

# Forschung am Lehrstuhl für Netzarchitekturen und Netzdienste

Prof. Dr.-Ing. Georg Carle

carle@in.tum.de

## Gliederung:

Team → Themen → Projektüberblick → Einzelne Projekte → Zusammenfassung und Ausblick



# Team

Prof. Dr.  
Georg Carle



Dr.  
Nils  
Kammenhuber



## in Tübingen:

Lothar  
Braun



Holger  
Kinkelin



Dirk  
Haage



Tobias  
Bandh



Andreas  
Müller



Dr.  
Christian  
Hoene



Ali  
Fessi



Gerhard  
Münz



Ralph  
Holz



Marc  
Fouquet



Heiko  
Niedermayer



Kai  
Kamphenkel



Dr.  
Manfred  
Jobmann



Marc-  
Oliver  
Pahl



Ralph  
Kühne



Corinna  
Schmitt



Dr.  
Pavel  
Laskov





# Forschungsthemen

Audio/Video- und Echtzeit-Dienste

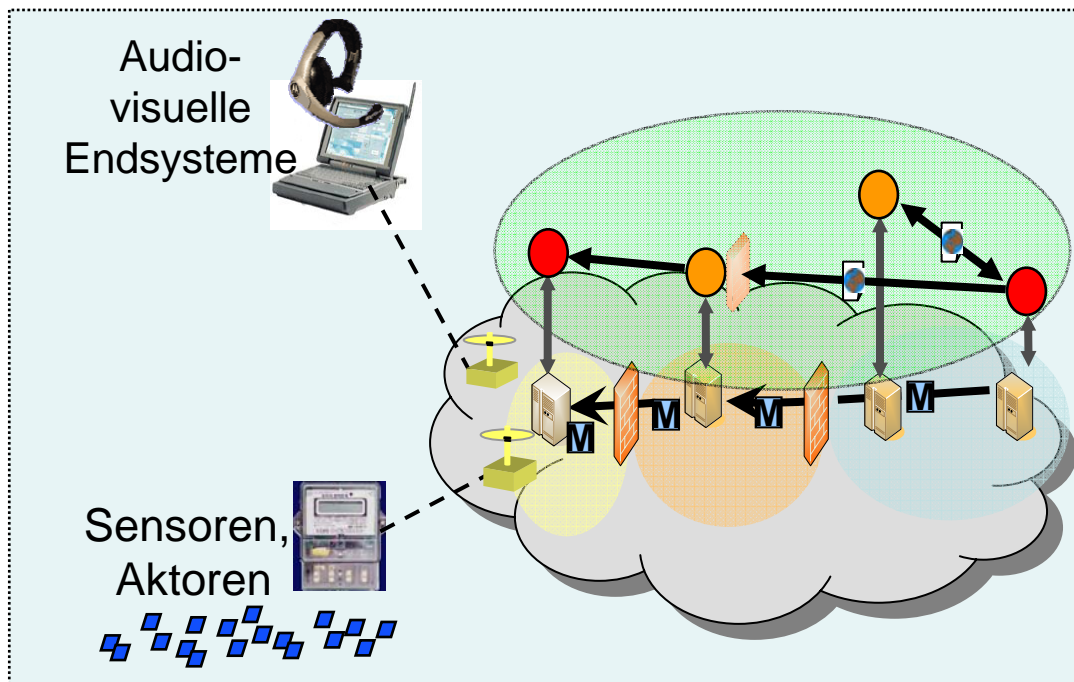
Peer-to-Peer- und Overlay-Netze

Mobilkommunikation

Netzinstrumentierung

**Autonomes  
Management**

**Netz-  
sicherheit**





## Aktuelle Projekte

- ❑ Europäische Projekte
  - EU-FP7-Projekt ResumeNet: Resilience and Survivability for future networking
  - EUREKA/BMBF-Projekt AutHoNe: Autonomic Home Networks
- ❑ Nationale Projekte
  - DFG-Projekt LUPUS: Lasttransformationen und ihre Nutzung zur Prognose und zum Verständnis von Verkehren in Netzen mit Sicherheitsanforderungen
  - BMBF-Projekt ScaleNet: Scalable efficient and flexible next generation converged mobile wireless networks
  - BW-FIT SpoVNet: Spontane Virtuelle Netze
  - BW-FIT AmbiSense: Kooperation autonomer mobiler Systeme unter Berücksichtigung ambienter Sensoren
- ❑ Industrieprojekte
  - France-Telecom-Projekt SASCO: Situated Autonomous Service Control
  - Siemens/NSN-Projekt SelfMan: Management for Self-Organizing Networks
  - Siemens/NSN-Projekt TC-NAC: Netzzugangskontrolle mit Trusted Computing
- ❑ Forschungsnetzwerk
  - COST-TMA “Data Traffic Monitoring and Analysis for future networks”



# Projektschwerpunkte

	Autonomic / Self-Org. Man.	Netz- Sicherheit	Instrumen- tierung	P2P und Overlays	Mobilkom- munikation
EU ResumeNet	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	
EU AutHoNe	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
DFG LUPUS		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
BMBF ScaleNet	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>
NSN SelfMan	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>		
NSN TC-NAC		<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/>
France-Telecom SASCO	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
BWFIT SpoVNet		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
BWFIT AmbiSense			<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>

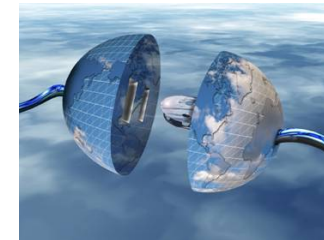


# EU FP7-Projekt ResumeNet

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



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



- Konsortium:

- Strategie: D<sup>2</sup>R<sup>2</sup>DR

## 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

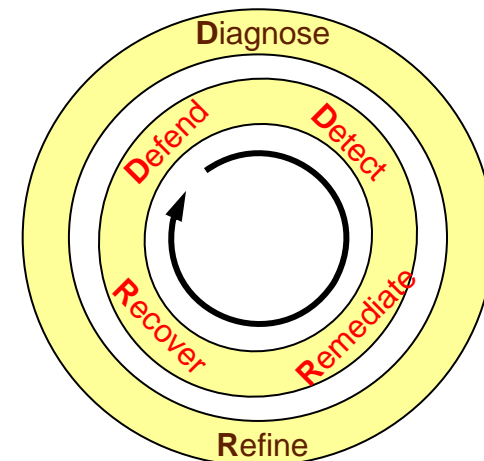
Netherlands

Uppsala Universitet

Sweden

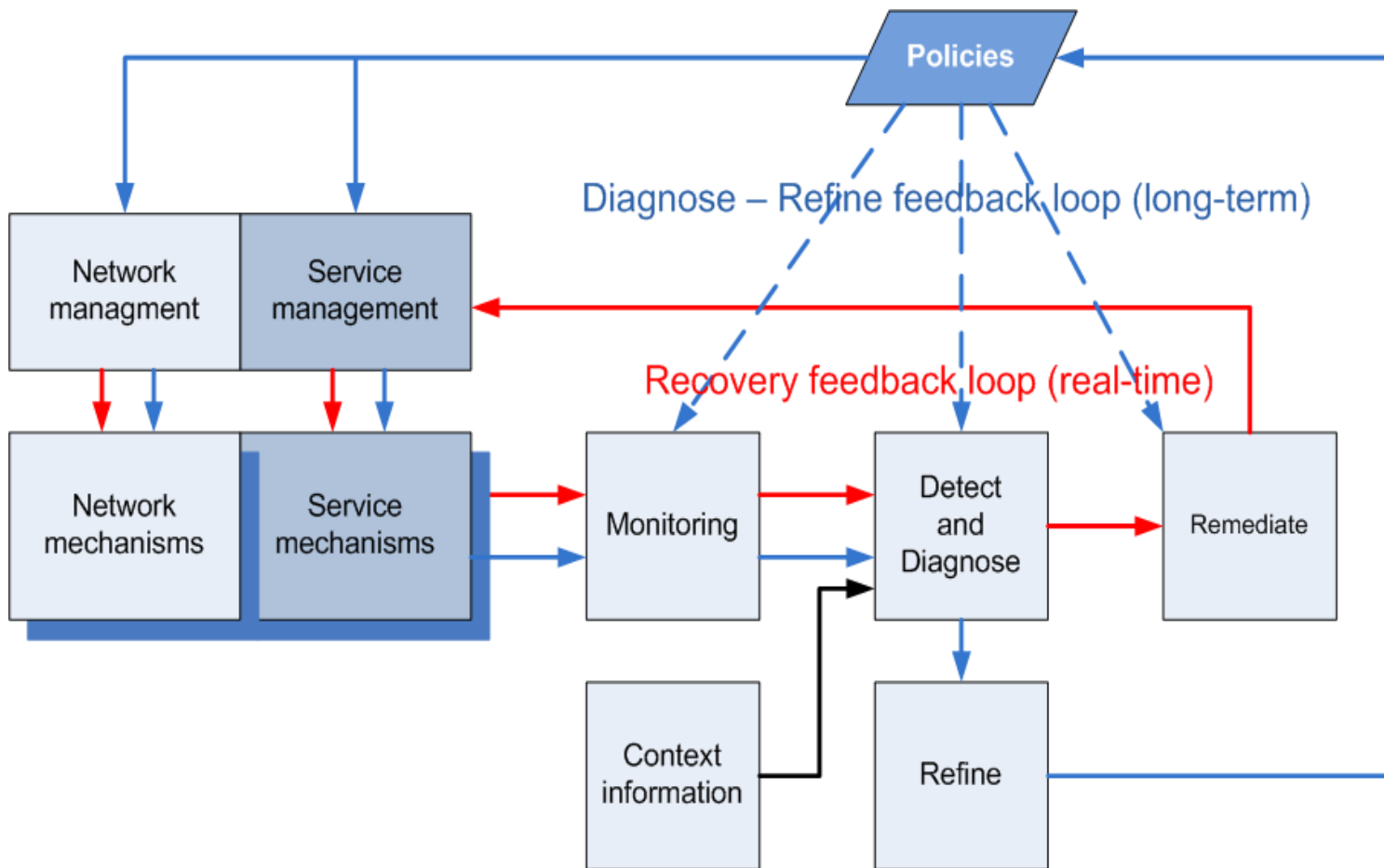
Université de Liège

Belgium





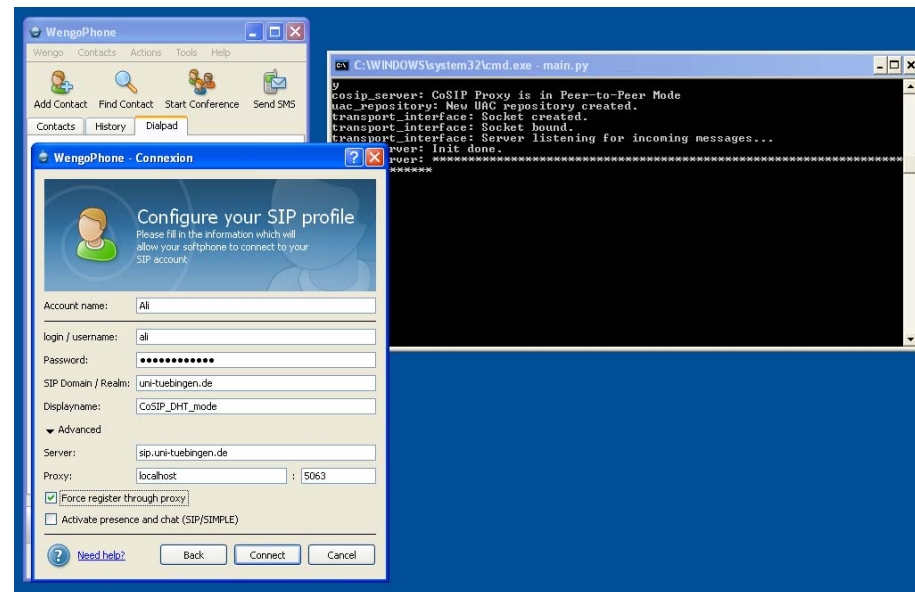
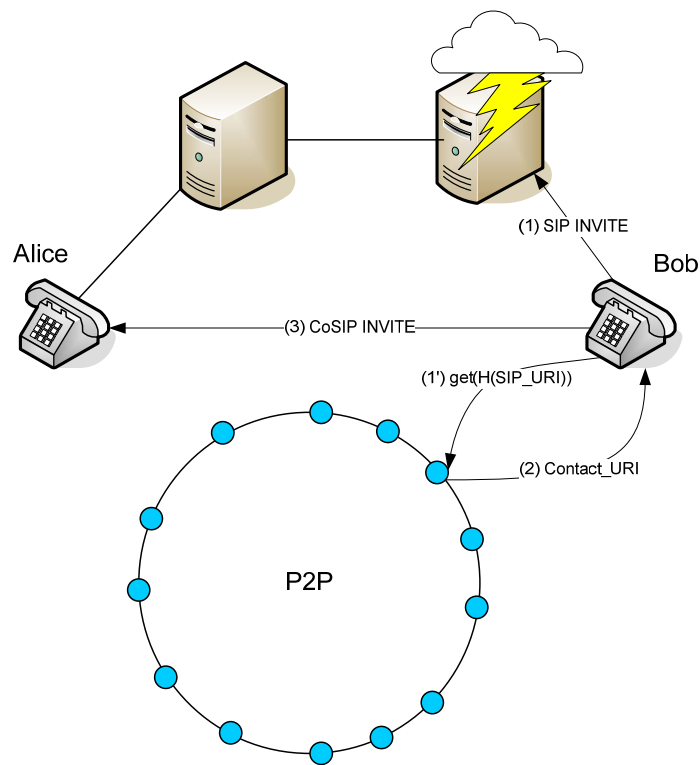
# Network and Service Resilience Architecture





# Robuste Dienstleistung (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

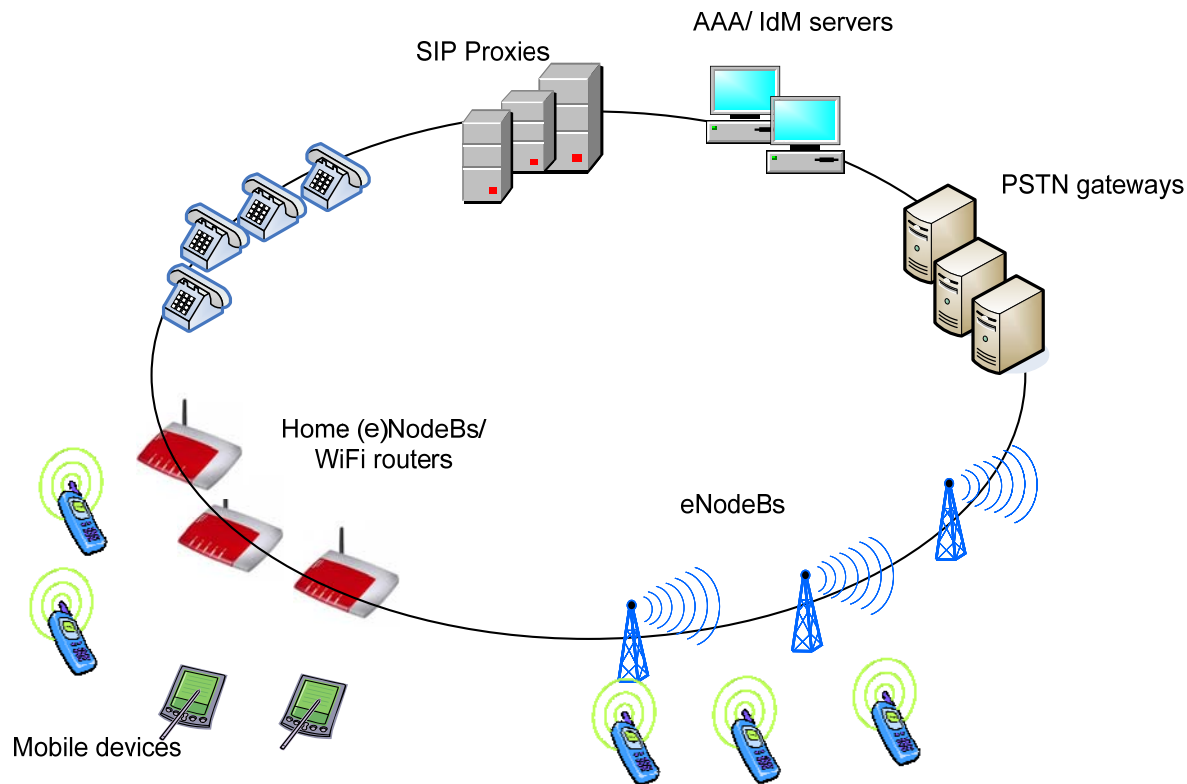






## Robuste Dienstleistung (2)

- 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



**Bundesministerium  
für Bildung  
und Forschung**





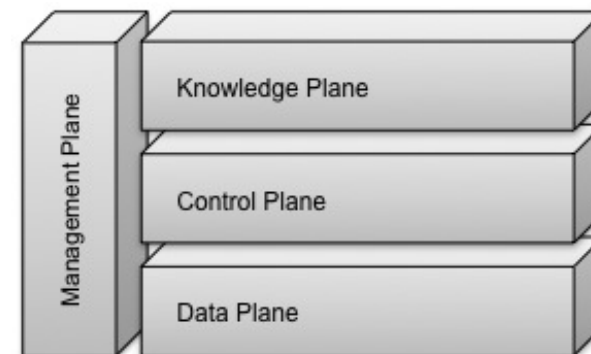
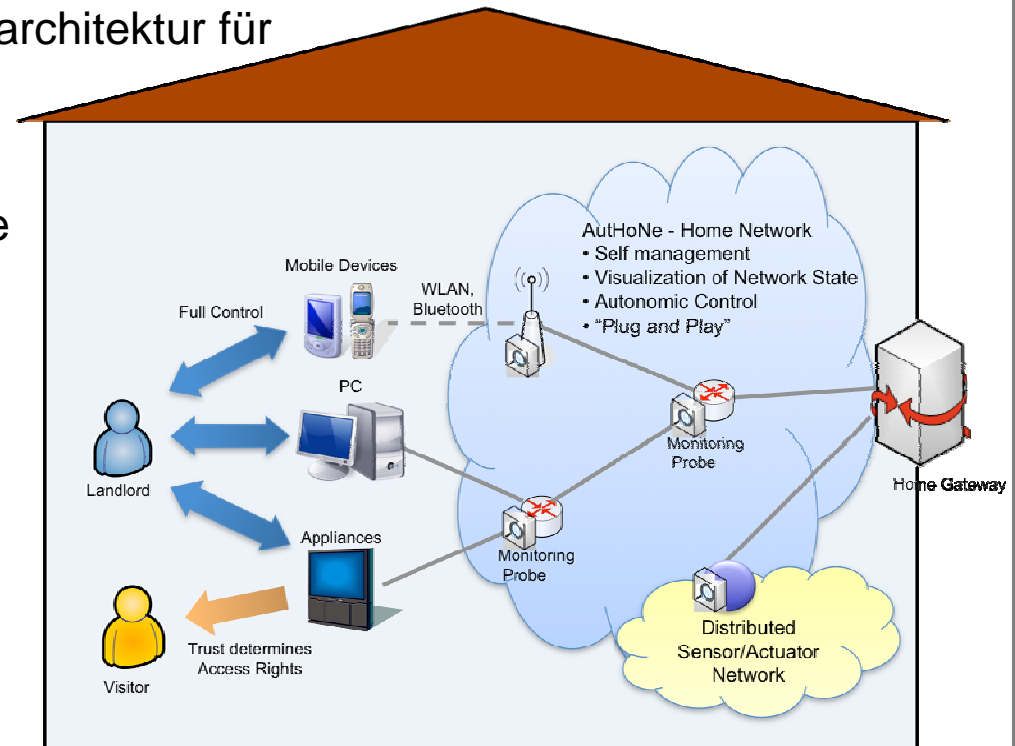
# AuthoNe: Projektziele

## □ Entwicklung einer Kommunikationsarchitektur für

- Sensoren und Aktuatoren
- Multimediageräte
- Computer, PDAs, Mobiltelefone
- Home appliances

## □ AuthoNe-Framework unterstützt

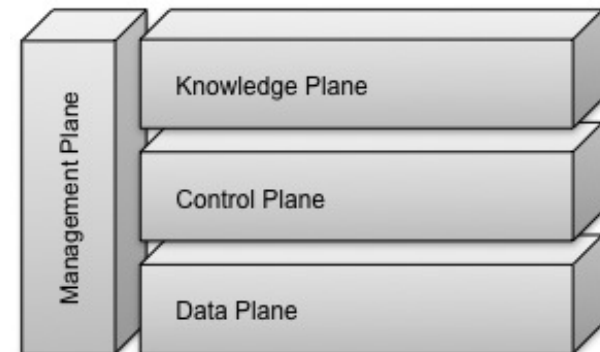
- Einfache Benutzerinteraktion
- Self\* - Eigenschaften
  - Konfiguration
  - Schutz
  - Optimierung
  - Heilung
- Sicherheitsmechanismen
  - Nutzerorientiert
- Lokaler sowie entfernter Dienstzugriff





## AutHoNe: Beiträge

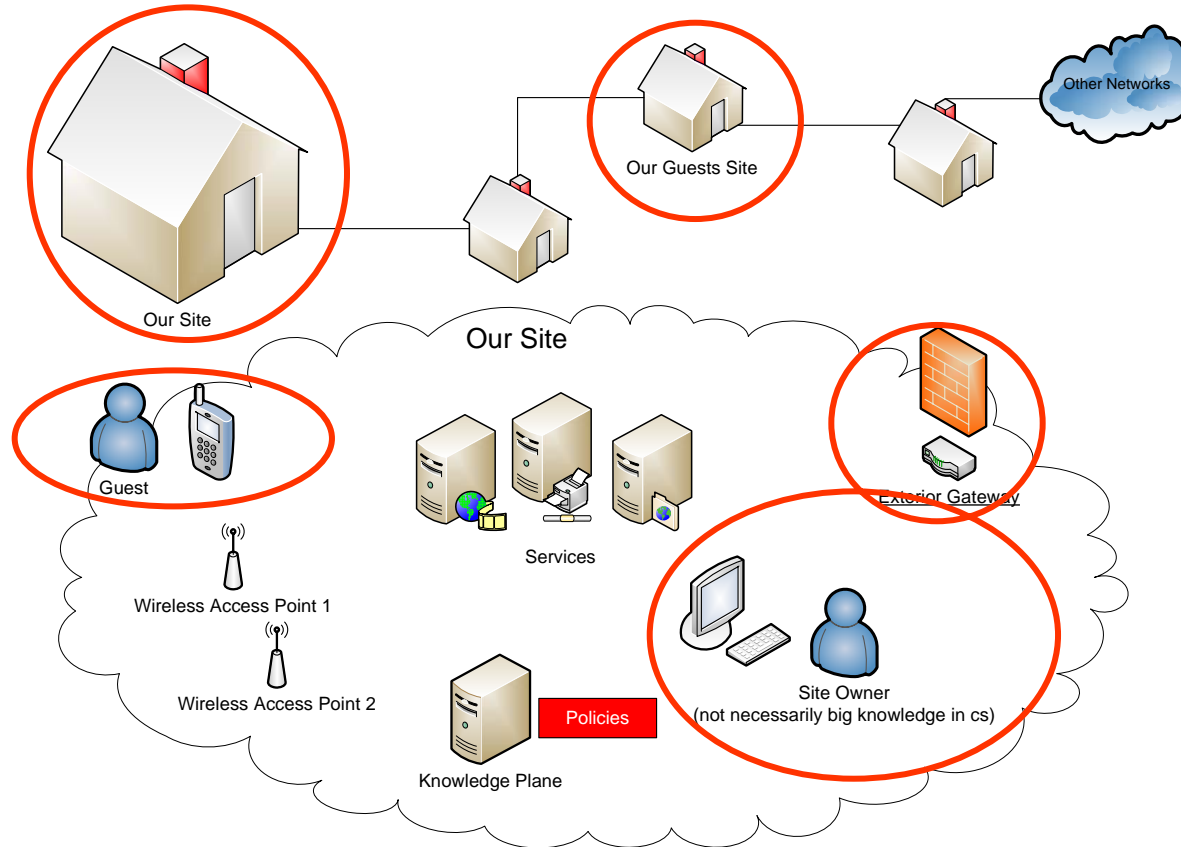
- Entwicklung einer Wissensschicht (Knowledge Plane)
  - Verteilter Ansatz der Architektur
  - Integriert relevante Netzinformationen und leitet daraus Wissen her
  - Basis für Entscheidungen im Netzwerk
  
- Untersuchung von
  - Techniken für autonomes Management
  - Nutzermobilität
  - Interaktionsmöglichkeiten für Benutzer
  - Self\*- Funktionalitäten
  - Mechanismen und Protokollen für eine sichere Kommunikationsarchitektur
    - AA(A)
  - Middlebox (NAT/Firewall) Traversal Mechanismen





# AuthHoNe: Szenario

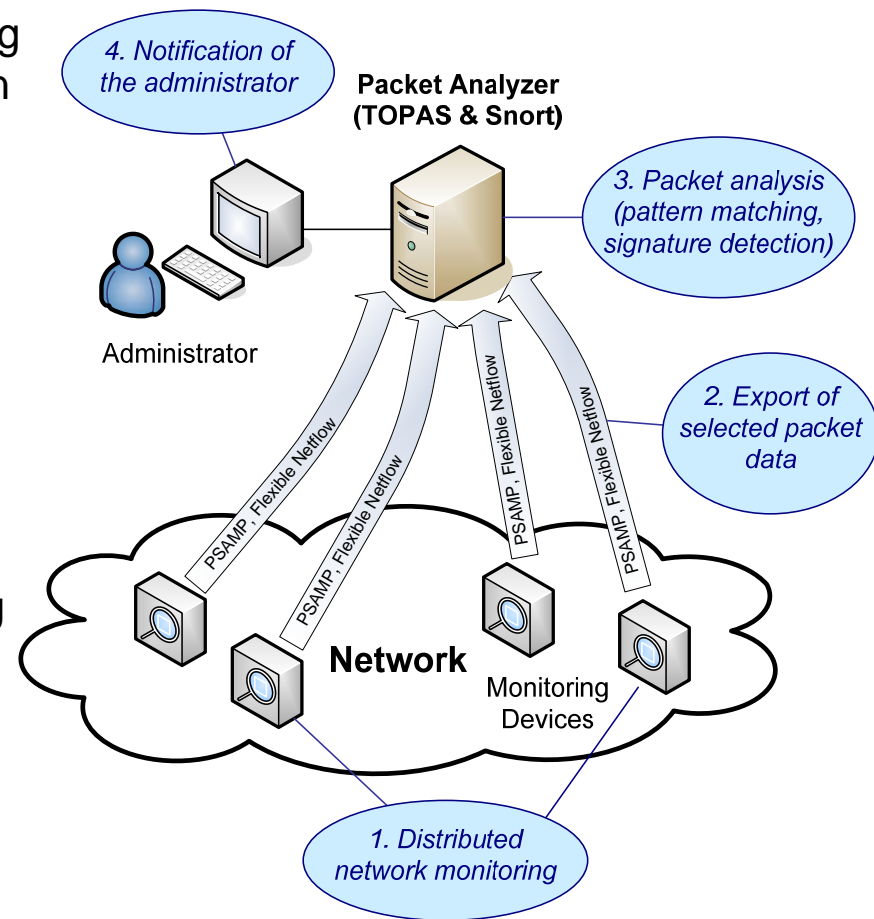
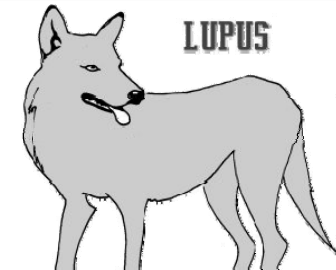
- ❑ Identitätsmanagement
- ❑ Wissenssammlung
- ❑ Benutzerschnittstelle?
- ❑ 2 Homes, Identifikation, Mobilität, Services





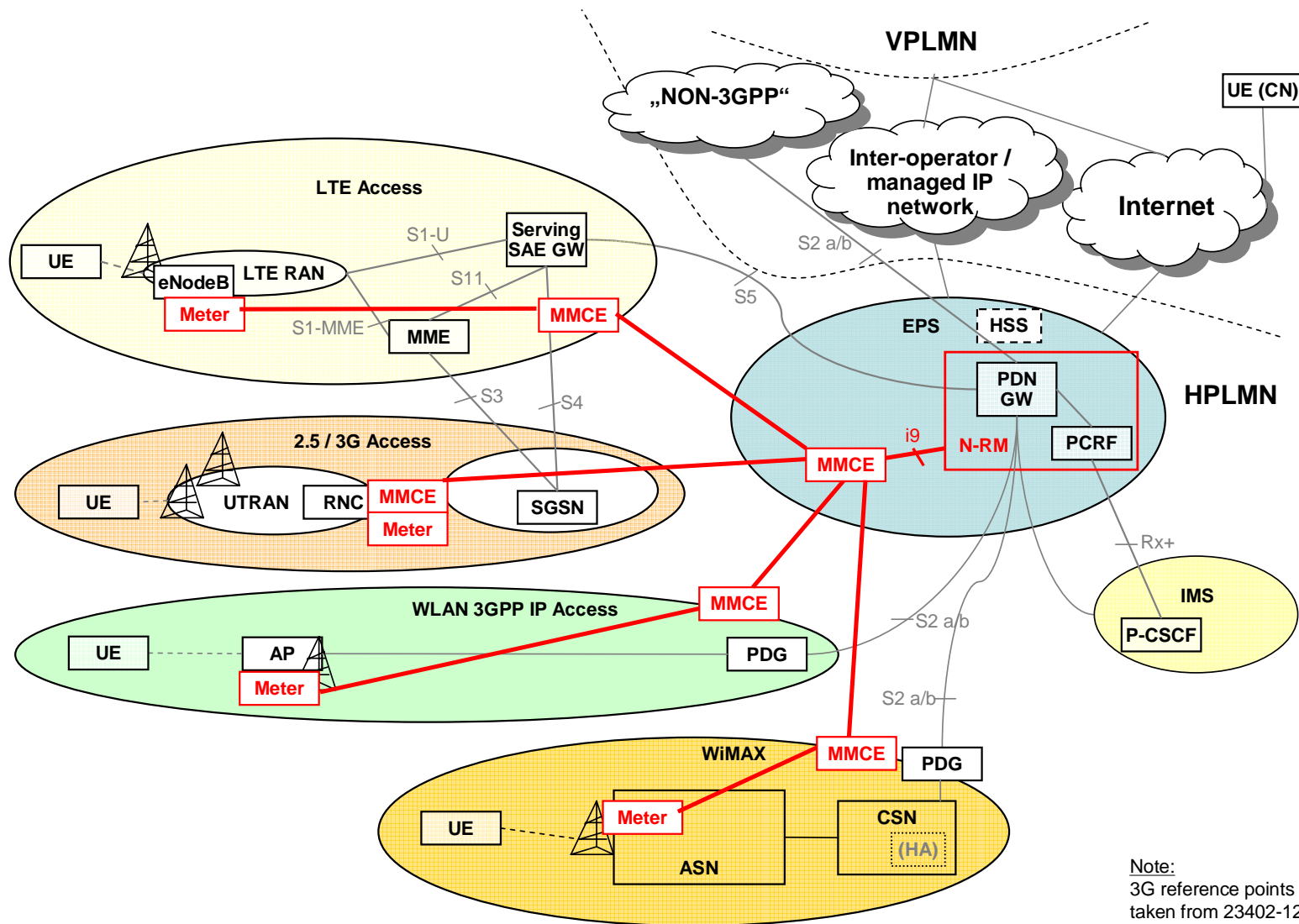
# DFG-Projekt LUPUS

- Projektpartner: Universität Hamburg (Prof. Wolfinger)
- Projektziele:
  - Modellierung von Datenströmen
  - Verkehrsmessung zur Charakterisierung und Klassifizierung von Verkehrsströmen
  - Neuartige Modellierungs- und Analyseansätze  
⇒ Sicherheit und Leistungsfähigkeit
- Beiträge:
  - Paketauswahlmechanismen für die Signaturerkennung in Verbindungen
  - Charakterisierung von Verkehrsströmen: Messung von Paketankunftsprozessen
  - Klassifizierung und Anomalieerkennung durch Data-Mining-Methoden  
⇒ Probabilistische Algorithmen, Bloom-Filter, ...





# Projekte mit Nokia Siemens Networks - Beyond-3G-Netze





# BMBF-Projekt ScaleNet (in Kooperation mit NSN)

## Management heterogener Zugangsnetze

- Szenario: Handover zwischen verschiedenen Zugangsnetzen UMTS, LTE, WLAN

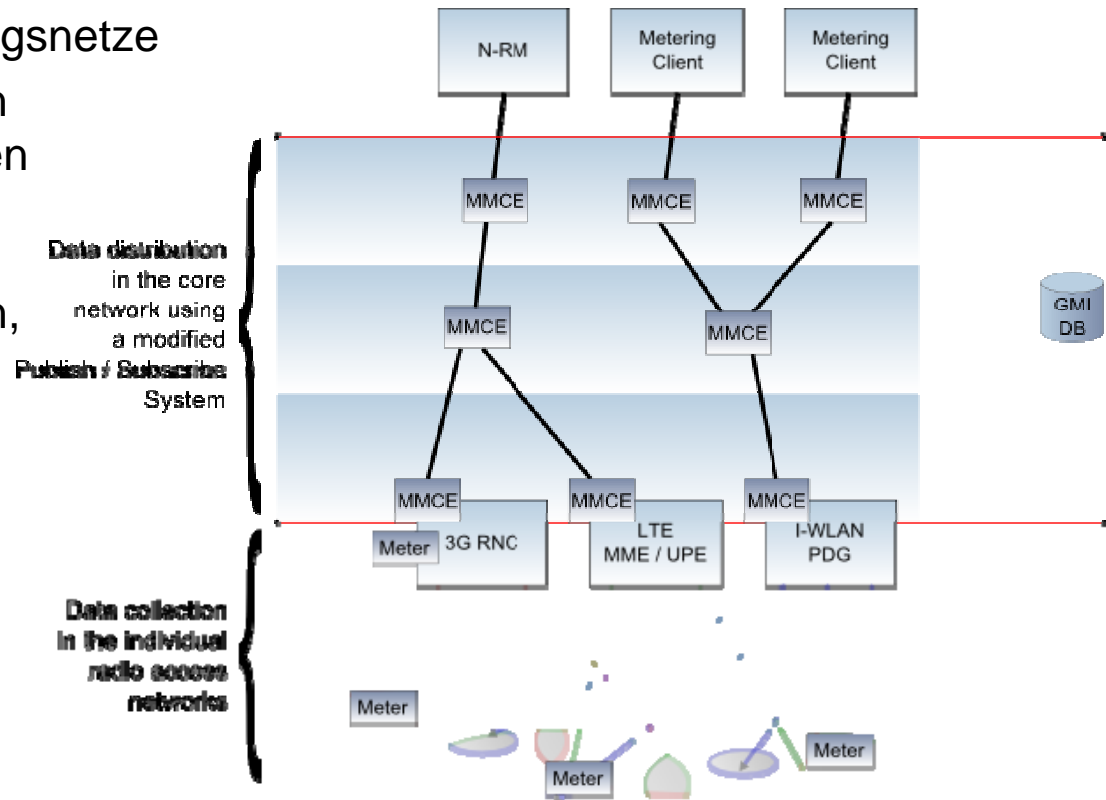
- Aufgabe: Messwerte erfassen, um Entscheidungen im Netz treffen zu können

- Benötigte Messwerte:

- Last in den Zellen
- Kanalqualität
- Position der Benutzer

- Generic Metering Infrastructure (GMI)

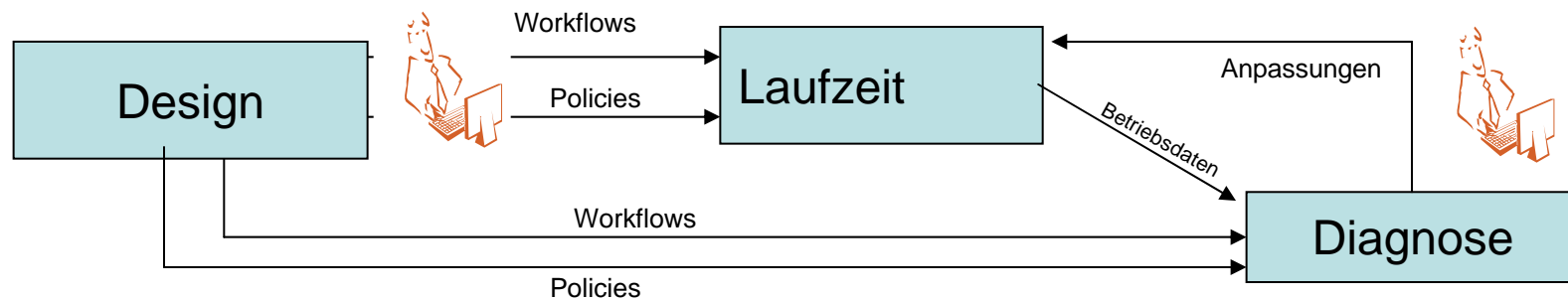
- Publish/Subscribe System angepasst an Mobilfunknetze
- Ziele: Effizienz, Skalierbarkeit, Flexibilität und Echtzeitfähigkeit
- Messaufträge: Periodisch, Getriggert, Request/Reply
- DNS-artige Adressierung der Daten, angelehnt an 3GPP Standards
- Optimierungen: Caching, Late Duplication, Protokolle für Backhaul-Links







# NSN-Projekt SelfMan: Management Selbstorganisierender Netze

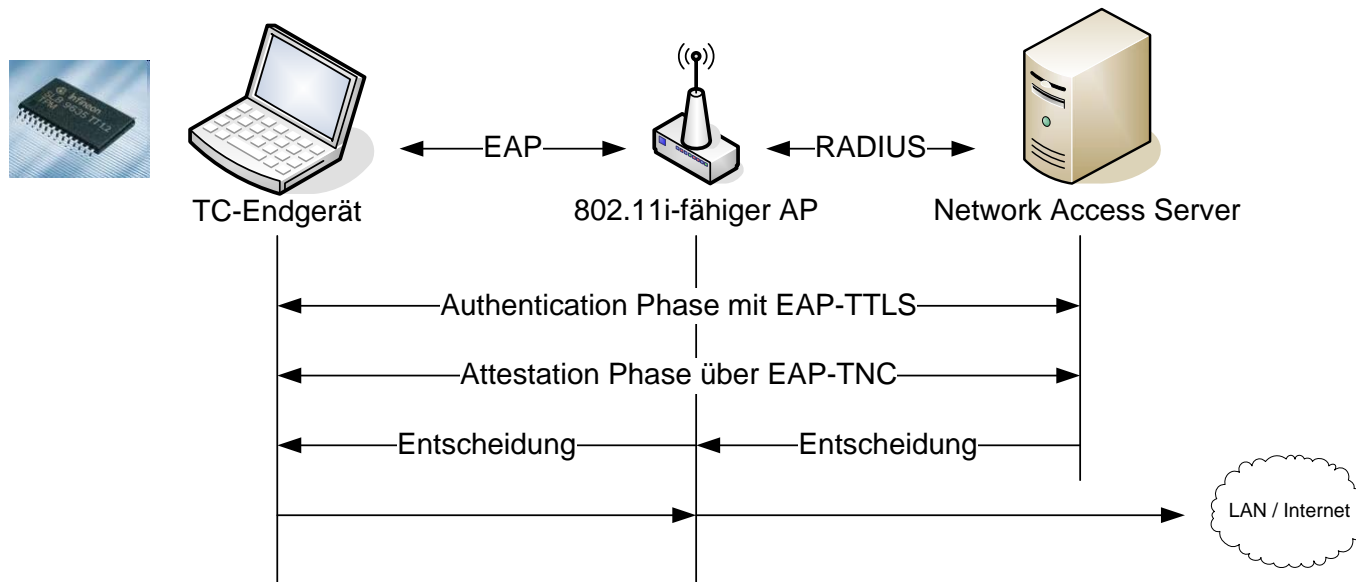


Design	Laufzeit	Diagnose
<ul style="list-style-type: none"><li>□ Spezifikation</li><li>- Abläufe, Bedingungen</li><li>Zusammenhänge</li><li>- Ziele: Konfigurationen, Optimierungen</li><li>⇒ Verhaltensvorgaben als Policies und Workflows in Laufzeitumgebung</li></ul>	<ul style="list-style-type: none"><li>□ System führt Workflows autonom aus</li><li>□ Workflows initiiert durch:<ul style="list-style-type: none"><li>- Ereignisse von außen</li><li>- Analyse von Betriebsdaten</li></ul></li><li>□ Elemente:<ul style="list-style-type: none"><li>- Workflow Execution Unit</li><li>- Policy Framework</li><li>- Wissensspeicher</li></ul></li></ul>	<ul style="list-style-type: none"><li>□ Speicherung von Messwerten</li><li>□ Analyse von Betriebsdaten</li><li>□ Anpassung von Workflows</li></ul>



# NSN-Projekt: Netzzugangskontrolle mit Trusted Computing

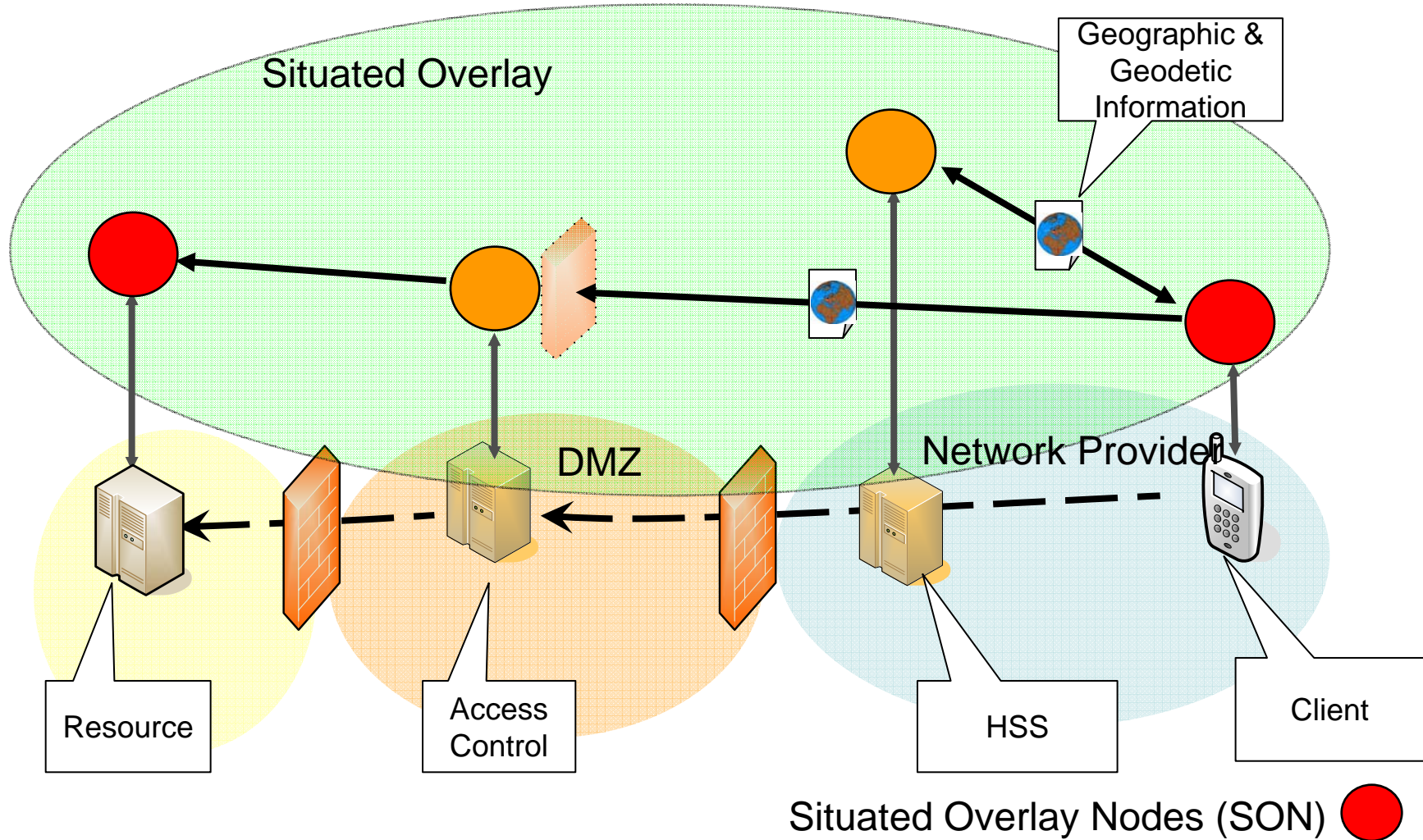
- Netzzugangskontrolle (Network Access Control – NAC)
  - für die Sicherheit des Netzes essentiell
- Traditionelle NAC-Ansätze authentisieren i.d.R. nur den User...
  - Problem: Passworte/Zertifikate zur Authentisierung können missbraucht werden
- ... und betrachten nicht die Konfiguration und Integrität des Geräts
  - Problem: mobile PC unter Benutzer-Kontrolle ggf. durch Malware kompromittiert
- Ansatz zur Erhöhung der Sicherheit durch NAC:
  - Zertifikate zur Authentisierung werden durch TPM geschützt
  - PC-Integrität/Konfiguration wird zuverlässig attestiert und netzseitig ausgewertet
  - Ansatz: Kombination von TC-Technologien mit NAC-Protokollen EAP-TTLS (Tunneled TLS) und EAP-TNC (Trusted Network Connect)





# France-Telecom-Projekt SASCO: Overlay Security

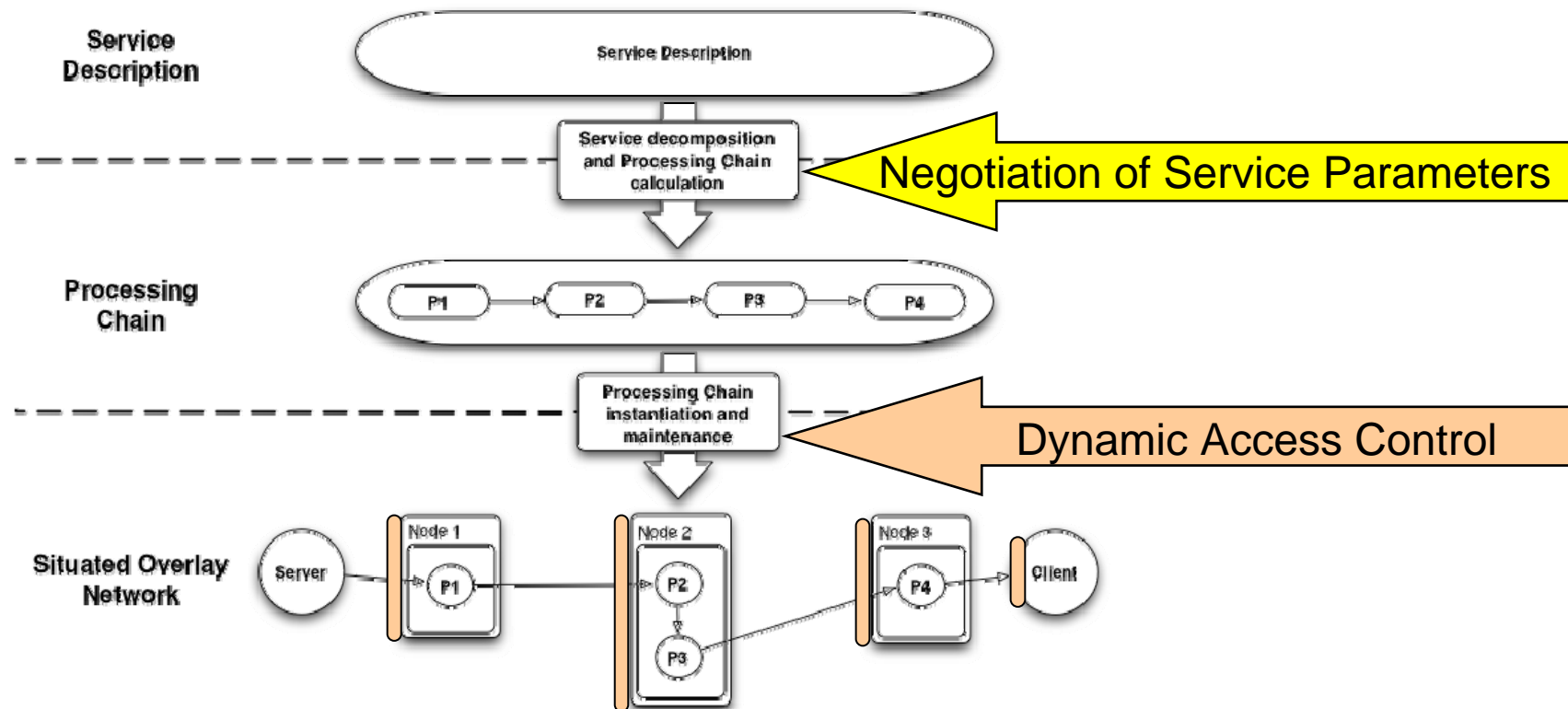
- Projekt SASCO
  - Kooperation mit France Télécom und Fraunhofer FOKUS





# 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

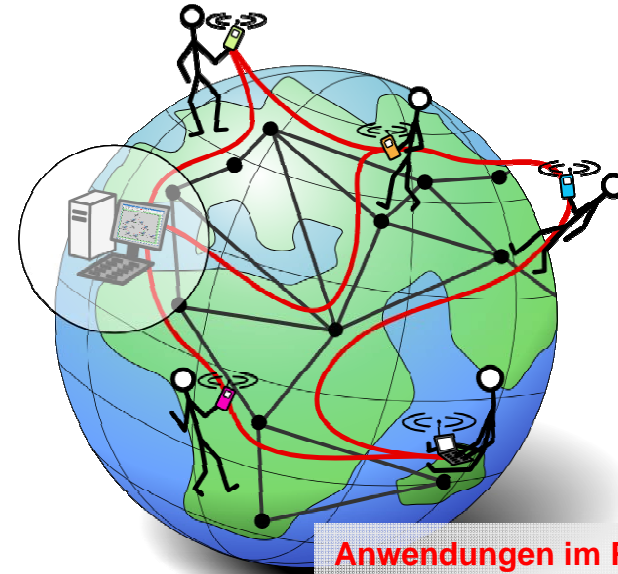
Prof. Dr. Paul Kühn  
Universität Stuttgart

Prof. Dr. Martina  
Zitterbart  
Universität Karlsruhe

Prof. Dr. Georg Carle  
TU München

Prof. Dr. Kurt  
Rothermel  
Universität Stuttgart

Prof. Dr. Wolfgang  
Effelsberg  
Universität Mannheim



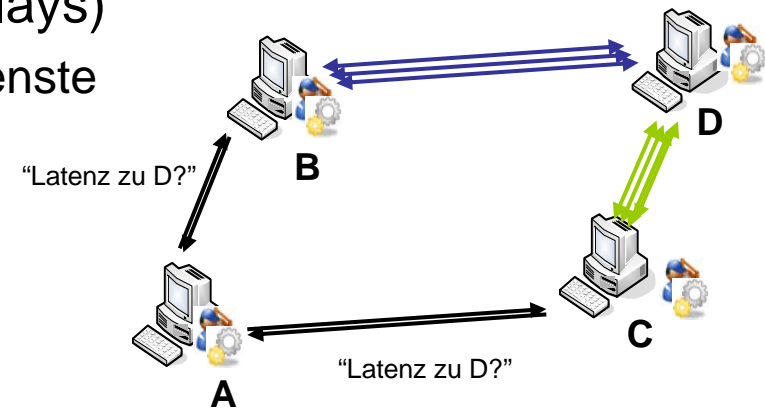
Anwendungen im Projekt:  
Video Streaming und  
Realzeitspiel

- 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



## 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



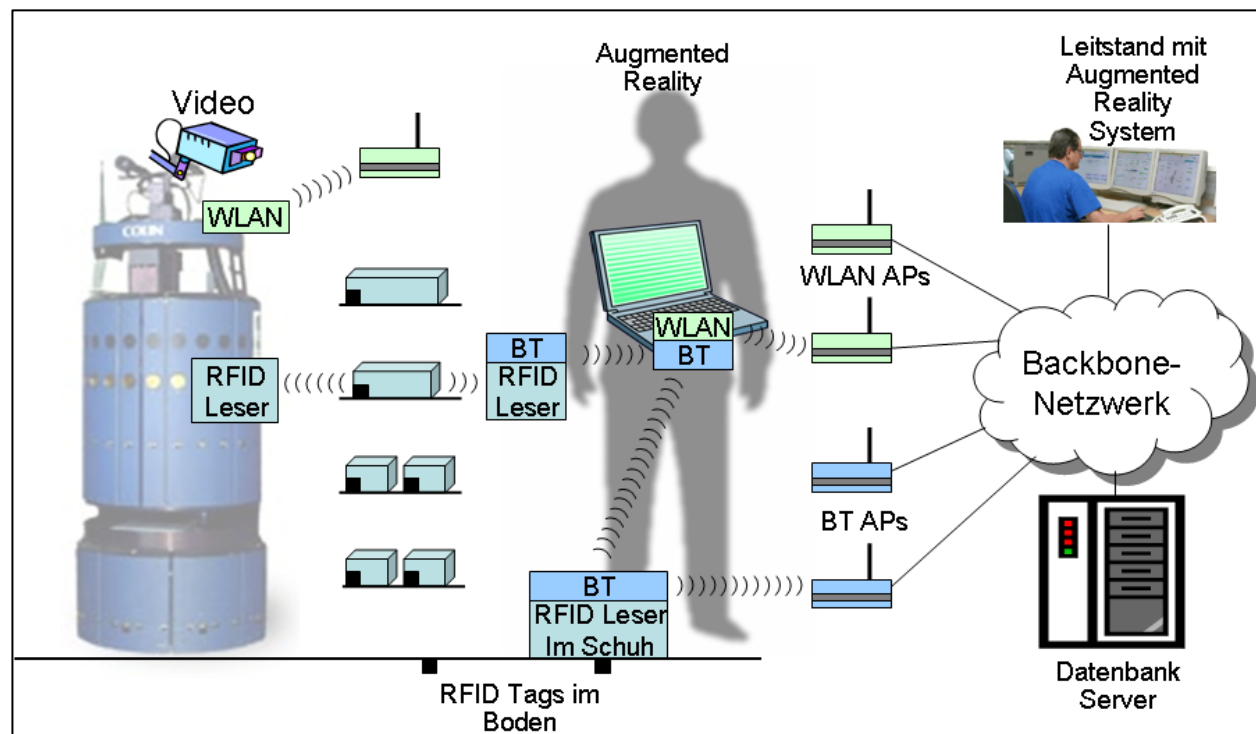
### Remote-Aufträge für CLIO

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



# BW-FIT-Projekt AmbiSense

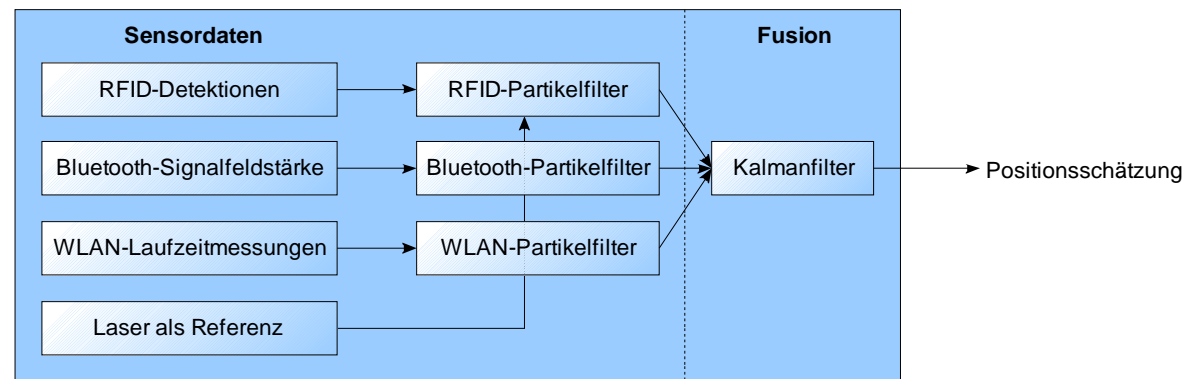
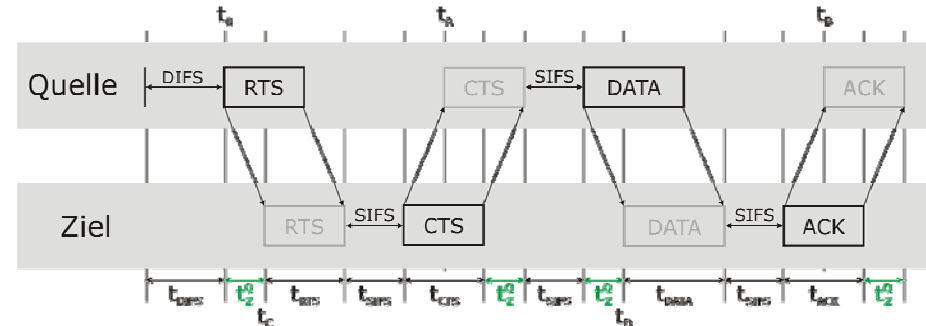
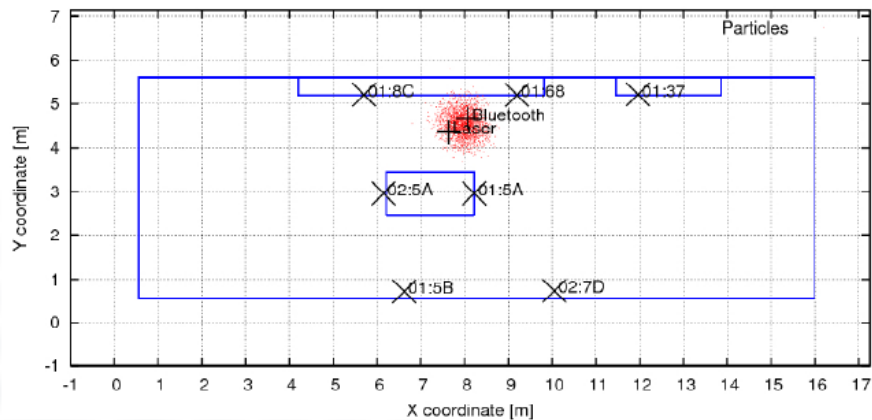
- ❑ AmbiSense: Kooperation autonomer mobiler Systeme unter Berücksichtigung ambienter Sensoren
- ❑ Partner: Prof. Zell, Rosenstiel, Straßer (Tübingen), Prof. Spath (Stuttgart)
- ❑ Anwendungsszenario
  - Zuordnung von Waren durch RFID
  - Ständige Positionsbestimmung
  - Abfrage von Zusatzinformationen
  - Darstellung auf PDA / Notebook mit Augmented-Reality-Technologie





# Ortsbestimmung mittels Sensorfusion

- ❑ Ziel: Robuste und präzise Ortsbestimmung mit WLAN, RFID, BT
- ❑ Laufzeitmessungen unter Ausnutzung von WLAN-Protokollabläufen
- ❑ Umsetzung: Statistische Fusionsverfahren (Kalman- / Partikelfilter)







## Zusammenfassung und Ausblick

- ❑ Beteiligung an Entwicklungen des Future Internet, zukünftiger mobiler Netze, Sensor-Aktor-Netze
- ❑ Technologien: P2P, Autonomes Management, Self\*-Funktionalitäten, UMTS/LTE, Trusted Computing, RFID, ...
- ❑ Themen, Technologien und Methoden: Anknüpfungspunkte für weiterführende Aktivitäten

