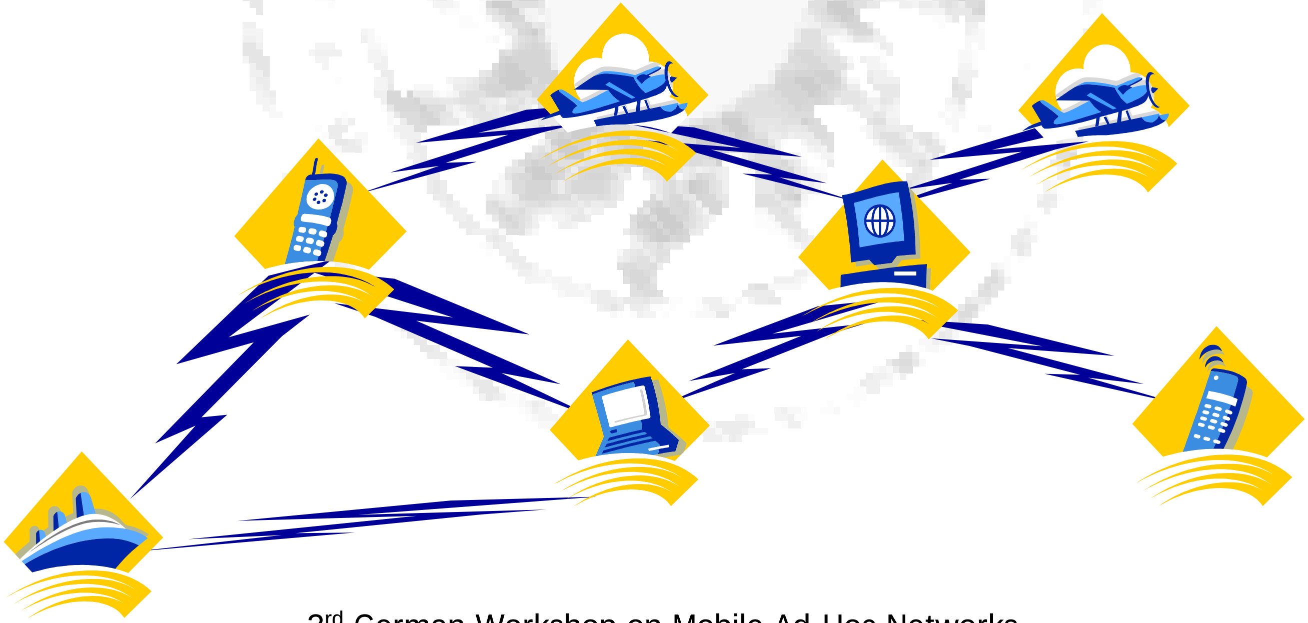
Requirements for Privacy-Enhancements in Mobile Ad Hoc Networks

Christer Andersson, Leonardo A. Martucci
and Simone Fischer-Hübner

Karlstad University - Sweden

Mobile Ad Hoc Networks

- Main characteristics
  - A wireless network
  - No central administration
  - Mobile nodes join and disjoin spontaneously.
  - The nodes both serve as hosts and routers



Ad Hoc Networks and Privacy

- Nature of data being transmitted on ad hoc networks
  - Vast amounts of possibly sensitive data
    - Personal data
      - General interests, communicating partners, Internet browsing, shopping preferences, ..
    - Location information
      - Location of your communicating peers, your location history, etc.
  - Behavioral Patterns

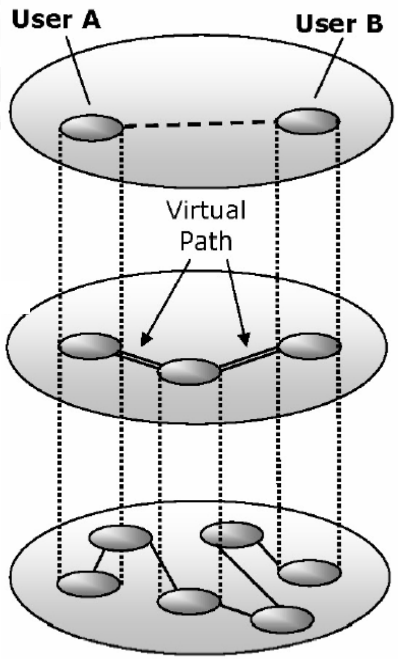
➡

Ad Hoc Networks and Privacy

- How to achieve privacy in ad hoc networks?

⇨ Anonymous Overlay Networks

  - Classic solution – good enough for ad hoc environment
  - Placed in-between ad hoc routing and application layers



Application Layer

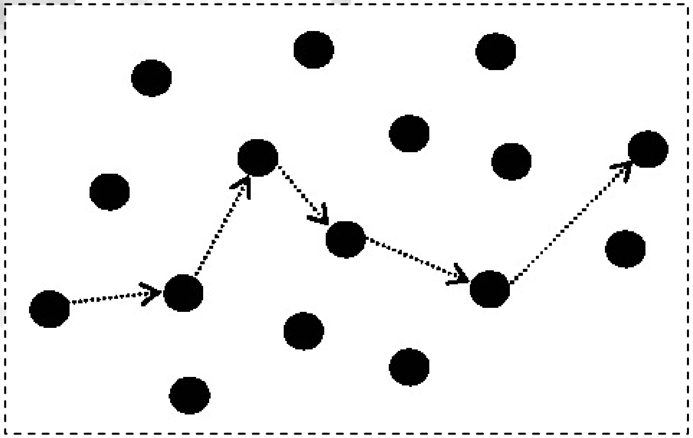
Anonymous Overlay Network

Ad Hoc Routing Layer

Anonymous Overlay Network

- Overlay network
  - A virtual network that is built on top of an existing network in order to implement network services not available in the existing network

- Anonymous overlay network
  - Provide anonymous services in networks where such services normally are lacking



Goal

- Define requirements for Anonymous Overlay Networks
  - Defined after mobile ad hoc network characteristics

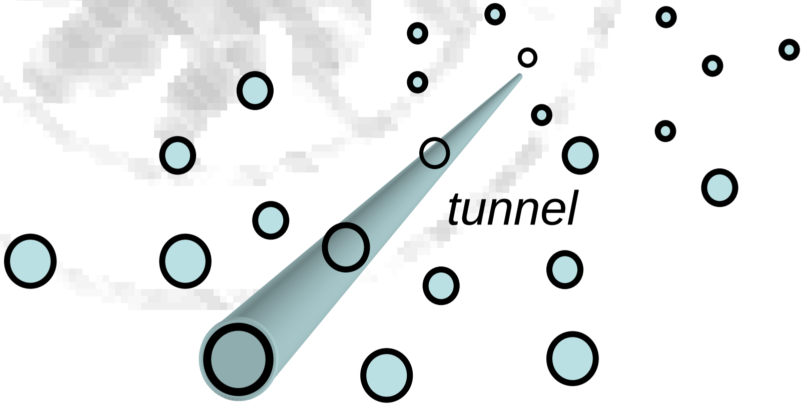
- Evaluate P2P anonymous overlay networks against the defined requirements

Overlay Network Requirements

- Six requirements were defined:
  - R1 – scalable solution
  - R2 – strong anonymity properties should be provided
  - R3 – fair distribution of workload among participants
  - R4 – performance-wise lightweight solution in terms of number of needed messages to set the anonymous path and number of high demanding operations
  - R5 – adherence to P2P model (no dependencies of fixed devices)
  - R6 – expected performance in dynamic topologies, especially regarding tunnel repairing

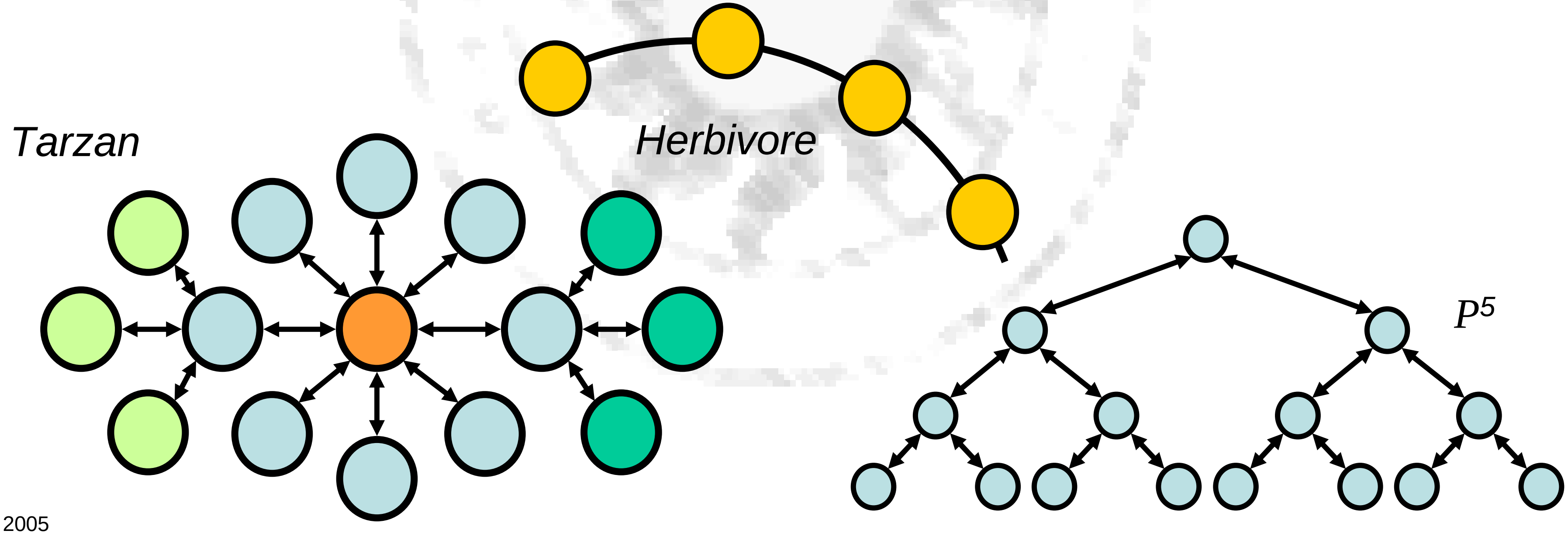
Anonymous Overlay Networks

- Well-known P2P anonymous overlay networks were evaluated:
  - Crowds – users are gathered in crowds of users and messages are forwarded among them.
  - Hordes – Crowds-like, but with a multicast return channel.
  - MorphMix – collusion detection mechanism in the tunnel setting.



Anonymous Overlay Networks

- Tarzan – messages are hidden in a continuous traffic flow; it also implements a collusion prevention mechanism
- Herbivore – nodes are divided in small anonymous clusters (“cliques”)
- P^5 – a continuous flow of messages is set in an binary tree



Evaluation of Anonymous Overlay Networks

- R1 - Scalability
  No clear evidence against the scalability of those mechanisms

- R2 - Strong anonymity properties should be provided
  Crowds, Hordes and MorphMix are not robust against strong adversaries. Tarzan mechanism is not suitable for ad hoc networks (IP Subnets)

- R3 - Fair distribution of workload
  MorphMix and P^5 have unbalanced workload distribution

Evaluation of Anonymous Overlay Networks

- R4 - Performance-wise lightweight solution
  Tarzan and P^5 rely on dummy traffic; MorphMix demands a lot of messages to set the paths and Herbivore presents high latency

- R5 - adherence to P2P model
  Crowds, Hordes are dependent on central devices. Herbivore and P^5 dependent on central parameters

- R6 - Performance in dynamic topologies
  MorphMix and Herbivore are not efficient in dynamic networks, as no tunnel repair is done.

Conclusion

- None of the analyzed mechanisms is fully suitable for use in mobile ad hoc environments

- Next Steps:
  - Design an overlay anonymous communication mechanism that adheres with the presented requirements and define trade-offs, if needed
  - Simulate the new mechanism

{christer.andersson, leonardo.martucci, simone.fischer-huebner}@kau.se