Overlay Networks in ScaleNet

Dipl-Inform. Ingmar Baumgart
Prof. Dr. Martina Zitterbart

VDE ITG 5.2.1 Fachgruppentreffen, Ericsson, Aachen, 5.5.06

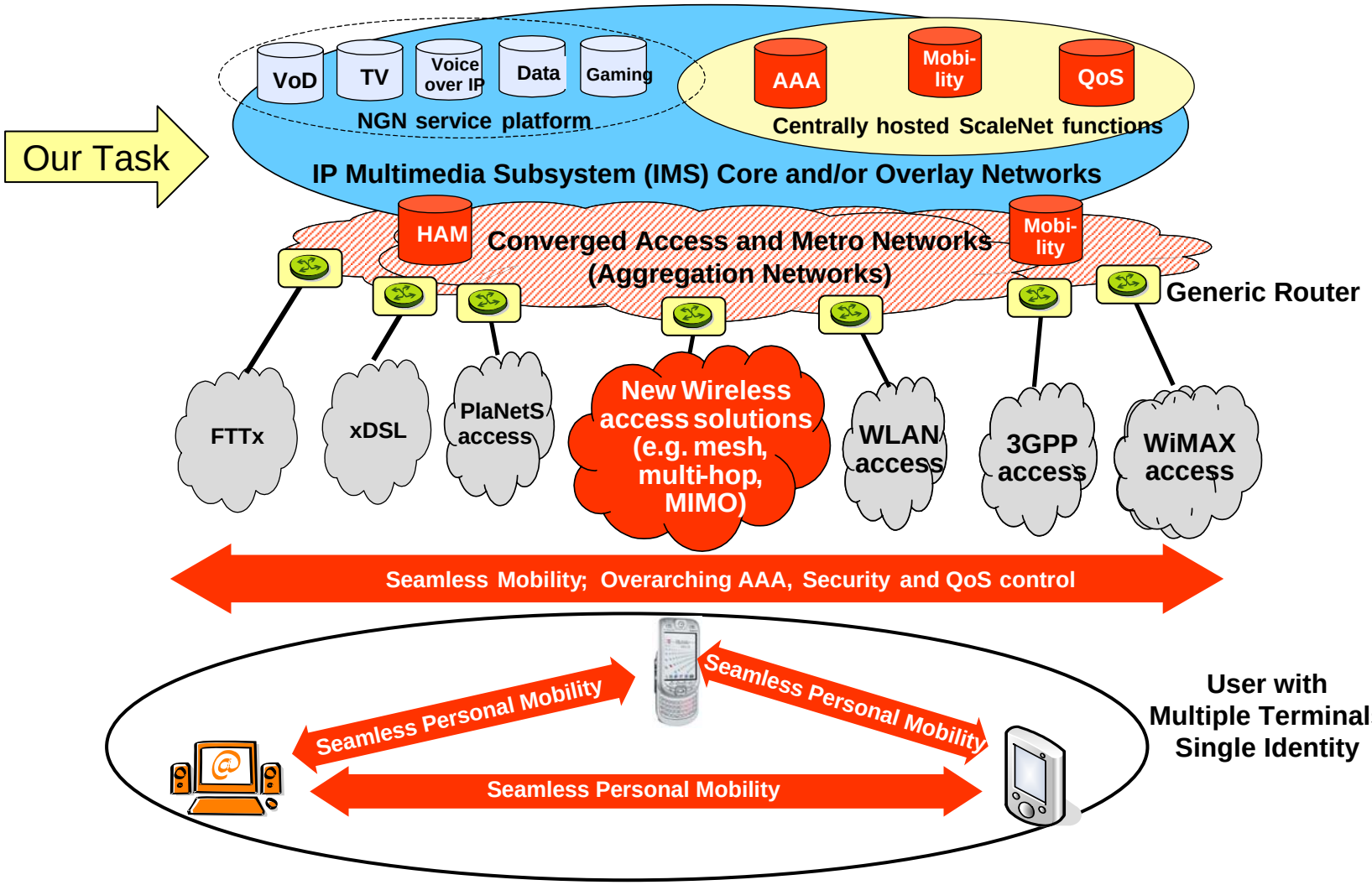
Institut für Telematik, Universität Karlsruhe (TH)

The ScaleNet Project

- ScaleNet: Scalable, efficient and flexible next generation converged mobile, wireless and fixed access networks
- Project duration: 1.7.2005 – 30.9.2008
- Partners:

ALCATEL
Deutsche Telekom
HHI
Institut Nachrichtentechnik Heinrich-Hertz-Institut
ERICSSON
Gefördert vom bmb+f Bundesministerium für Bildung und Forschung
Lucent Technologies Bell Labs Innovations
SIEMENS
QUALCOMM CDMA Technologies
TeleMatics

ScaleNet High Level Architecture



ITM Sub Project: Overlay Networks

- ITM sub project: Overlay technologies for flexible and cost-efficient introduction of new services in heterogeneous networks

- Why use overlay networks in ScaleNet?
  - Fast, cost-efficient deployment of new services
  - Flexibility (i.e. extension by new access networks)
  - Reduction of complexity in the core network

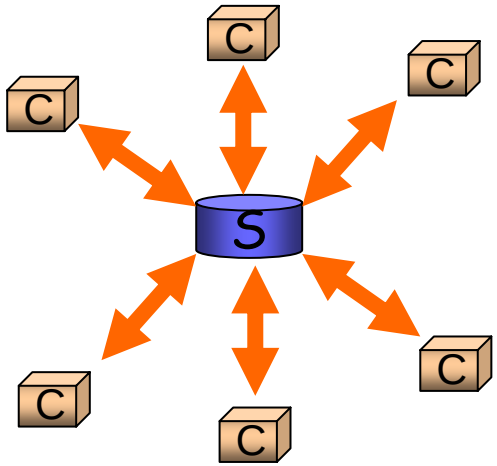
- ITM work packages:
  - Anforderungsanalyse an ein ScaleNet (AP 1.1)
  - Mitwirkung am Entwurf der ScaleNet-Gesamtarchitektur (AP1.2)
  - Overlay-Technologien für User-Plane (AP 3.2.8)
  - Entwurf einer generischen Overlay-Schnittstelle (AP 4.2.2)
  - Beteiligung an Gesamtdemonstrator (AP 5.6)

Overlay Networks

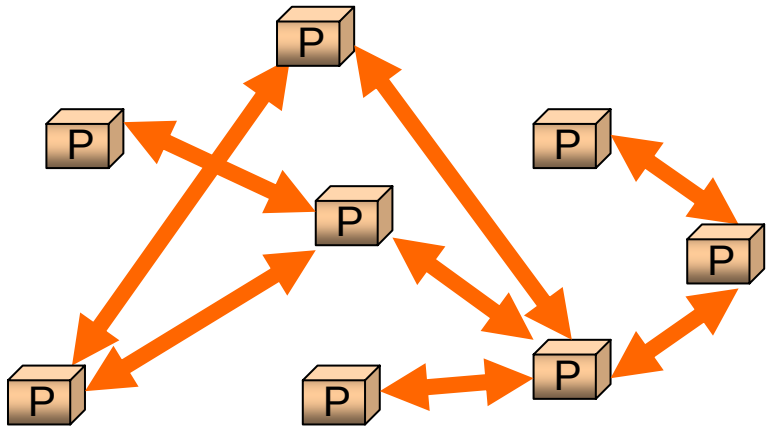
- What are overlay networks?
  - Two applications communicate via a path different from the path determined by the underlying network topology
  - Logical network above underlying topology
    - Independent routing
    - In most cases: Independent addressing scheme
- Overlay networks ≠ Peer-to-Peer systems
  - But: Most P2P systems are overlay networks
    - DHT, Gnutella, Freenet…
  - Overlay networks, that are not P2P
    - VPN, MPLS, …
  - Research focus: Peer-to-Peer systems

Peer-to-Peer Systems

- Equivalent, autonomous entities (peers)
- No central infrastructure elements
- Self organization
- Interaction of end-systems
- Shared resources in end-systems
- Moving the complexity to the edges of the network



Client/Server



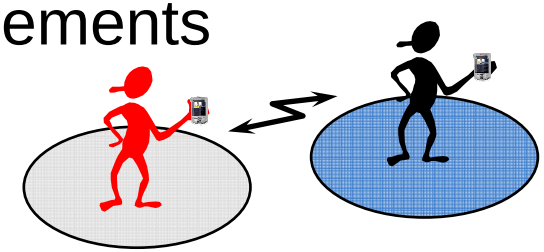
Peer-to-Peer

Advantages of P2P Systems

- Rapid introduction of new services
  - No changes in routers required
  - Realization of long demanded services:
    - Multicast
    - Anycast
  - No time-consuming standardization required
- Scalability
  - No costly central servers with scalability problems
- Reliability
  - No single point of failure
  - Protection against DoS attacks by redundancy and self organization

Overlay Networks in ScaleNet

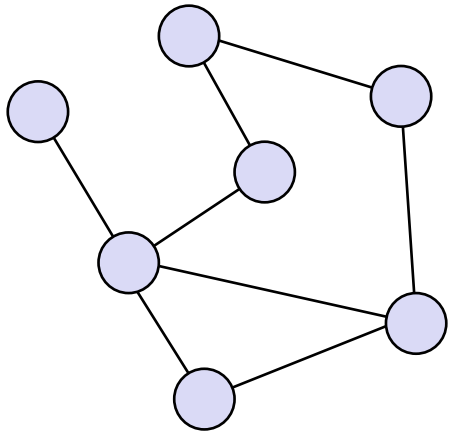
- Today's overlays are developed for use in the Internet
- ScaleNet scenario poses other requirements
  - Heterogeneous access networks
  - Heterogeneous terminals
  - Terminal mobility



- Overlays have to reflect changed requirements
  - Consequences of heterogeneous access networks and end-systems?
  - Consequences of terminal mobility?
  - How to optimize the overlays (topology adaption)?
  - Usage of cross-layer information for optimization?
  - Adequate overlay structures (structured vs. unstructured)?

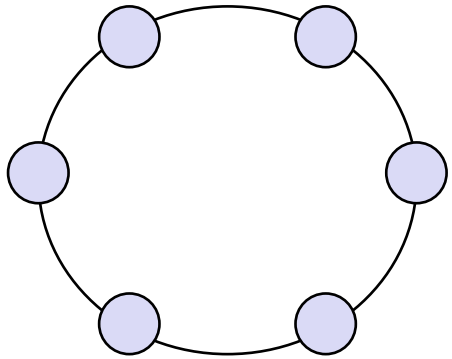
Two Kinds of P2P Overlays

- Unstructured overlays
  - Random choice of neighbors
  - Routing by flooding or random walk
  - Example: Gnutella, Freenet



Unstructured

- Structured overlays
  - Overlay neighbors are chosen to form a certain topology
  - Structured topology allows for efficient routing
  - Example: Chord, CAN, Pastry, Tapestry, Kademlia, Koorde



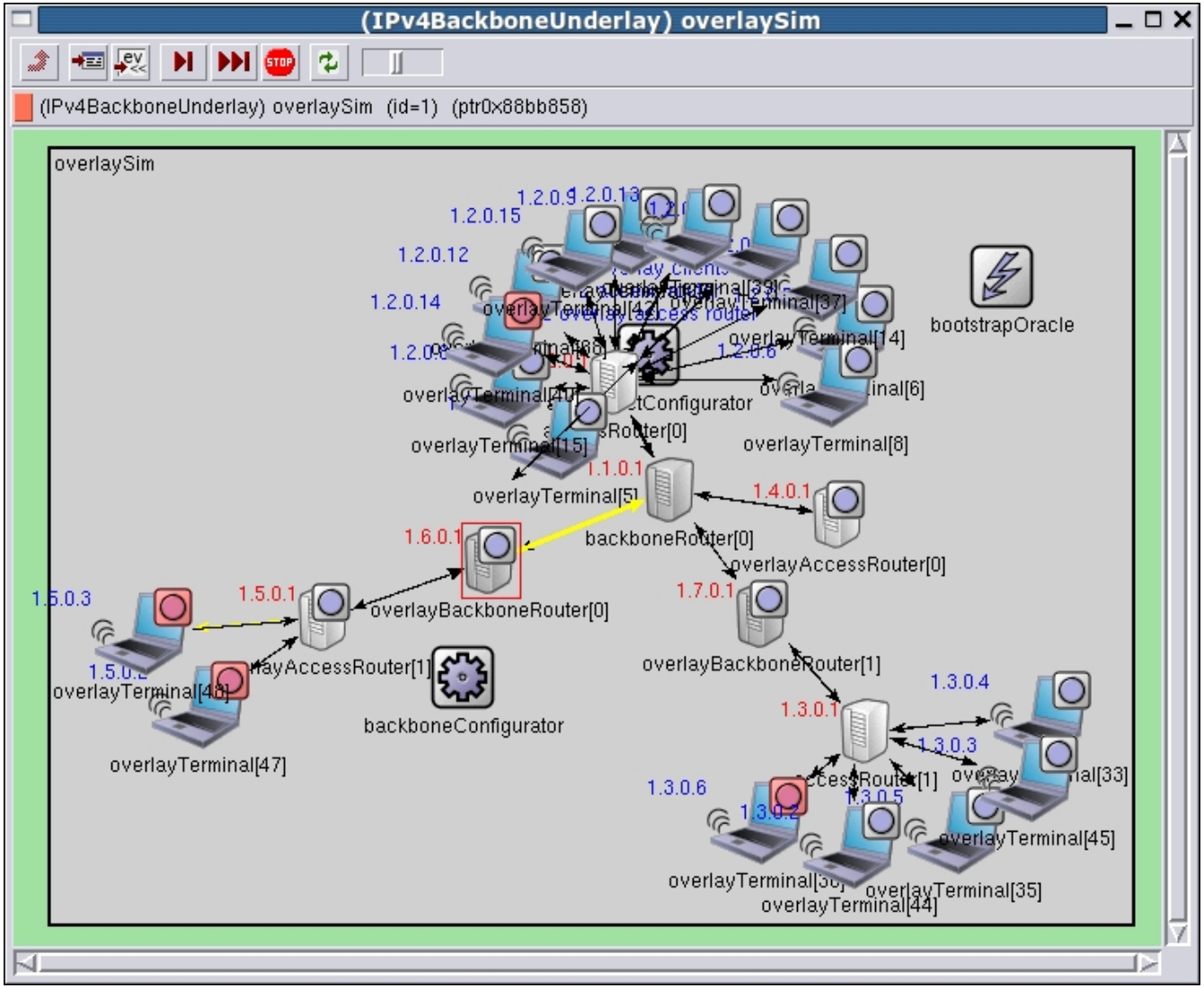
Structured

ITM Overlay Simulator

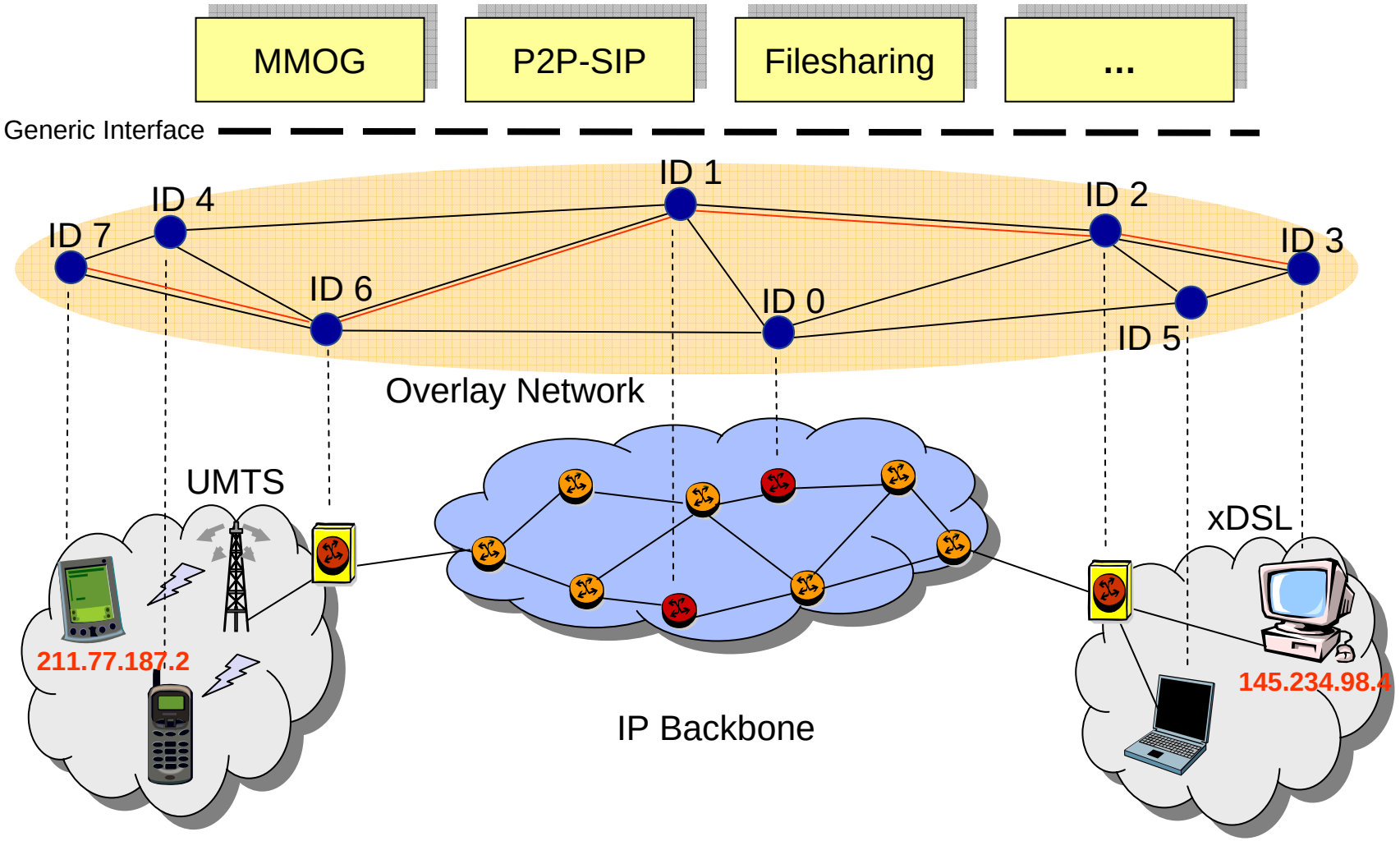
- Simulation environment OMNeT++
- Modular design:
  - Exchangeable overlay network
    - Chord, GIA, Kademlia, …
  - Configurable underlay
    - IPv4, IPv6, simple, realUDP, …
      - mobility
      - heterogeneity
  - generic interface
    - KBR, DHT, …
  - miscellaneous applications

→ simulation and analysis of different overlays over a typical ScaleNet underlay toplogy

ITM Overlay Simulator in Action



Architecture: ScaleNet-Overlays



ITM Overlay Scenarios

- Possible applications for overlay networks in ScaleNet:
  - Group communication (multicast, anycast)
  - Distributed storage
  - Mobility support

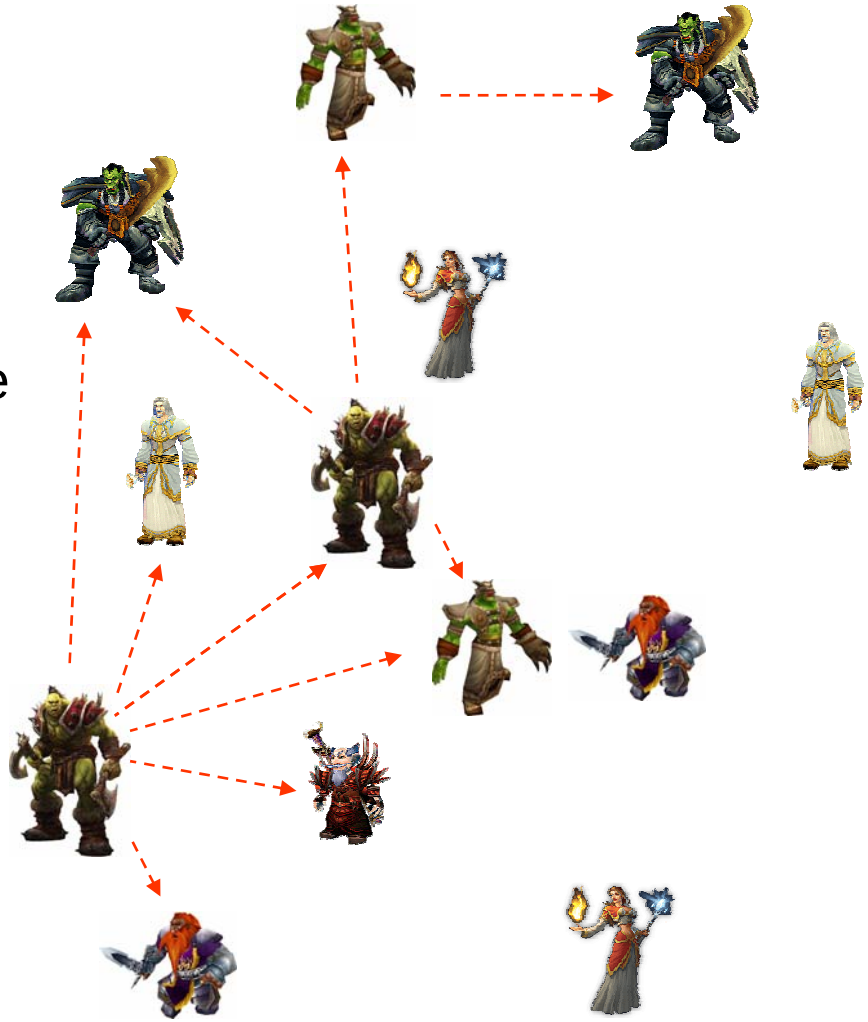
- We focus on two scenarios:
  - Massively Multiplayer Online Gaming (MMOG)
    - Application Layer Multicast
    - Large number of participants
    - Low latency / QoS support
  - Peer-to-Peer SIP
    - Distributed storage of SIP identities
    - Security

Massively Multiplayer Online Gaming

- Current situation in commercial MMOGs: „Server Farms“
  - Unicast connection between every player and one of the servers
  - Does not scale with the number of players
  - Does not support more than a few thousand players
- Use of overlay technologies to avoid this bottleneck
  - Not all communication has to go through the central server
- Requirements
  - Low latency
  - Highly dynamic multicast groups
  - Security
    - Must not introduce new ways of cheating

Multicast

- Group chat
  - Players in the same group/party communicate
  - Groups stay active for a longer time
  - Possible high bandwidth use (voice/video chat)
- Event messages
  - Send to all nearby players
  - No fixed groups
  - Communication partners change frequently



Peer-to-Peer SIP

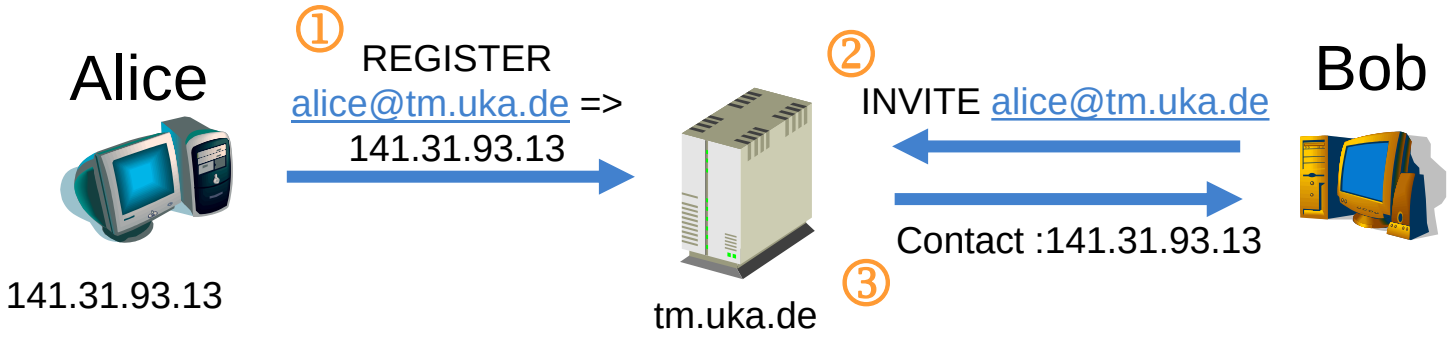
- What is P2P-SIP?
  - Using a peer-to-peer network for SIP user registration and location lookup

- Why P2P-SIP?
  - Cost reduction (no servers needed)
  - Scalability
  - Reliability (No single point of failure, self healing)
  - Failover for server-based SIP networks (in emergency cases)
  - NAT traversal

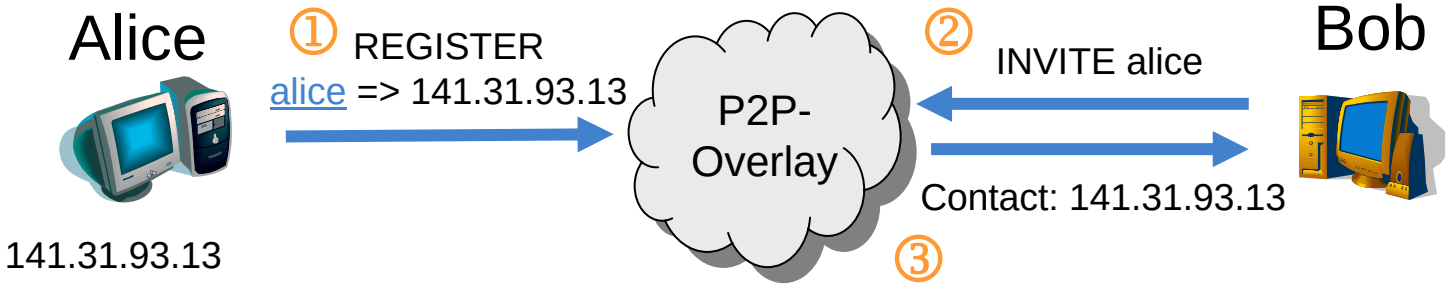
➔ Skype (largest VoIP provider in the world) also uses P2P technologies, but no open standard

Server-based SIP vs. P2P-SIP

- Call setup with server-based SIP:

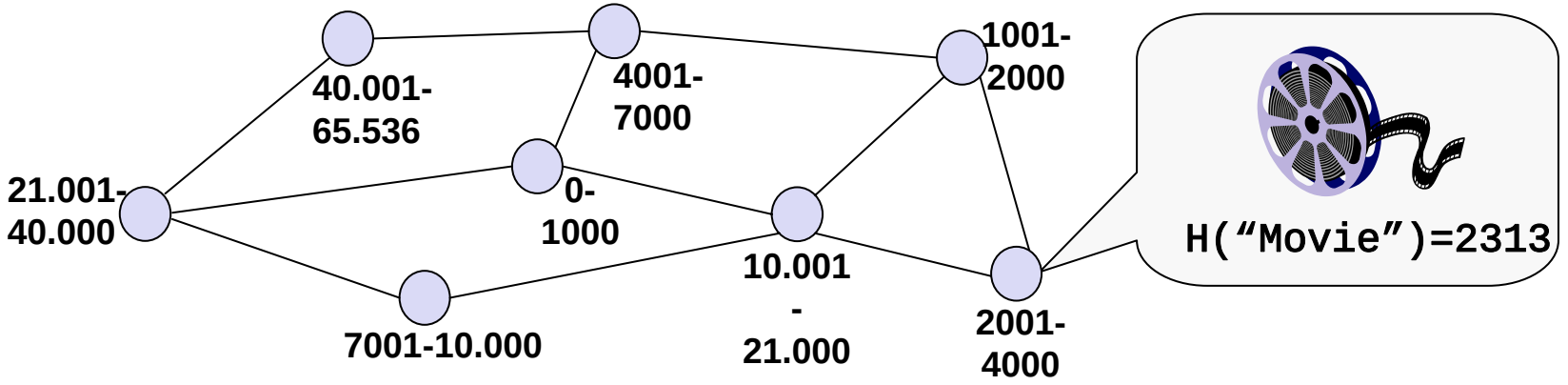


- Call setup with P2P-SIP:



Distributed Hash Tables (DHTs)

- Main idea
  - Distributed storage of (key, value) pairs
  - Efficient lookup of keys
- Challenges:
  - Equal distribution of content in the network
  - Continuous maintenance due to churn
    - Assigning of key ranges to joining nodes
    - Takeover and redistribution of key ranges in case of node failures



DHT security: Common attacks

- Attacks on routing
  - Node ID selection
    - By carefully choosing a node ID an attacker can control access to target objects
  - Routing table maintenance
    - DoS attack by distribution of faulty routing table updates
  - Message forwarding
    - Malicious nodes along the route between sender and target node can modify or drop messages to a key
- Attacks on data storage:
  - Malicious nodes can modify or delete locally stored data items

P2P-SIP: Open issues

- Unique assignment of user names
- Security
  - Security of Distributed Hash Tables
  - DoS resistance
  - Prevent stealing of user names
- Optimization
  - Selection of most suitable DHT structure (Chord, Kademlia,…)
  - Reduce bandwidth / lookup latency by
    - Topology adaptation
    - Load balancing
- Deployment
  - Gateways to server based SIP networks

➔ Still no open standard for P2P-SIP
  - IETF: Ongoing discussion on forming a P2P-SIP WG

Next steps

- Implementation and analysis of additional overlay protocols (GIA, Kademlia, …)
- Implementation of a SIP-proxy for P2P-SIP
  - Unique assignment of user names
  - Prevent stealing of user names
  - Secure DHT based on Kademlia

- Analysis of attacks on already deployed DHTs (e.g. eMule-Kademlia)
- Detailed analysis of QoS requirements for MMOGs (latency and bandwith)

Thanks!

Questions?