Privacy and Anonymity in Personal Networks

Martin Jacobsson, Ignas Niemegeers
TU Delft
The Netherlands

PerSec 2005

Kauai Island, March 8, 2005

Disclaimer: The work presented here was funded in part by the Commission of the European Union under the project IST MAGNET. This work expresses the view of the authors and not necessarily the general view of the MAGNET project.

Outline

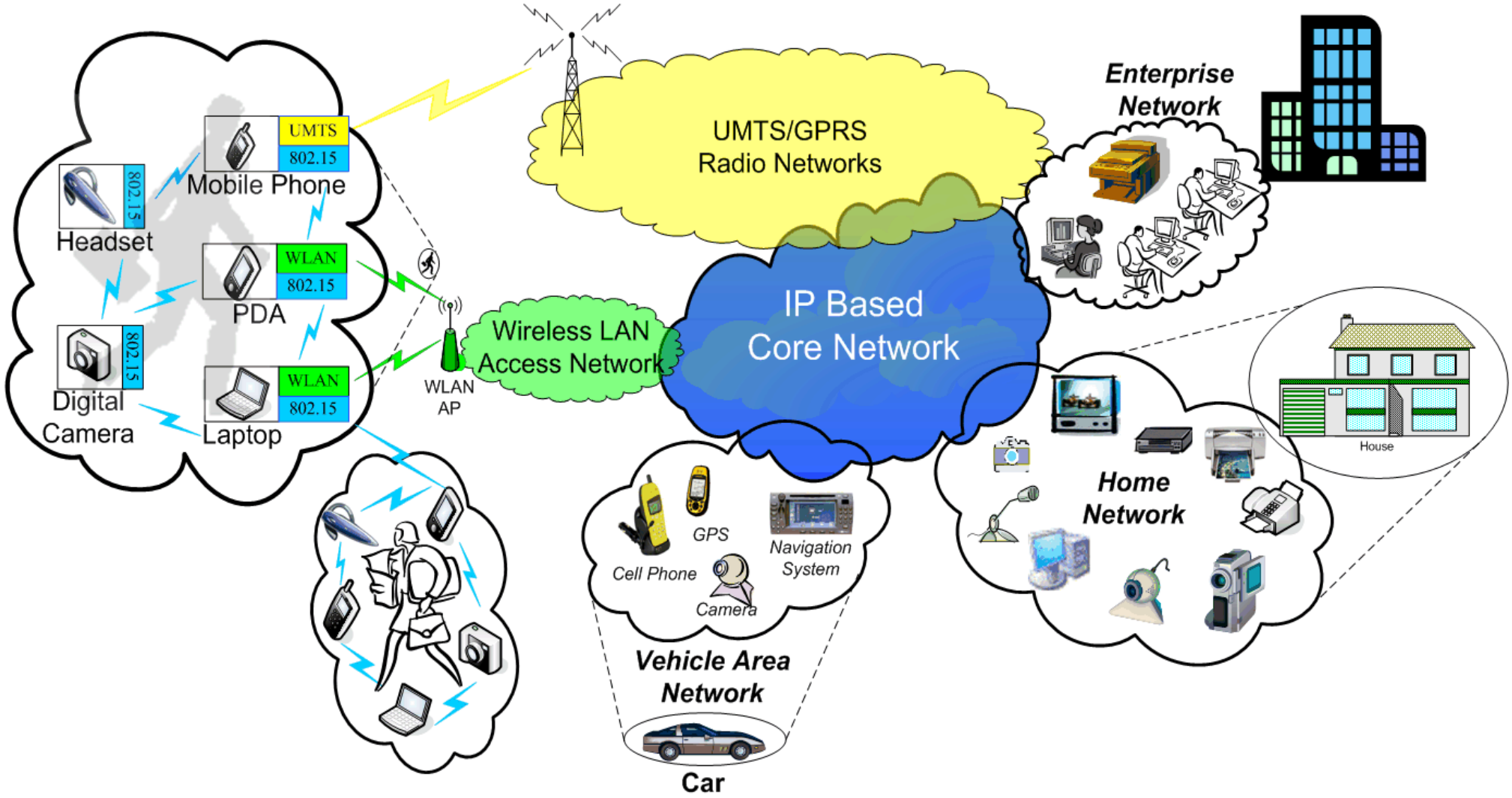
- Introduction to Personal Networks (PN)
- The proposed PN architecture
- Security implications of the architecture
- A possible implementation
- Conclusions

Introduction to Personal Networks (PN)

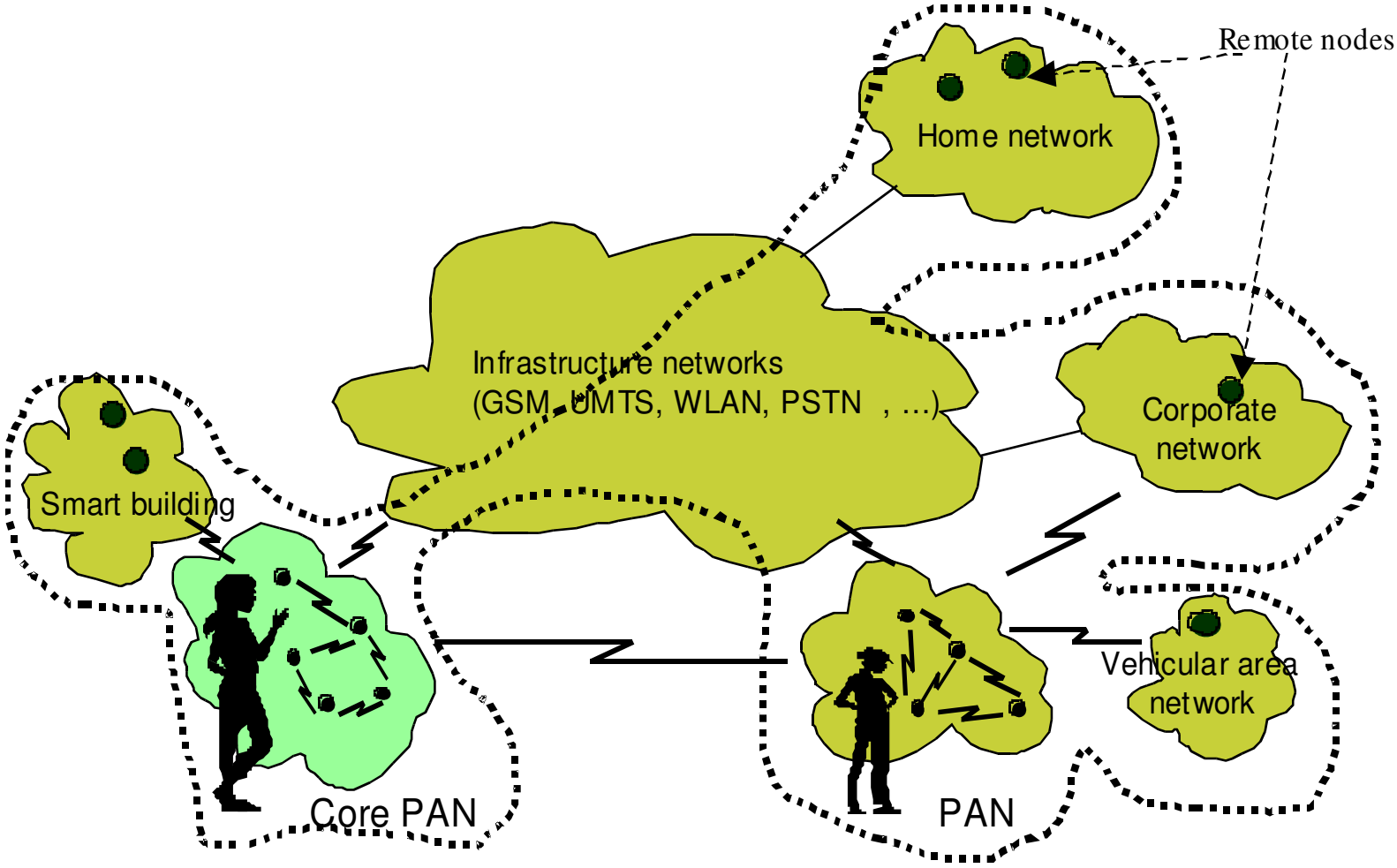
From PANs to Personal Networks

- Personal Area Network (PAN)
  - Network consisting of personal devices in the close vicinity of the person (Personal Operating Space or POS)
- Personal Network (PN)
  - Network centered around a person and his/her needs
  - Resources and devices are not necessarily in the close vicinity of the person
  - Dynamic in composition, configuration and connectivity depending on time, place and circumstances
  - Core consisting of a PAN extended with personal resources or resources belonging to others.

An example of a PN



Abstract PN view



From: I.G. Niemegeers and S.M. Heemstra de Groot,

"Research Issues in Ad-Hoc Distributed Personal Networking",

Journal on Wireless Personal Communication, Kluwer, Vol. 26, No. 2-3, 2003, pp. 149-167

Composition of a PN

- A Private-PAN (P-PAN) around a person consisting of local personal devices and services
- Remote personal devices and services

- Local foreign devices and services
- Remote foreign devices and services
- Interconnecting structures

The proposed PN architecture

The Personal Identifier (PID)

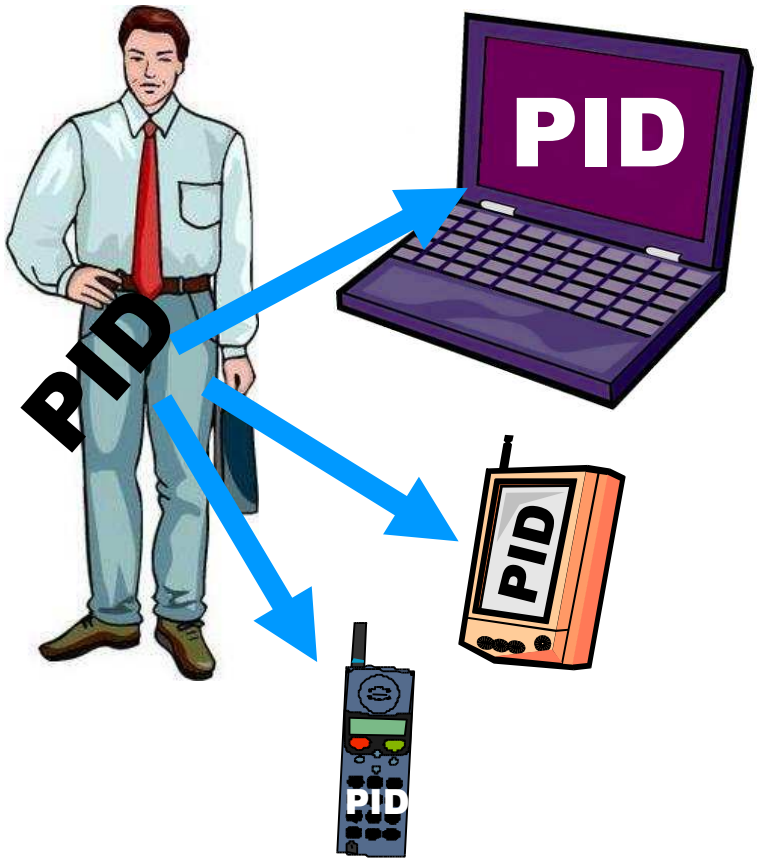
PID is:

- An abstract concept – a security policy model
- About trust relationships between Nodes
- PID models ownership – ease of use

PID is NOT:

- An implementation or implementation design!

Personalization of Nodes

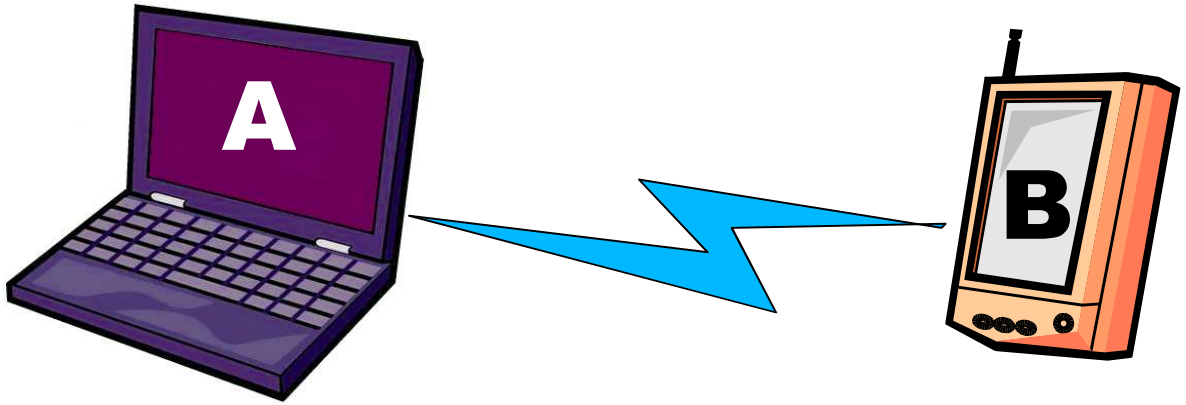


How can the PID be entered:

- Using the keyboard
- Upload it from another Node:
  - Cables
  - Near Field Communication (NFC)
- Removable media
- SIM-card

Personal Identifier (PID) may be some kind of secret key

When one Node meets another Node



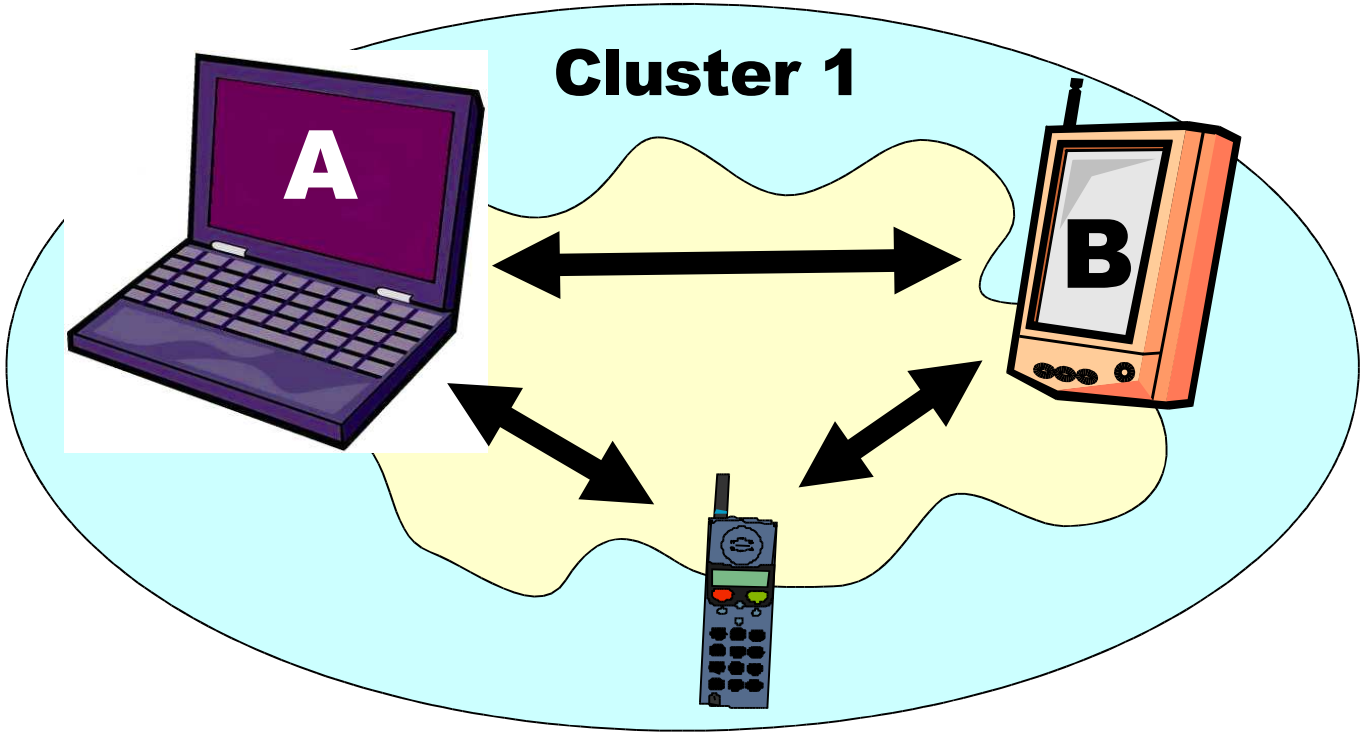
$\{Hello, A\}_{PID}$ →

$\{Hello, B\}_{PID}$ ←

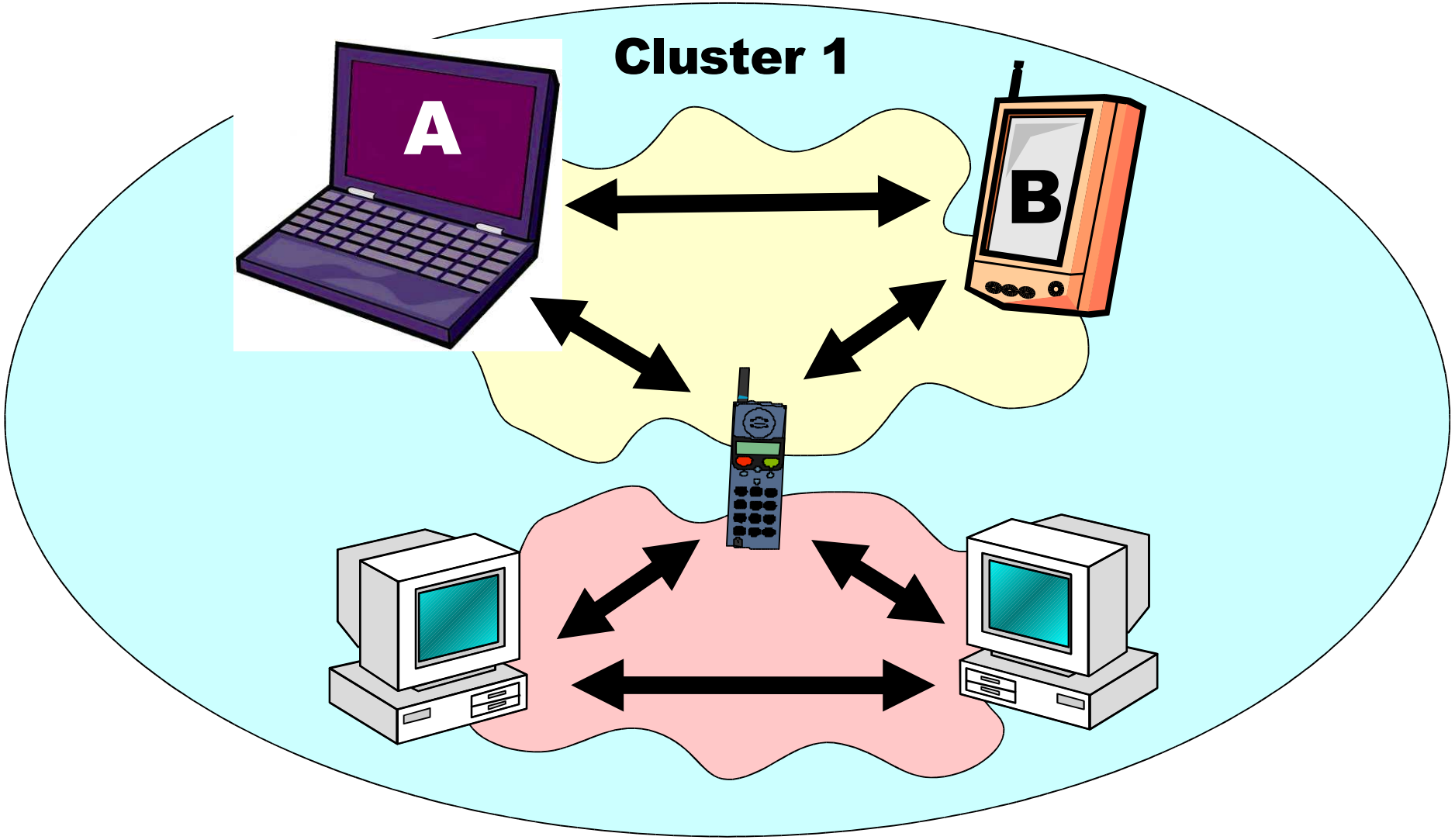
$\{Mgmt\ Data\}_{PID}$ ↔

$\{Data\}_{PID}$ ↔

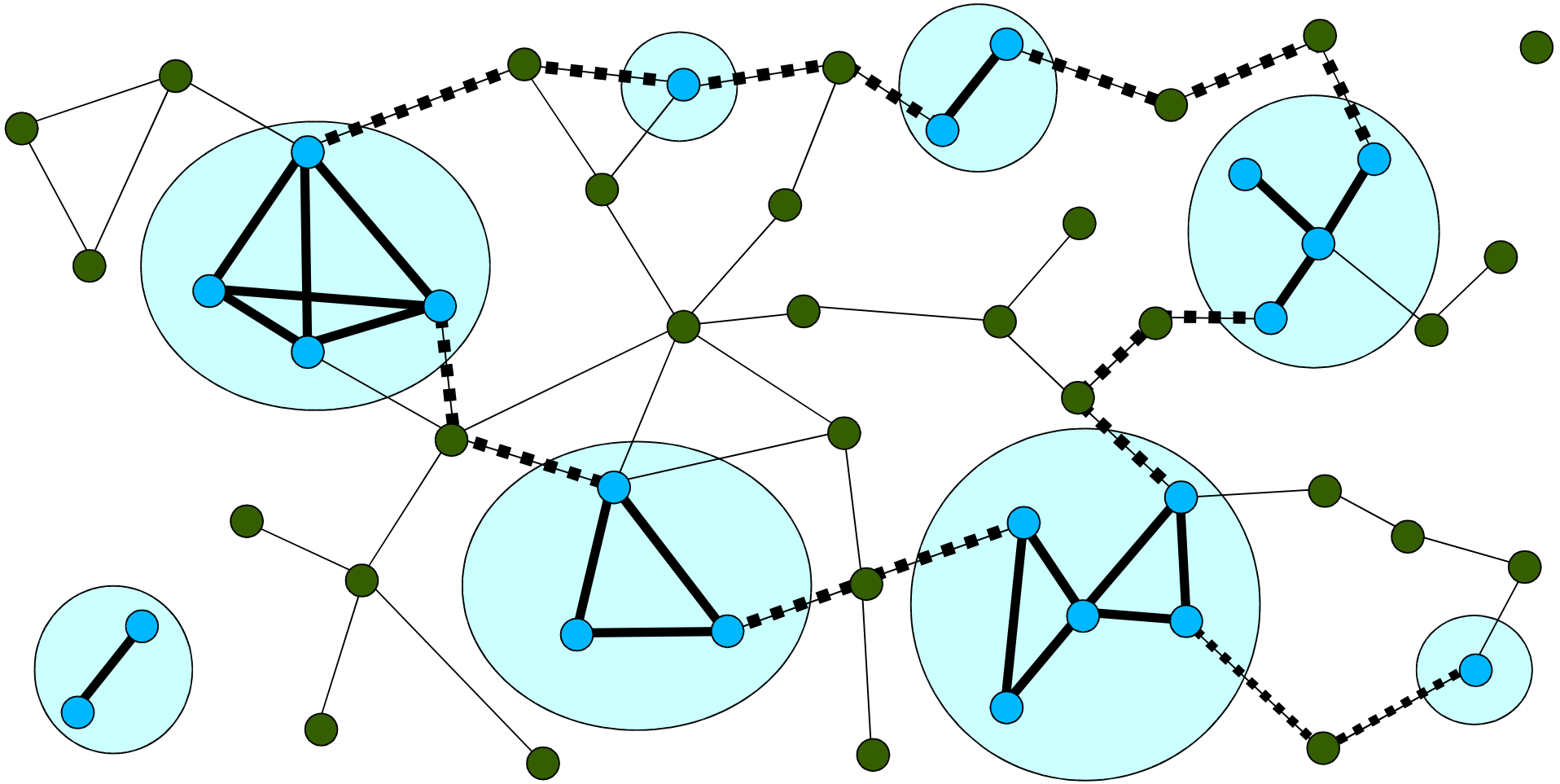
… and a Cluster is formed



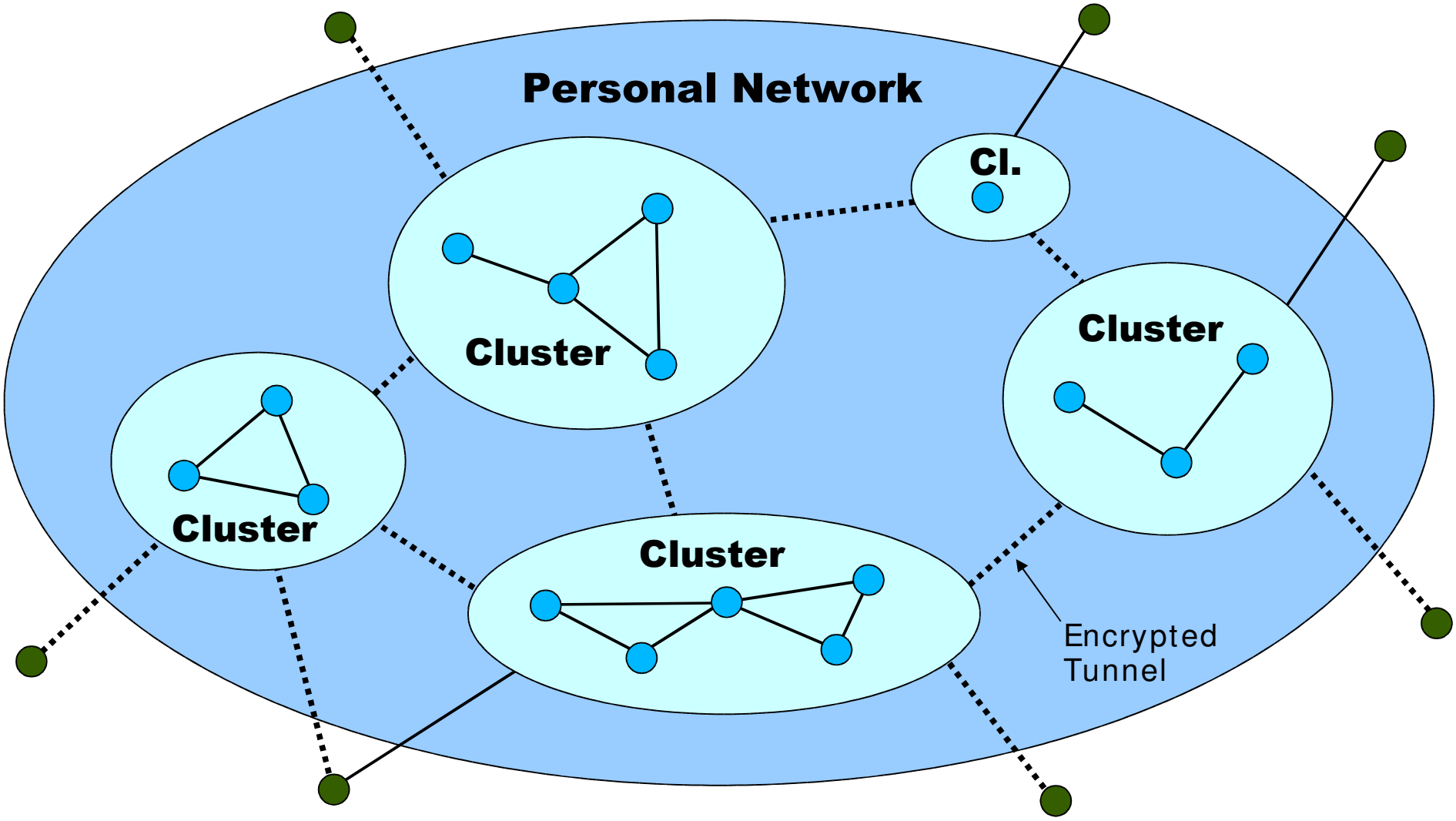
A Cluster can be multi-hop



The big picture



The architecture



Cluster conclusions

- Nodes in a Cluster share the same PID
- PID can be used to protect intra-Cluster communication, including intra-Cluster routing.
- Clusters are dynamic. Node joining and leaving as well as Cluster merging and splitting are common events.

Network functionality of a Cluster

- Secure packet forwarding
  - Offering data integrity and encryption
- Intra-Cluster routing and addressing
  - Mobile ad-hoc routing, automatic addressing
- Intra-Cluster Broadcasting/flooding capabilities
  - For service discovery, context information, routing, ...
- Edge/border/gateway node identification
  - To establish connections with Foreign Nodes and other Clusters. Edge nodes enforce security.

PN conclusions

- Consists of one or more dynamic Clusters
- Clusters are interconnected by tunnels
- Since all Nodes share the same PID, data traffic can be encrypted.
- A Node needs the correct PID to join a PN.
- However, inter-Cluster communication is dependent on Foreign Nodes and their routing mechanisms.

Network functionality of a PN

- Establishment and maintenance of encrypted tunnels between all Clusters
- Inclusion of new Nodes and exclusion of compromised Nodes
- Secure and anonymous setup and maintenance of communication with Foreign Nodes.

Security implications of the architecture

Anonymity

- Definition: A Node must never reveal its identity, including addresses, names, PIDs, etc unless the user approves it or is aware of it.
- This includes all steps:
  - A Node meets another Node
  - Communication between Personal Nodes
  - Communication between Personal Nodes and Foreign Nodes of already known Personal Networks
- Otherwise, tracking of users becomes possible by anyone!

Anonymity Solutions

- The procedure to detect Personal Nodes must never reveal identities to non-Personal Nodes.
- MAC-addresses are not kept constant.
- Network layer and up is encrypted with help of the PID.

PN security implications

- Personal Networks is person centric
- Personal Networks also have to focus on interactions with other persons:
  - Partner, children and family
  - Team work and colleagues
  - Friends and acquaintances
  - …
- And we still need security and privacy

Sharing and borrowing of Nodes

- The architecture is strongly focused around the owner concept - a person owns a Node!
- Sharing and borrowing will be a requirement:
  - Families share Nodes in the house, car, etc
  - Friends borrow each other's Nodes
  - Employees borrow company equipment for trips, etc.
  - ...
- Renting will also be a requirement:
  - Car with electronic equipments, ...

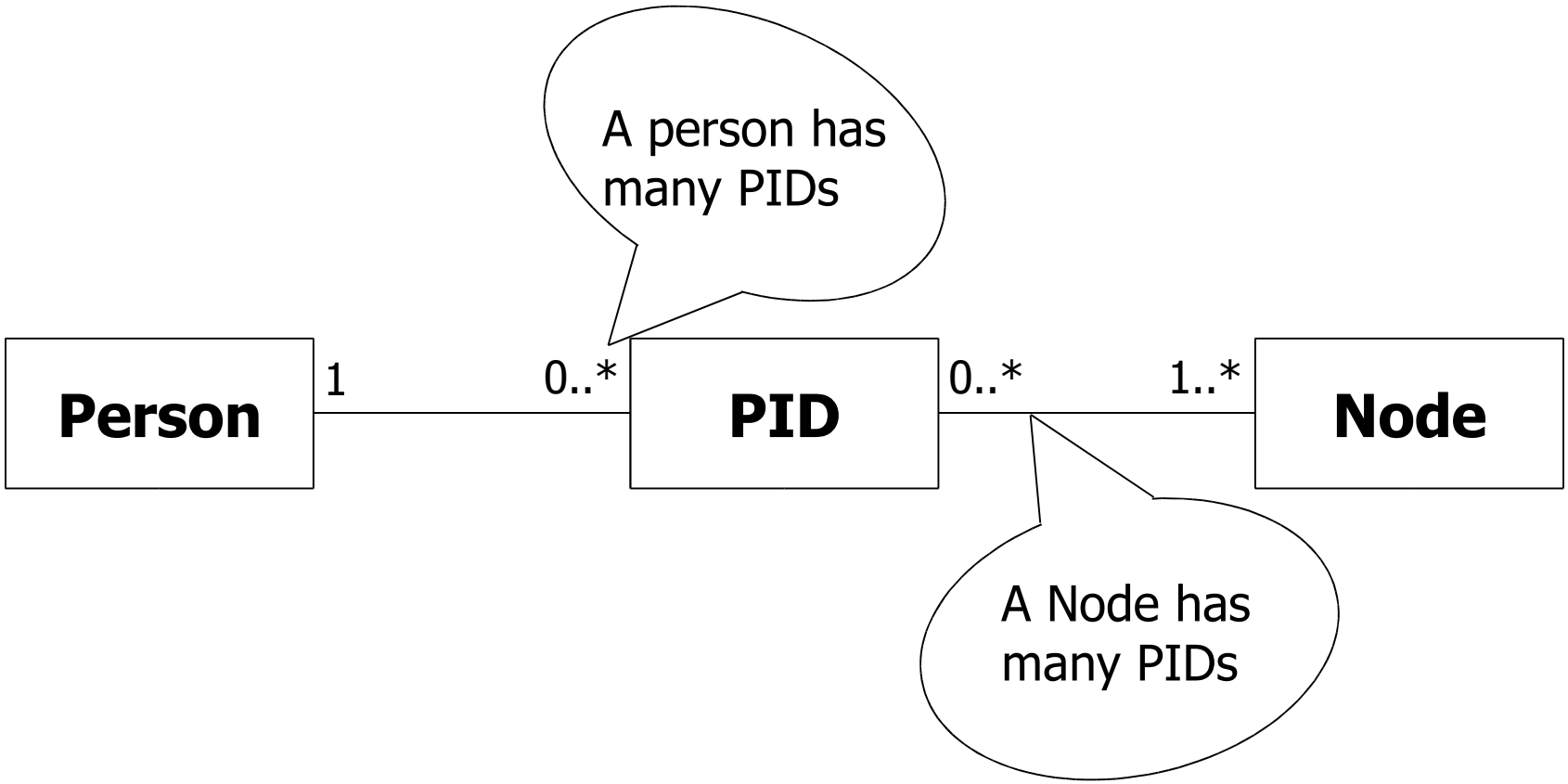
Personal vs. professional life

- A working person does not want two separate PNs, one professional PN and one private PN.
  - Only one agenda, email account, etc
  - Manage private activities from office
  - Distance working from home

The Person - PID - Node relation (1)

- A person can have two (or more) PIDs:
  - One private PID for private Nodes
  - One professional PID for the company's Nodes
  - Or more...
- A Node can be equipped with many PIDs:
  - For a family sharing a Node
  - For persons with several PIDs
  - ...

The Person - PID - Node relation (2)



Theft of devices and data

- If a Node possesses a PID, it can join that PN – What if such a Node is stolen?
- Since PIDs are different, lost Nodes can be excluded – Is this good enough?

- Data can be stolen or modified before the PID is excluded!
- There is still a need for an authentication/access rights system at the service/application layer.

PN security summary

- PID protects anonymity/privacy and routing traffic
- PID does not protect everything, because:
  - PID is insufficient for most Foreign Node communication
  - Theft of one single PN Node would compromise the whole PN
- Therefore, an application/service layer security mechanism is still needed!

A possible implementation

Requirements of a PID implementation

- Anonymous detection of Personal Nodes
- Enabling secured connections between Personal Nodes
- Personalization of not yet Personal Nodes must be easy and always possible
- Compromised Personal Nodes can be excluded
- Enabling secure communication with other Personal Networks

Extended node pairing method

- A Person pairs his Nodes (e.g. as in Bluetooth)
  - During the pairing procedure, the Nodes exchange keys, etc.
- However, n Nodes means n(n-1)/2 pairings...

- Therefore, we introduce a “transitive rule”:

If A and B are paired and B and C are paired

Then A and C are also paired

This method implements the PID model

- We know from set theory (relations):
  - Since the pairing is reflexive, symmetric and transitive, then it is an equivalence relation and divides the set of all Nodes into partitions.
- Each partition is a Personal Network
- Some things still needs to be worked out:
  - The cryptographic and practical details
  - Exclusion of compromised Nodes is not addressed
  - Sharing is not possible (Nodes with multiple PIDs)

Conclusions

Conclusions and remarks

- PID is a security policy model, that models ownership of communicating Nodes
- PID is person centric which leads to some problems when looking at interactions between persons, such as sharing and borrowing of Nodes.
- IST-MAGNET is working on an implementation (not addressing all requirements)

Further Information

- MAGNET website: http://www.ist-magnet.org/

- Martin Jacobsson, Jeroen Hoebeke, Sonia Heemstra de Groot, Anthony Lo, Ingrid Moerman, Ignas Niemegeers, "**A Network Layer Architecture for Personal Networks**", In the Proceedings of Workshop on "My Personal Adaptive Global Net: Visions and beyond", Shanghai, China, November 11-12, 2004.
- Weidong Lu, Anthony Lo, Ignas Niemegeers, "**On the Dynamics and Self-Configuration of Personal Networks**", In the Proceedings of Workshop on "My Personal Adaptive Global Net: Visions and beyond", Shanghai, China, November 11-12, 2004.
- Kaisa Nyberg, Dorgham Sisalem, "**Establishing Security in Personal Area Networks**", In the Proceedings of Workshop on "My Personal Adaptive Global Net: Visions and beyond", Shanghai, China, November 11-12, 2004.

Questions