Peer-to-Peer Systems and Security

IN2194

Dipl.-Inform. Heiko Niedermayer

Christian Grothoff, PhD
Prof. Dr.-Ing Georg Carle

Course organization IN2194

- Lecture
  - Monday, 10:15-11.45, MI 00.13.009A weekly
  - Thursday, 14:15-15.45, MI 00.13.009A first weekly, then typically bi-weekly
- Exercises
  - Typically bi-weekly Thursday, 14:15-15.45, MI 00.13.009A
- Students are requested to subscribe to lecture and exercises at www.net.in.tum.de ⇨lehre ⇨ vorlesungen ⇨ Informationen des Lehrstuhls

  http://www.net.in.tum.de/de/lehre/ss10/vorlesungen/vorlesung-peer-to-peer-systeme-und-sicherheit/
- Email list, svn access
  - for subscribers of course
- Questions and Answers / Office hours
  - Prof. Dr. Georg Carle, carle@net.in.tum.de
    - Upon appointment (typically Monday 16-17)
  - Heiko Niedermayer, niedermayer@net.in.tum.de
  - Christian Grothoff, Ph.D., grothoff@net.in.tum.de
- Course Material
  - Slides are available online. Slides may be updated during the course.

Grading

- Course is 5 ECTS
  - 3 SWS lectures
  - 1 SWS exercises

    including practical assignment (programming project)
- Exercises
  - ~5 exercise sheets
  - Prepare for the oral examination
  - Successfully participating at exercises gives a bonus of 0,3 for overall grade
- Practical assignment
  - will be graded
- Our concept for grading
  - Final examinations will be oral and give an individual grade.
    You must pass the oral exam for being successful in the course.
  - For overall grade, grade of practical assignment gives 20% of final grade

Questions

- Who studies what?
  - Diploma degree?
  - Master in Informatics?
  - Master in Information Systems [Wirtschaftsinformatik]?
  - Other Master courses?
  - Bachelor in Informatics?

- Which previous relevant courses?

Courses offered by I8

- Lectures

  SS:

  - Introduction to Computer Networking and Distributed Systems (IN0010)
  - Discrete Event Simulation (IN2045)

  WS:

  - Master Course Computer Networks (IN2097)
  - Network Security (IN2101)
- Seminars
  - Seminar – Network Architectures and Services: Network Hacking (IN0013)
  - Advanced Seminar - Innovative Internet Technologies and Mobile Communications (IN8901)
  - Advanced Seminar – Future Internet (IN8901)
  - Advanced Seminar – Sensor Networks(IN0014), with Prof. Baumgarten
- Lab Courses
  - Bachelor Practical Course - Internet Lab (IN0012)
  - Master Practical Course – Computer Networks (IN2106)

Motivation

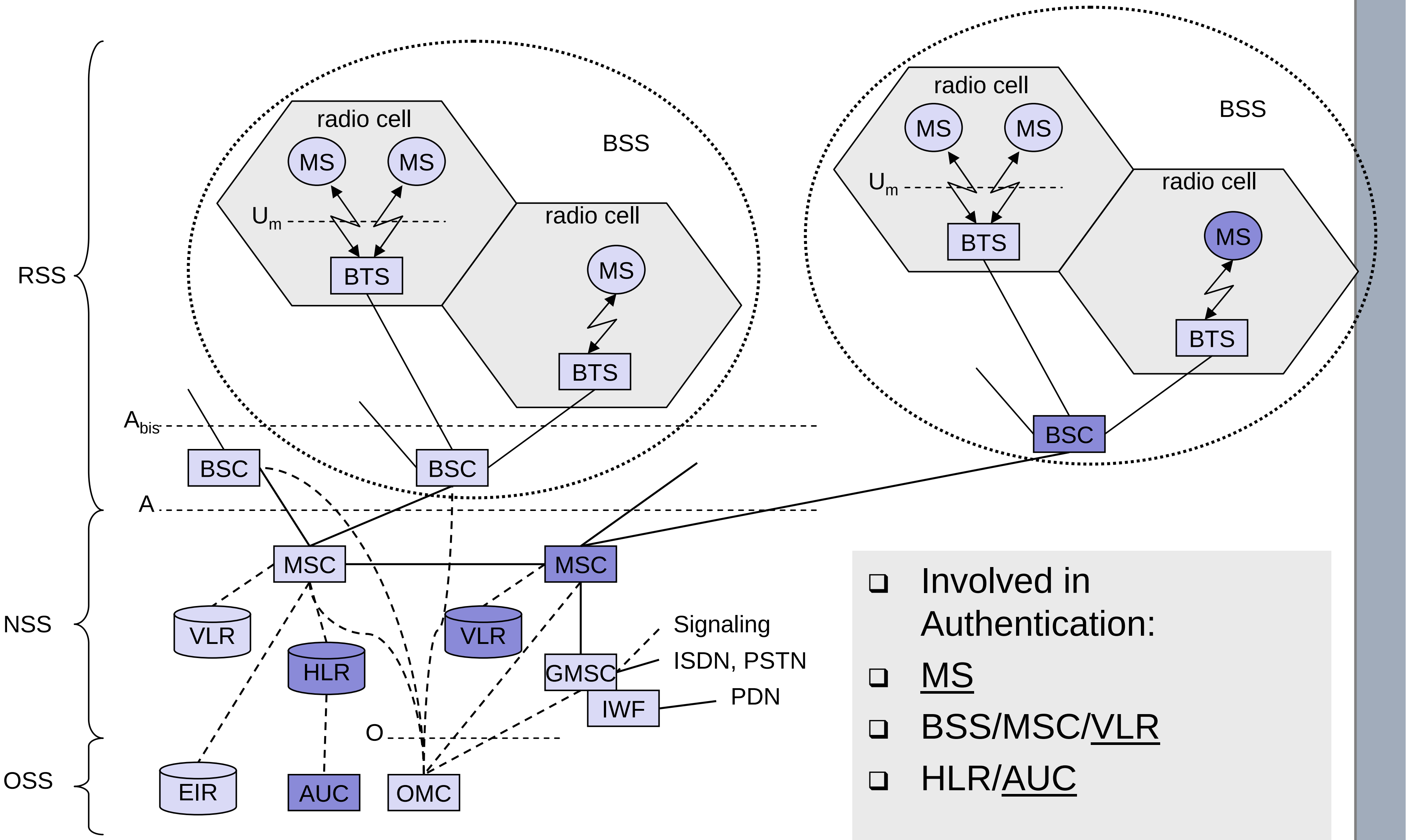
The power of P2P

Peer-to-Peer Systems

Very popular due to file-sharing
Responsible for majority of the traffic of the Internet!

- ❑ Network of equals (peers)
  - ⇨Users can offer new services
- ❑ Users and their computers at the edges of the Internet share their resources (bandwidth, CPU, storage).
  - ⇨Inherent scalability with growing
- ❑ Self-organization of the system
  - ⇨No traffic management
- ❑ Autonomy from central entities like central servers
  - ⇨Robustness

Architecture of a Telecommunication Network (GSM)



- ❑ Involved in Authentication:
- ❑ MS
- ❑ BSS/MSC/VLR
- ❑ HLR/AUC

GSM

Some GSM Components

AUC	Authentication center
BSC	Base station controller
BSS	Bas station system
BTS	Base transceiver station
IMSI	International mobile subscriber identity
HLR	Home location register
LAI	Location area identifier
MS	Mobile station (e.g. a mobile phone)
MSC	Mobile switching center
MSISDN	Mobile subscriber international ISDN number
TMSI	Temporary mobile subscriber identity
VLR	Visitor location register

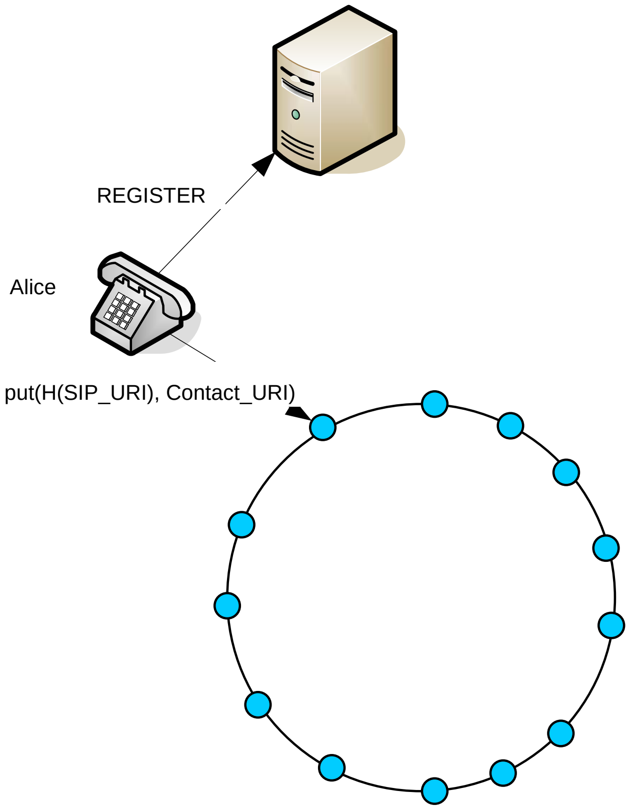
Challenge: Availability / Resilience

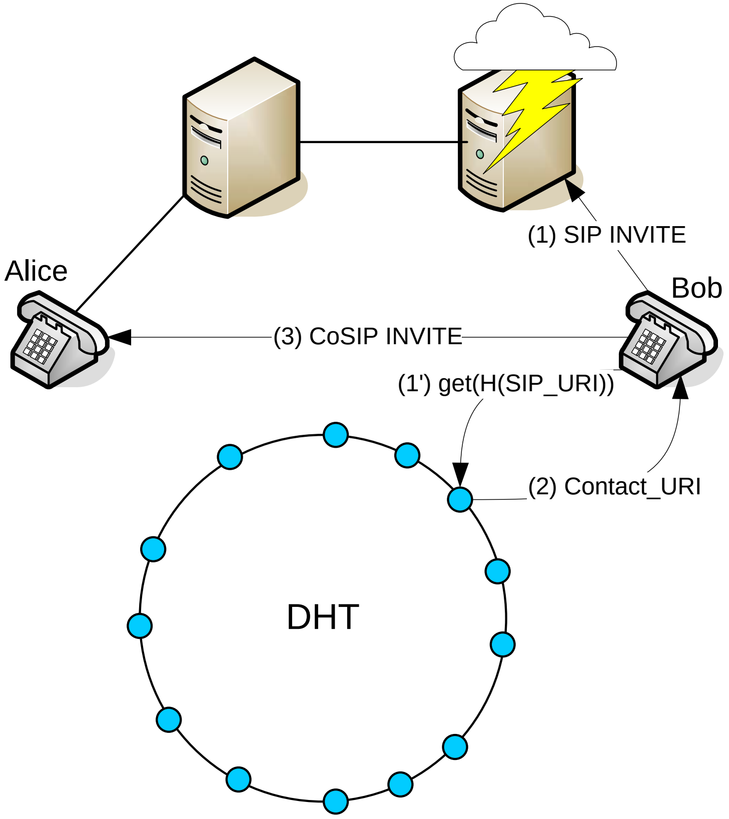
Related Research Activities at the Chair I8

- Goal:
  - Improve the resilience/security of network services
  - using the Peer-to-Peer networking paradigm
  - taking Voice over IP (VoIP) as an example

Cooperative SIP (CoSIP)

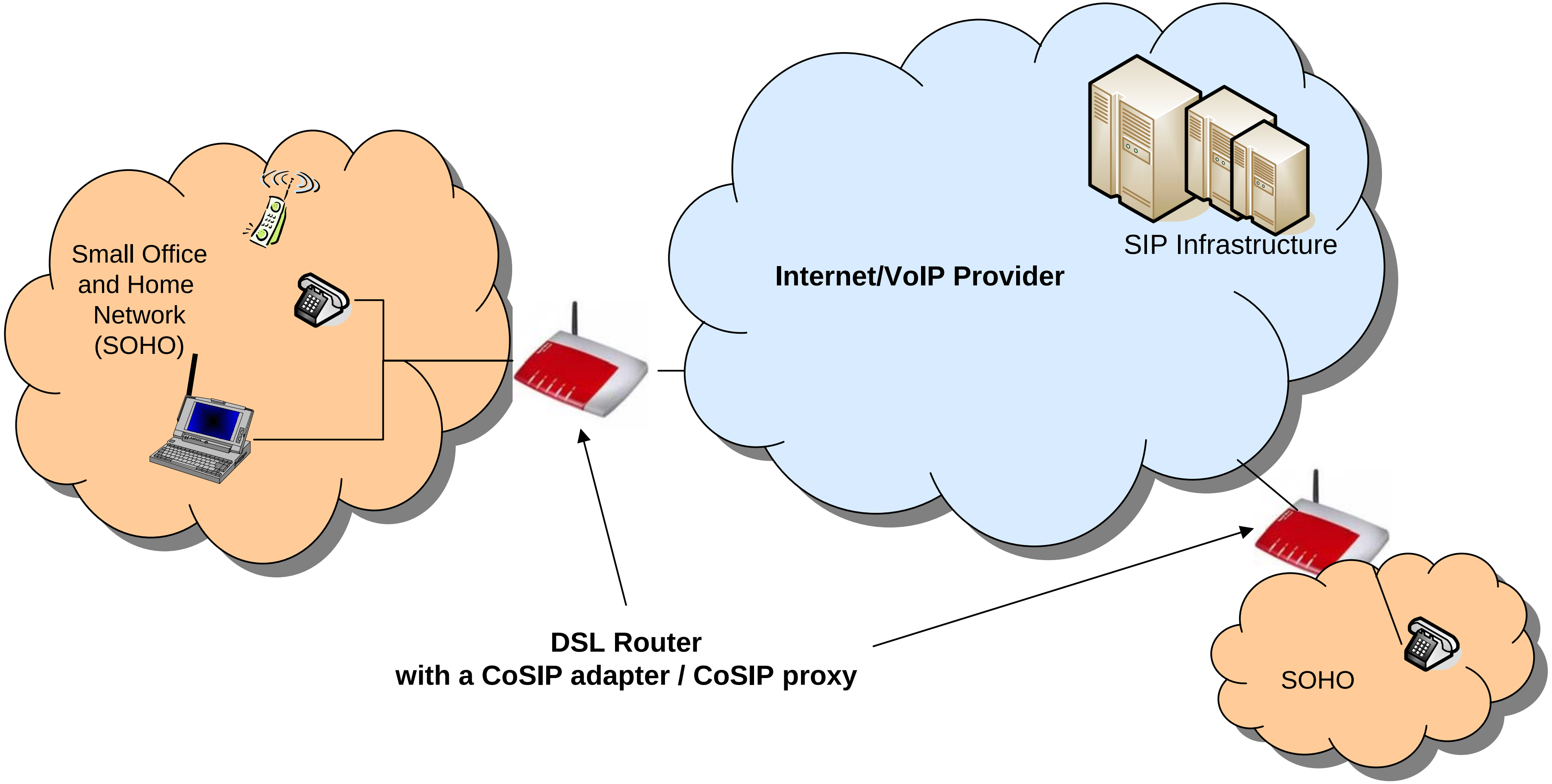
- User registration with CoSIP
- Session establishment with CoSIP





Application of CoSIP in the fixed network

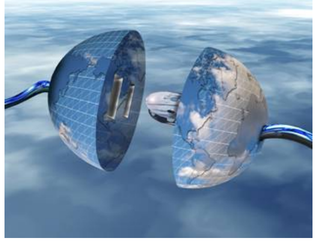
- CoSIP adapter/ proxy in DSL routers
- CoSIP adapters organize themselves into a P2P network



EU FP7 Projekt ResumeNet

- "Resilience and Survivability for future networking: framework, mechanisms, and experimental evaluation"

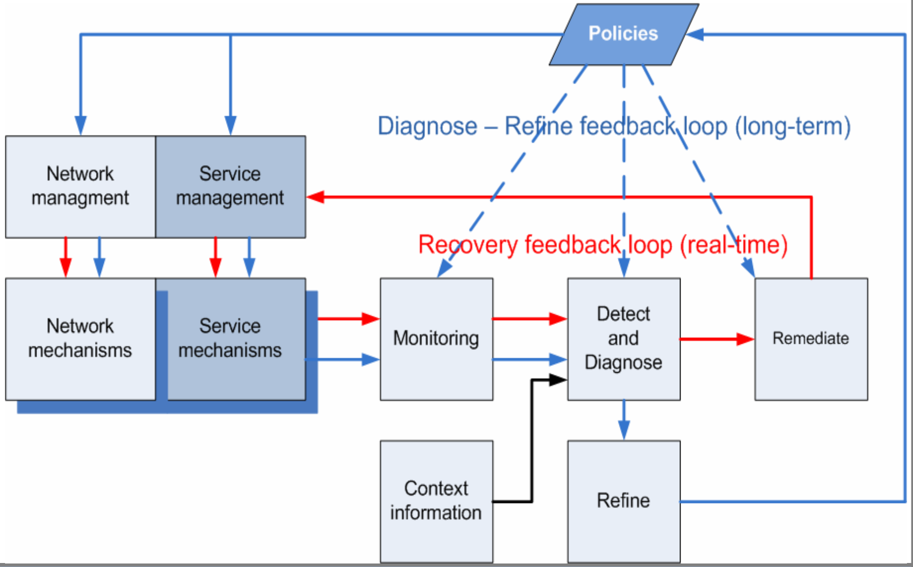
- A EU Project of the FIRE Research Programme („*Future Internet Research and Experimentation*")



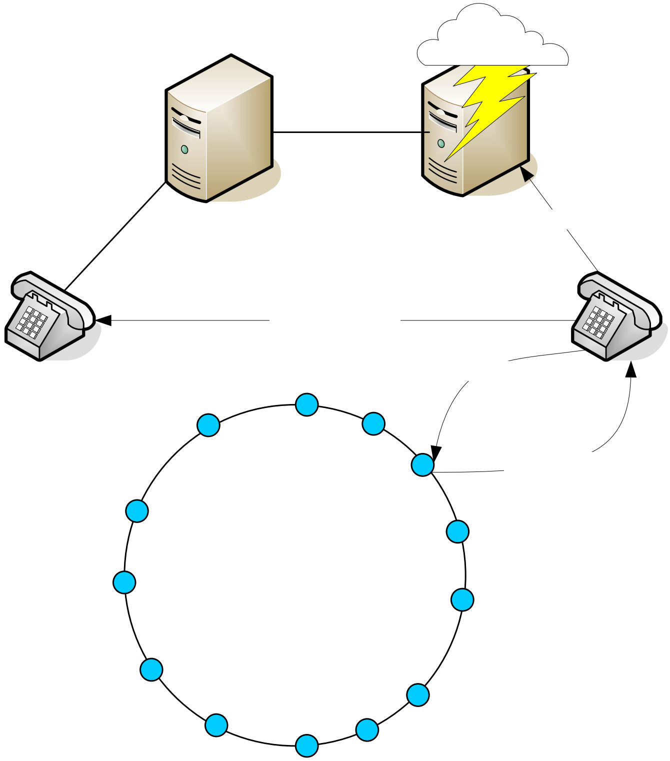
- Consortium:

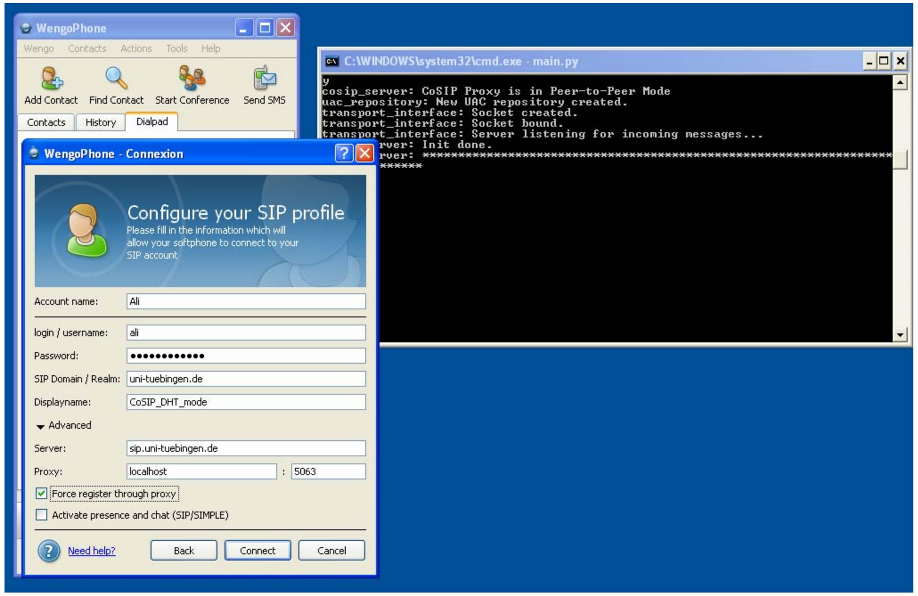
ETH Zürich	Switzerland
Lancaster University	United Kingdom
Technical University Munich	Germany
France Telecom	France
NEC Europe Ltd	United Kingdom
Universität Passau	Germany
Technical University Delft	Netherlands
Uppsala Universitet	Sweden
Université de Liège	Belgium

- Strategy: D^2R^2DR



Robust Service Provisioning (Service Resilience)





Configure your SIP profile

Please fill in the information which will allow your softphone to connect to your SIP account

Account name: Ali

login / username: ali

Password: ●●●●●●●●●●●●●

SIP Domain / Realm: uni-tuebingen.de

Displayname: CoSIP_DHT_mode

Advanced

Server: sip.uni-tuebingen.de

Proxy: localhost : 5063

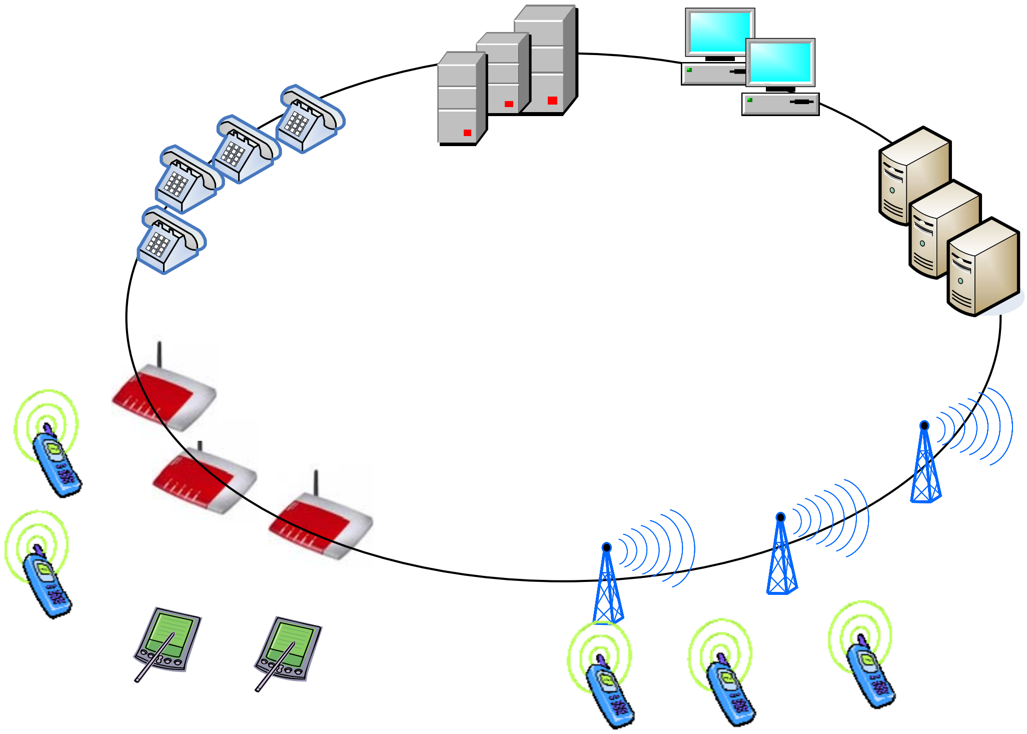
☑ Force register through proxy

☐ Activate presence and chat (SIP/SIMPLE)

```
y
cosip_server: CoSIP Proxy is in Peer-to-Peer Mode
uac_repository: New UAC repository created.
transport_interface: Socket created.
transport_interface: Socket bound.
transport_interface: Server listening for incoming messages...
rver: Init done.
rver: ***************************************************************
******
```

Robust Service Provisioning (2)

- Approach:
  - Hybrid p2p overlay network
  - Peers with different roles, verifyable identity, virtualisation
- Goal:
  - Cooperation of end nodes and infrastructure
    for high reliability, service quality, scalability



Further selected research at I8– Network Architectures and Services

Projektschwerpunkte

	Autonomic / Self-Org. Man.	Mobile comm.	Measure-ments	P2P and Overlays	Netzwork Security
EU ResumeNet	☑			☑	☑
EU AutHoNe	☑	☑	☑	☑	☑
DFG LUPUS			☑	☑	☑
BMBF ScaleNet	☑	☑	☑		
NSN SelfMan	☑		☑		
NSN TC-NAC		☑			☑
France-Telecom SASCO	☑	☑		☑	☑
BWFIT SpoVNet			☑	☑	☑
BWFIT AmbiSense		☑	☑		

AutHoNe - Autonomic Home Networking

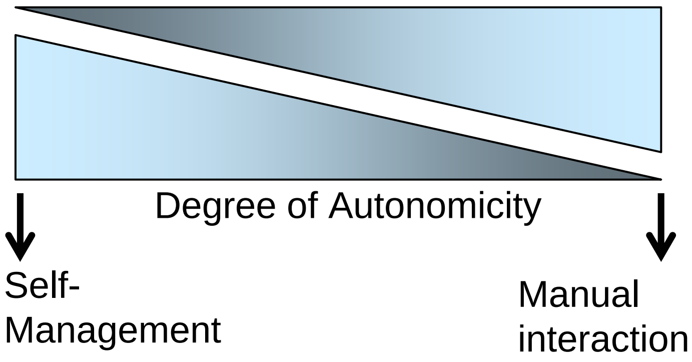
- EUREKA-Celtic/BMBF-Project

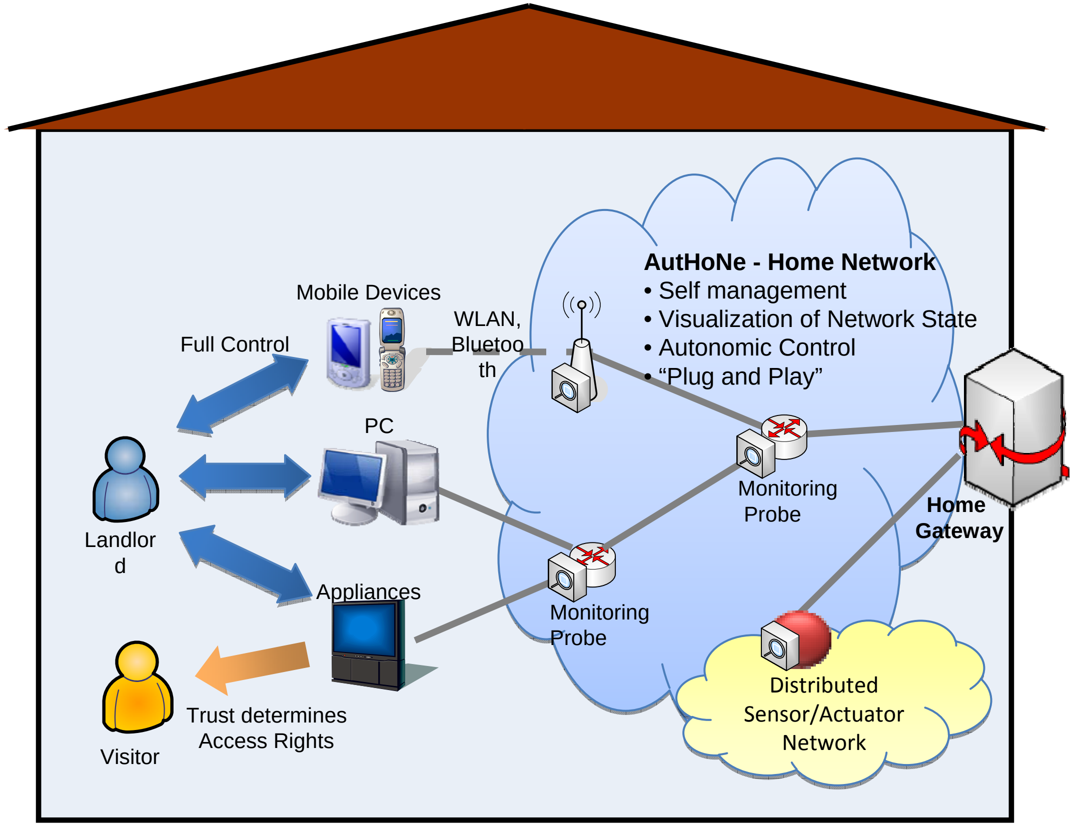
- Partner in Germany
  - TU München
  - Fraunhofer FOKUS
  - Siemens Corporate Technology
  - Hirschmann Automation and Control

- EU/Celtic Partner
  - France Telecom, Frankreich
  - Sony-Ericsson, Schweden
  - Ginkgo Networks, Frankreich
  - Univ. Pierre et Marie Curie, Paris (UPMC-LIP6), Frankreich
  - Universität Lund, Schweden

Autonomic Home Networks

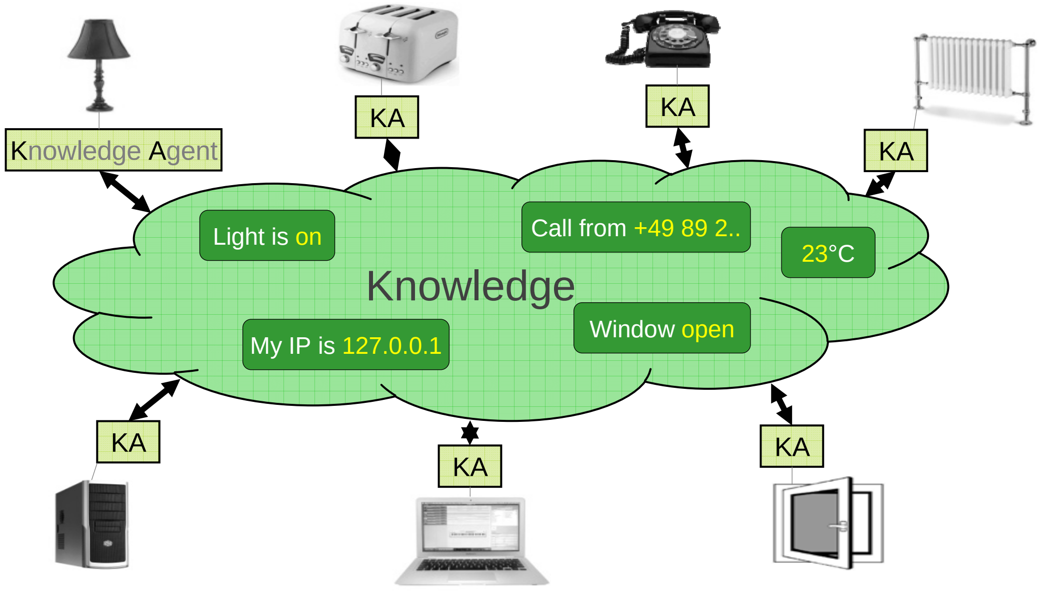
adaption to users and environment



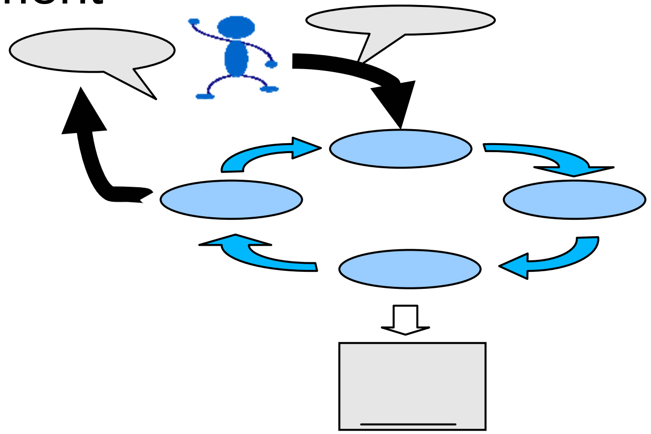


Basic concepts

- Knowledge Platform

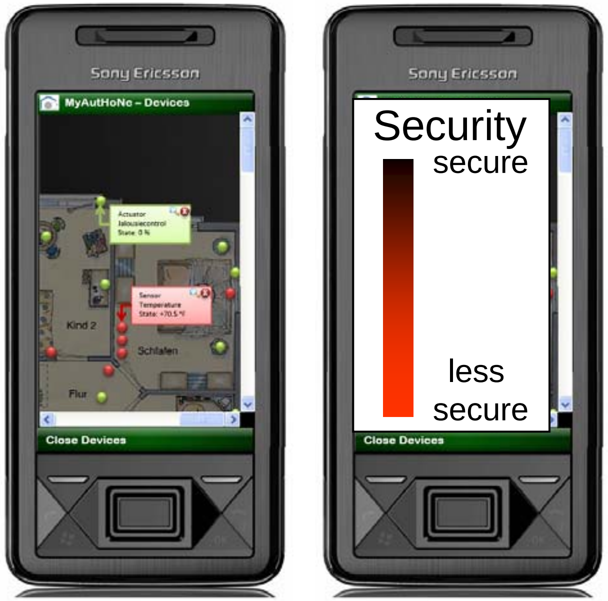


- Autonomous Configuration and Management



Basic concepts

- User Control
  - User-friendly
  - Modes for normal users and experts



No remote access

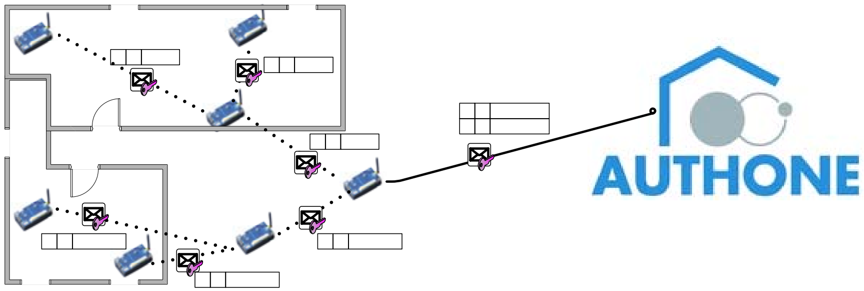
Only remote access by owner (no administrative control)

...

Remote access by friends

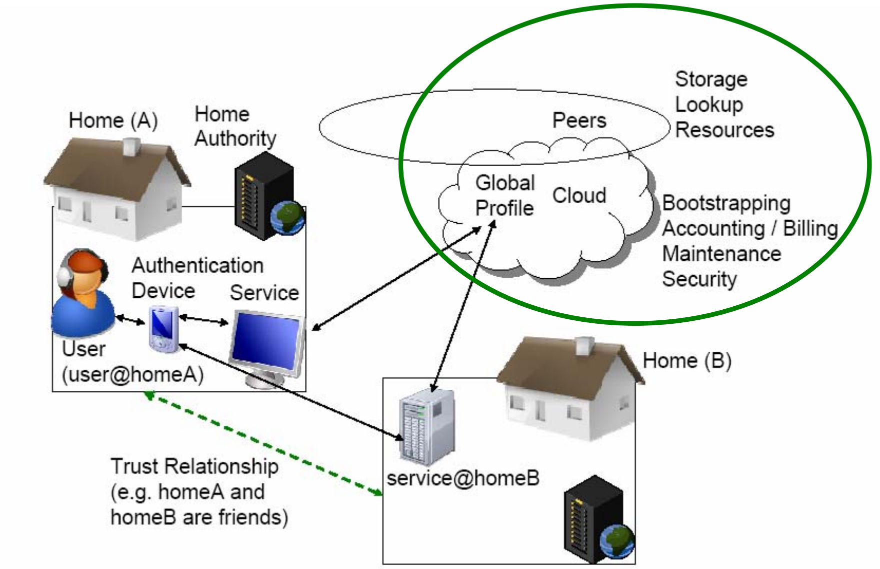
...

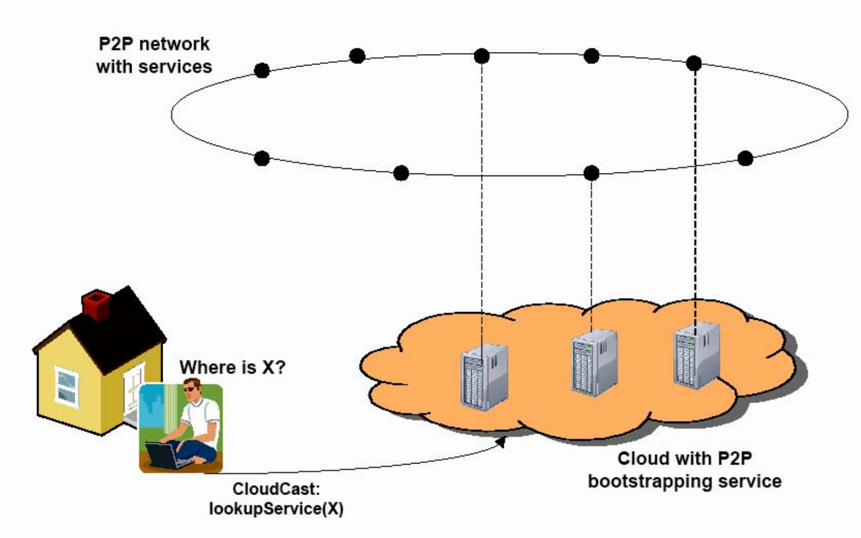
- Interaction with Environment
  - Sensors
  - Actuators



Home Networks with Cloud and P2P services

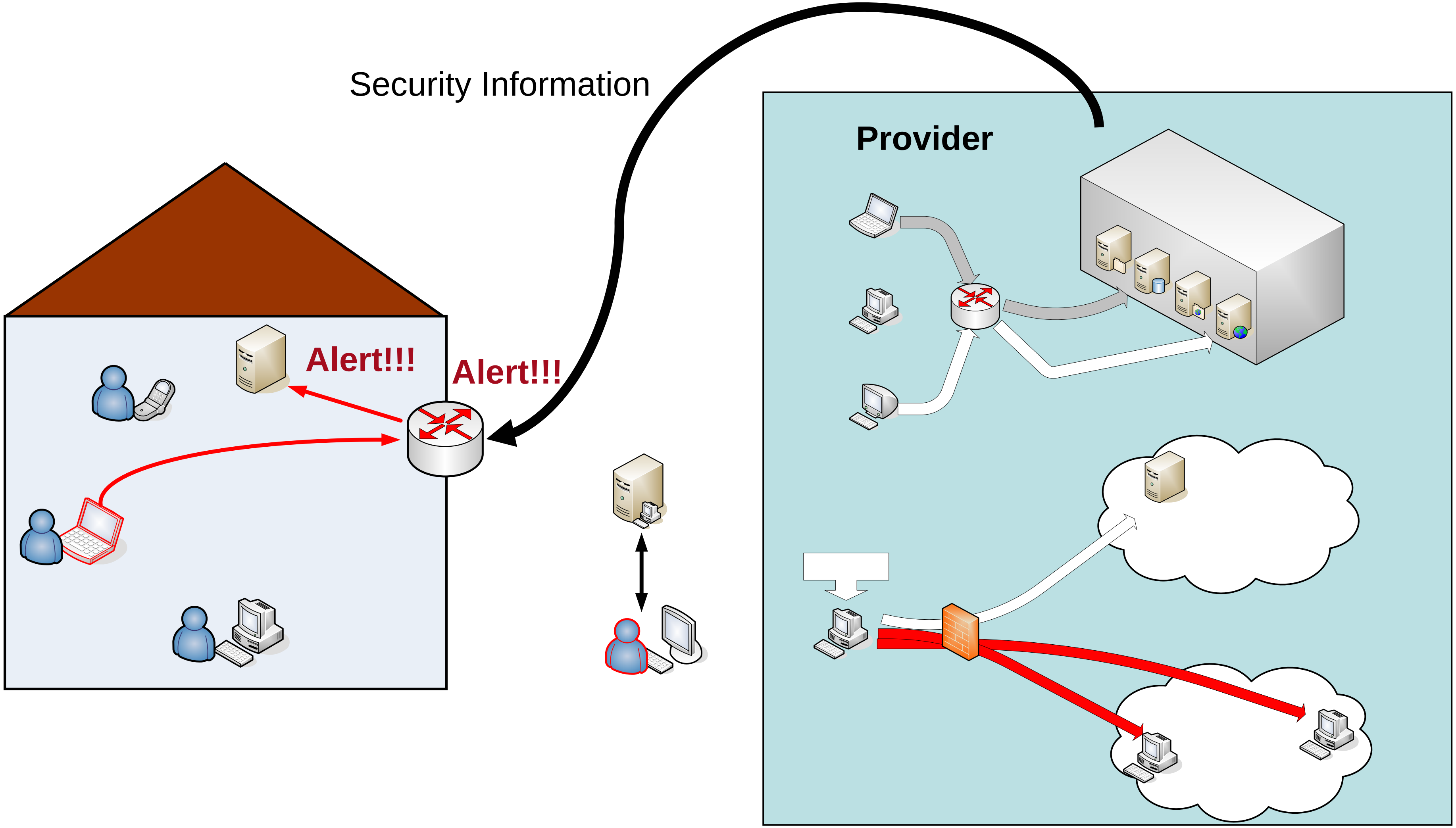
- AutHoNe provides Self-Management
  - Knowledge plane
  - Zero Configuration
- Cloud Computing
  - Computation and Storage in the network
  - Reliable resources
  - Pay and get more resources
  - Security Anchor → Provider and its accounting
- In combination with Peer-to-Peer
  - Use existing resources at edge
  - Scalability
  - Non-critical tasks and replication
- Bootstrapping and lookup of services
  - CloudCast to a near-by service cloud for lookup or processing





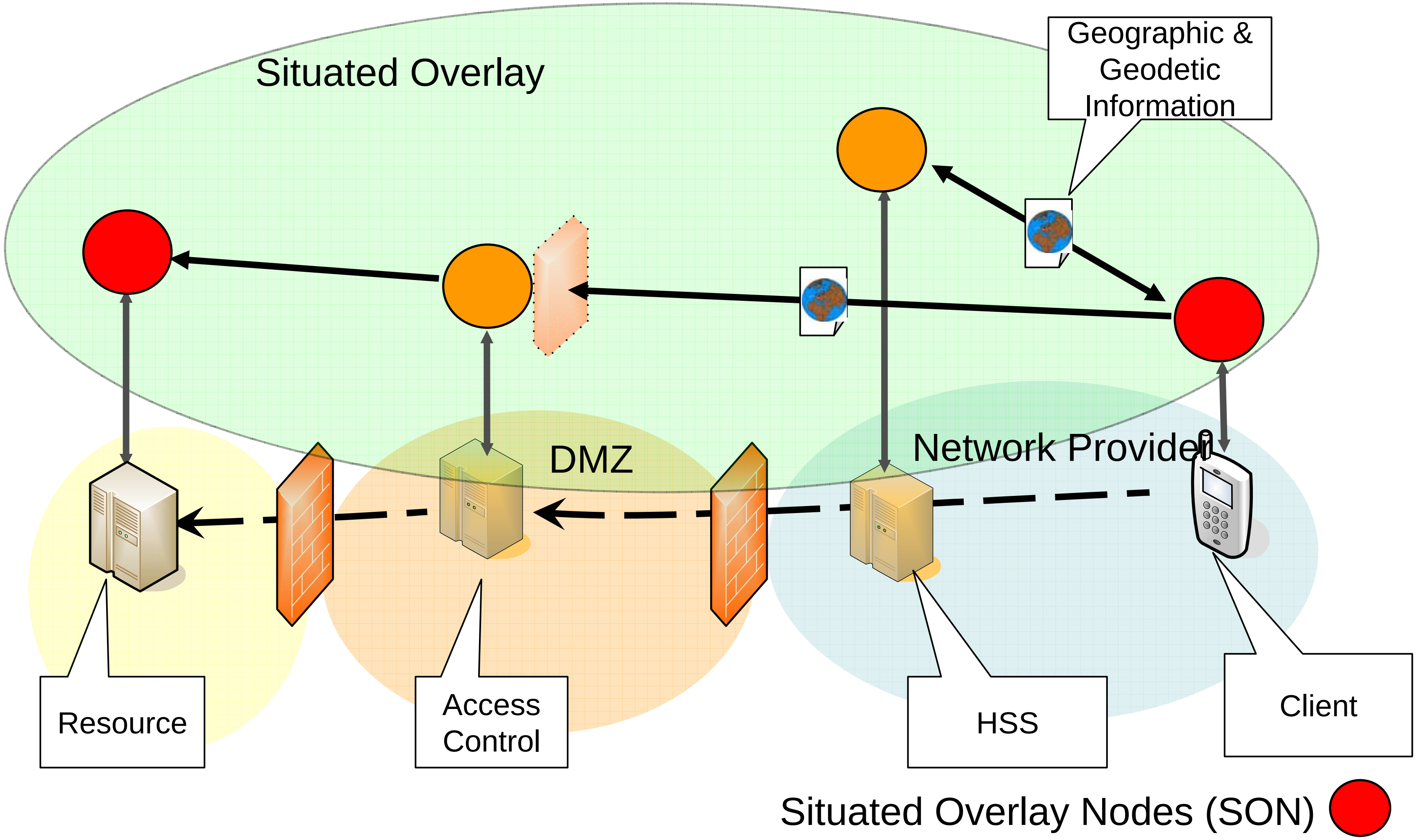
Detecting Command and Control Traffic

- Provider-guided attack detection in home networks

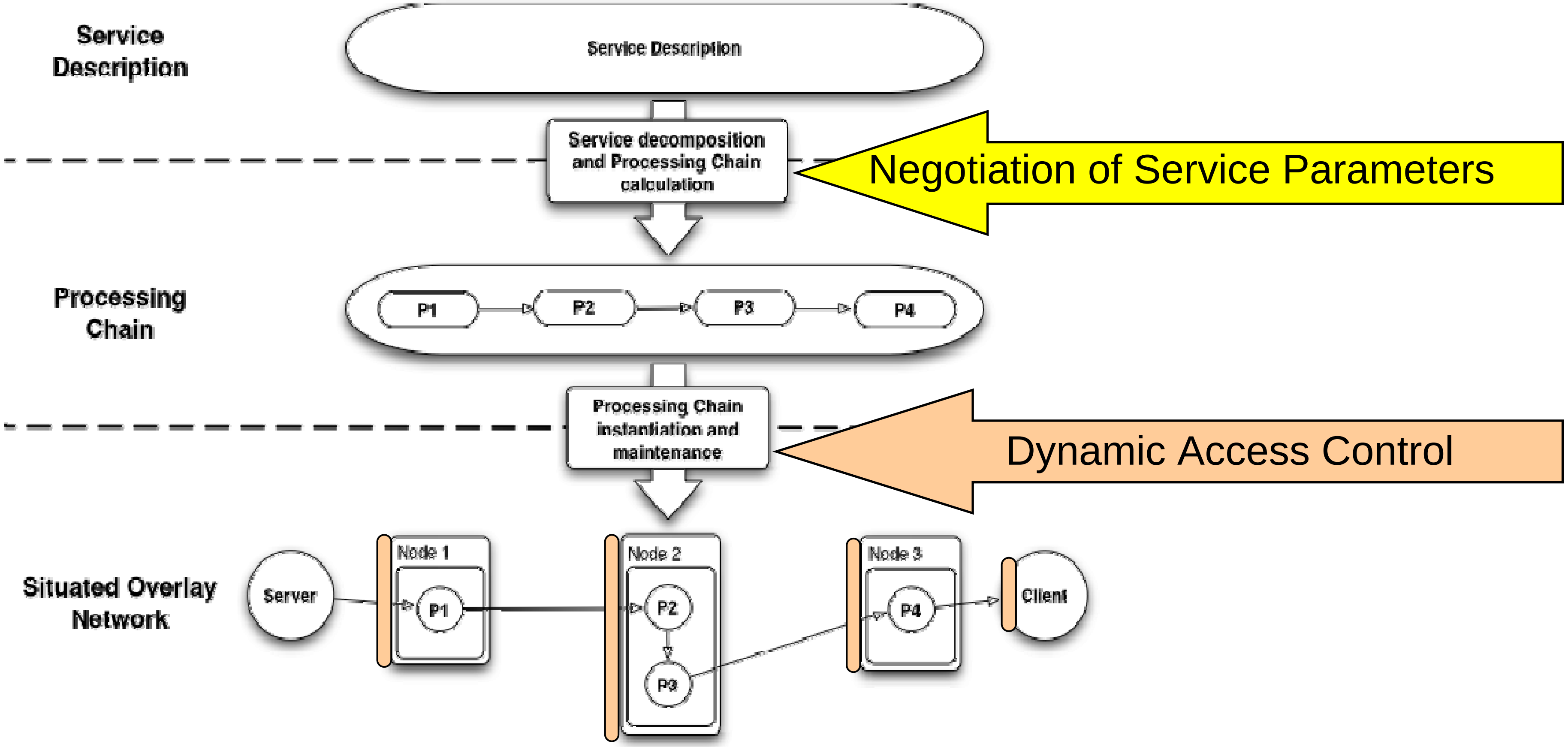


France-Telecom-Project SASCO: Overlay Security

- Project SASCO
  - Cooperation wit France Télécom and Fraunhofer FOKUS



SASCO: Situated Autonomic Service Control



BWFIT SpoVNet: Cross-Layer-Information for Overlays

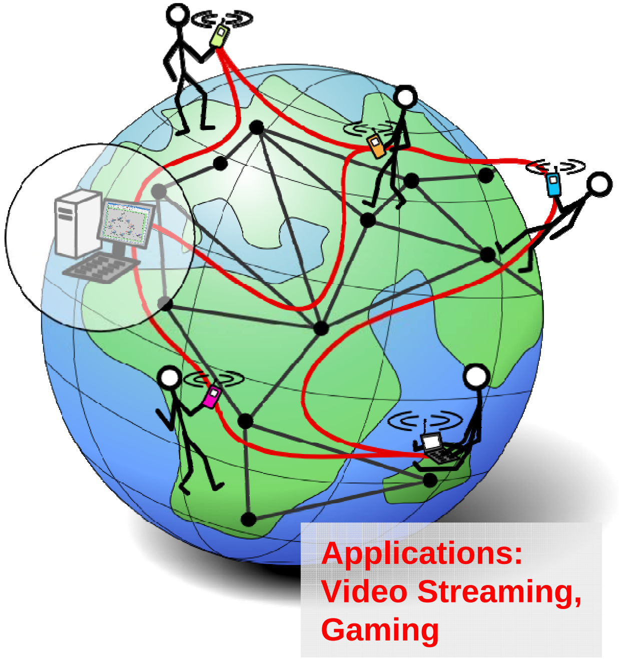
Prof. Dr. Paul Kühn
Universität Stuttgart

Prof. Dr. Martina Zitterbart
Universität Karlsruhe

Prof. Dr. Georg Carle
TU München

Prof. Dr. Kurt Rothermel
Universität Stuttgart

Prof. Dr. Wolfgang Effelsberg
Universität Mannheim

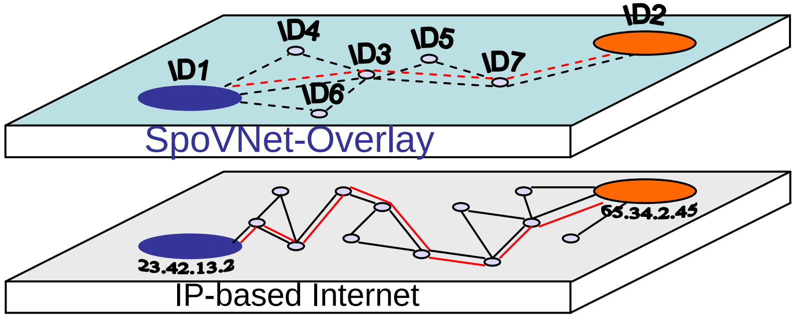


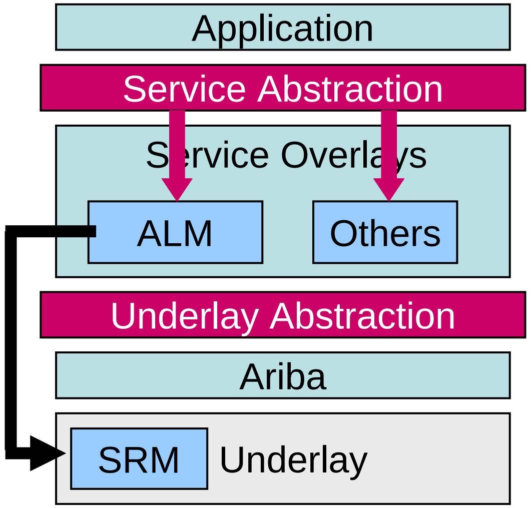
Applications: Video Streaming, Gaming

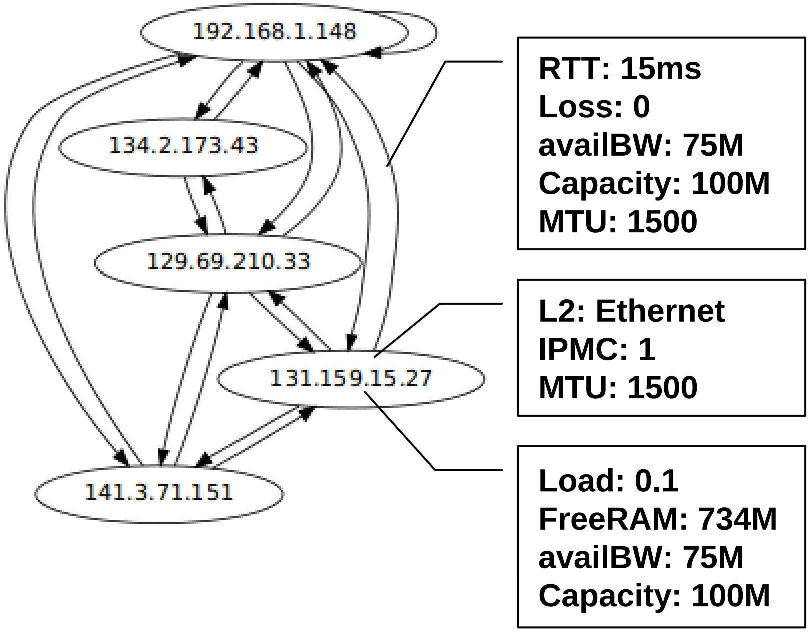
- SpoVNet: Spontanous Virtual Networks
- Flexible, adaptive and spontaneous service provisioning
- Approach: overlays
  - Let-1000-networks-bloom instea of One-size-fits-all
  - Tailored architekture for applications and networks
  - Cross-Layer-Information supports QoS decisions and optimisation
  - No dedicated infrastructure needed

SpoVNet - Spontaneous Virtual Networks

- Partners: KIT (Zitterbart), Uni Stuttgart (Kühn, Rothermel), Uni Mannheim (Effelsberg)
- Future Internet Approach
  - Locator/Identifier-Split
  - On demand overlay creation
  - Service overlays
  - UNISONO (@TUM) Cross-layer Information Service







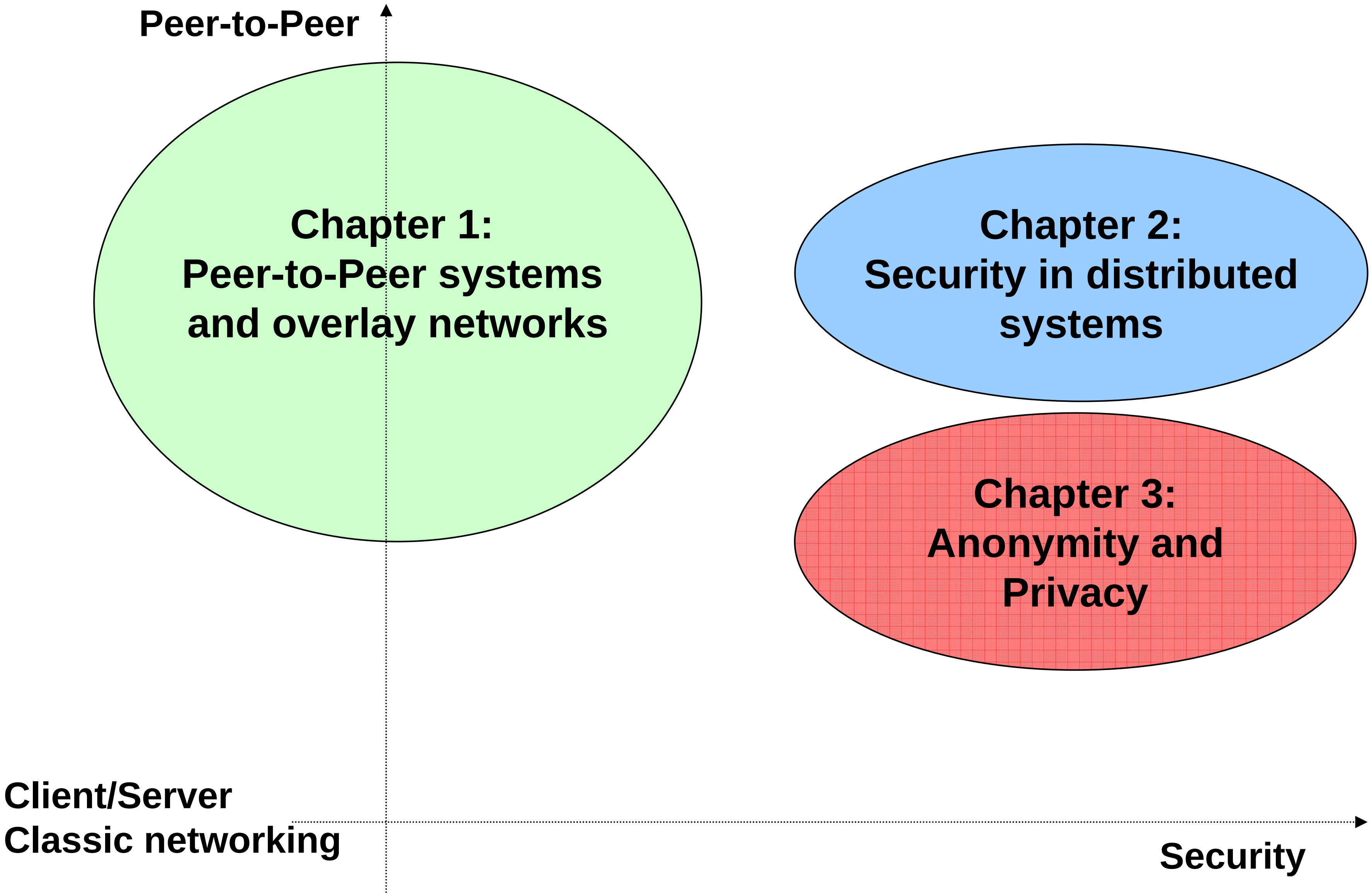
RTT: 15ms
Loss: 0
availBW: 75M
Capacity: 100M
MTU: 1500

L2: Ethernet
IPMC: 1
MTU: 1500

Load: 0.1
FreeRAM: 734M
availBW: 75M
Capacity: 100M

The lecture…

Course Overview



Peer-to-Peer Systems

- Network of equals
- No distinction between client and server
- Users and their computers at the edges of the Internet share their resources (bandwidth, CPU, storage).
- Self-organization of the system
- Autonomy from central entities like central servers
- Peers come and go → continuously changing environment

➡ Very popular due to file-sharing and content distribution networks that today are responsible for majority of the traffic of the Internet

Security

… but …

- ❑ Highly decentralized systems are not very secure.
- ❑ What about peers that do not cooperate?
- ❑ What about attacks or misuse?

… still….

- ❑ Peer-to-Peer systems are useful for censor-resistance, DoS resilience, etc.

➡ Security is an important issue especially for serious applications. Decentralized systems have their drawbacks, but also a high potential for improvements!

Anonymity & Privacy

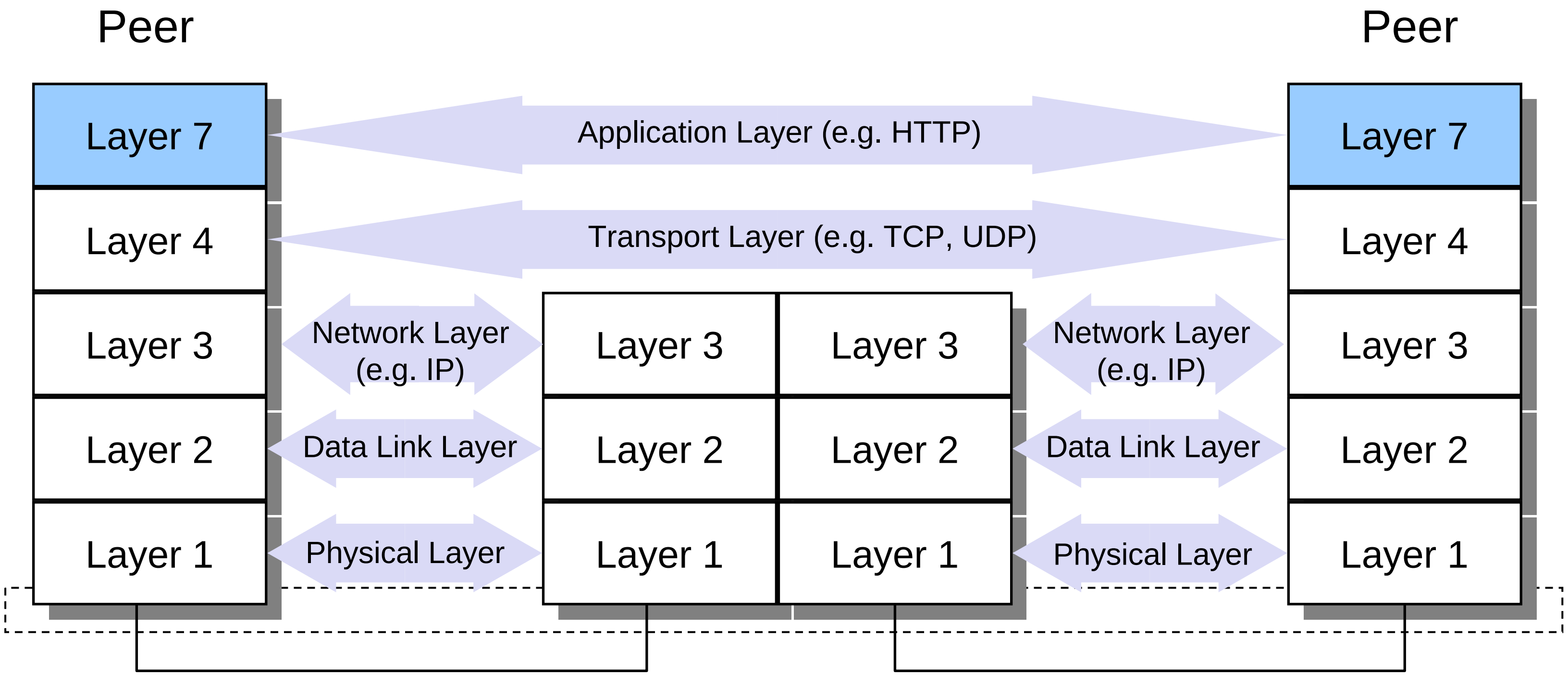
- In our daily life we are often an anonymous entity among a mass of other entities.

- Pseudonymity: An entity hides behind a pseudonym, so that anyone (but an authority) only knows the pseudonym, but not the true identity. The pseudonym can be tracked.
- Anonymity: Hide the identity, the usage/traffic patterns, and relationships from other entities or observers. No tracking.

➡ Traffic Analysis can reveal information that is leaked even if encryption is used. Technologies like Onion Routing can make these attacks harder.

Where are we?

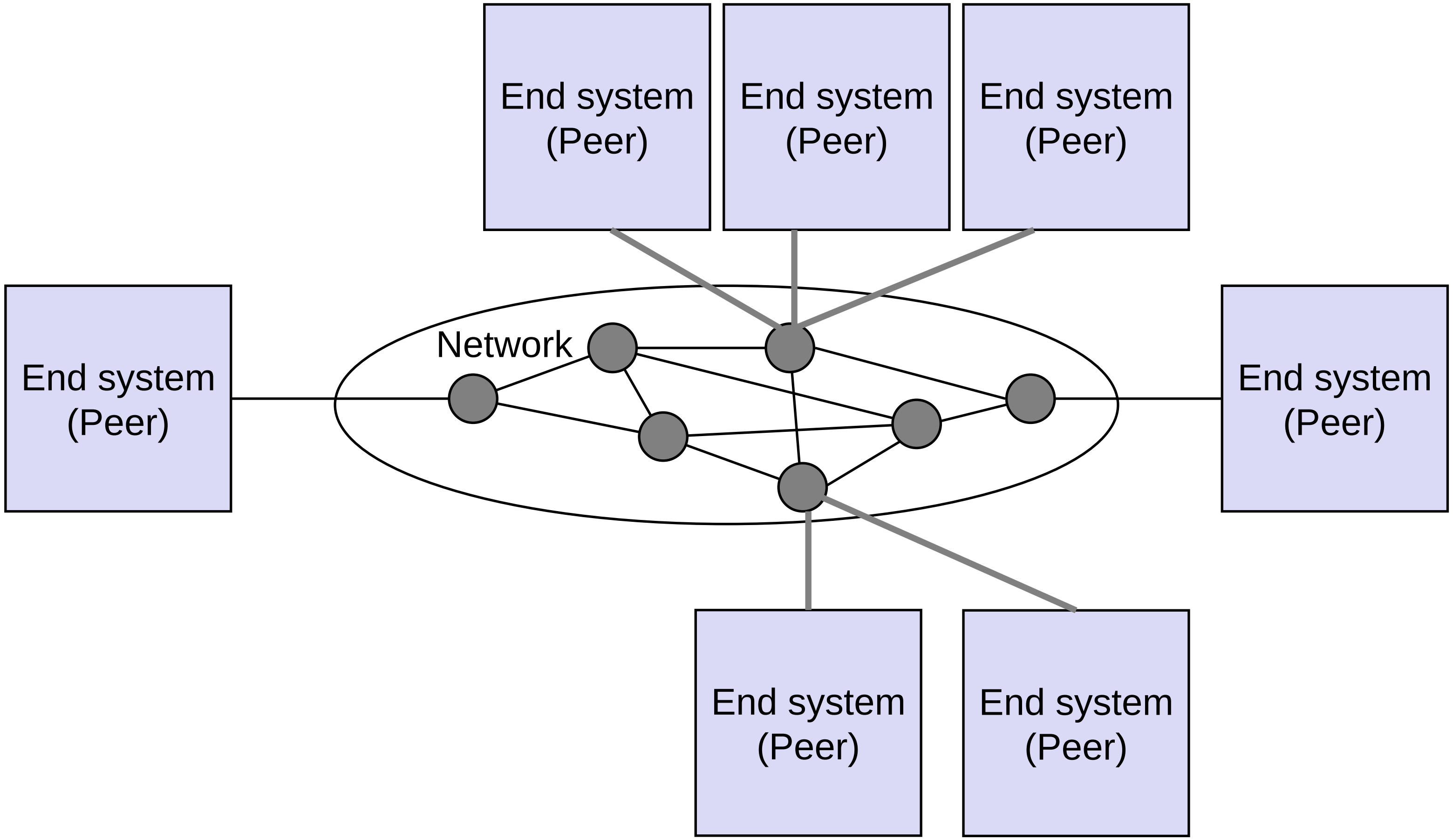
… on the network stack...



… on application layer <u>with some exceptions</u>.

Where are we? II

Who is contributing / doing the work?


End system (Peer)
End system (Peer)
End system (Peer)
End system (Peer)
Network
End system (Peer)
End system (Peer)
End system (Peer)