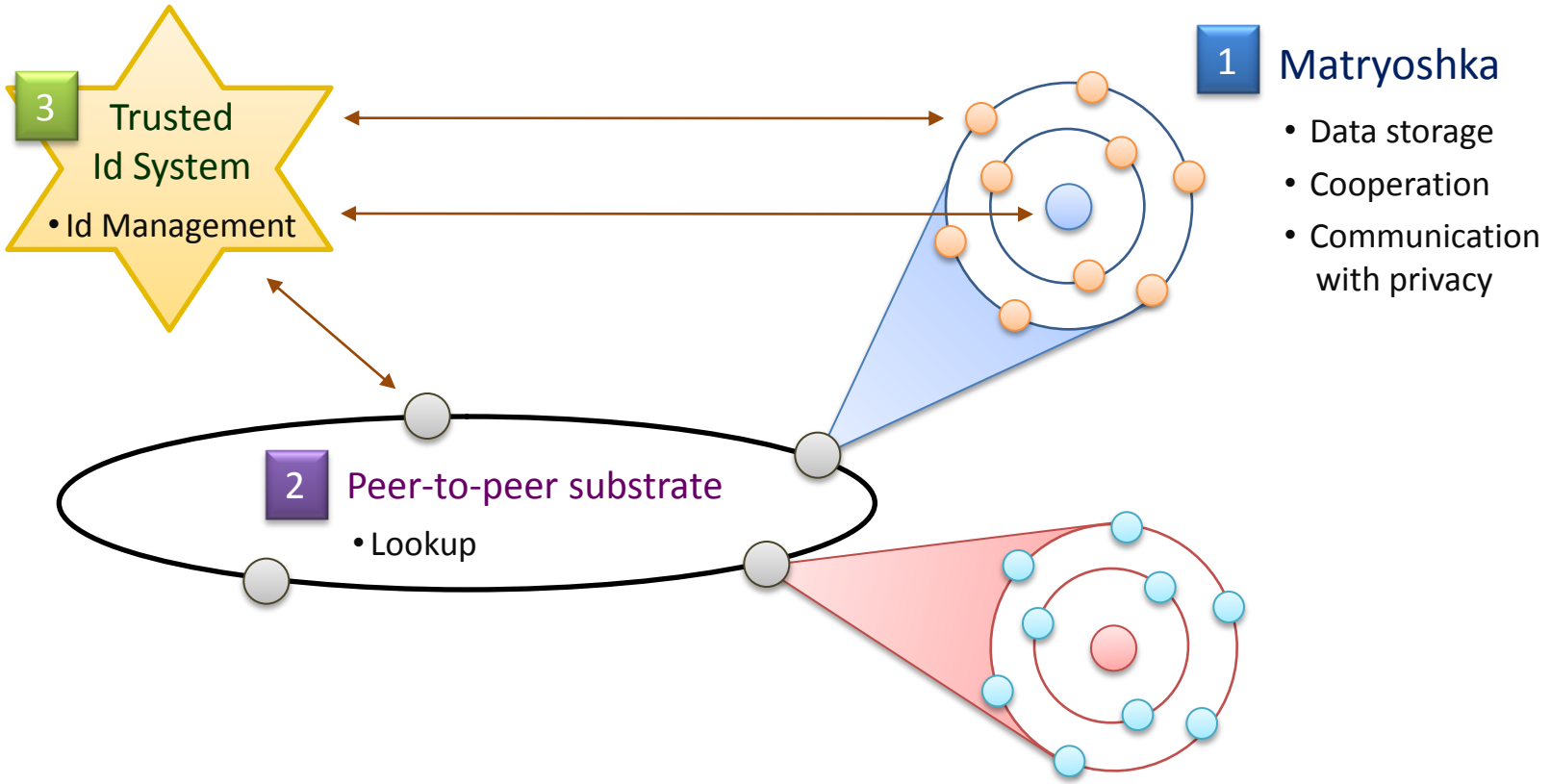
The “Big Brother” problem

- OSNs market value is increasing
  - 580 million US$ ➡ myspace (2005)
  - 15 billion US$ ➡ Facebook (2007)
- Do users actually care about privacy?

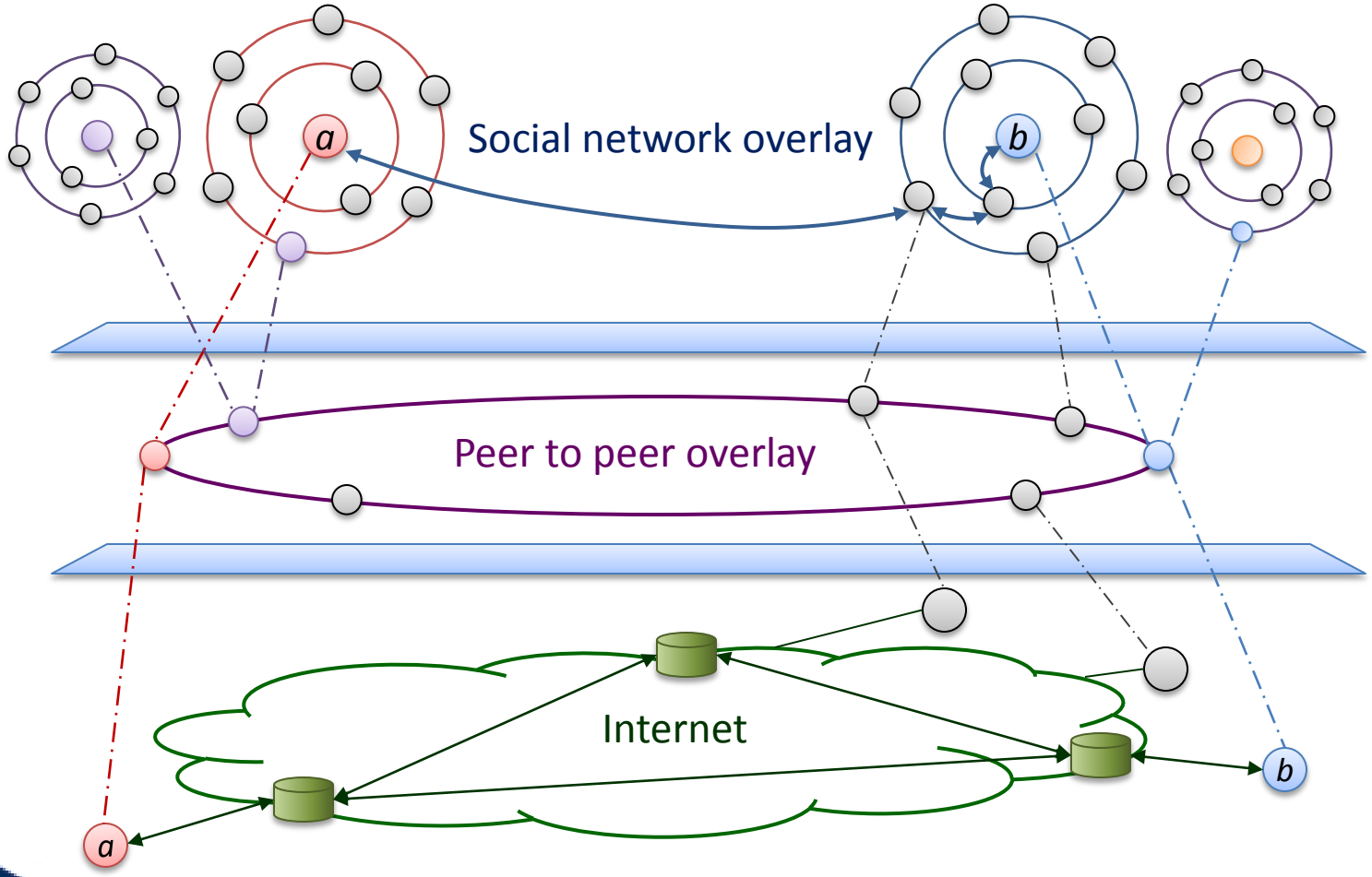
Safebook - Design Principles



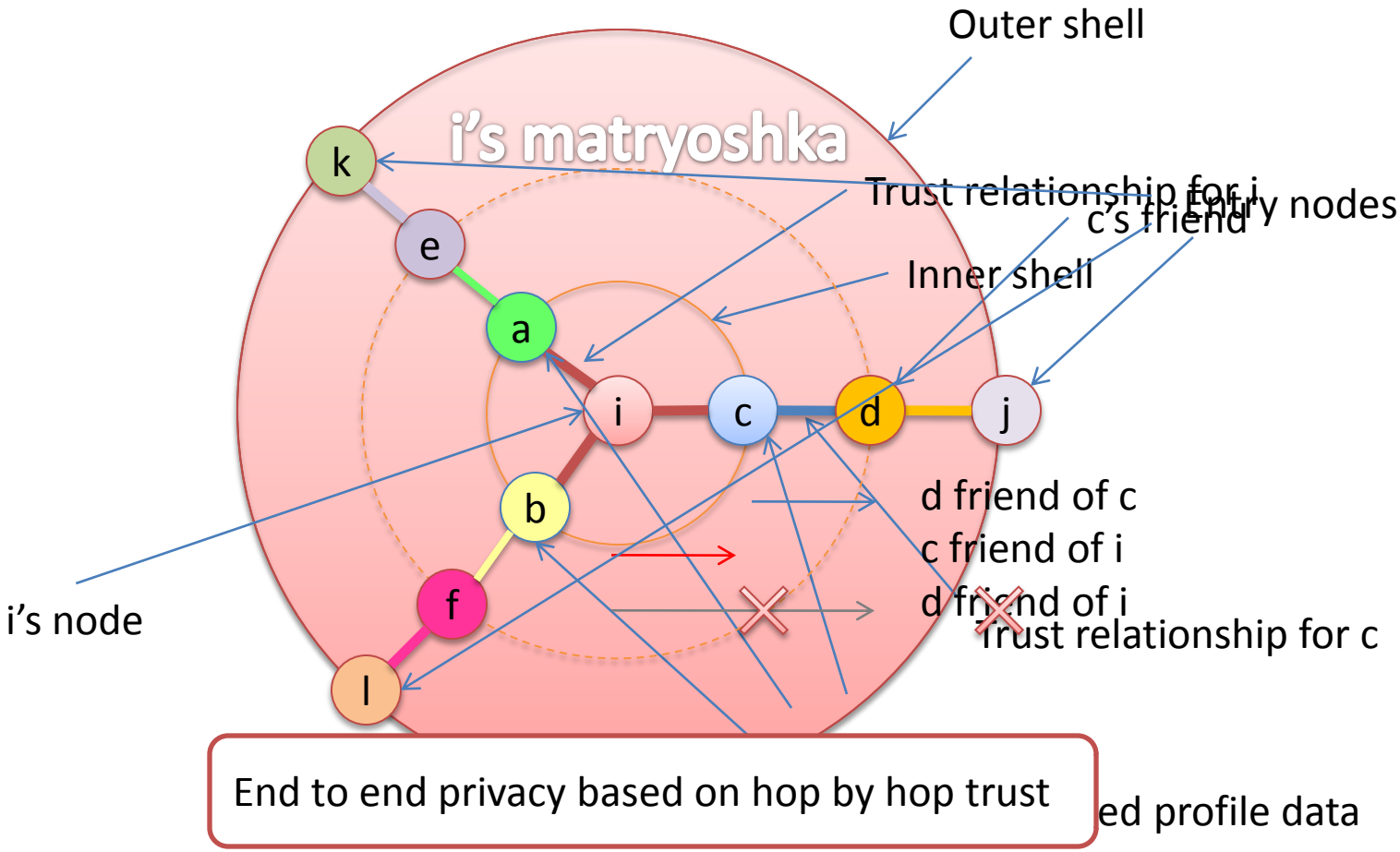
Safebook - Components



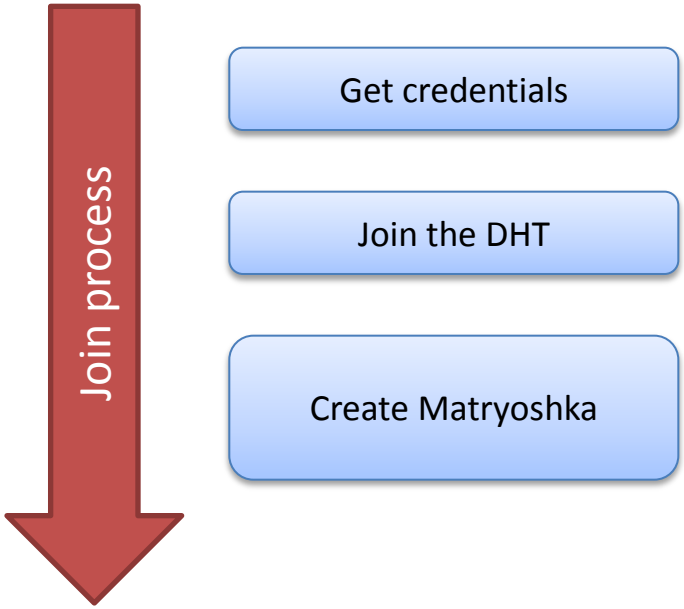
Safebook - Overlays



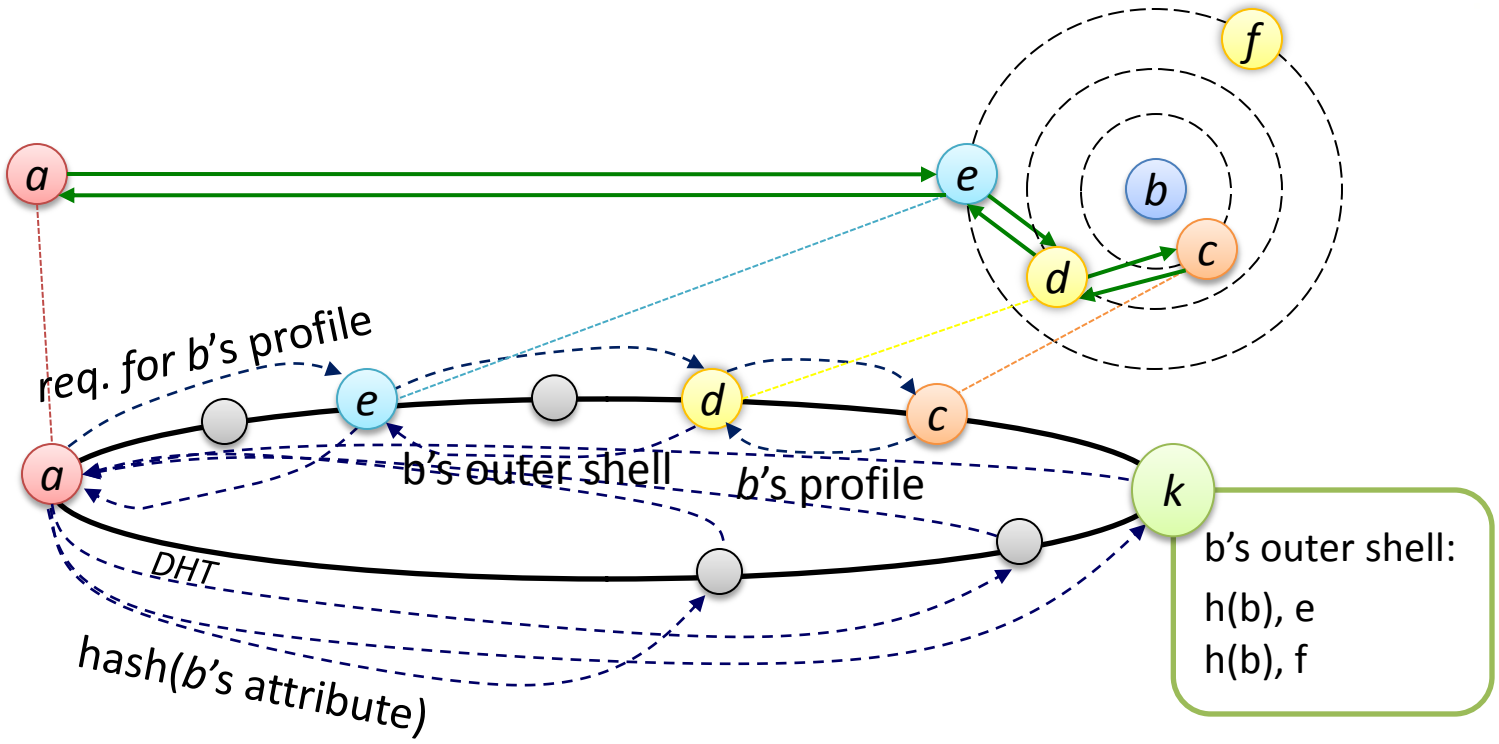
Safebook - Matryoshka



User Registration



a looks for *b*



lookup

- *a* looks for *b*'s entry nodes
- *k* provides *b*'s outer shell nodes

data request

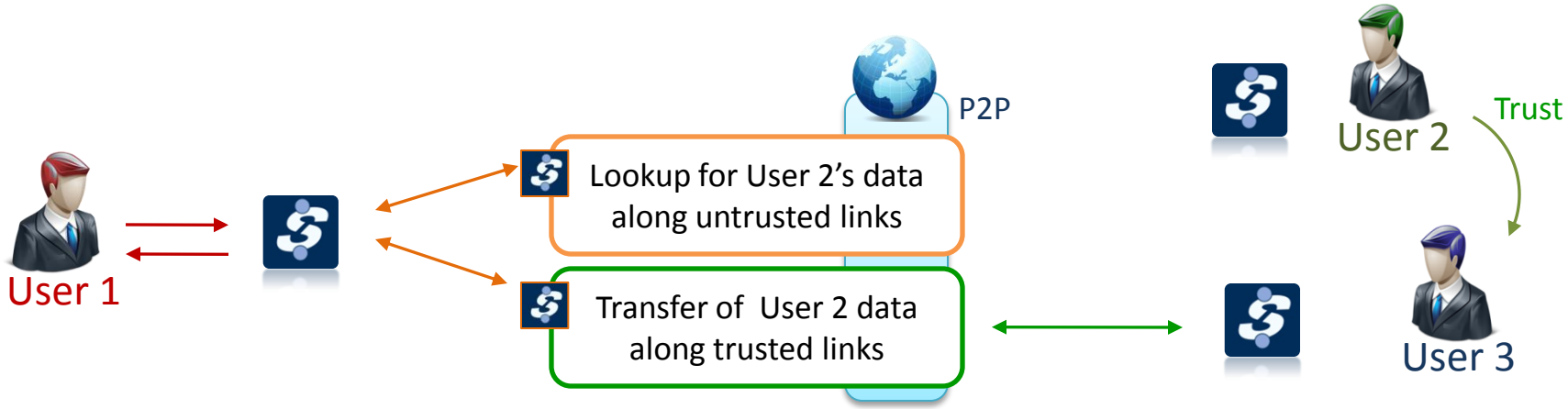
- *a* sends profile data request to an entry node serving b

Data reply

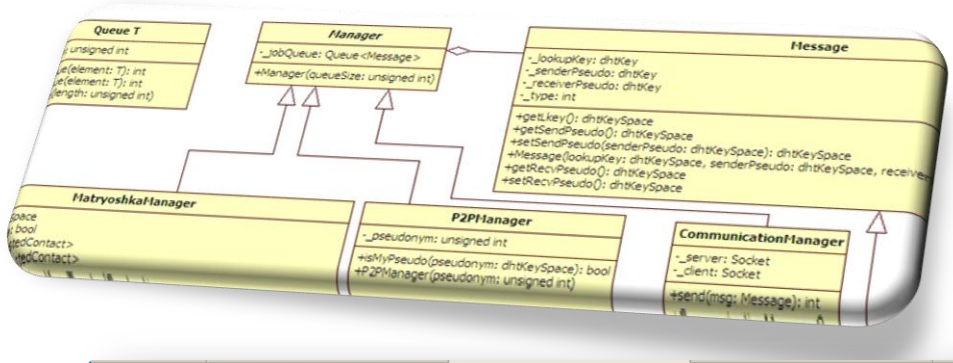
- One of b's inner shell nodes answers

Data retrieval

- User 1 wants to get User 2's profile data
- User 2's data is stored by User 3



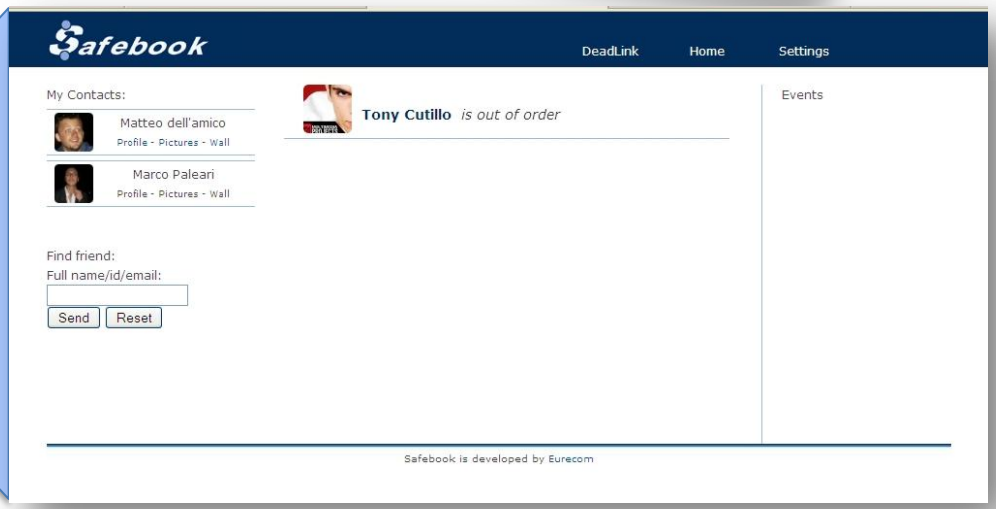
Safebook Prototype



Safebook = Resident Program

User

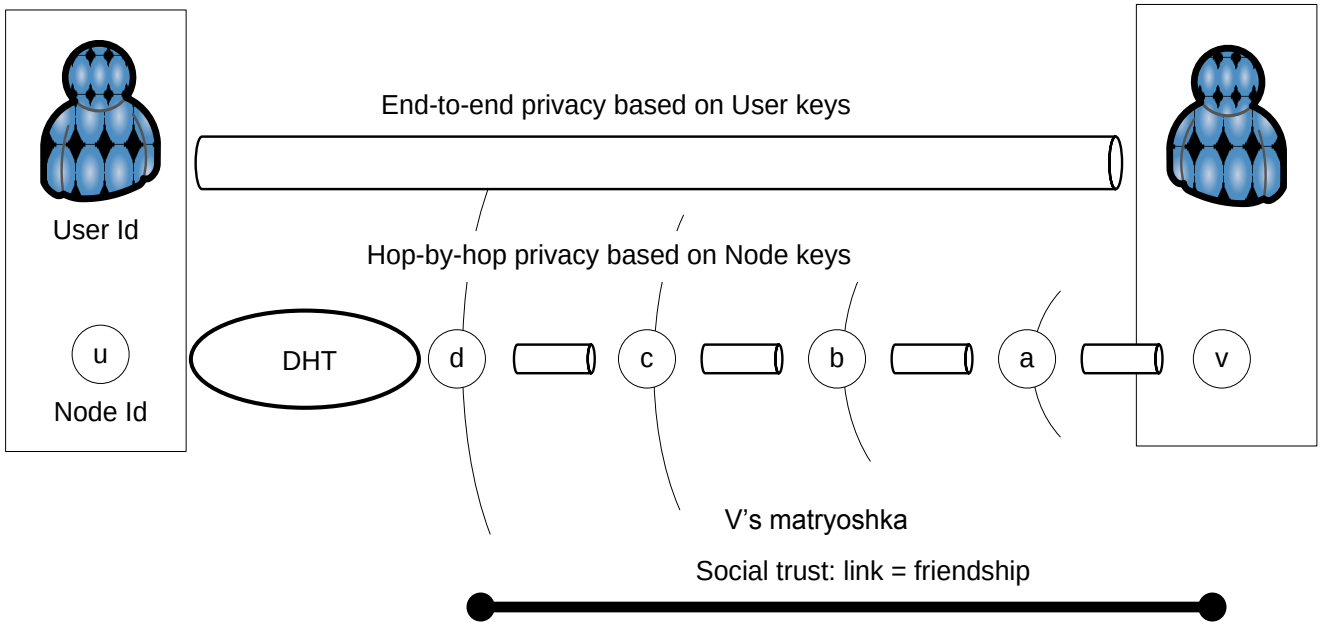
- User interface
- Trust logic
- Data interface
- P2P logic
- Encryption logic
- Communication Interface



http://localhost:8080

Privacy by Design

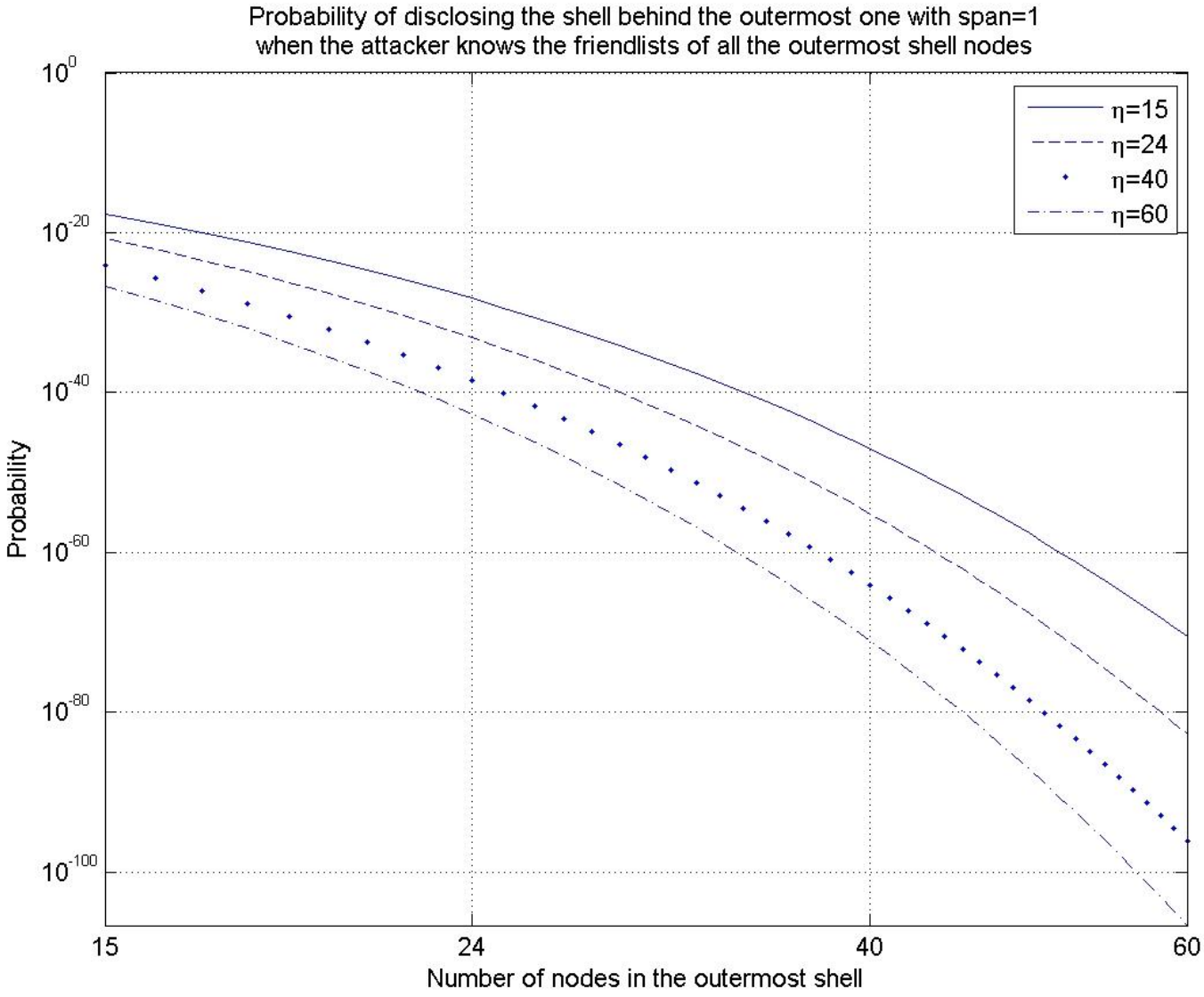
- Privacy through layering
- Unlinkability of IDs across layers
- Anonymous communication in matryoshkas



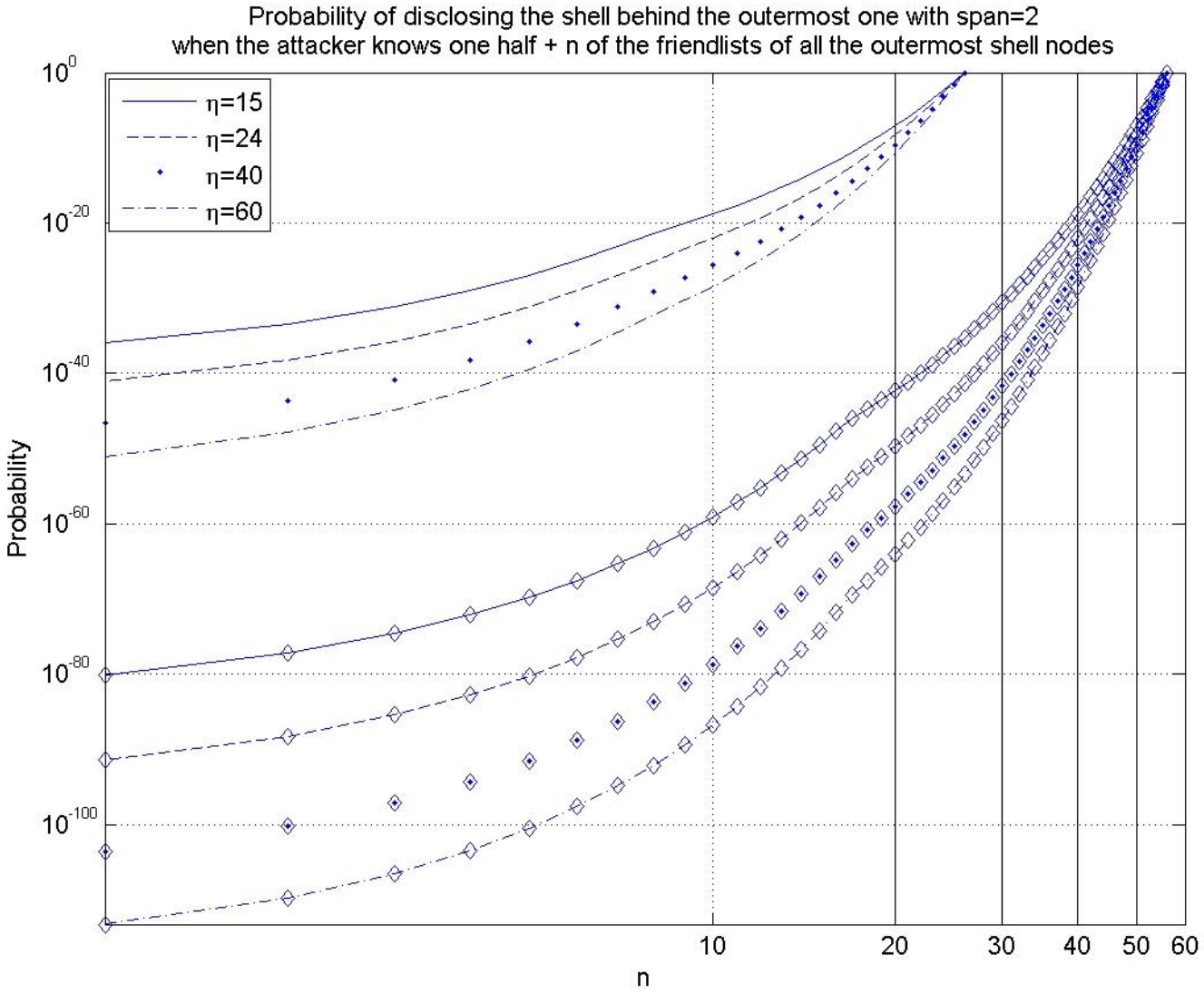
Security and Privacy

- Privacy
  - Friendship relations hidden through Matryoshkas
  - Untraceability - pseudonymity and anonymous routing
- Cloning and DoS prevention – ID mgr
- Access control – data encryption and key management
- Availability - replication at friends' nodes

Guessing inner layers – Span = 1



Guessing inner layers - Span =2



Performance

P2P overlay

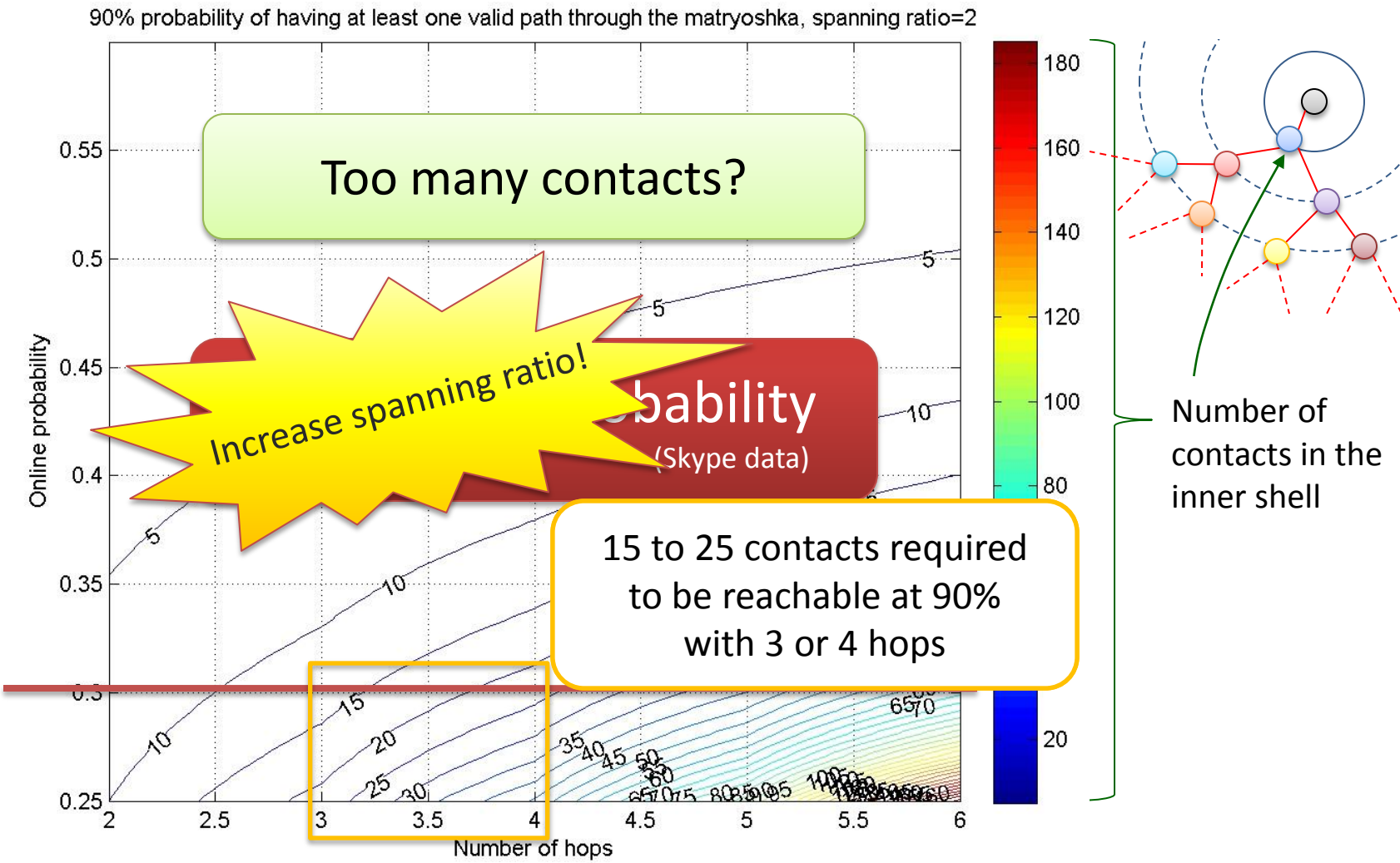
- Rely on existing studies

Matryoshka

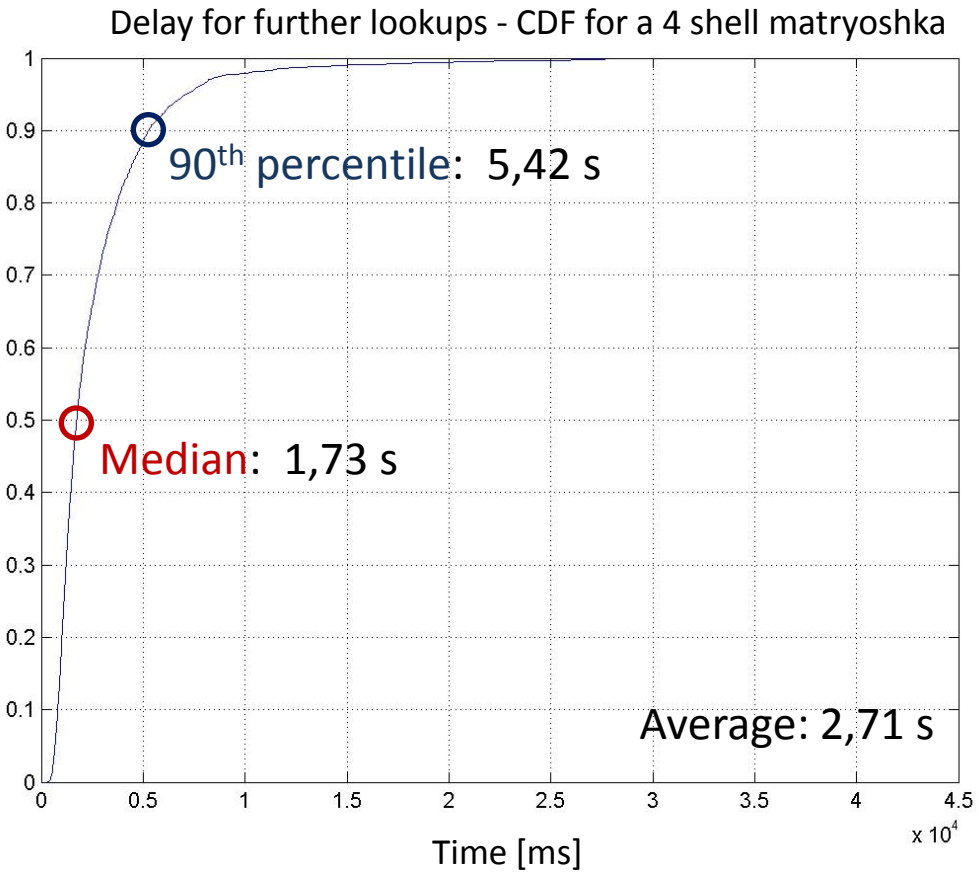
- End-to-end reachability/delay based on node liveness
- Analogy with P2P

Derive architectural parameters

Reachability



Delay



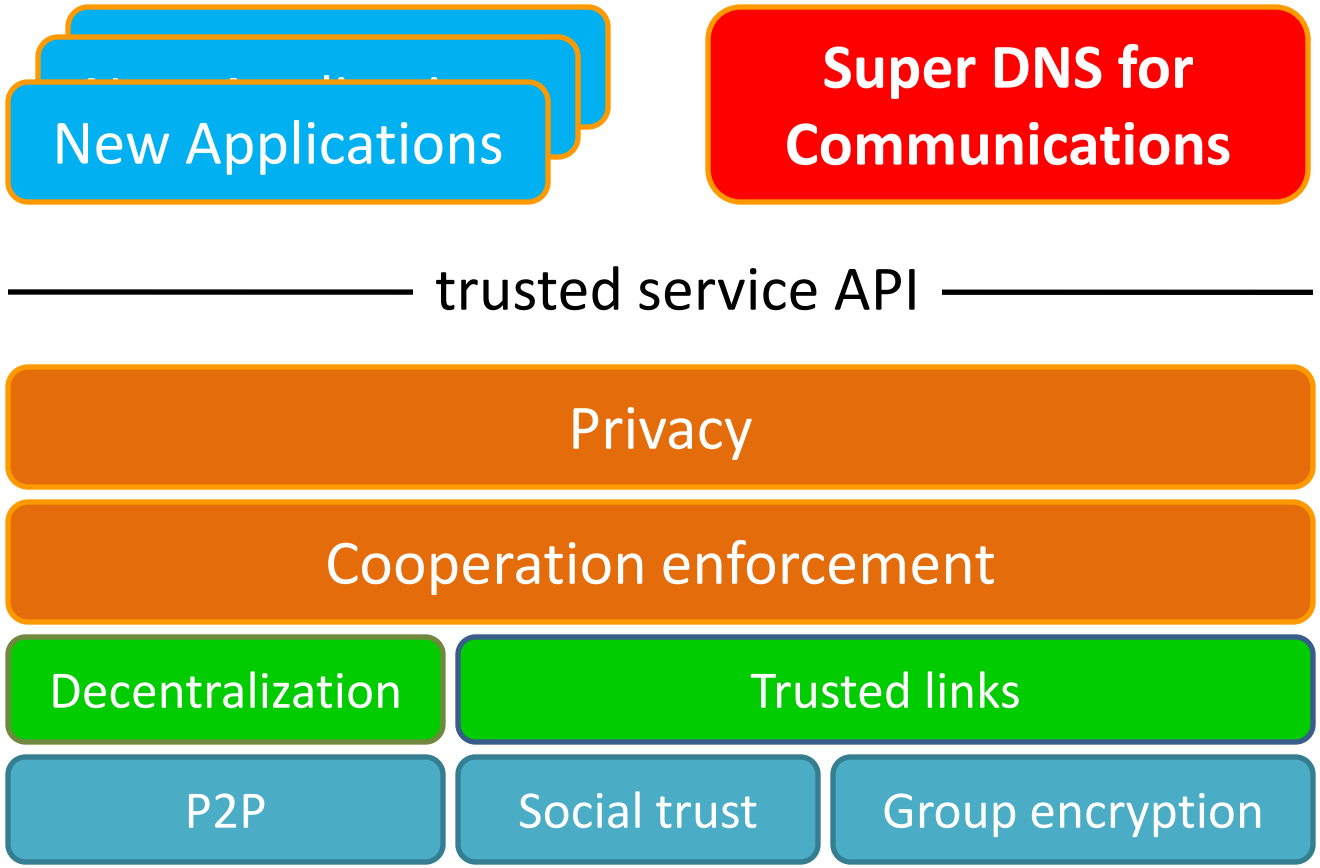
Total lookup time:

$T_{dl} = T_{DHT} + T_{Mat}$

- Further lookups: $T_{DHT}=0$ thanks to caching

(*) Data computed by applying the montecarlo sampling technique on single hop delay measurements and on delay measurement for a successful DHT key lookup in KAD

Safebook Summary



Publications

- Leucio Antonio Cutillo, Refik Molva, Thorsten Strufe
  Privacy preserving social networking through decentralization
  WONS 2009, 6th International Conference on Wireless On-demand Network Systems and Services, February 2-4, 2009, Snowbird, Utah, USA ,
- Leyla Bilge, Thorsten Strufe, Davide Balzarotti, Engin Kirda
  All your contacts are belong to us : automated identity theft attacks on social networks
  WWW'09, 18th Int. World Wide Web Conference, April 20-24, Madrid, Spain
- Leucio Antonio Cutillo, Refik Molva, Thorsten Strufe
  Leveraging Social Links for Trust and Privacy in Networks
  INetSec 2009, Open Research Problems in Network Security, April 23-24, 2009, Zurich, Switzerland
- Leucio Antonio Cutillo, Refik Molva, Thorsten Strufe
  Safebook: Feasibility of Transitive Cooperation for Privacy on a Decentralized Social Network
  3rd IEEE WoWMoM Workshop on Autonomic and Opportunistic Communications