08/08/2007

Identity Deployment and Management

in

Wireless Mesh Networks

Leonardo A. Martucci[†], Albin Zuccato[‡]
and Simone Fischer-Hübner[†]

[†] Karlstad University [‡]TeliaSonera R&D

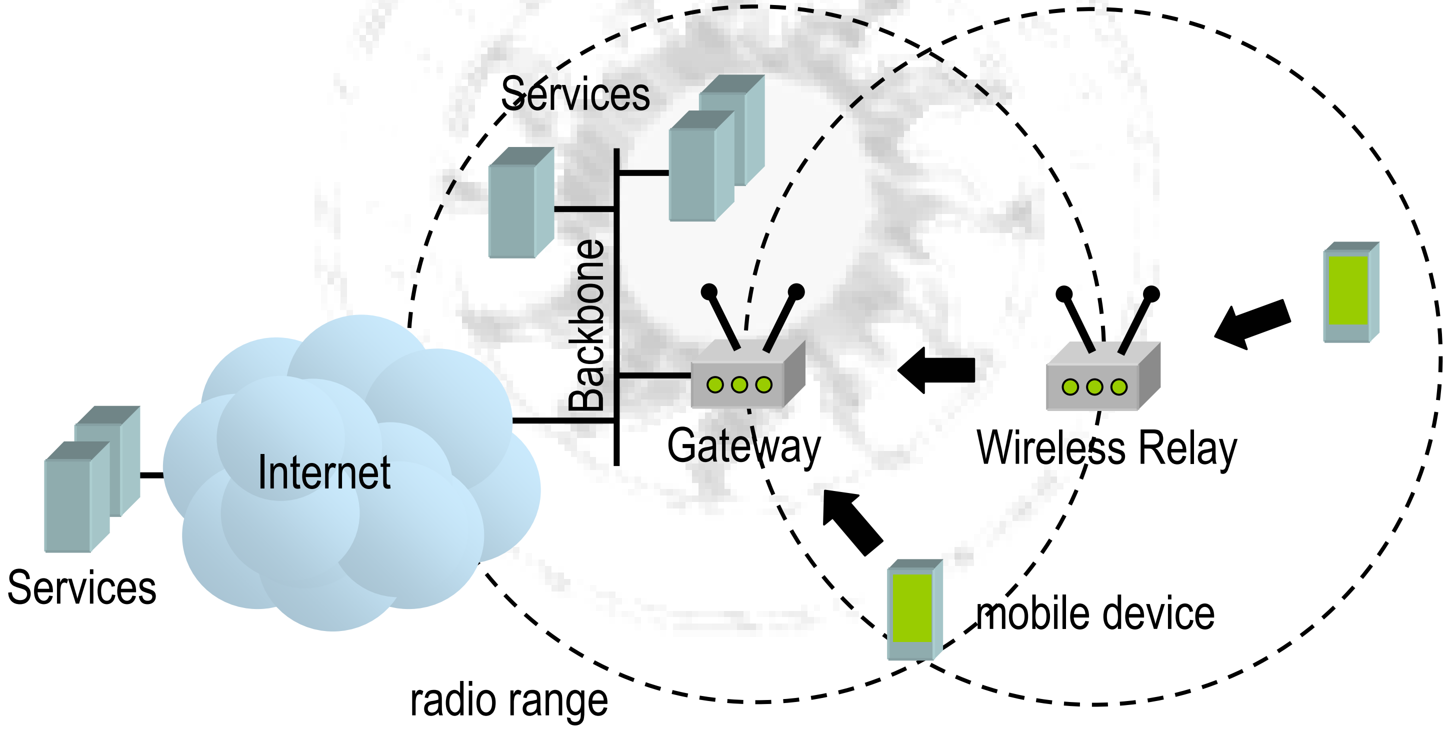
IFIP/FIDIS SS

Outline

- Wireless Mesh Networking
    - introduction, challenges and threats
- Requirements and Objective
- Identities and IdM System
- Business Model

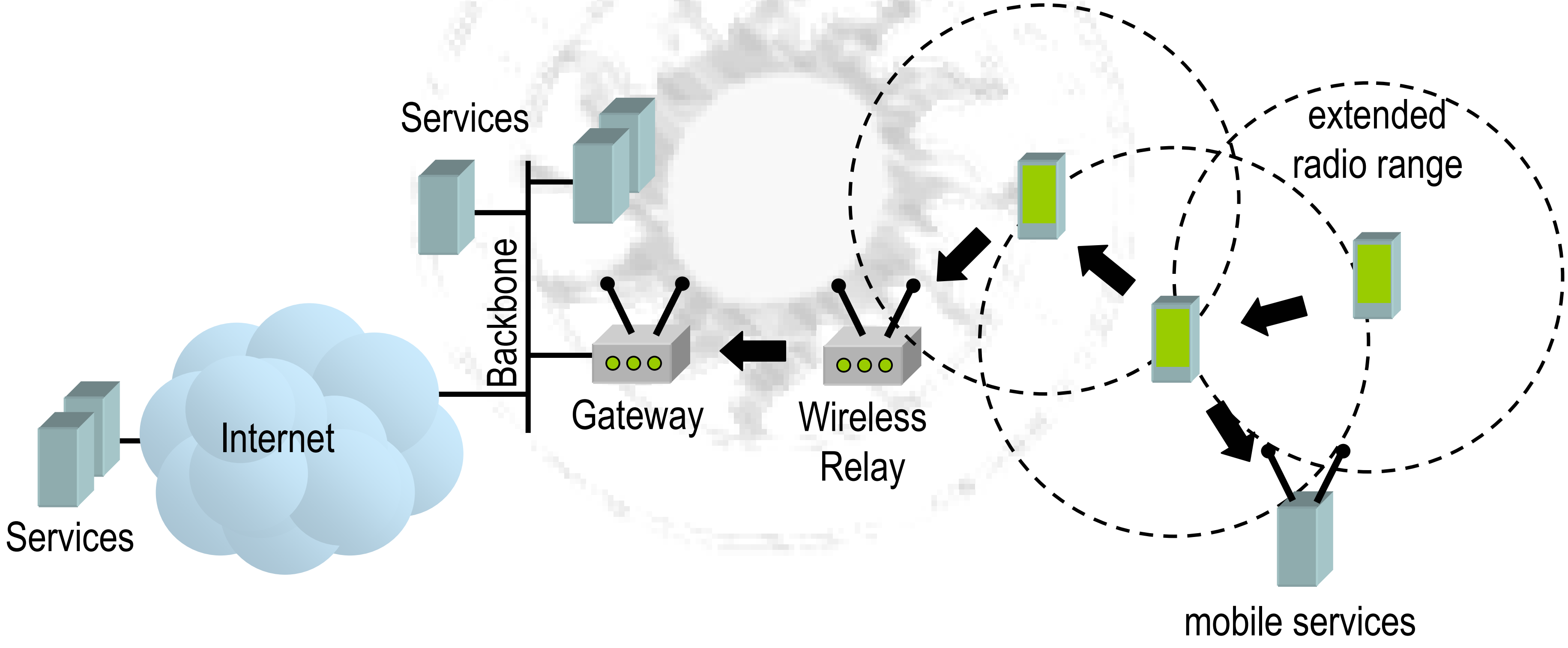
Wireless Mesh Networks

- Extension of the network radio range using wireless relays
  - affordable technical solution – but not yet standardized



+ Ad Hoc Networking

- To increase the network radio range even further
  - using client devices to route data

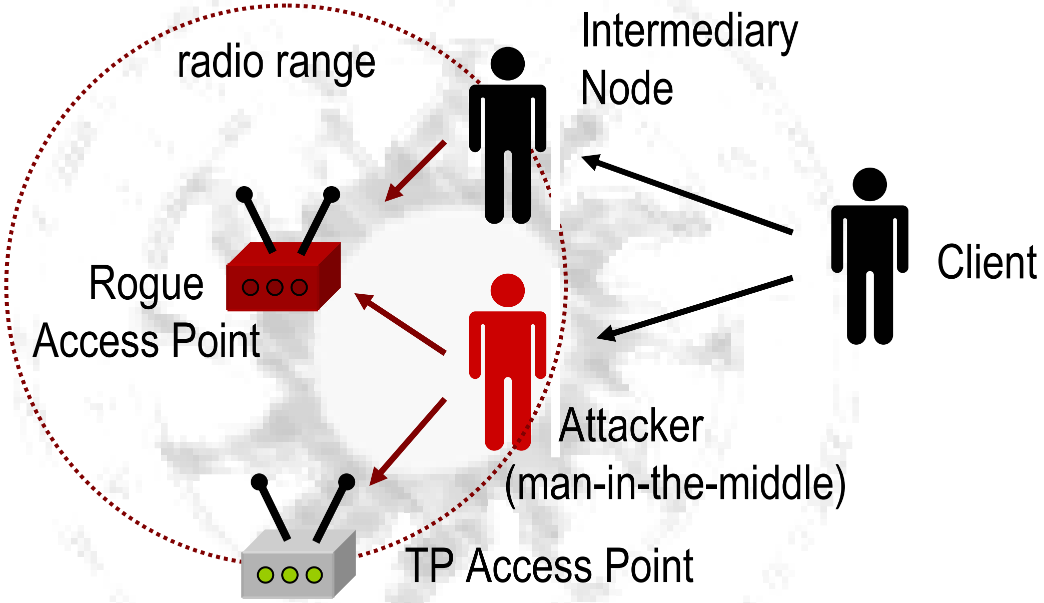


A Challenging Scenario

- Performance Aspects
  - e.g. routing, QoS, transport layers, roaming, convergence.
- Economic and Business Problems
  - e.g. differentiated billing, rewarding, user cooperation
- ➡ Security and Privacy Aspects
  - e.g. identity management, privacy, authentication mechanisms

Threats and the Trivial Solution

- Security and Privacy threats include:



- Trivial Solution ⇨ PKI deployment on the Telecom Provider
  - good enough for security purposes, but not good for privacy

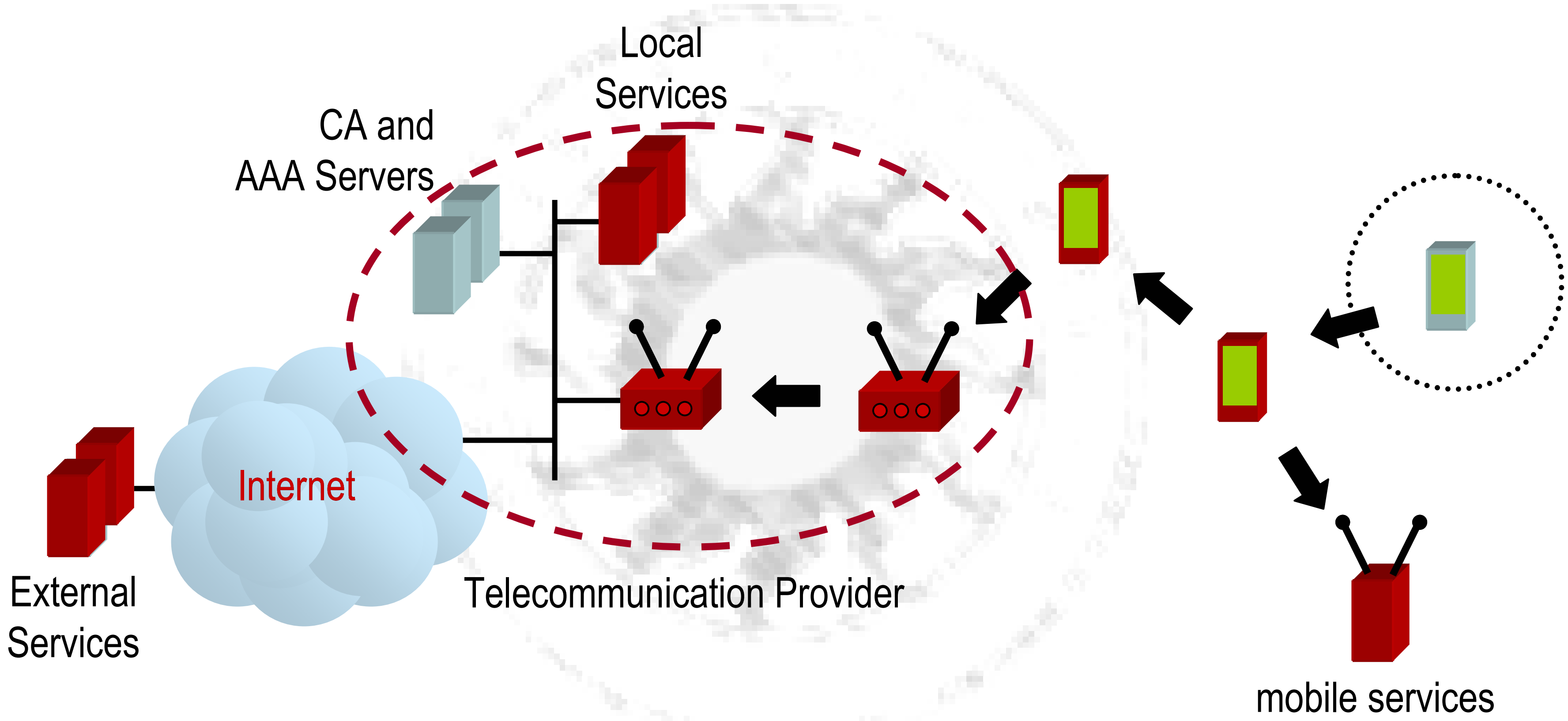
Requirements and Objective

- Objective

  ⇨ *specification of the identifiers needed in a wireless mesh network scenario that can support the provisioning of both security and privacy*

- System Requirements
  - TP must be able to identify users and revoke identities - full non-revocable anonymous network access is undesirable
    - impossible to detect misbehaving users, difficult for billing
  - anonymity towards other network users and network services
    - untraceable identifiers ⇨ location privacy
  - authentication of peer devices even on the absence of an AS

Anonymous Towards Whom ?



Identifiers and Anonymity

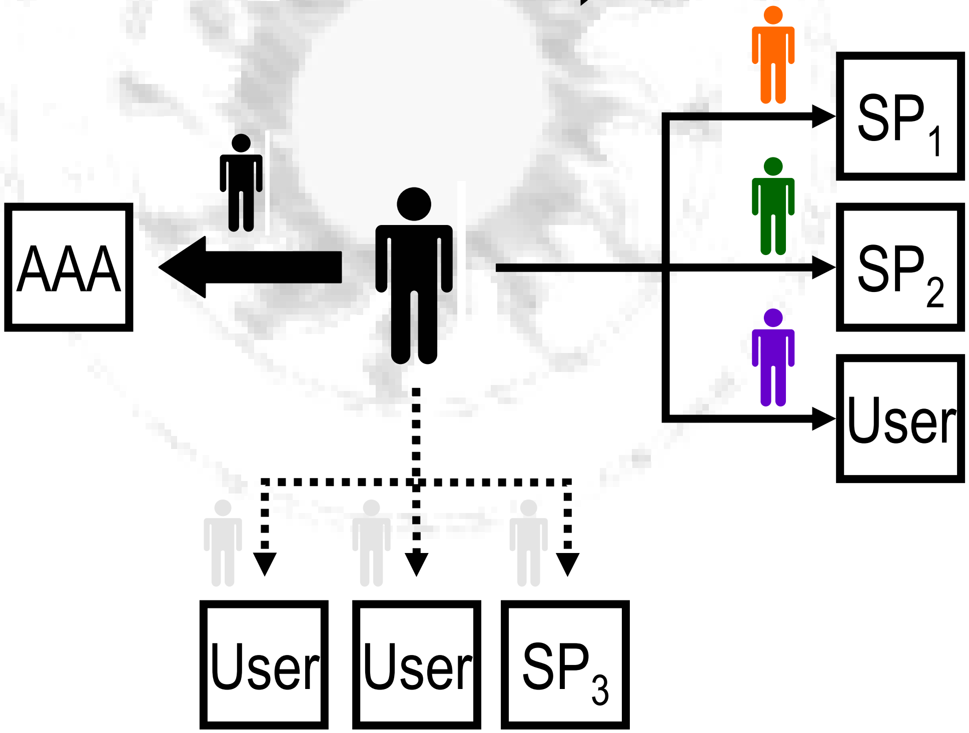
- Anonymous Attribute Certificates (ATC)
  - based on ZK proofs of knowledge
  - structured as composition of group cert and X.509 attribute cert
  - revocable, but no support for sharing detection

➡ Anonymous Credentials
  - based on blind signatures or ZK proofs of knowledge
  - can be used independently from the presence of an AS
  - different properties depending on its construction

    ⇨ multiple show, revocable, detection of credential sharing

Identity Management

- Following the 3 type categorization for IdM (M.Hansen)
  - account management (AAA) ➡ TP
  - profiling ➡ SP (service customization and CRM)
  - management of own identities ➡ users

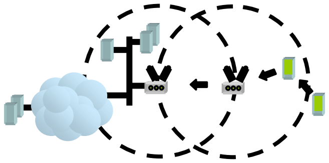


Business Model: TP point of view

- Telecomm Provider Main Assets:
  - Customers
    - unsatisfied with inappropriate handling of personal data
    - must be protected from potential SP harassment
    - privacy is a value-added service and can be advertised
  - Deployed Network Infrastructure
    - mesh + ad hoc is convenient to expand the network

      ➡ but it means losing control over part of the it
  - Technical Competence
    - IdM infrastructure can be provided as a service to other players that demand a similar product

Summary



- Wireless Mesh Networking + Ad Hoc Networking
  - challenging, but rewarding, scenario for telecomm providers
- Privacy needs to be addressed
  - identity management system and anonymous credentials

- Business Model brief description

Questions?