Chair for Network Architectures and Services
Department of Informatics
TU München – Prof. Carle

Peer-to-Peer Systems and Security
IN2194

Prof. Dr.-Ing Georg Carle
Dipl.-Inform. Heiko Niedermayer

Organisatorisches

Schein
- 60 % der Übungsaufgaben sinnvoll bearbeitet und mind. 1x gute Lösung vorgerechnet
  - Sinnvoll = Versuch ersichtlich, eine richtige Lösung zu finden.
  - Universitäre Selbstverantwortung: relevant für die Note ist die Prüfung.
- *Prüfung am Ende mündlich bei Prof. Carle*
  - Einzig relevant für die Note.

Übungsbetrieb
- 5 Übungen und Übungsblätter
- Raum 03.07.023
- Übungstermin
  - Donnerstags 10-12 Uhr
- 5 ECTS ⇨ Zusatzaufgaben (auch praktisch)

Anmeldung
- Über die Webseite des Lehrstuhls http://www.net.in.tum.de
  http://www.net.in.tum.de/de/lehre/ss09/vorlesungen/vorlesung-peer-to-peer-systeme-und-sicherheit/

Peer-to-Peer Systems and Security

Motivation

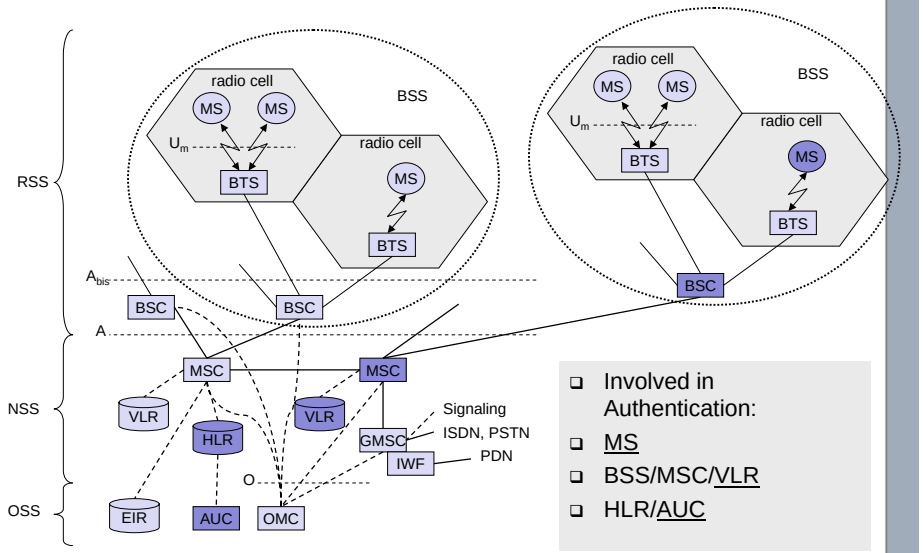
The power of P2P

Peer-to-Peer Systems

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

- Network of equals (Peer: Ebenbürtiger / Gleichgestellter)
  ⇨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

Authentication in GSM



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

GSM

Some GSM Abbreviations	
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

Press Reports

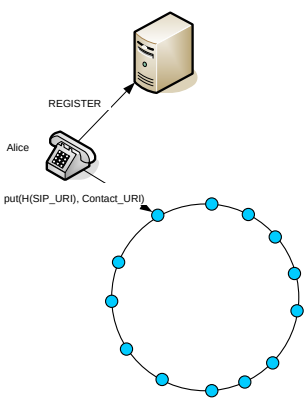
- *„Deutschlandweite Störungen im Handynetz von T-Mobile“,* Christian Feld, WDR, April 21st 2009.
  - <http://www.heise.de/newsticker/T-Mobile-GAU-Gratis-SMS-als-Entschaedigung--/meldung/136581>
    T-Mobile hatte im vergangenen Jahr alte HLR-Systeme, die Verbindungen zwischen Mobilfunkstationen und Endgeräten steuern, durch eine neue Systemplattform von Nokia Siemens Networks (NSN) ersetzt, auf der Software des britischen Netzwerkspezialisten Apertio läuft, den NSN Anfang 2008 übernommen hatte. An dem neuen System seien nun Updates vorgenommen worden, erklärte Pölzl. Dabei sei es dann zu einem Softwareproblem gekommen. Die genauen Ursachen würden im Detail noch ergründet. Der Bundesnetzagentur muss das Unternehmen nun Auskunft über Ausmaß und Ursache der Panne erteilen.
- *“Der Ausfall eines Servers der Deutschen Telekom hat am Montagabend [29. Okt. 2007] und in der Nacht zu Dienstag stundenlang zu Ausfällen im Telefonnetz in ganz Deutschland geführt.”* Press article, Financial Times, October 2007
- *“Skype Outage Continues For Some, Businesses Affected”,* Press Article, PC World, August 17th 2007
- *“VoIP-Störung bei United Internet”,* Press Article, heise newsticker, July 2006.

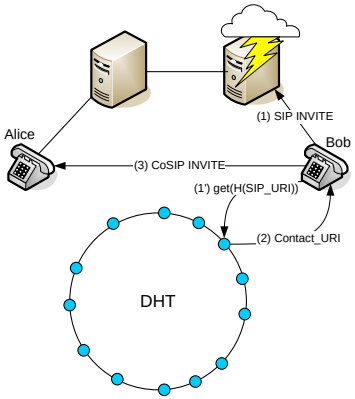
Related Research Activities at the Chair I8

- *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)

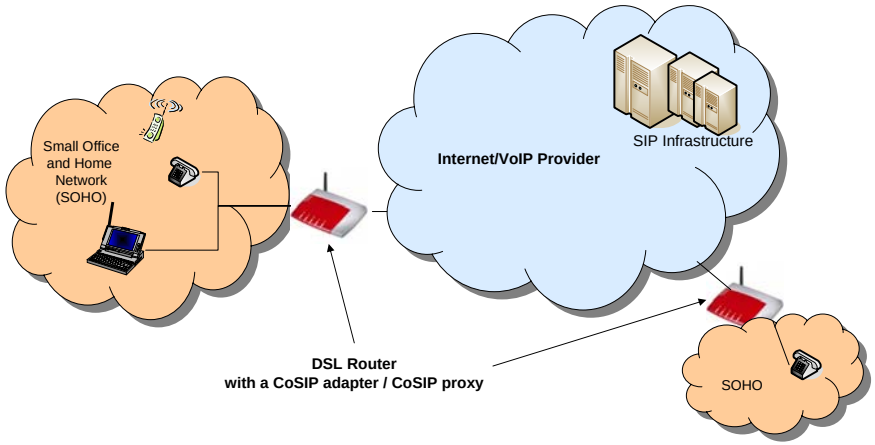
- User registration with CoSIP
- Session establishment with CoSIP





Application of CoSIP in the fixed network

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



Weitere ausgewählte Forschung am Lehrstuhl für Netzarchitekturen und Netzdienste – I8

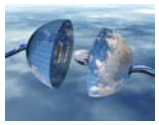
Projektschwerpunkte

	Autonomic / Self-Org. Man.	Mobilkom-munikation	Instrumen-tierung	P2P und Overlays	Netz-Sicherheit
EU ResumeNet	☑			☑	☑
EU AutHoNe	☑	☑	☑	☑	☑
DFG LUPUS			☑	☑	☑
BMBF ScaleNet	☑	☑	☑		
NSN SelfMan	☑		☑		
NSN TC-NAC		☑			☑
France-Telecom SASCO	☑	☑		☑	☑
BWFIT SpoVNet			☑	☑	☑
BWFIT AmbiSense		☑	☑		

DHT

EU FP7-Projekt ResumeNet

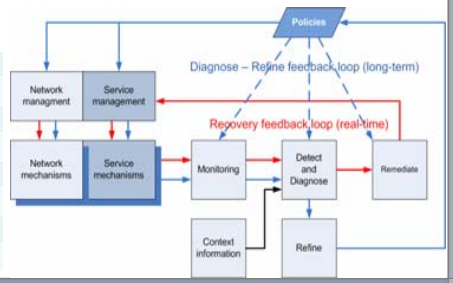
- "Resilience and Survivability for future networking: framework, mechanisms, and experimental evaluation"



- Ein Projekt im Rahmen des FIRE-Programms („*Future Internet Research and Experimentation*")
- Konsortium:

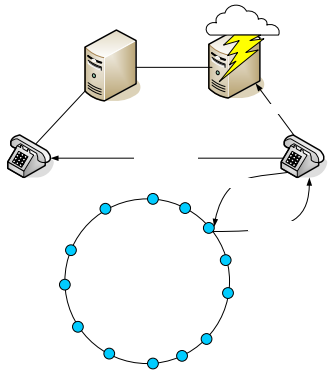
ETH Zürich	Switzerland
Lancaster University	United Kingdom
Technical University Munich	Germany
France Telecom	France
NEC Europe Ltd	United Kingdom
Universität Passau	Germany
Technical University Delft	Netherlands
Uppsala Universitet	Sweden
Université de Liège	Belgium

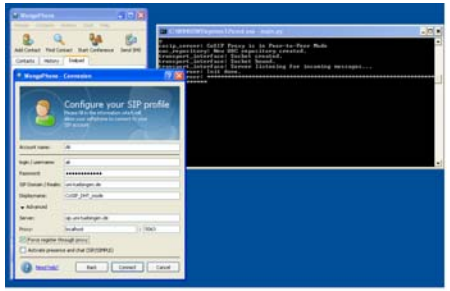
- Strategie: D^2R^2DR



Robuste Diensterbringung (Service Resilience)

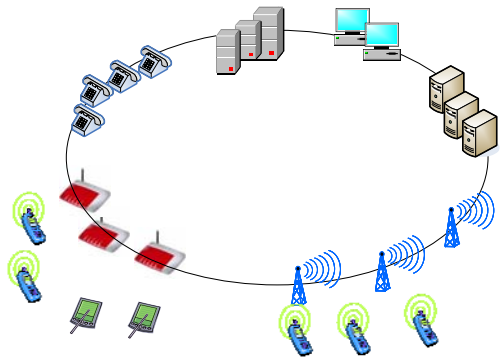
- Kombination von P2P- und Client/Server-Ansatz
- Hohe Ausfallsicherheit bei gleichzeitigem Schutz von P2P-Verwundbarkeit
- Beispiel-Anwendung CoSIP: Nebenläufige Signalisierung bei Voice over IP





Robuste Diensterbringung (2)

- Ansätze:
  - Hybrides P2P-Overlay-Netzwerk
  - Peers mit verschiedenen Rollen, verifizierbarer Identität, Virtualisierung
- Ziele:
  - Kooperation zwischen End-Knoten und Infrastruktur für bestmögliche Zuverlässigkeit, Dienstgüte, Skalierbarkeit



AutHoNe - Autonomic Home Networking

- EUREKA-Celtic/BMBF-Projekt
- Partner in Deutschland
  - 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

AUTHONE

EUREKA

Bundesministerium für Bildung und Forschung

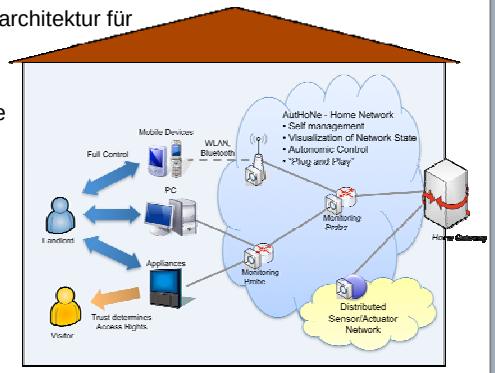
CELTIC Telecommunication Solutions

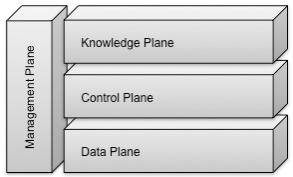
(1) SI

(SIP_URI

AutHoNe: Projektziele

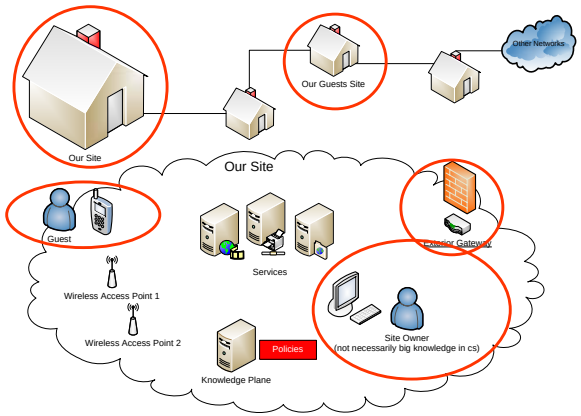
- Entwicklung einer Kommunikationsarchitektur für
  - Sensoren und Aktuatoren
  - Multimediageräte
  - Computer, PDAs, Mobiltelefone
  - Home appliances
- AutHoNe-Framework unterstützt
  - Einfache Benutzerinteraktion
  - Self* - Eigenschaften
    - Konfiguration
    - Schutz
    - Optimierung
    - Heilung
  - Sicherheitsmechanismen
    - Nutzerorientiert
  - Lokaler sowie entfernter Dienstzugriff





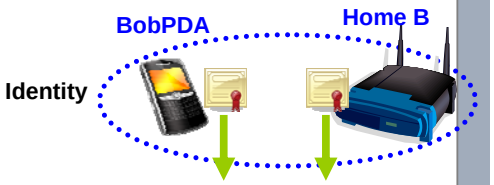
AutHoNe: Szenario

- Identitätsmanagement
- Wissenssammlung
- Benutzerschnittstelle?
- 2 Homes, Identifikation, Mobilität, Services



Addressing

- **EntityID is...**
  - hash over entity's public key



- **Authone address...**
  - consists of entityIDs
    - **entityID.homeID.authone**
  - is bounded to identity
  - supports inter-home addressing

EntityID

$BobPDA_{ID} = hash(pubkey_{BobPDA})$
$HomeB_{ID} = hash(pubkey_{HomeB})$

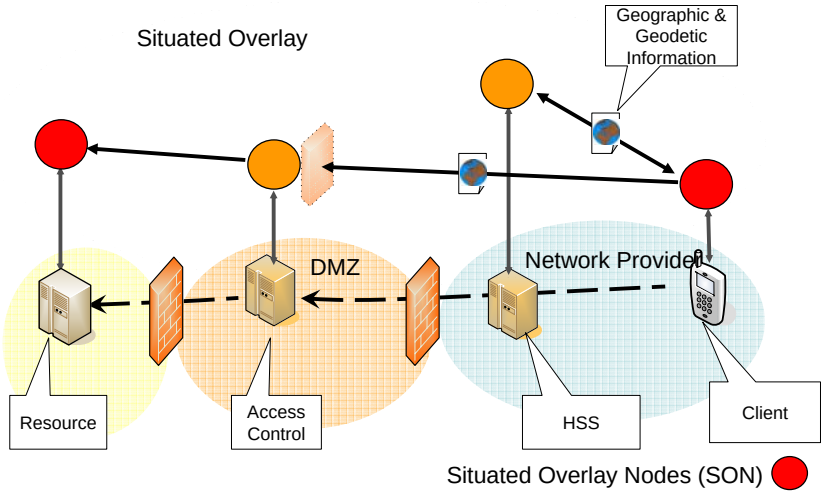
Authone address = $BobPDA_{ID}.HomeB_{ID}.authone$

IP address

- **Lookup service**
  - Translates **Authone address** to **IP address**
  - Provided by special node(s) (e.g. home gateway)

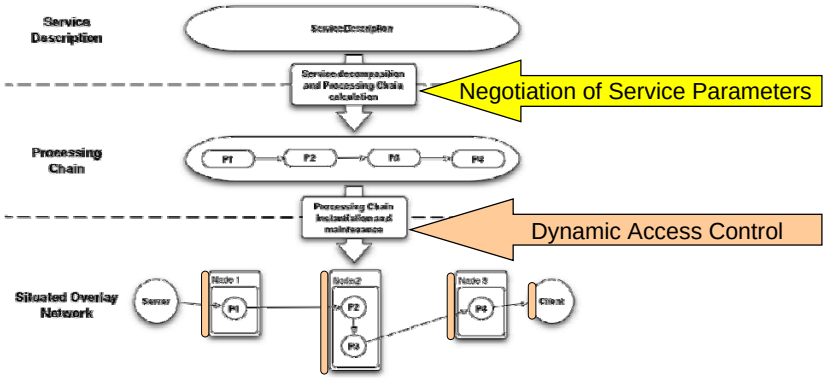
France-Telecom-Projekt SASCO: Overlay Security

- Projekt SASCO
  - Kooperation mit France Télécom und Fraunhofer FOKUS



SASCO: Situated Autonomic Service Control

- Ziel
  - Selbstorganisierende Dienstplattform als Alternative zum 3GPP IMS
  - Integration von Peer-to-Peer-Technologien und Zugriffskontrolle
- Ansatz



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

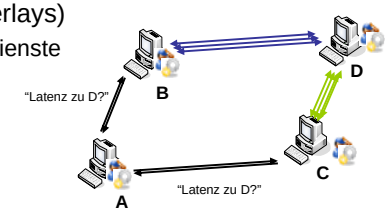
Anwendungen im Projekt: Video Streaming und Realzeitspiel

- SpoVNet: Spontane Virtuelle Netze
- Flexible, adaptive und spontane Bereitstellung von Diensten
- Ansatz über Overlays
  - Let-1000-networks-bloom anstelle von One-size-fits-all
  - Zugeschnittene Architekturen für Anwendungen und Netze
  - Dienstgüte-Unterstützung durch Cross-Layer-Information und Optimierung
  - Keine dedizierte Infrastruktur erforderlich

BW-FIT SpoVNet: Cross-Layer-Information for Overlays

Beiträge

- CLIO (Cross-Layer-Information for Overlays)
  - Informationsdienst für Anwendungen/Dienste
  - Messungen
    - Innovative Messverfahren
    - Overlay-übergreifender Dienst
    - Privacy-freundliche Datenhaltung
  - Anomalieerkennung auf Overlay-Daten
- Sicherheit für SpoVNet
  - Beteiligung am Entwurf der Sicherheitsarchitektur
  - Sicherheitskomponente

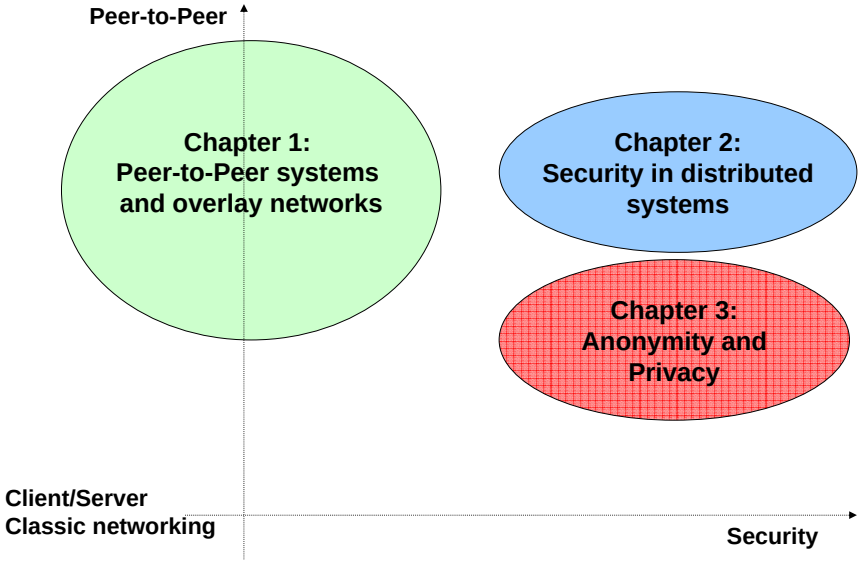


Remote-Aufträge für CLIO
z.B. Netzbeitritt Autorisierung nur, wenn Peer gut genug an andere Knoten angebunden ist (nützlich für Realzeitspiel)

Peer-to-Peer Systems and Security

The lecture…

Course Overview



Peer-to-Peer Systems

- Network of equals (Peer: Ebenbürtiger / Gleichgestellter)
- 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!

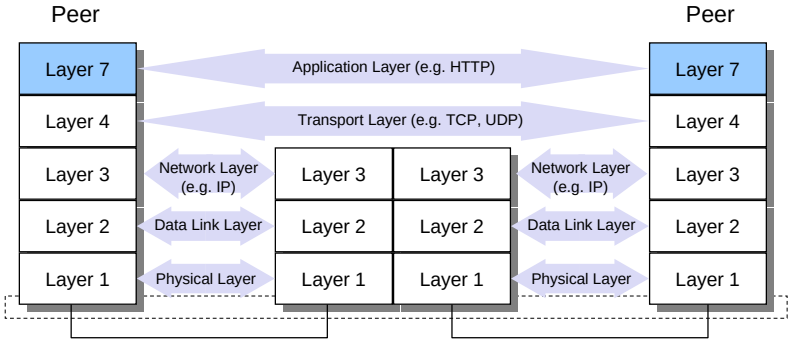
Anonymity & Privacy

- 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 with some exceptions.

Where are we? II

Who is contributing / doing the work?