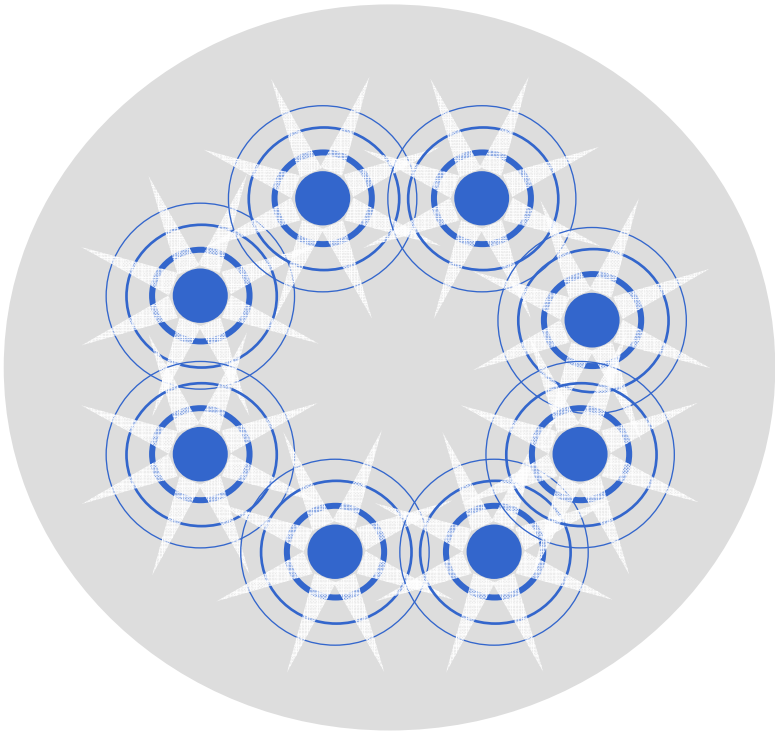
Sicherheit in Sensornetzen

Erik-Oliver Blaß
Institut für Telematik
Universität Karlsruhe



Was sind Sensornetze?

Buzzwords

Invisible Computing

Pervasive Computing (= “durchdringend”)

Ubiquitous Computing (=“allgegenwärtig”)

Ambient Intelligence (=“umgebend”)

Wearable Computing

Wireless Sensornetworks

Organic Computing,

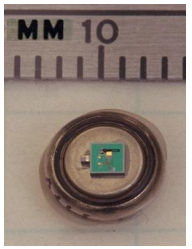
“Self-X”:
Self-Organizing,
Self-Healing, …,

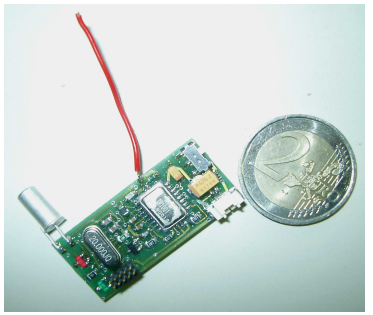
Was sind Sensornetze?

Netzwerke von Kleinst-Computern, den Sensoren

- Batteriebetrieben
  180 mAh Kapazität
  (≈1/10 eines Handys)
- Microcontroller CPU,
  8-Bit 7MHz ATMEL
  kein Cache, keine branch prediction etc.
  ⇒ ca. 7 MIPS (≈1/5 eines Gameboys)
  Main Memory: 4 KByte RAM (≈1/8000 eines PDAs)
- Wireless-Link: Bluetooth/Zigbee mit
  250 kBit/s (1/400 eines LAN)
- Hardware zum Beobachten von
  Ereignissen, z.B. Temperatur, Licht, etc

Smart Dust

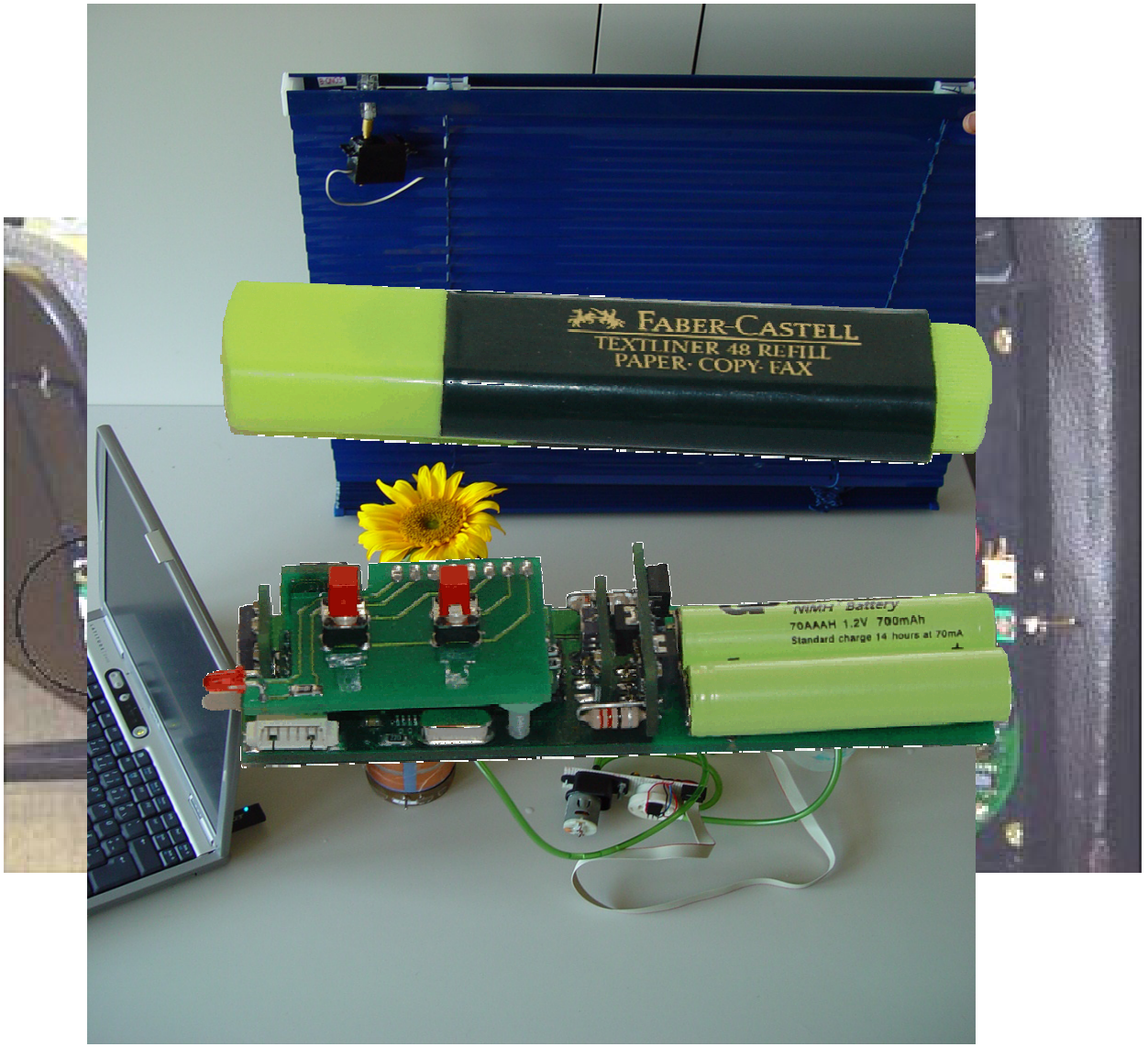




Sensornetze sind

- Pervasive – oft in alltägliche Objekte integriert
- Self-X – selbstorganisierend

Beispiele


FABER-CASTELL
TEXTLINER 48 REFILL
PAPER· COPY· FAX
70AAAH 1.2V 700mAh
Standard charge 14 hours at 70mA

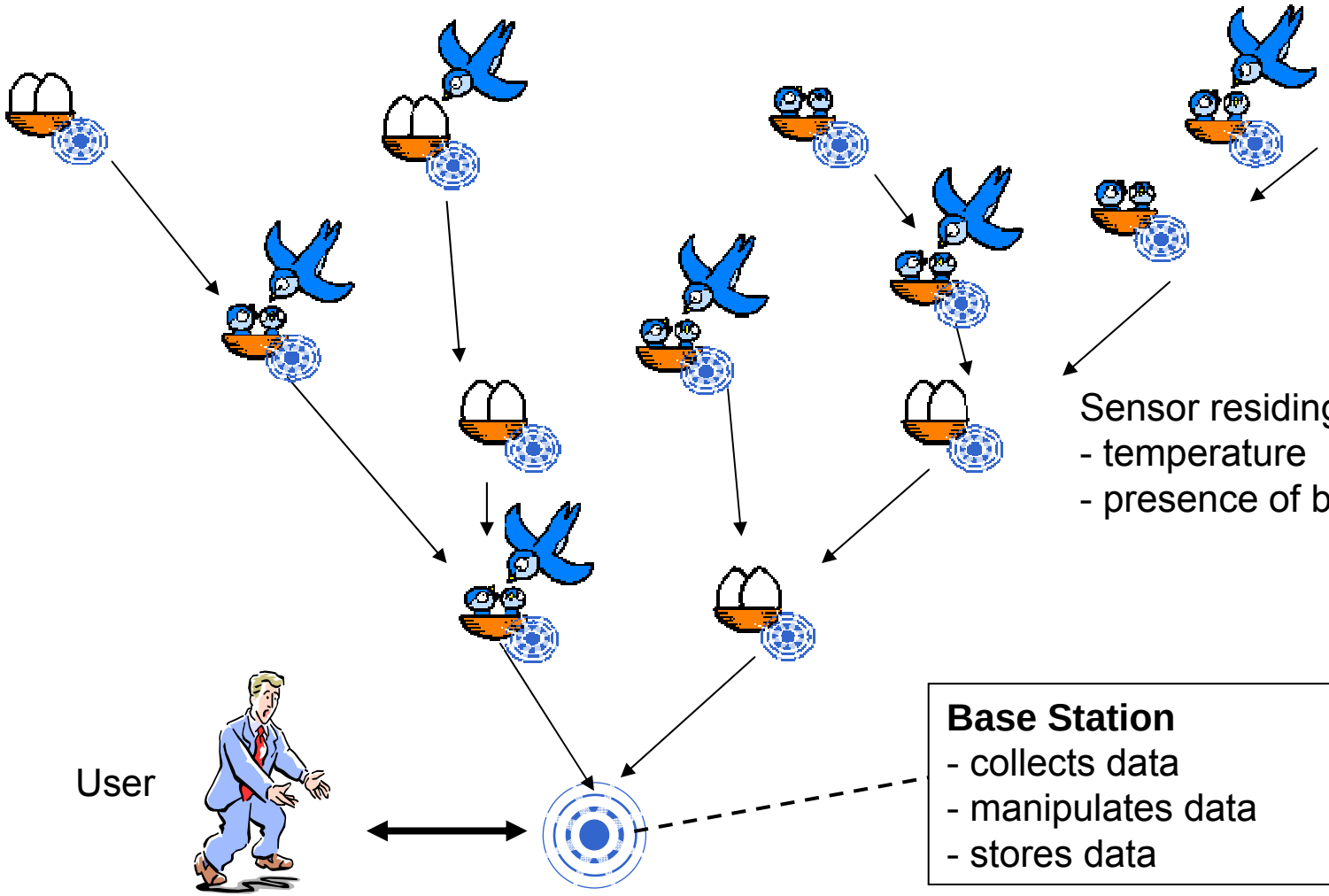
Beispiele

K-SNeP

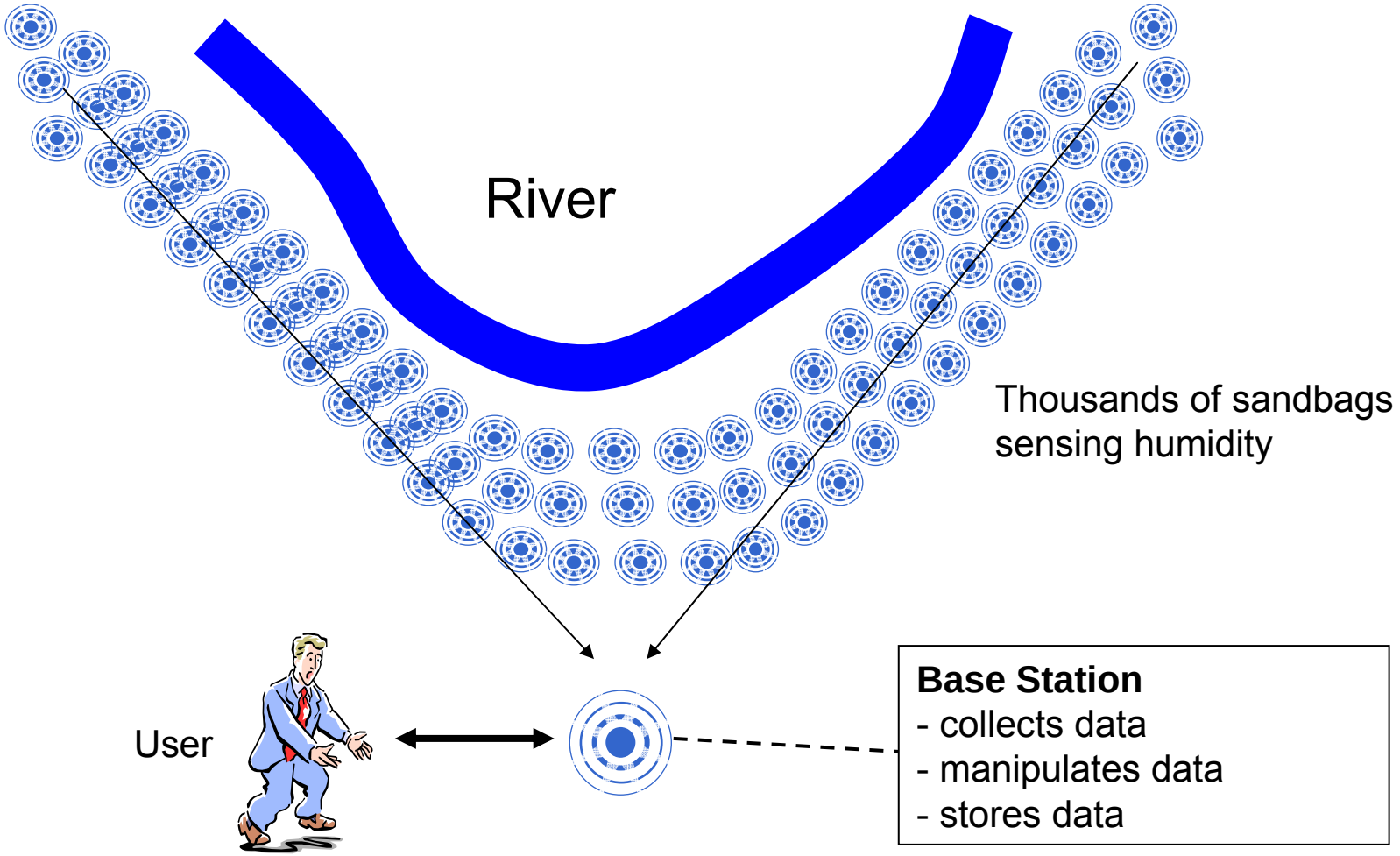
Karlsruhe Sensor
Network Platform

Erik-Oliver Blaß, Hans-Joachim Hof, Bernhard Hurler, Martina Zitterbart, *Erste Erfahrungen mit der Karlsruher Sensornetz-Plattform*, GI/ITG KuVS Fachgespräch "Drahtlose Sensornetze", Berlin, Germany, Jul 2003.

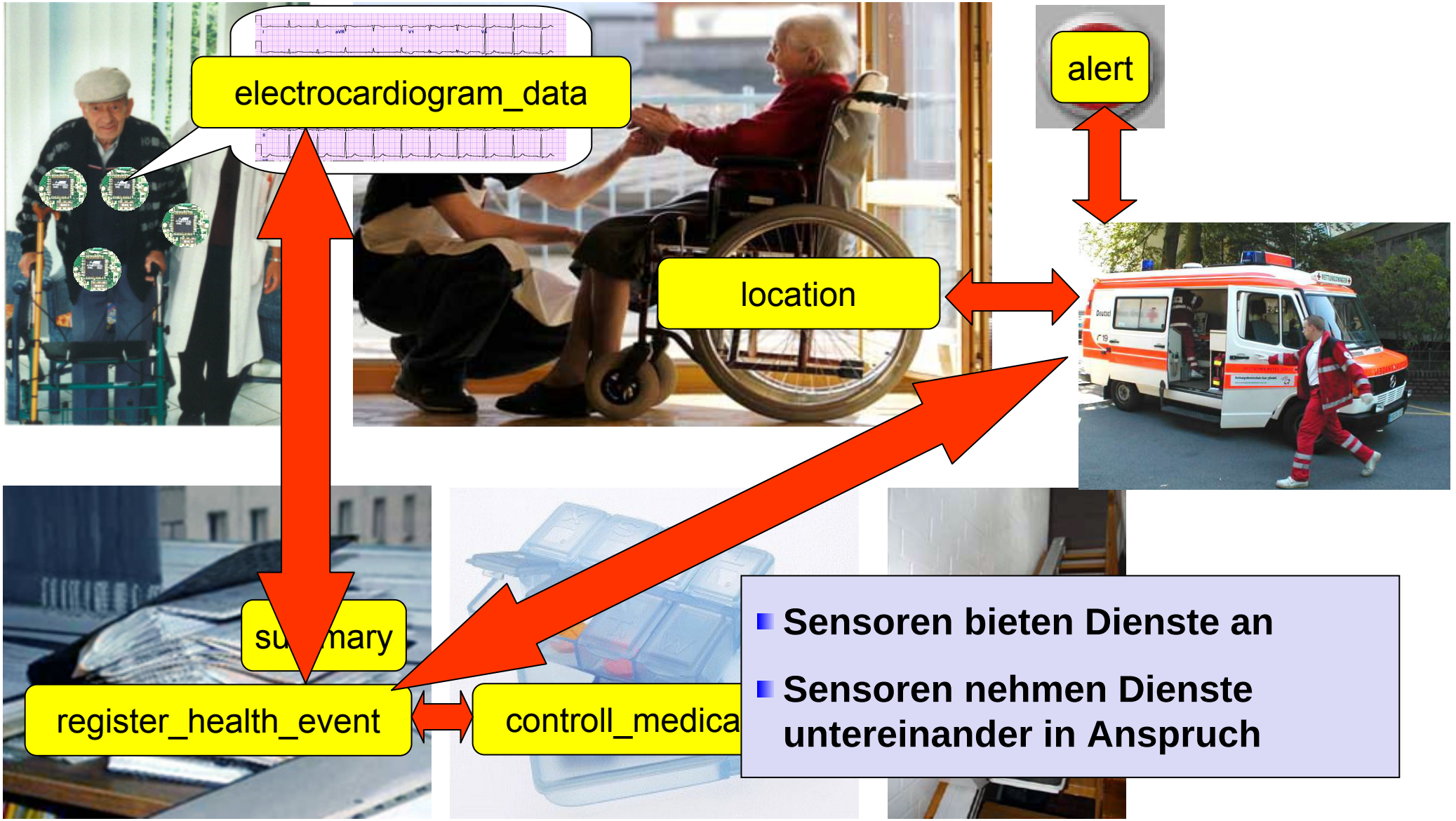
Environmental observation



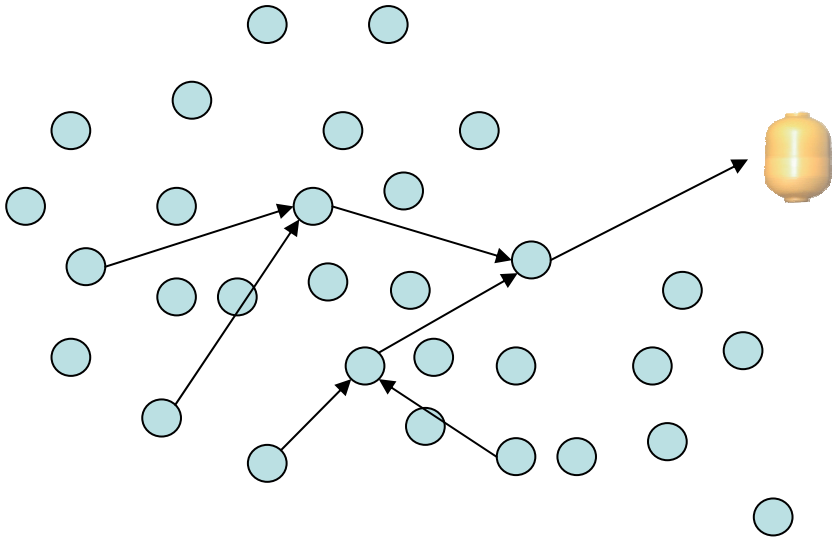
Disaster management



Dienst-Orientierte Sensornetze

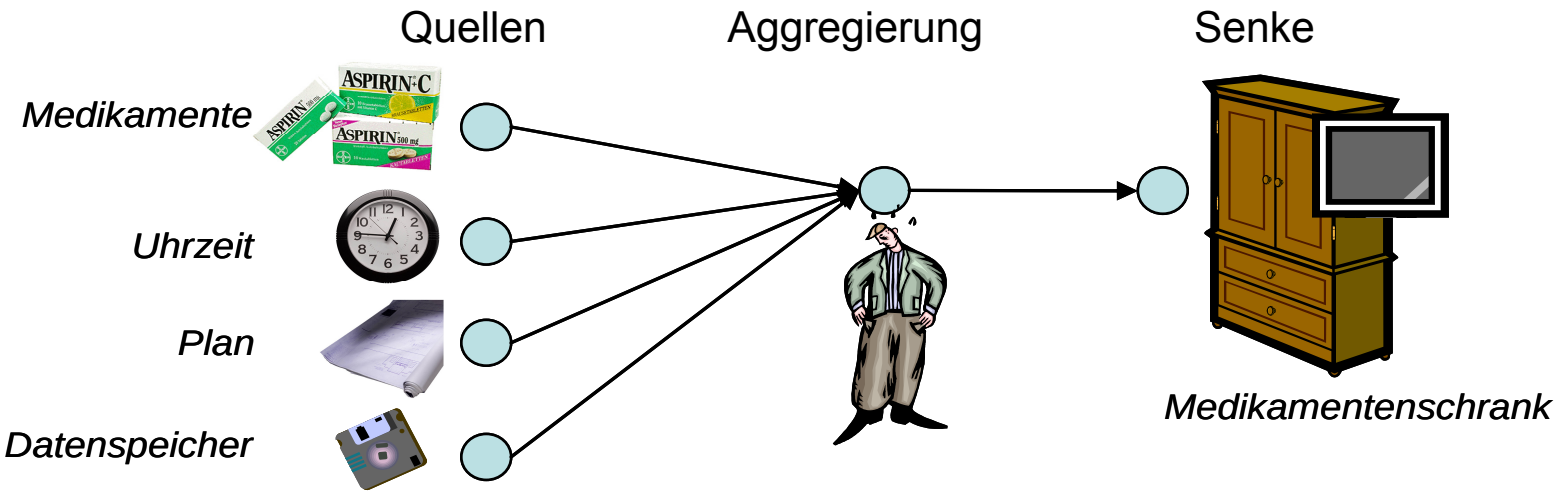


Typische Kommunikation im Sensornetz



„Aggregierung“

Typische Kommunikationsform in Sensornetzen ist „Aggregierung“



In Sensornetzen problematisch sind…

…typische UbiComp-Themen:

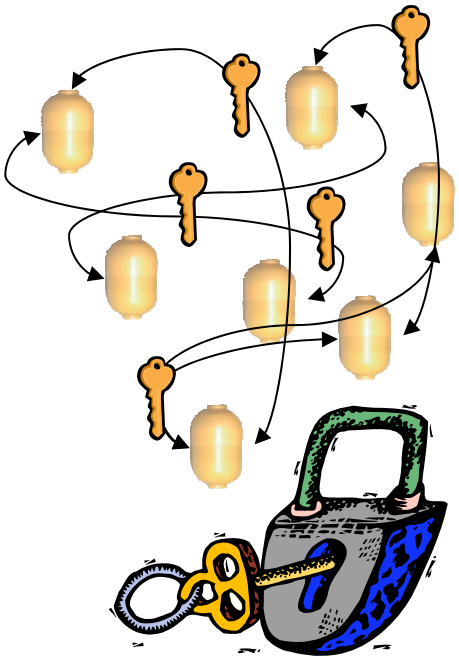
- Privatsphäre
- RFID-Chips
- Metro, WalMart
- Überwachbarkeit
- Anonymität
- Verfolgbarkeit, etc.

} „Big-Brother“ Problematik

Sicherheit in Sensornetzen am ITM

Forderung

- Sensible Dienste sollen auch im Sensornetz „sicher“ erbracht werden.
- Klassische Anforderungen: Authentizität, Integrität, Vertraulichkeit usw.
- Neue Angriffe gegen Robustheit und Verfügbarkeit,
  z.B. „Sleep Deprivation Torture“



Klassische Lösungen ungeeignet

- Extreme Hardwarelimitierung: Wenig Speicher/CPU etc.
  - ⇨Asymmetrische Kryptographie u.U. unmöglich?
- Ad-Hoc-Kommunikation
  - „Keine Abhängigkeit von einer festen Kommunikationsinfrastruktur“
    ⇨ Keine Infrastruktur-Einrichtungen nutzbar, z.B. CA einer Public-Key-Infrastruktur, da zum Teil nicht erreichbar, offline, etc.
  - „Spontane Vernetzung“
    ⇨ Keinerlei Vorwissen mehr über das Gegenüber
    ⇨ So ein gemeinsamer Vertrauens-Anker für Authentizität unmöglich
- Autonomes Handeln von Systemen
  - ⇨ Keine menschliche Interaktion möglich
  - ⇨ Kein Abstimmen von Geräten, Pairing durchführbar

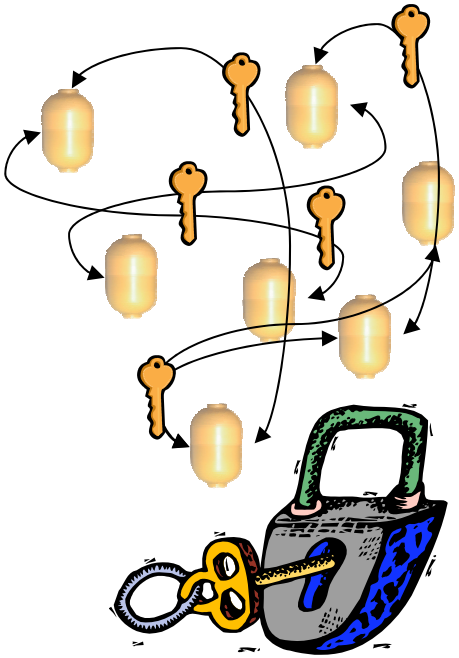
Zwei Problemfelder erkennbar

1. Sichere Dienst-*Vermittlung*

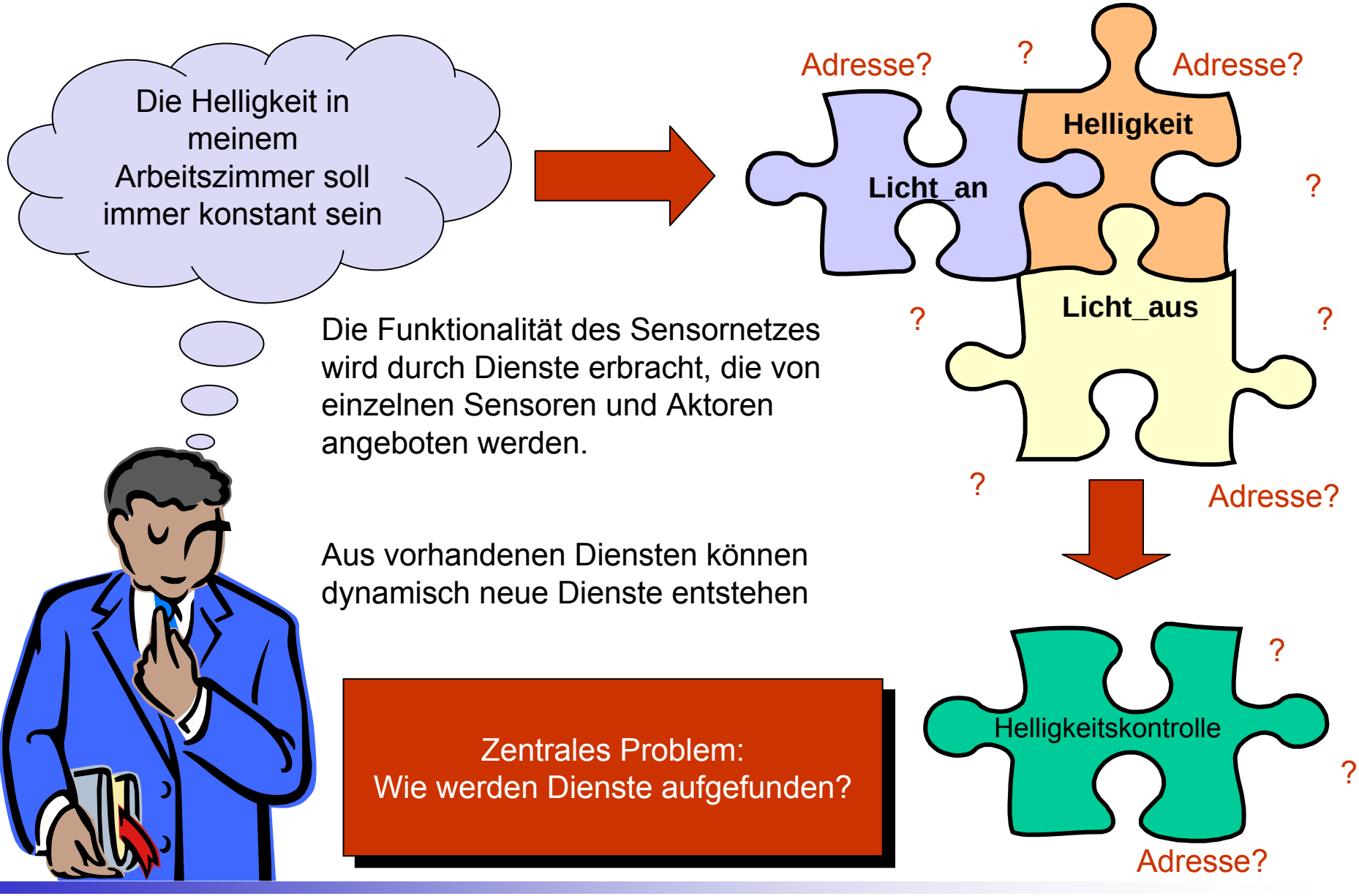
- Registrieren eines neuen Dienstes
- Finden eines registrierten Dienstes

2. Sichere Dienst-*Inanspruchnahme* (=„sicherer Datentransport“)

- Effiziente Schlüsselverteilung
- Effiziente Algorithmen
- Robuster Datentransport



Diensteorientierte Sensornetze



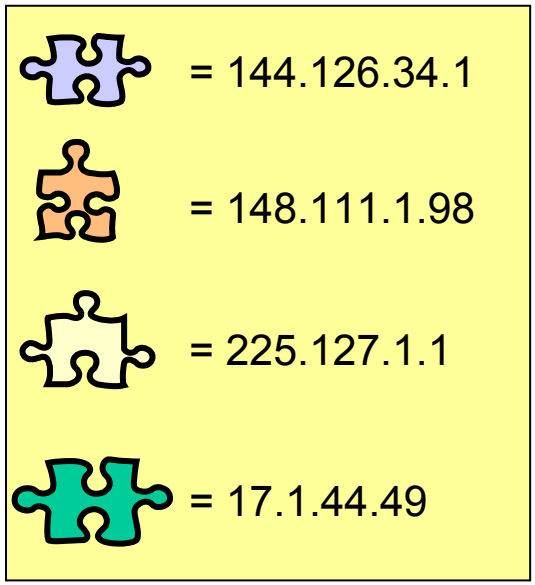
Die Funktionalität des Sensornetzes wird durch Dienste erbracht, die von einzelnen Sensoren und Aktoren angeboten werden.

Aus vorhandenen Diensten können dynamisch neue Dienste entstehen

Zentrales Problem:
Wie werden Dienste aufgefunden?

Auffinden von Diensten

Gesucht:

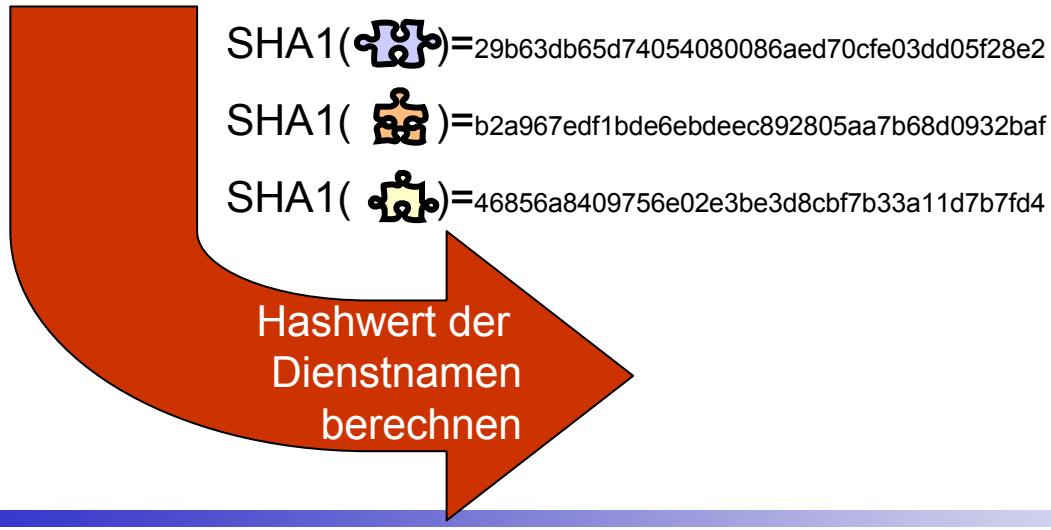


Aber: Es gibt im Sensornetz keine zentrale Instanz, die diese Liste verwalten könnte

⇨ Verteilte Speicherung auf den Sensorknoten selbst

⇨ Overlay Content Addressable Networks zur Speicherung (Distributed Hash Table)

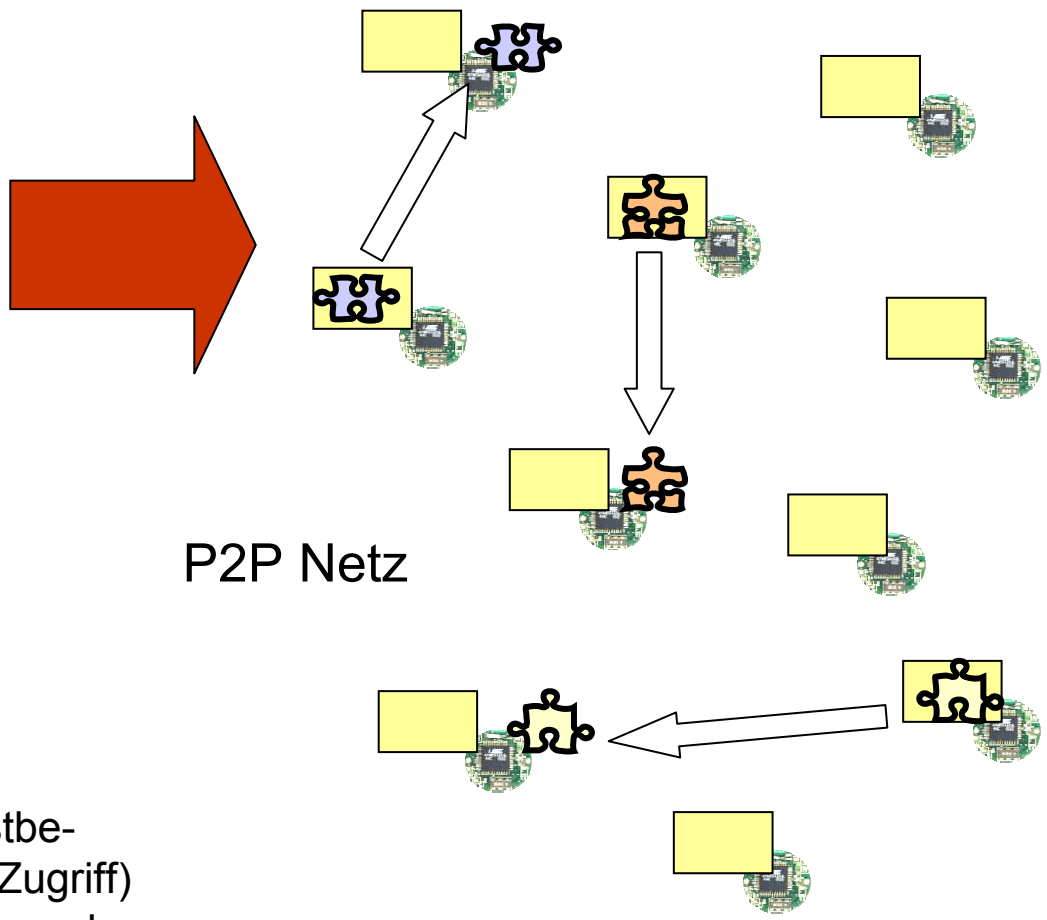
⇨ Nicht nur Adresse sondern Dienstbeschreibung speichern



Hash-Wert	Inhalt
29b63db65d7405408008 6aed70cfe03dd05f28e2	Dienstbeschr.
b2a967edf1bde6ebdeec 892805aa7b68d0932baf	Dienstbeschr.
46856a8409756e02e3be 3d8cbf7b33a11d7b7fd4	Dienstbeschr.

Verteilte Speicherung und Sicherheit

Hash-Wert	Inhalt
29b63db65d7405408008 6aed70cfe03dd05f28e2	Dienstbeschr.
b2a967edf1bde6ebdeec 892805aa7b68d0932baf	Dienstbeschr.
46856a8409756e02e3be 3d8cbf7b33a11d7b7fd4	Dienstbeschr.



Sicherheitsüberlegungen:

- ❑ Robustheit
- ❑ Integrität veröffentlichter Dienstbeschreibungen
- ❑ Vertraulichkeit von Teilen der Dienstbeschreibung (z.B. für Schlüssel zum Zugriff)
- ❑ Authentifizierung von Dienstanbieter und dem die Dienstbeschreibung speichernden Knoten

Secure Content Addressable Networks

Ergebnis:

- Starres Routing
  - Unmöglich durch Angriff Routing zu verändern
- Verteiltes Speichern von Informationen, verteilte Datenbank, Redundanz durch Verwendung mehrerer Hash-Funktionen
  - Teilweiser Netzausfall/feindliche Netzübernahme für das Gesamtnetz nicht von Bedeutung
- Durch Dienstbeschreibung feststehender Speicherort
  - Angreifer muß in der Lage sein, gezielt Knoten ausschalten zu können
- Gespeichert werden zu Adressen nur Hash-Werte
  - Knoten wissen nicht, welche Informationen sie vorhalten

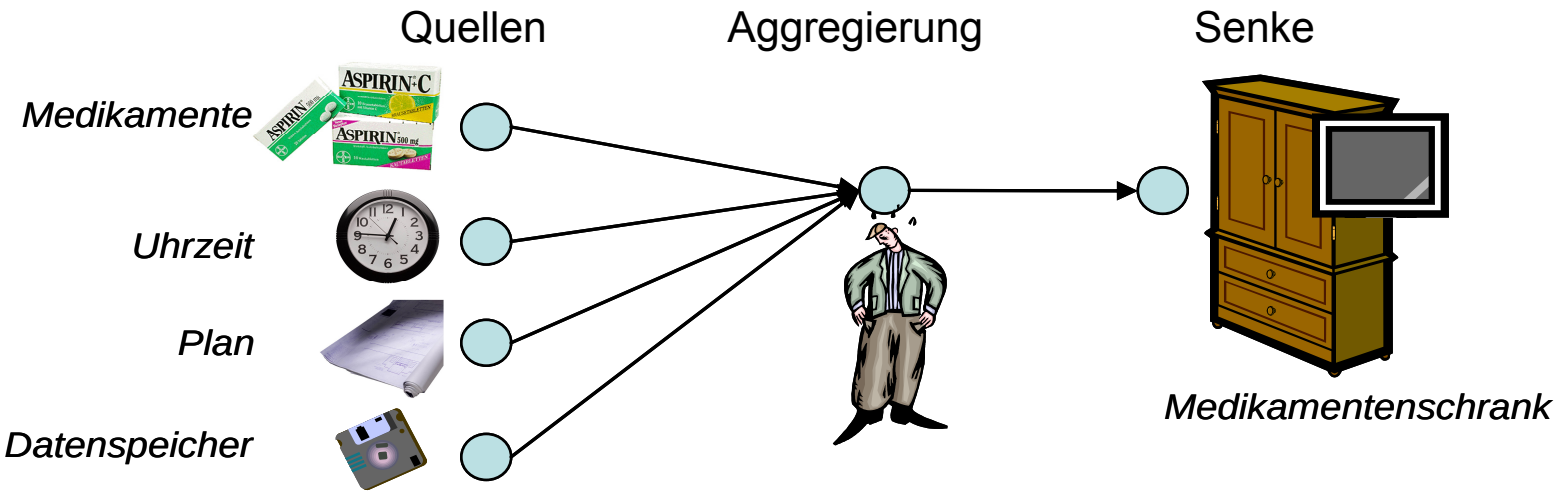
Erik-Oliver Blaß, Hans-Joachim Hof, Martina Zitterbart, *S-CAN: Sicheres Overlay für Sensornetze*, 2. GI/ITG KuVS Fachgespräch Drahtlose Sensornetze, Mar 2004

Artur Hecker, Erik-Oliver Blass, Houda Labiod, *COMPASS: Decentralized Management and Access Control for WLANs*, IEEE International Conference on Personal Wireless Communications, Aug 2005 (to appear)

Hans-Joachim Hof, Erik-Oliver Blaß, Thomas Fuhrmann, Martina Zitterbart, *Design of a Secure Distributed Service Directory for Wireless Sensornetworks*, First European Workshop on Wireless Sensor Networks, Jan 2004

Hans-Joachim Hof, Erik-Oliver Blaß, Martina Zitterbart, *Secure Overlay for Service Centric Wireless Sensor Networks*, First European Workshop on Security in Ad-Hoc and Sensor Networks, Aug 2004

Typische Kommunikationsform in Sensornetzen ist „Aggregierung“



Problem: Wie kann ein aggregierender Datentransport in Sensornetzen abgesichert werden?

- Schutz sensibler Daten vor Abhören, Verändern,…
- Zusicherung von Authentizität, Nicht-Abstreitbarkeit usw. **trotz** Aggregierung
- Effiziente Lösungen sind gesucht!

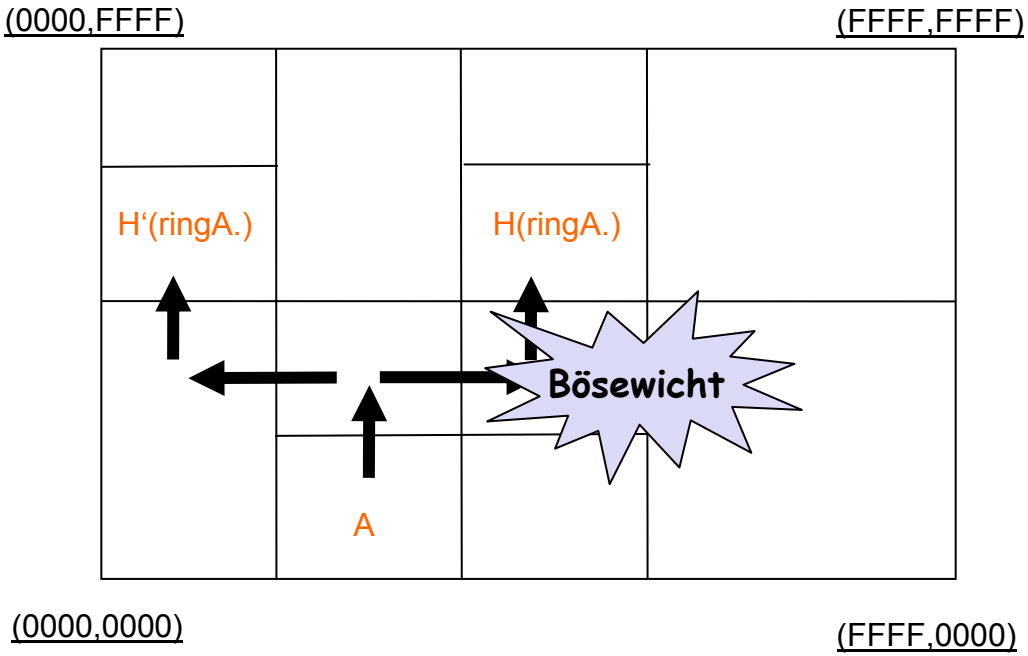
Sicherer Datentransport

Vor Datentransport notwendig: Schlüsselverteilung

- Keine typischen „single key“, „single point of failure“ Lösung
- Vermeide teures „re-keying“
- Verzichte auf Unterstützung durch Basisstation
- Skalierbare, dynamische, selbstorganisierende Lösung

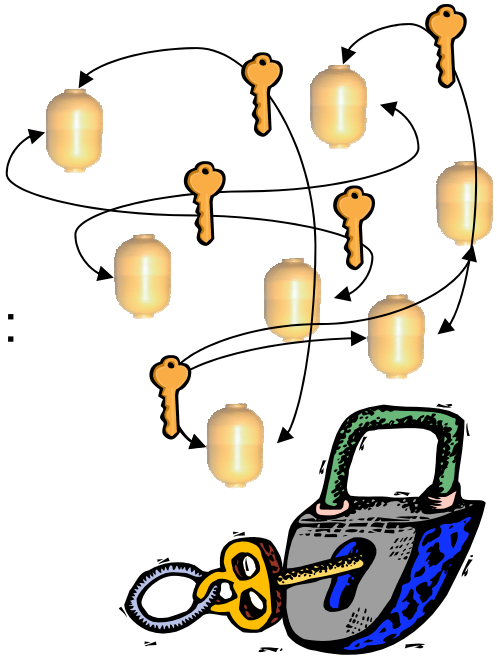
Erste Ansätze sind beispielsweise

- Verteilen von Schlüsseln über das S-CAN
  - S-CAN ermöglicht sicheres Store und Retrieve von Daten
  - Sicherheit durch redundantes Speichern und Abfragen
- Identitätsbasierte Authentifizierung
  - „Der Sensor- bzw. sein Dienstname ist sein Schlüssel“
  - Beschaffung und Überprüfung von Schlüsseln entfällt
- Ganz anders: Benutze Hierarchie im Sensornetz



Effiziente Chiffrieralgorithmen sind notwendig

- Algorithmen sind Grundlage jedes Protokolles
- Welche der klassischen Verfahren eignen sich für den Einsatz auf Sensorhardware?
- Asymmetrische Kryptographie im Allgemeinen schwierig: RSA, ECC, NTRU,…
- Gesucht: Geeignete Implementierungen auf Mikrocontrollern
  - AES ca. 40 KBit/s
  - SHA-1 ca. 5 KBit/s
  - Allerdings z.B. 5s für 163 Bit Punktmultiplikation, etwa 30s für 1024 Bit RSA Exponentieren



Erik-Oliver Blaß, Martina Zitterbart, *Towards Acceptable Public-Key Encryption in Sensor Networks*, The 2nd International Workshop on Ubiquitous Computing, May 2005 (to appear)

Was „kostet“ Sicherheit?

- Overhead durch Sicherheitsprotokoll muss gering bleiben
- Aufstellung eines Kostenmodells
  - Betrachtet Energie-, Speicherverbrauch, Rechenzeit, Anzahl zu versendender Nachrichten
  - Erlaubt den Vergleich verschiedener Sicherheitsprotokolle für verschiedene Hardwareplattformen
  - Qualitative Aussagen über Eignung verschiedener Verfahren möglich

$$cost = \frac{rounds * \sum corefctcst\ (textlength / oplength) + storage}{cpuspeed * buswidth * (RAM + ROM)}$$

Fragen und Diskussion

Fragen?