Personal Networks and Federations for Health

I.G. Niemegeers, S.M. Heemstra de Groot, M. Jacobsson

TU Delft and WMC B.V., The Netherlands

MobileHealth
First ACM MobiHoc Workshop on Pervasive Wireless Healthcare
Paris, May 16, 2011

TU Delft

Overview

- Introduction to Personal Networks
- The architecture of Personal Networks
- Networking
- Security
- Federations of Personal Networks
- Applications to health

A bit of history and acknowledgements

- Concepts presented originated in 2000 at Ericsson Research and TU Delft, The Netherlands
- Inspired by the work of Robin Kravetz at University of Illinois: Moped project
- Concepts worked out and prototyped in several large research projects: EU FP6 MAGNET and MAGNET-Beyond, and Dutch Freeband PNP2008 project
- Many small projects
- Parallel to Mobile VCE project in UK: Personal Distributed Environments (Irvine and Dunlop)

Technology drivers

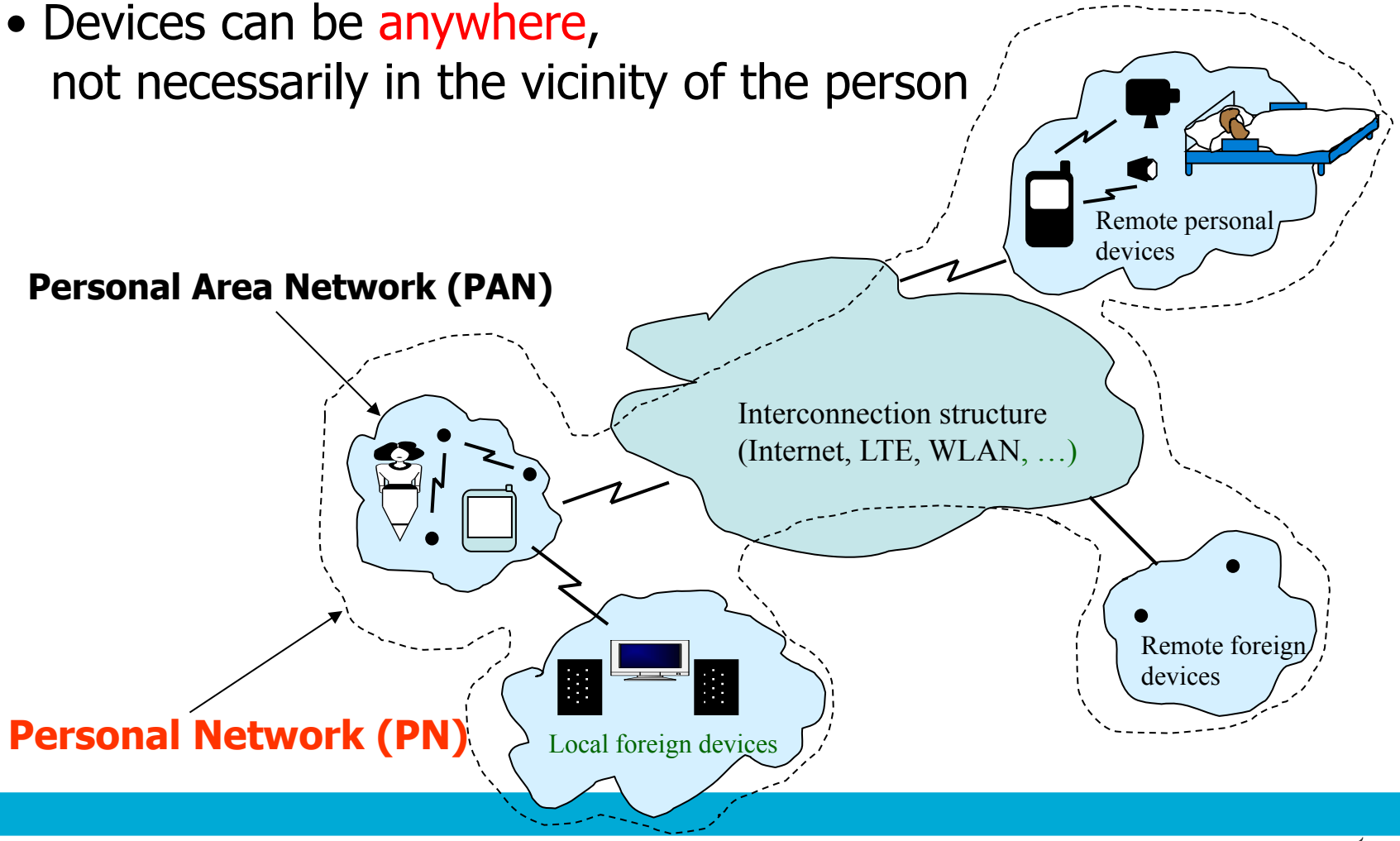
- Number and diversity of personal devices is growing tremendously (vision of pervasive computing, driven by Moore's law)
- Low cost air-interfaces covering a range of needs are becoming commonplace
- Infrastructure (Internet) access is becoming ubiquitous to fixed and mobile users, covering a wide range of user needs
- Growth of IP capable devices (e.g., IPv6 6LoWPAN)

What are Personal Networks (PN)?

- Devices belonging to a user self-organize to form a geographically distributed secure overlay network of personal devices
- A platform for a multitude of personal applications and services to support private and professional activities in a person-centric, unobtrusive, dependable and trustworthy way
- A tool to cooperate with others through federation and interact with non-PN systems (Federations of PNs)

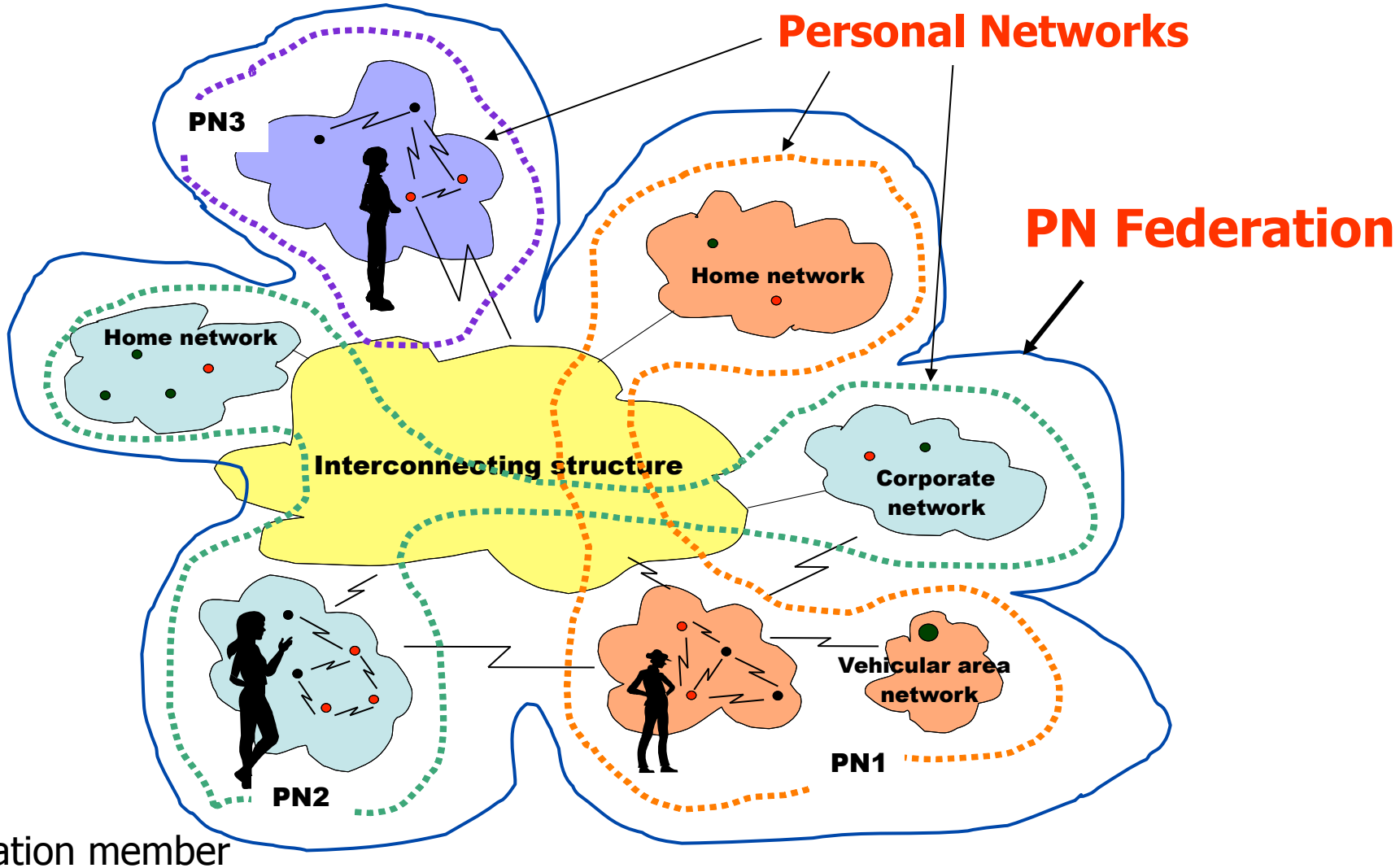
Personal Network (PN)

- Network centered around a person and her/his needs
- Devices can be anywhere,
  not necessarily in the vicinity of the person



TU Delft

PN Federation (Fednet)



- Federation member

Key ideas of PN Federation

- Cooperation of multiple PNs
- Using selected resources and services of each other
- Driven by purpose or opportunity
- Temporary or long term for achieving a specific goal

TU Delft PN Prototype

- Software platform running on your devices providing:
  - Secure ubiquitous communication
  - Automatic configuration
  - Network technology independence
  - Integration with common operating systems (Linux, others under development)
- Developed at TU Delft over the past six years

Research projects with PN-like goals

- Universal Personal Networking (UPN): early 1990s at Siemens, no breakthrough
- Life-Works: more recent, Siemens
- Moped: University of Illinois, Kravets (2001)
- Personal Mobile Hub: IBM Research, Husemann et al. (2004)
- CoolTown: HP, Debaty and Caswell (2001)
- Mobile People Architecture: Stanford, Maniatis et al. (1999)
- Personal Distributed Environment: Mobile VCE, UK, Dunlop and Irvine (2003)
- MyNet: Nokia and MIT, Arvind and Hicks (2006)
- IST PACWOMAN and SHAMAN: EU FP7 (2002)

Commercial developments with a PN flavor

- Microsoft's Personal Cloud (2010 announcement)
- Intel' innovation vision
- Apple's MobileMe
- Drop Box (product)
- P2P Universal Computing Consortium (PUCC): Japanese universities and companies, e.g. NTT Docomo, NEC, Toshiba, since 2004, demo at CCNP 2008 CES
- 3GPP: Personal Networks as part of AIPN (2009)
- ECMA Technical Report on Personal Networks (December 2010)

PN architecture

PN Requirements

- Easy cross-device applications support based on service oriented architectures (SOA)
- Secure personal communication
- Automatic addressing and network configuration
- Routing, broadcasting and mobility
- Wireless technology and operating system independent
- Context-awareness
- Virtualization

Core Concept

- Distinguish between:
  - **Personal Nodes** – Devices owned/used/controlled by you
  - **Foreign Nodes** – All other devices
- One single and simple security system independent of link-layer technologies

Personal Network = The set of all Personal Nodes

Personalization of Nodes

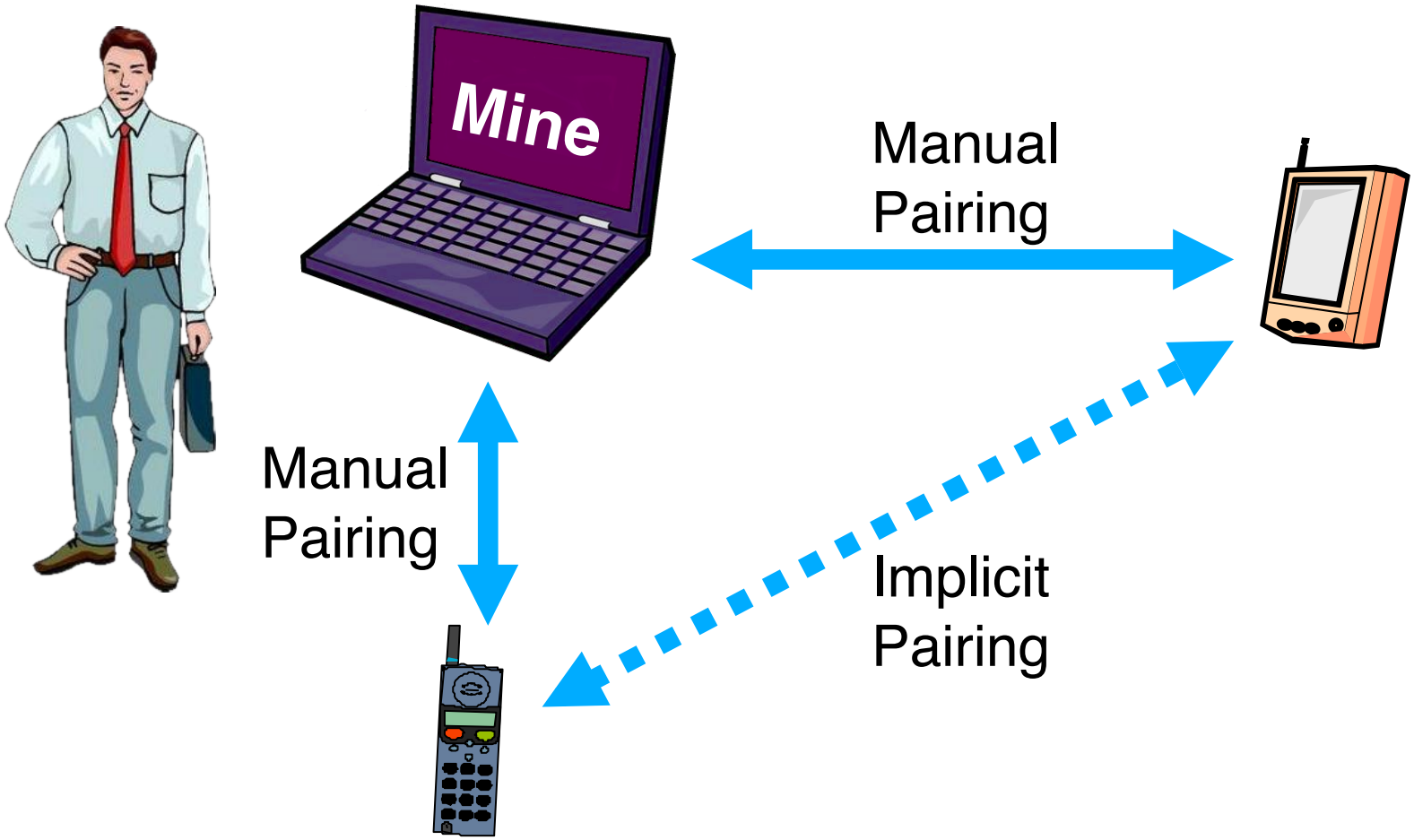
Cluster and PN Formation

- A security mechanism is used to separate Personal from Foreign Nodes. Clusters contains only Personal Nodes.
- A PN is formed by constructing inter-Cluster tunnels between Personal Clusters.

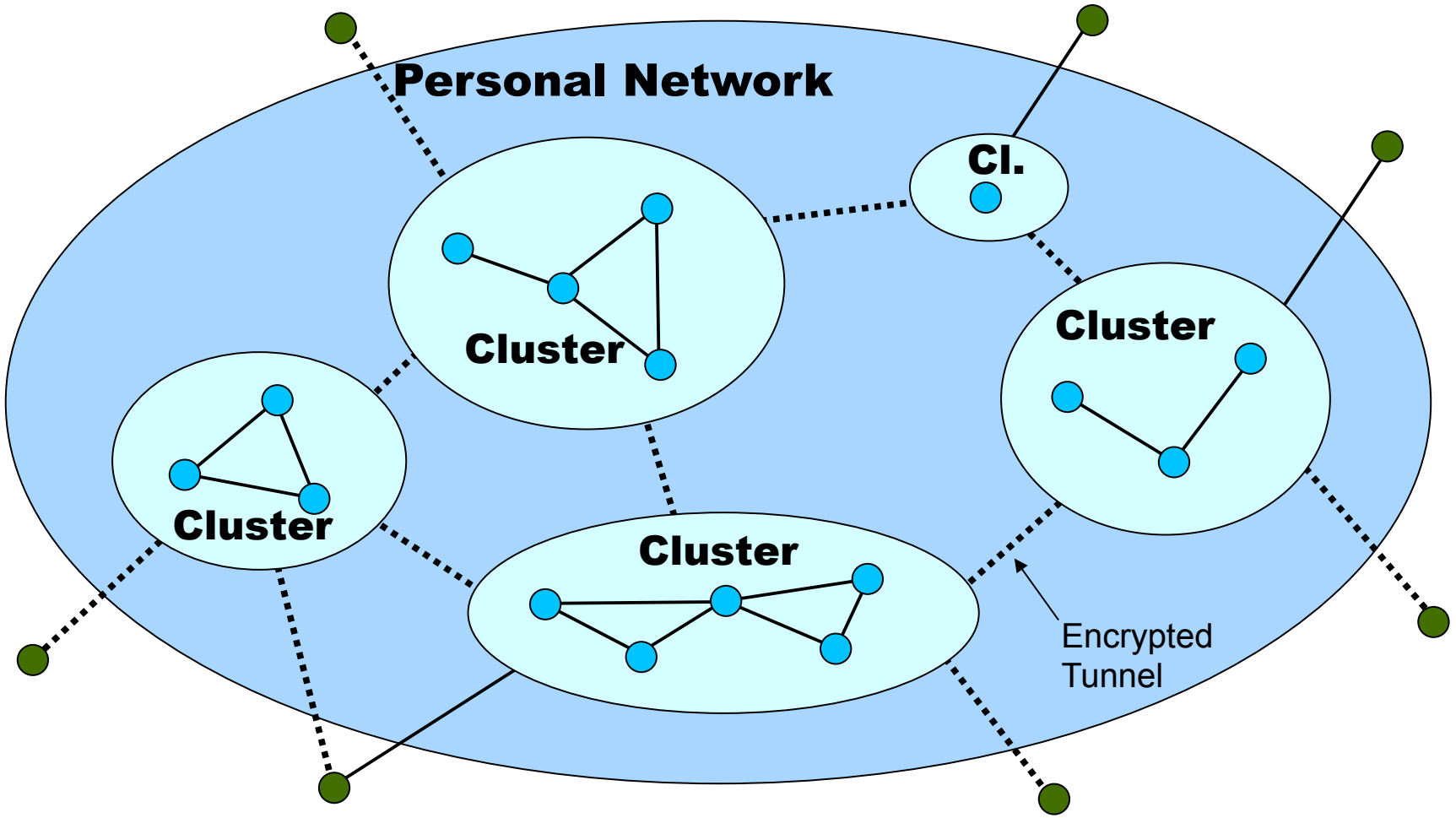
Personalisation

- A new Node is included into the PN (or personalized) by pairing it with a Node already personalized. It becomes a Personal Node.
- An intra-PN security mechanism makes sure that encryption keys are distributed to the new Node and that the PN is aware of the new Node.
- Configuration of a new Node (such as addressing).

Personalization of Nodes

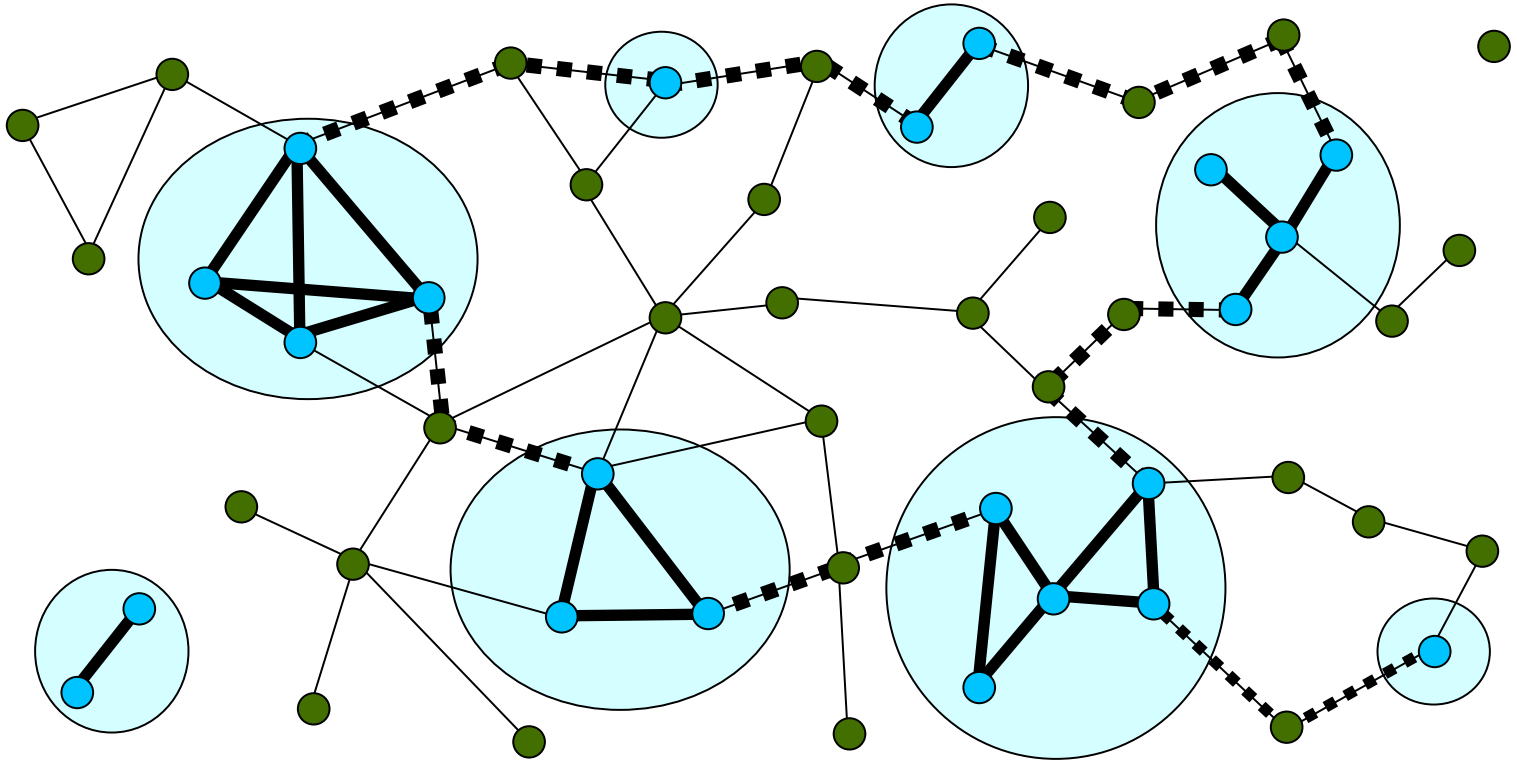


The Network Architecture

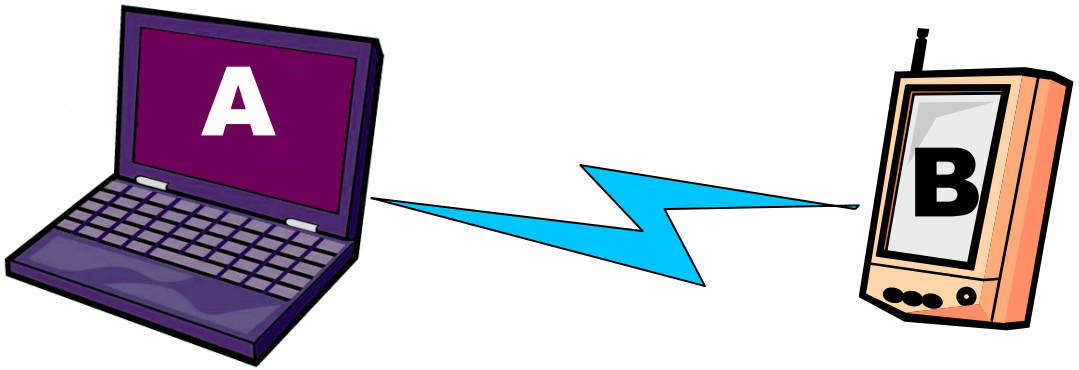


TU Delft

The Big Picture



When a Node meets another Node



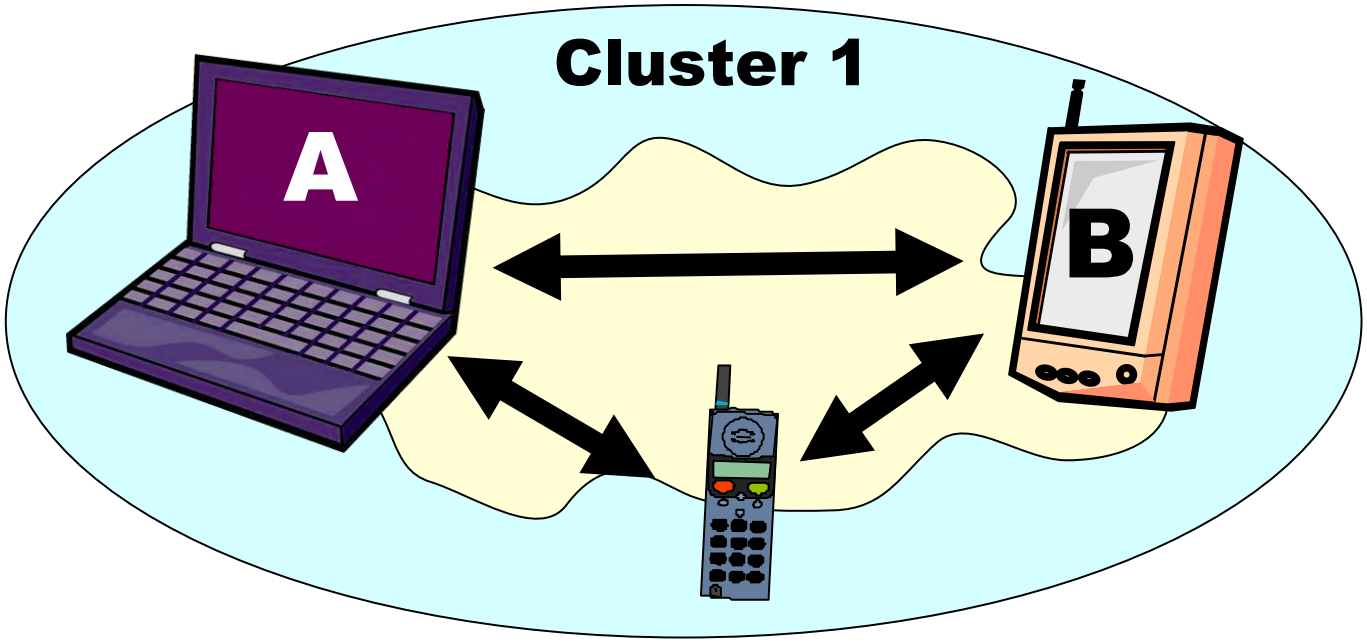
$\{\text{Hello, A}\}_{\text{PID}}$

$\{\text{Hello, B}\}_{\text{PID}}$

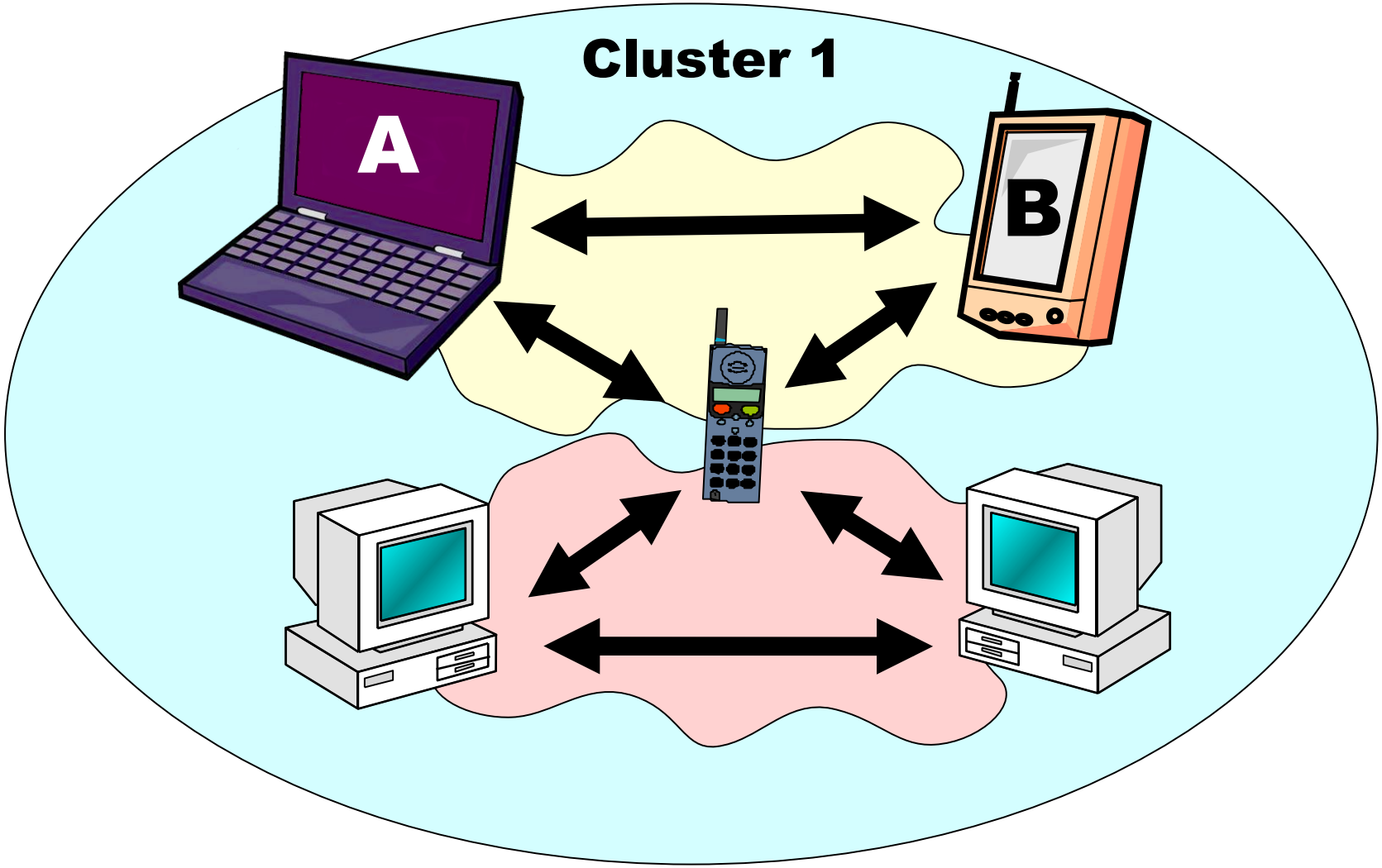
$\{\text{Mgmt Data}\}_{\text{PID}}$

$\{\text{Data}\}_{\text{PID}}$

Personal Networks

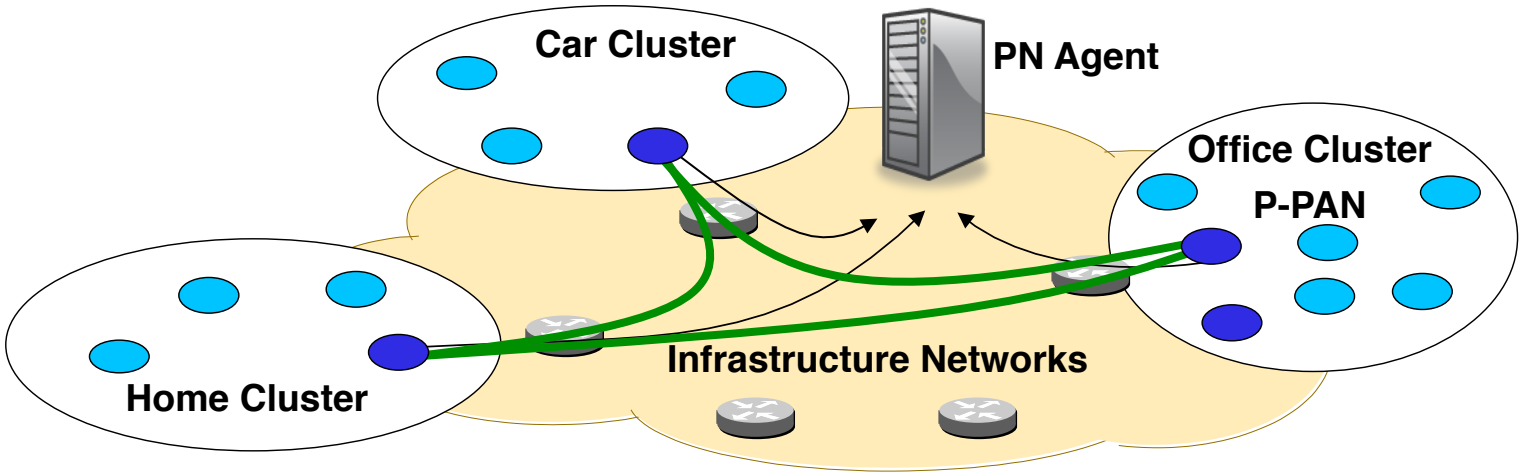


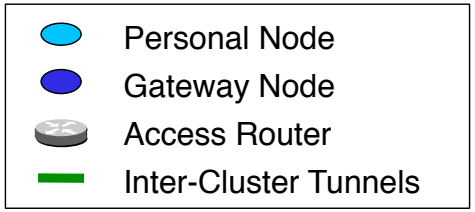
Personal Networks



TU Delft

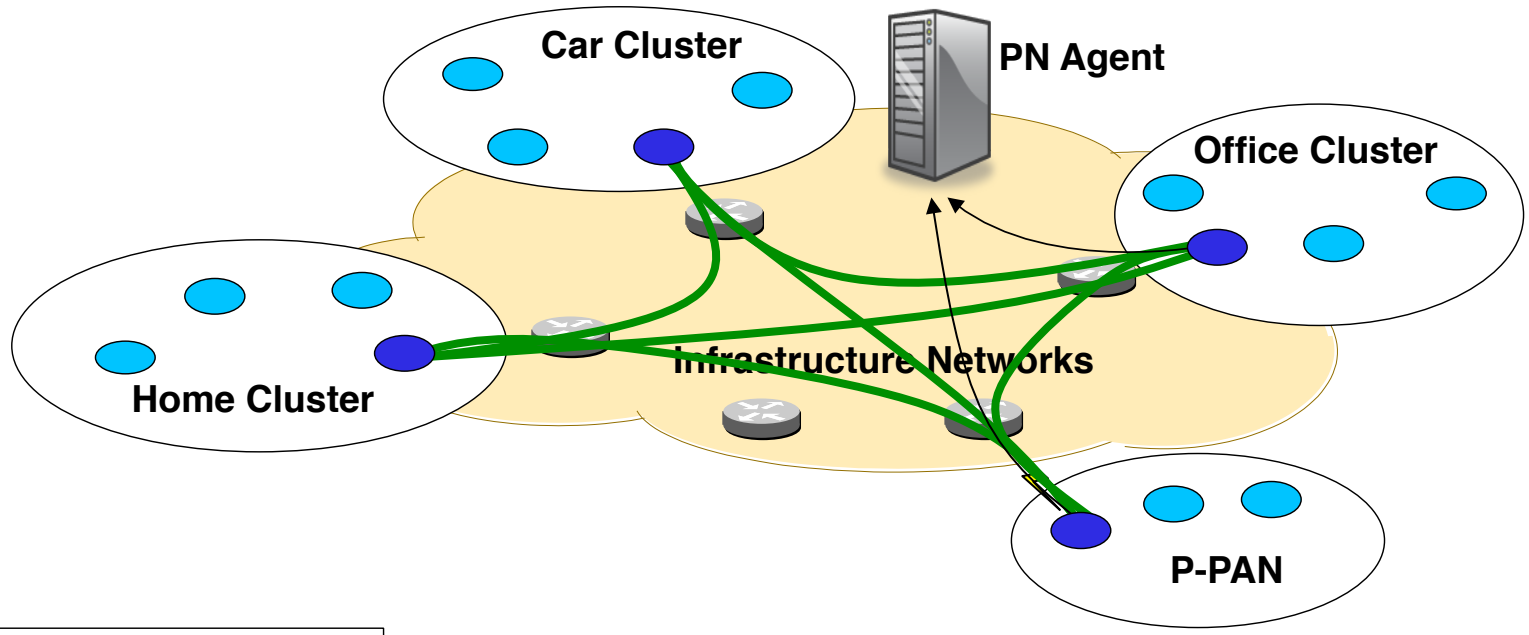
Personal Networks





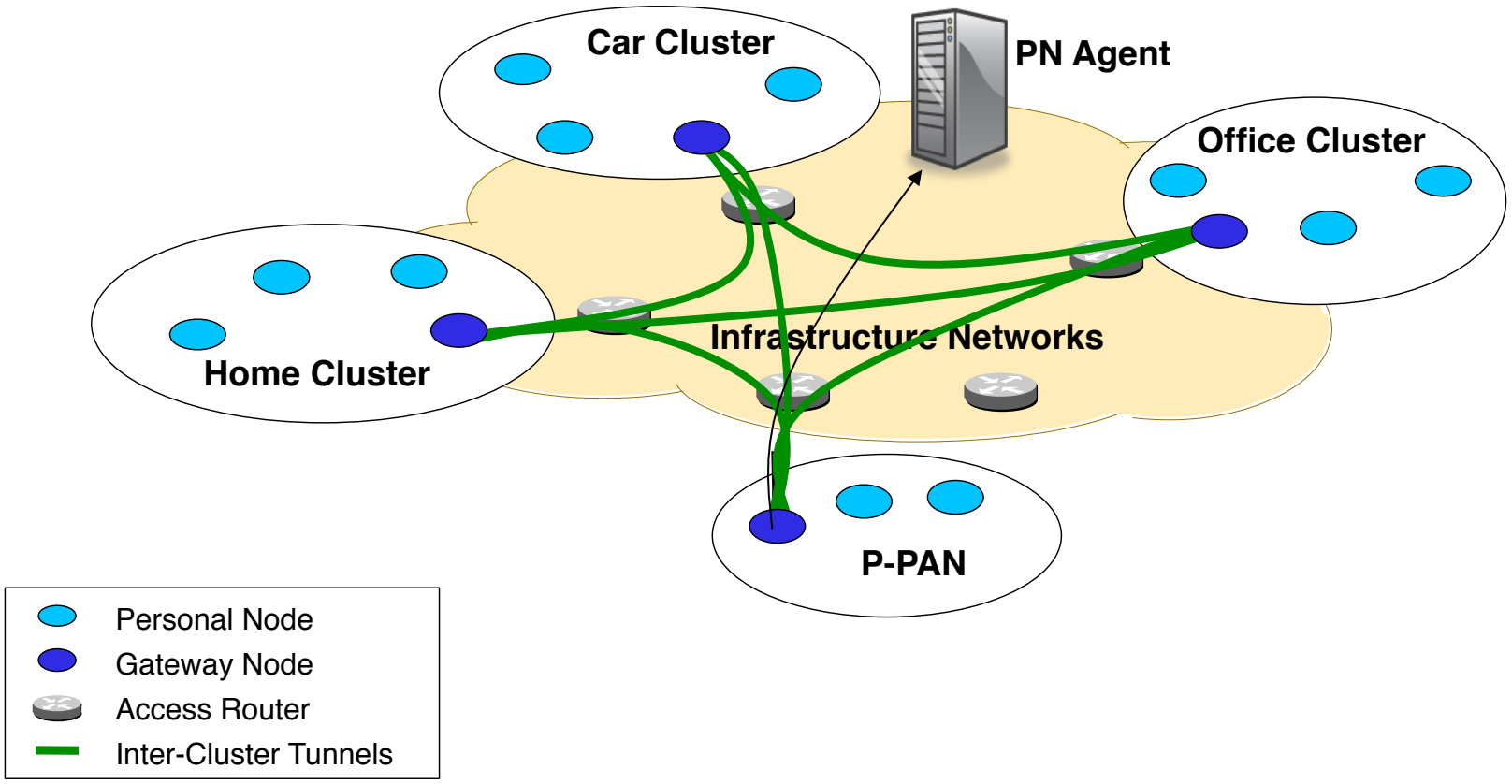
TU Delft

Personal Networks



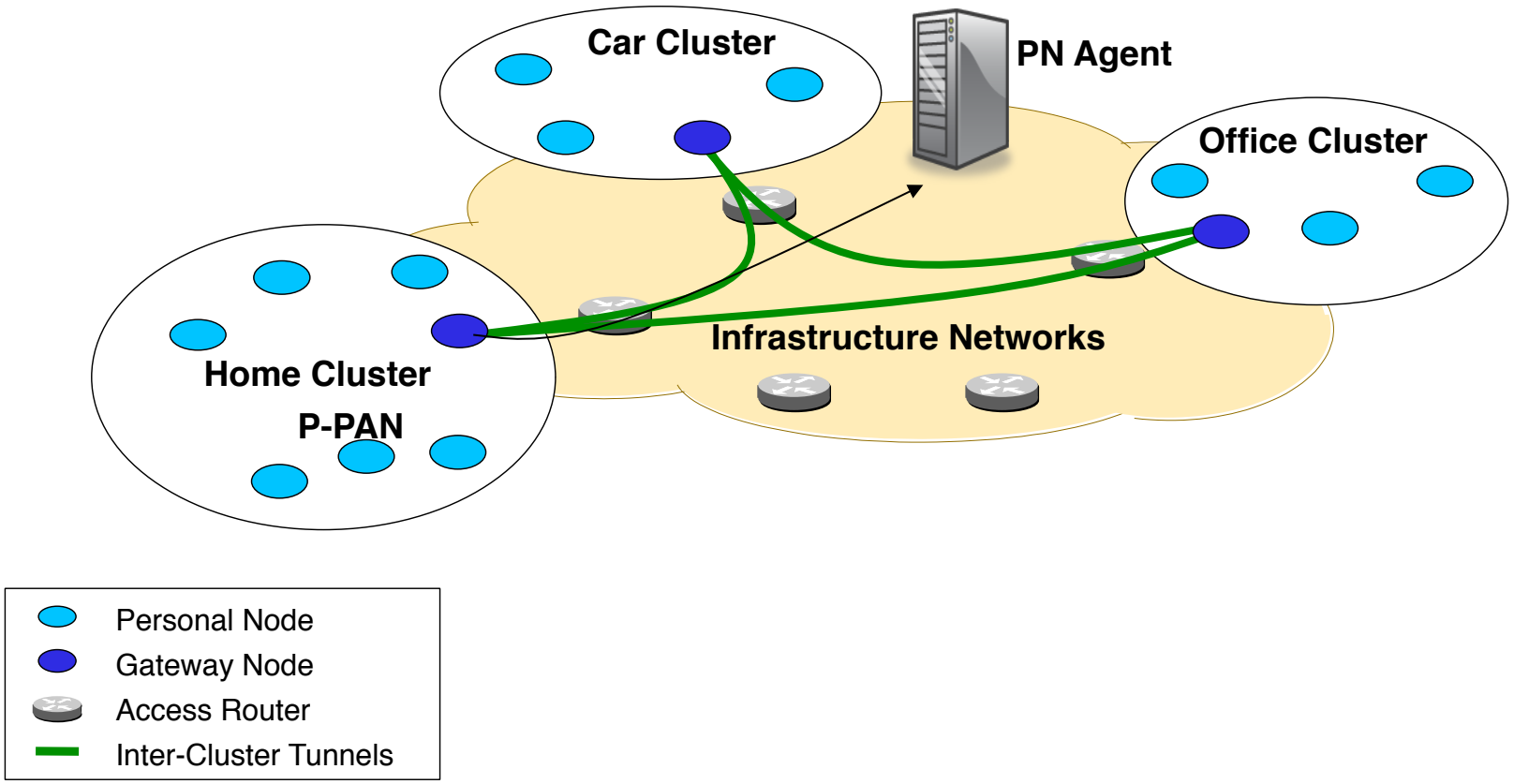
TU Delft

Personal Networks



TU Delft

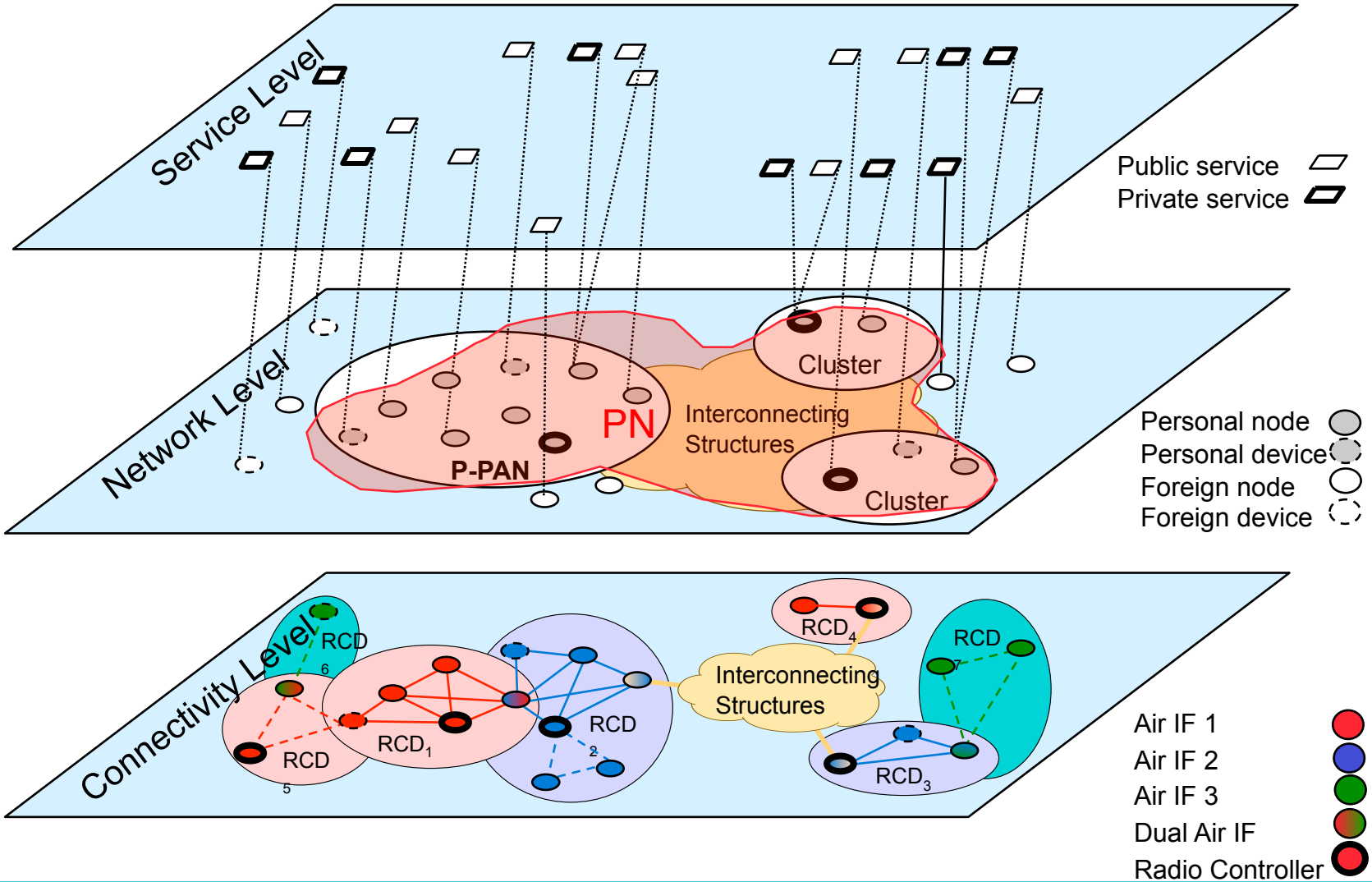
Personal Networks



TU Delft

PN Networking

Three Layer View



TU Delft

Addressing

- Each PN Node has an IP address
- Flat addressing within the PN
- Unique within the PN
- Assigned at the time of personalization
- Never changes
- TCP / UDP sessions are unaffected by mobility
- We used IPv6, but IPv4 is no problem

Cluster Routing

Mobile Ad Hoc (MANET) Routing

- Support Mobility / Dynamic Links
- Support Wireless / Heterogenous Links

MANET protocols used in our prototypes:

- OLSR – Optimized Link State Routing
- WRP – Wireless Routing Protocol

Proactive protocols work the best for clusters:

- Small and dense networks
- Many node-node flows
- Many short-lived sessions

Flooding

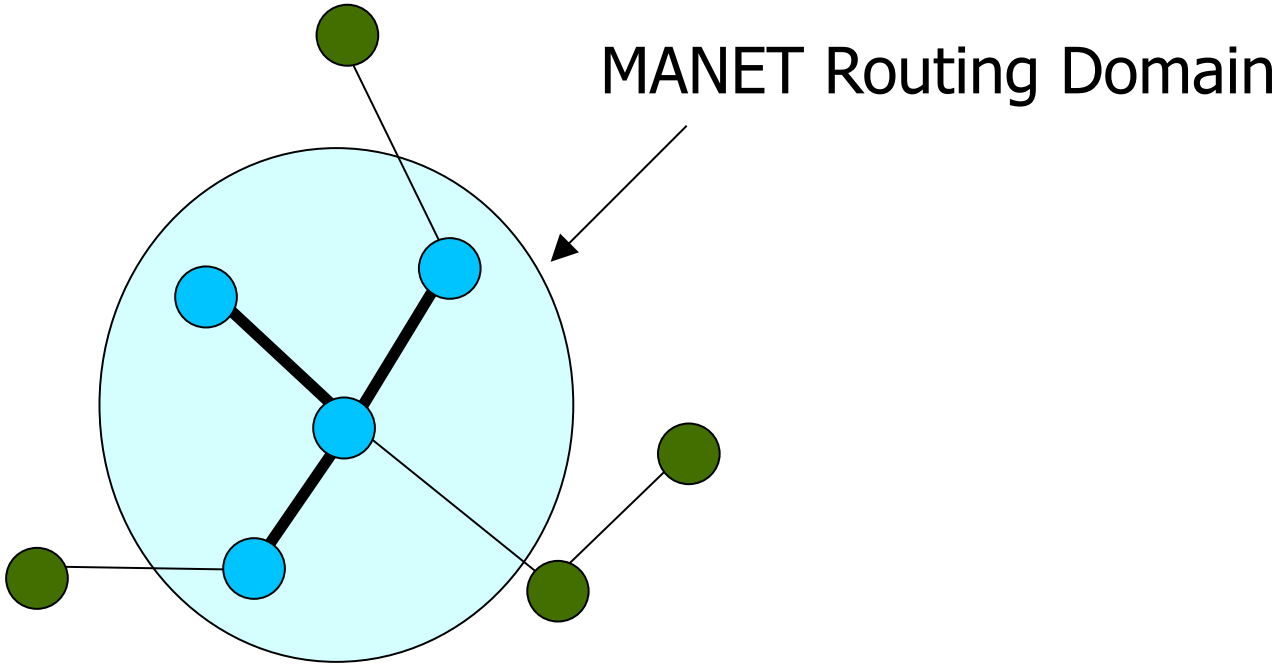
Cluster-wide / PN-wide Broadcasting

- Service discovery
- Context information dissemination
- Various network organization protocols
- Multicast applications

Existing ad hoc flooding protocols:

- Blind Flooding
- CBB – Counter-based Broadcasting
- SMF – Simplified Multicast Forwarding

Personal Node Recognition



Personal Node Recognition

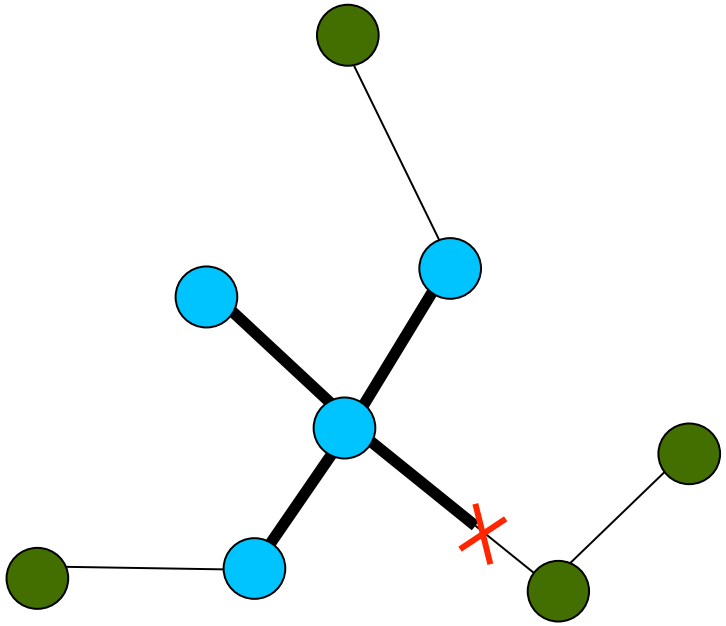
Personal Neighbour Node Authentication:

- Based on personalization
- Filter out the other neighbors
- Encrypt packets between personal nodes

Introduce a ”layer” below networking:

- Implements personal neighbour node discovery and authentication
- Expose higher layers (e.g. routing) only to authenticated neighbours
- MANET routing protocol can be unmodified

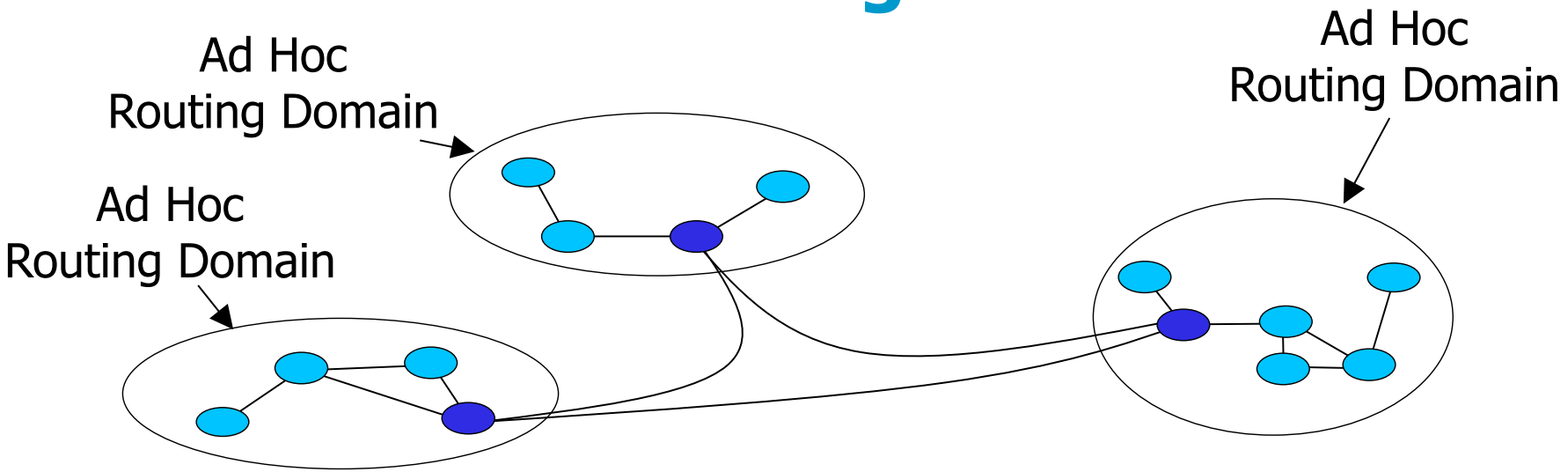
Personal Node Recognition



Inter-Cluster Tunneling

- Encrypt traffic over the Internet:
  based on keys established via personalization
- Supports mobility within PNs
- End-to-end packets (IP and upwards) are transmitted unchanged and tunnelled.

Inter-Cluster Routing

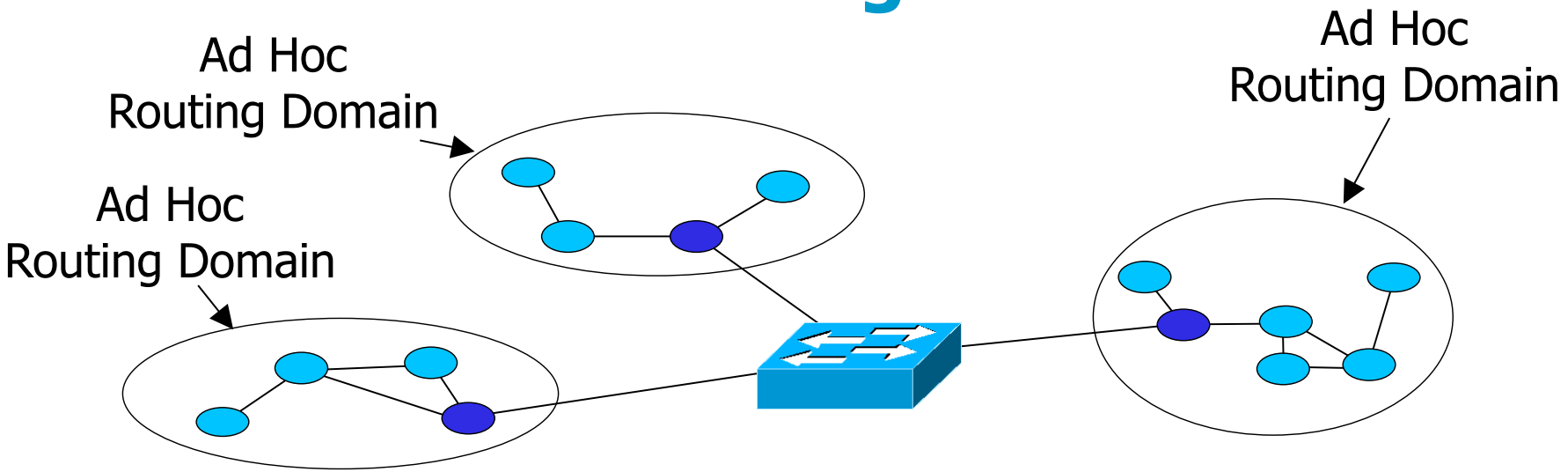


Flat Ad Hoc Routing across an entire PN is possible!

However, the tunnel links are special

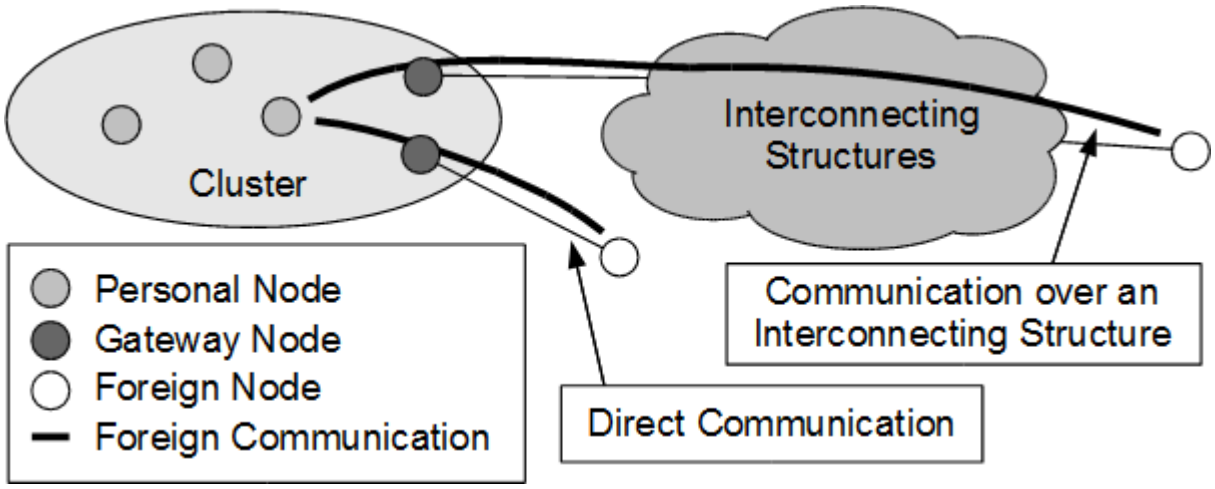
- Slow, usually the bottlenecks
- Most topology changes in a Cluster only have local consequences within that Cluster

Inter-Cluster Routing



- Each Cluster is its own ad hoc routing domain
- The tunnel inter-connect acts as a network switch
- Gateway Nodes keep track of which Node is in which Cluster
- Packets to Nodes in other Clusters are forwarded over the tunnels by the Gateway Nodes

Foreign Node Communication



Service vs. Network Level

Network Level:

- Using NAT/NAPT
- End-to-end IP connectivity
- Access control based on port numbers only

Service Level:

- Using Service-Level Proxies
- Two sessions instead of one (mainly problem for TCP)
- Finer granularity access control

PN security

PN Security

- Device personalization
  - Imprinting
  - PN Formation Protocol
  - Eviction of nodes
- Establishment of secure communication
  - Unicast
  - Broadcast
  - Inter-cluster

Imprinting

Based on the "**resurrecting duckling**" policy model (Stajano)

- A new device (**duckling**) starts in the un-imprinted state
- The device becomes imprinted when the first master device (**mother**) provides it with cryptographic material
- Other imprinting attempts will fail if the devices is imprinted state
- The master device can "kill" (remove the cryptographic material of) the device and bring it back to the un-imprinted state

Imprinting in PN

- Using public key infrastructure PKI adapted to the PN environment
  - PN certification authority (PNCA) signs the public key of duckling during imprinting
  - Generated certificate and PNCA certificate is stored in duckling
  - PKI light weight solutions with elliptic curve cryptography (ECC) (MAGNET Beyond project)
- Shared key
  - Pair-wise key with mother
  - Simple but with limited scalability

Certified PN Formation Protocol (PNFP)

- From European Project Magnet Beyond
- Two phases
  - Imprinting
  - Establishment of pair-wise keys

Eviction of personal nodes

- Certificates are issued by PNCA have limited life time: certificates need to be renewed
- For eviction before expiration of certificate:
  a certificate revocation list (CRL) signed by the PNCA is sent to all nodes in the PN using PN-wide broadcasting

Secure broadcast

- Use of unicast-only flooding protocol:
  reliable but not efficient
- Distribute a cluster-wide broadcast key:
  key distribution may be a problem
- Each node has a broadcast key for broadcasting to its neighbors: most efficient solution

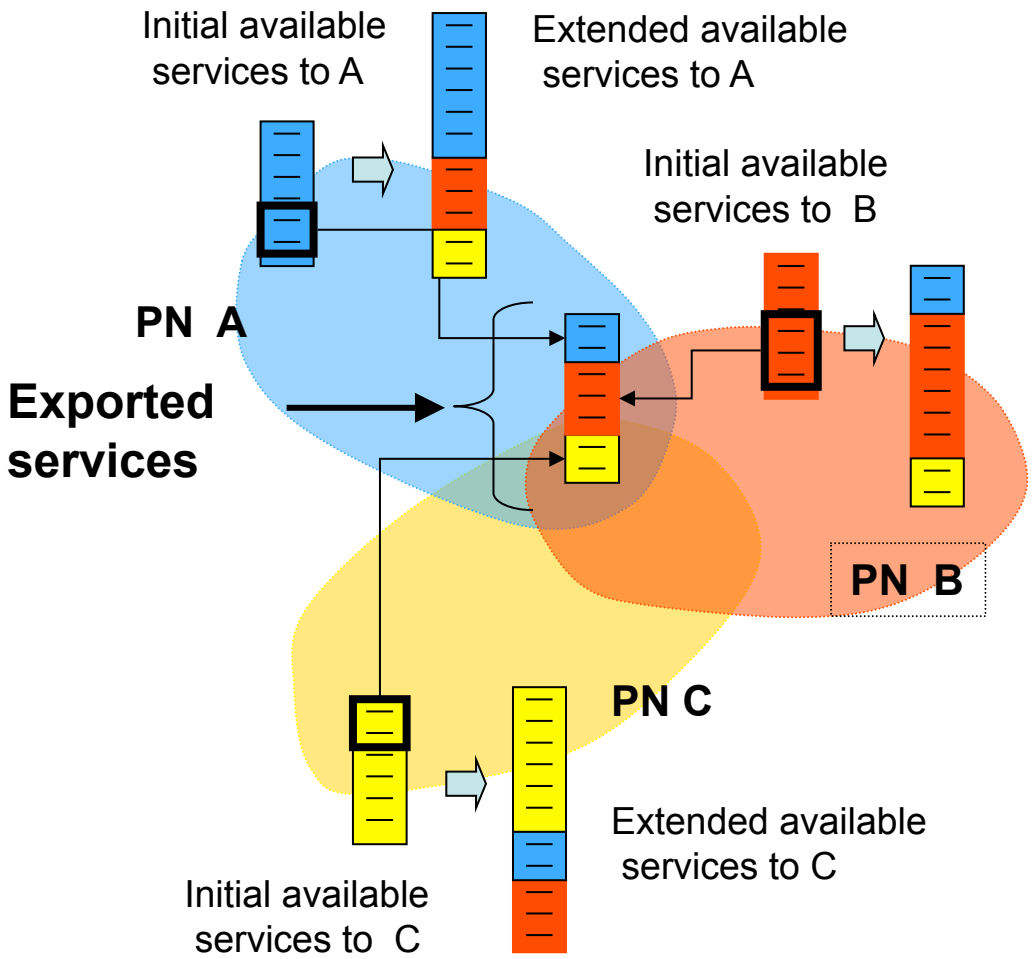
Secure inter-cluster communication

- Gateways nodes are responsible for securing inter-cluster communication
- IPSec tunnels
- Algorithm for key establishment similar to the second phase of the CPFP
  - Gateway nodes exchange PNCA certificates
  - After successful authentication session keys are generated

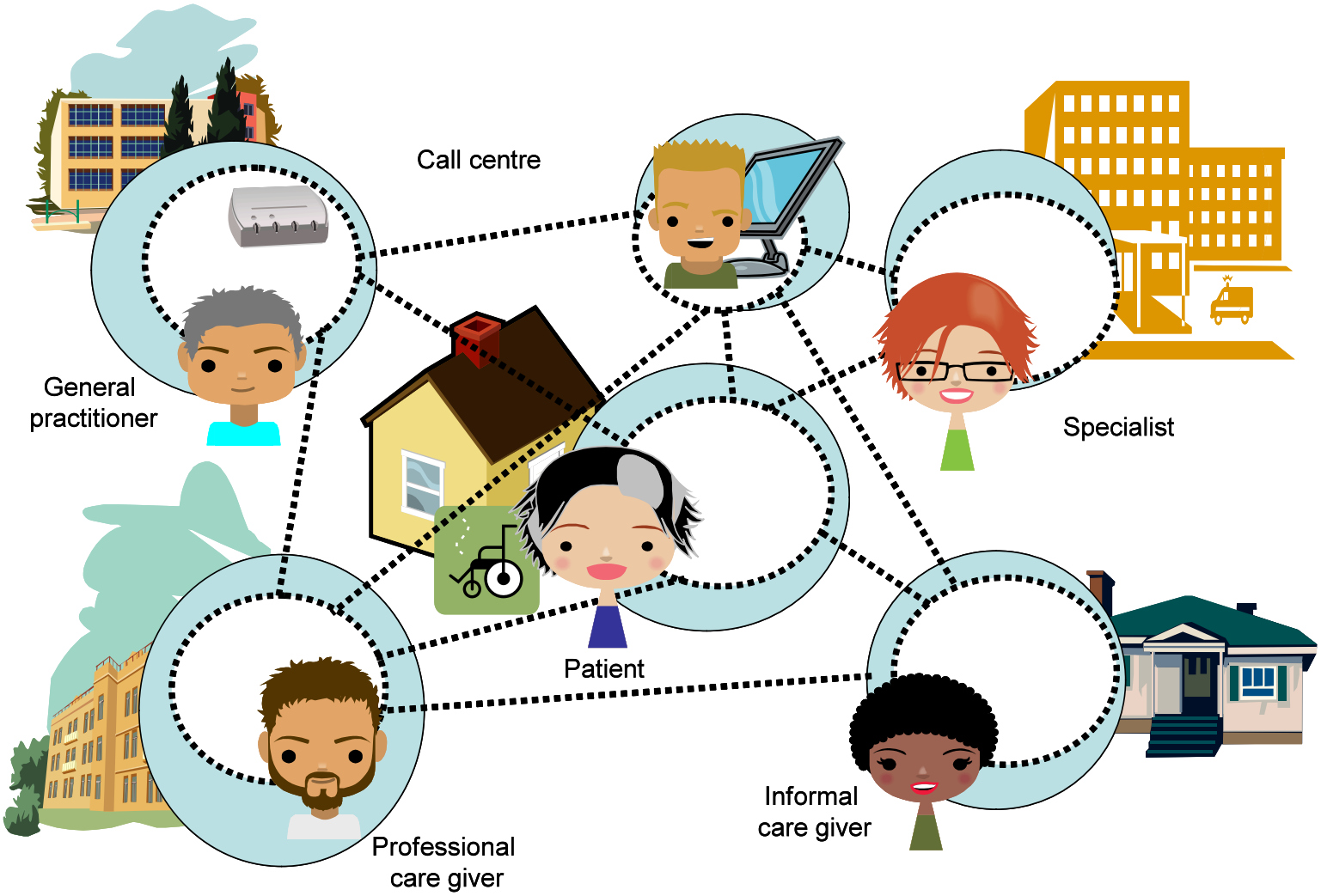
PN Federation (Fednets)

A cooperation of independent PNs with the purpose of achieving a specific common goal

PN federation concept



PN Federation for Health



TU Delft

pucc
P2P Universal Computing Consortium

Healthcare Monitoring System
- For a long and healthy life -

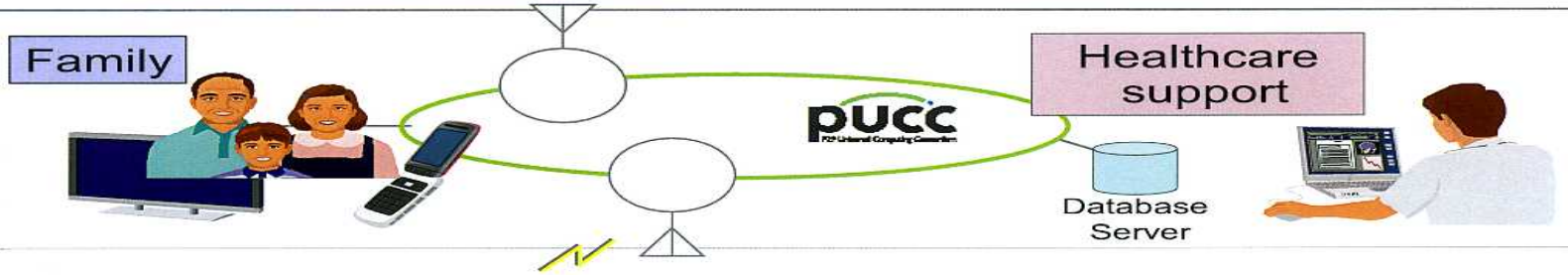
Healthcare monitoring wristband device

Acceleration

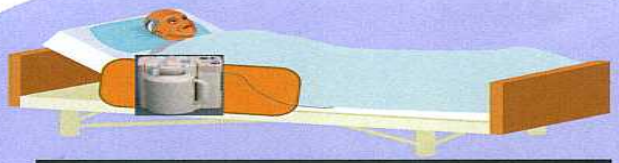
Body temperature

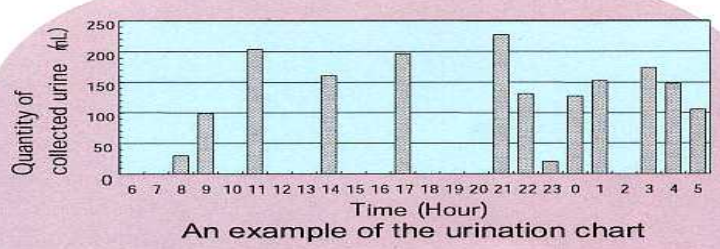
Exercise Volume
Daily rhythm

- Monitors the user regularly and gathers data.
- Transfers gathered data to healthcare supporters to control user's daily healthcare.



Automatic urine collection system

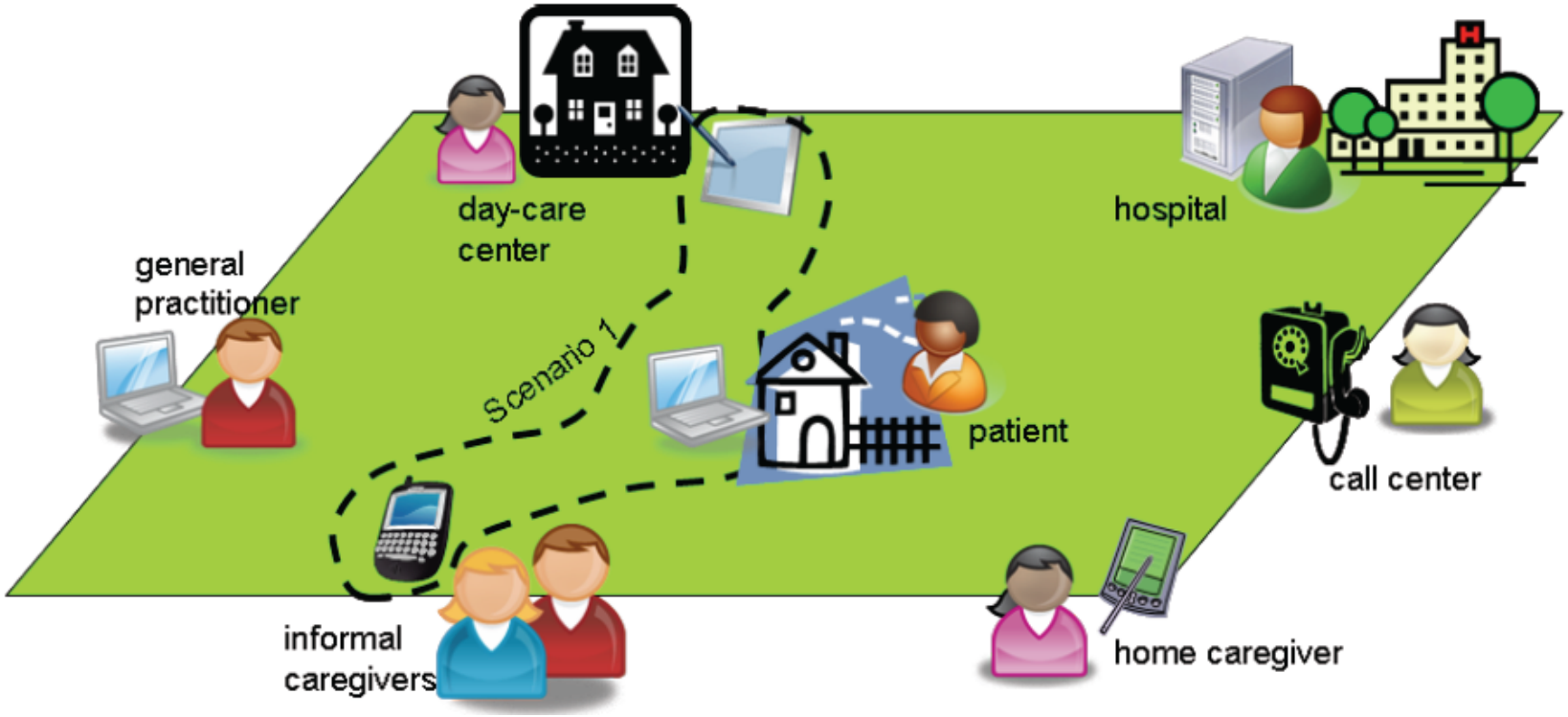




An example of the urination chart

- Creates a urination chart.
- Allows nurses to provide high-quality healthcare such as knowing the amount of water to give and when to take patients to the bathroom.

ECMA Homecare Scenario

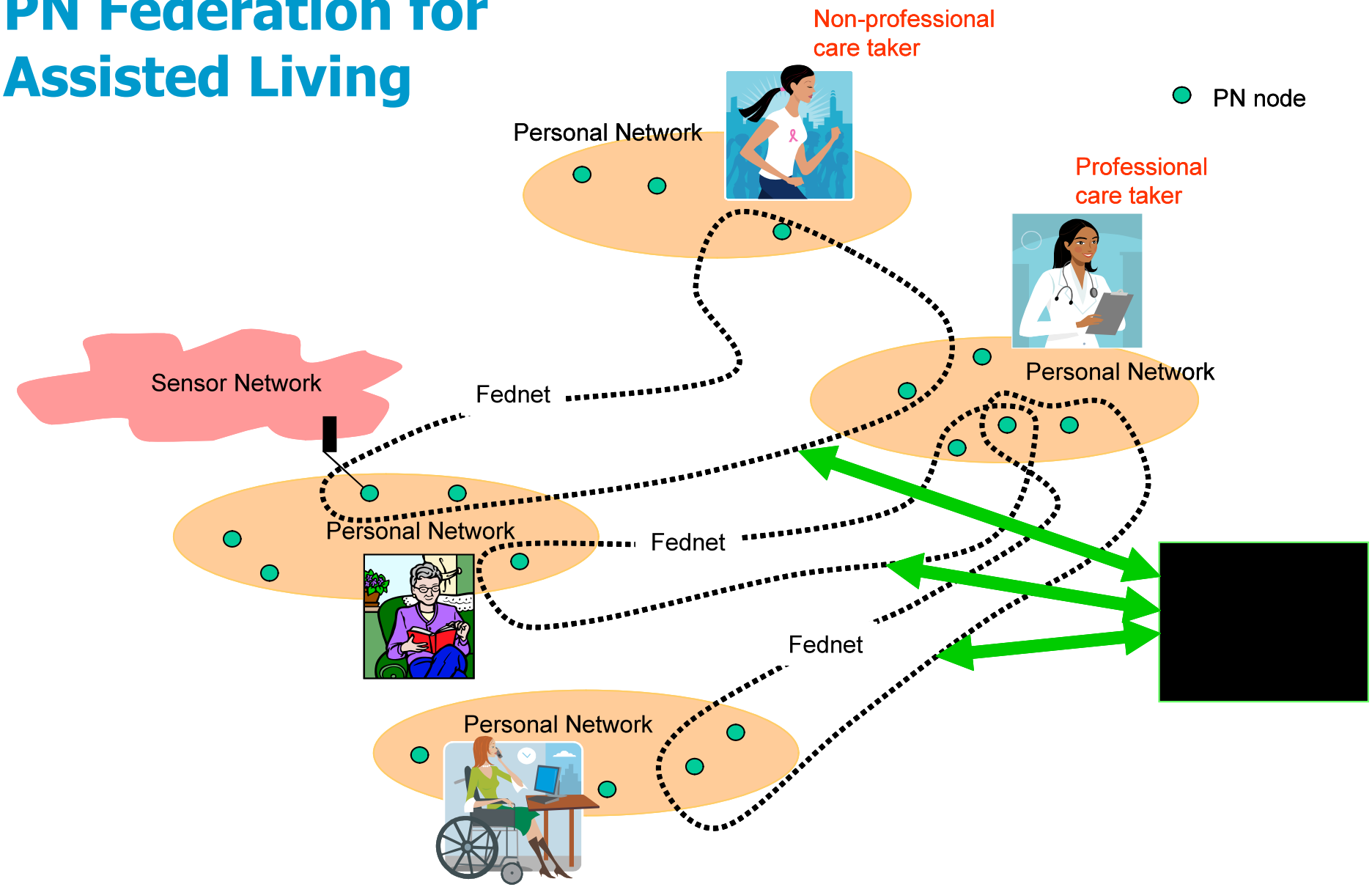


Ecma TC32 PN&F Editing Group, "Personal Networks and their Federations," *Ecma Technical Report*, 2009.
http://www.ecma-international.org/memento/TC32-PNF-M.htm

Rehabilitation of Stroke Patients

- PN consisting of sensing, actuating and remote monitoring systems
- Involvement of additional sensing systems not intended for medical applications (e.g., smart phone sensors)
- Involvement of rehabilitation-professionals through Federations
- Dynamic adaptation to phases of rehabilitation and to context

PN Federation for Assisted Living



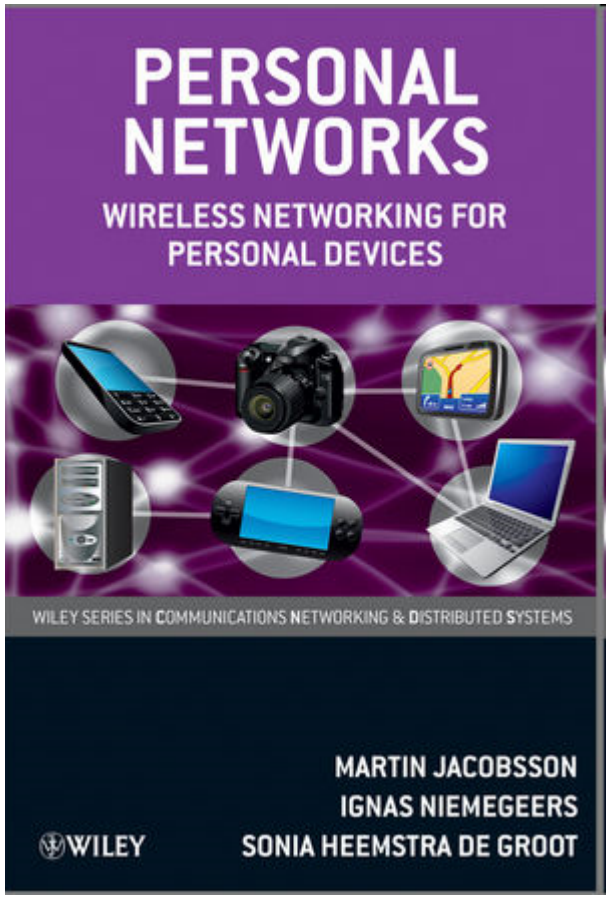
Further reading

Personal Networks: Wireless Networking for Personal Devices

Martin Jacobsson
Ignas Niemegeers
Sonia Heemstra de Groot

Wiley Series on Communications, Networking and Distributed Systems

Wiley, 2010



TU Delft