Falk Uebernickel

Datenschutzfreundliche Gestaltung von Location Based Services

Saarbrücken, 6. Mai 2004

Gliederung

1. Überblick

2. Methoden und Verfahren unterhalb der Anwendungsschicht

3. Gestaltungsmöglichkeiten auf der Anwendungsschicht
   1. Methoden zur Pseudonymisierung
   2. Methoden zur Positionsverschleierung

Möglichkeiten der datenschutzfreundlichen Gestaltung

- obere Schichten bauen auf dem Datenschutzniveau der Tieferen auf
- zusätzliche Gestaltungsmöglichkeiten:
  - organisatorische Anordnung der Beteiligten (Datenverteilung)
  - nationale Gesetzgebung

Gliederung

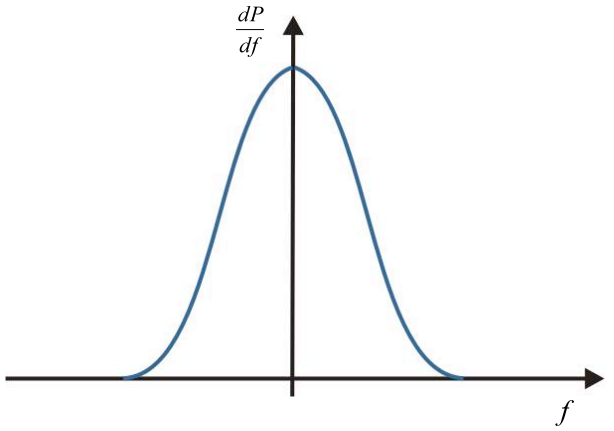
1. Überblick

2. **Methoden und Verfahren unterhalb der Anwendungsschicht**

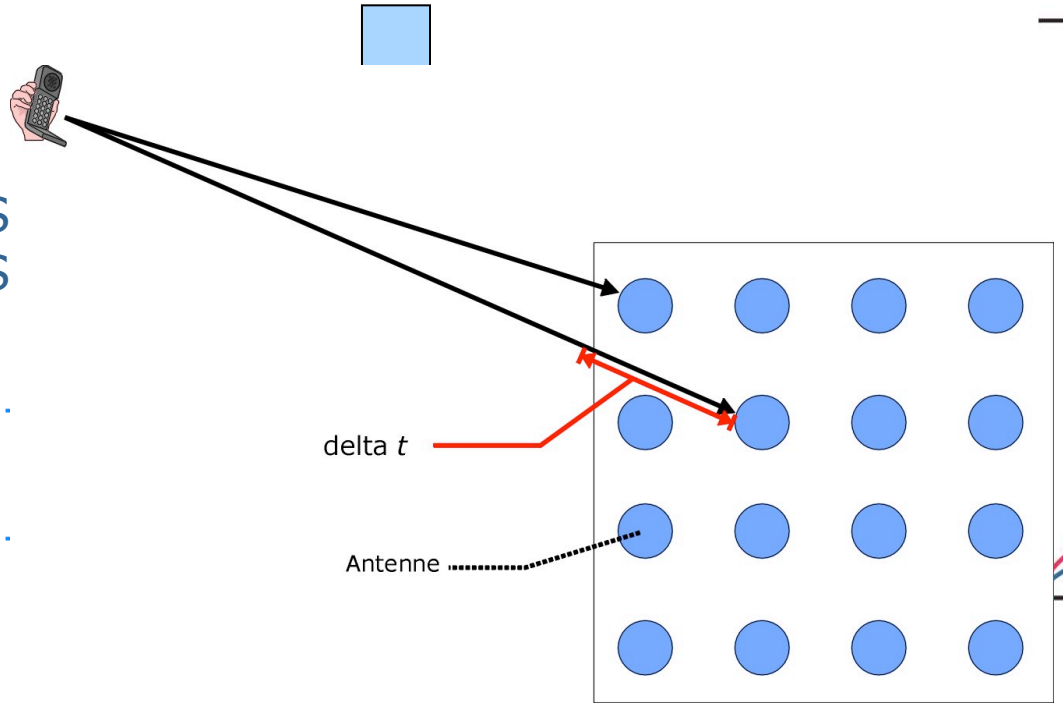
3. Gestaltungsmöglichkeiten auf der Anwendungsschicht
    1. Methoden zur Pseudonymisierung
    2. Methoden zur Positionsverschleierung

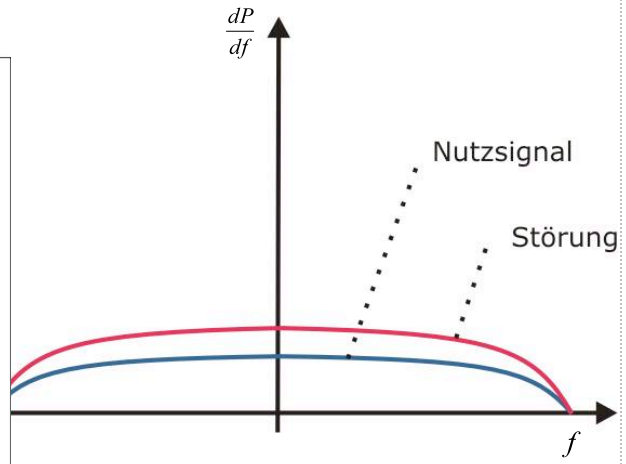
Schutz vor Endgerätepeilung (Bandspreizverfahren)

- Angreifer kann durch Peilung den Aufent-haltsort des Nutzers bestimmen
  - Antennen – Arrays
  - spezielle Antennen zur Peilung



- S
  S





MAC-Adresswechsel in IEEE 802.11b WLAN's (1)

- Problemstellung:
  - in jeder Kommunikationssituation identifiziert sich der WLAN-Client auf der MAC-Schicht mit einem Gerätepseudonym
  - WLAN-Client ist durch benachbarte Access-Points verfolgbar

Gefahr der Bewegungsprofilerstellung beim Netzbetreiber

→ nicht vertrauenswürdige Access-Point-Betreiber

→ hohe Dichte an Access-Points in Stadtbereichen

→ sehr genaue Ortungsmöglichkeiten in WLAN's

MAC-Adresswechsel in IEEE 802.11b WLAN's (2)

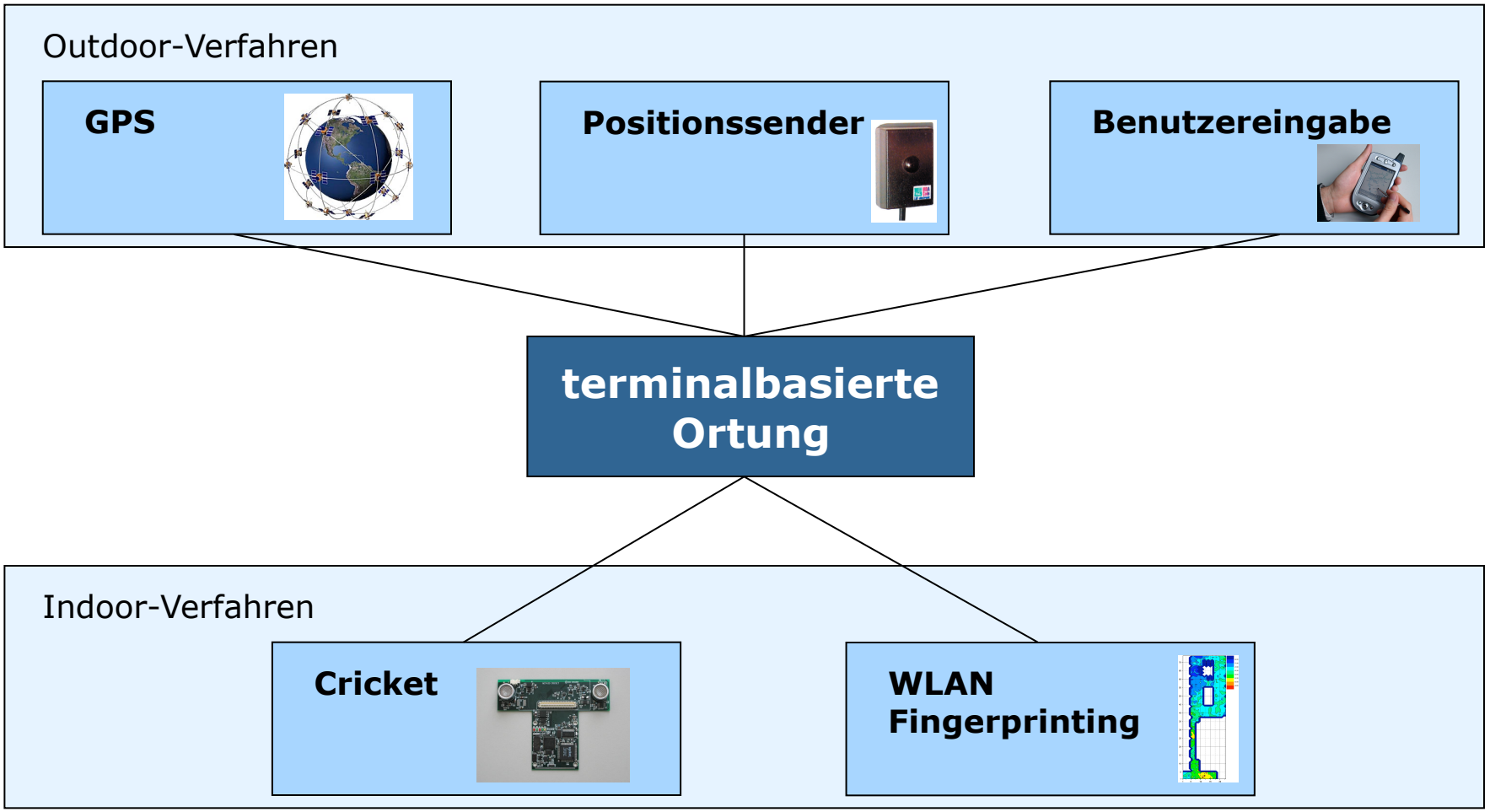
- Lösungsmöglichkeit:

  → kontrolliertes und permanentes Wechseln der MAC-Adresse

- mögliche Wechselzeitpunkte:
  - in zufälligen Zeitabständen
  - bei großen Signalstärkeänderungen
  - wenn keine Kommunikation stattfindet
  - gleitender Übergang → der Client hält zu einem Zeitpunkt mehrere MAC-Adressen gleichzeitig

- Nachteile:
  - Angebot von serverähnlichen Diensten nicht möglich

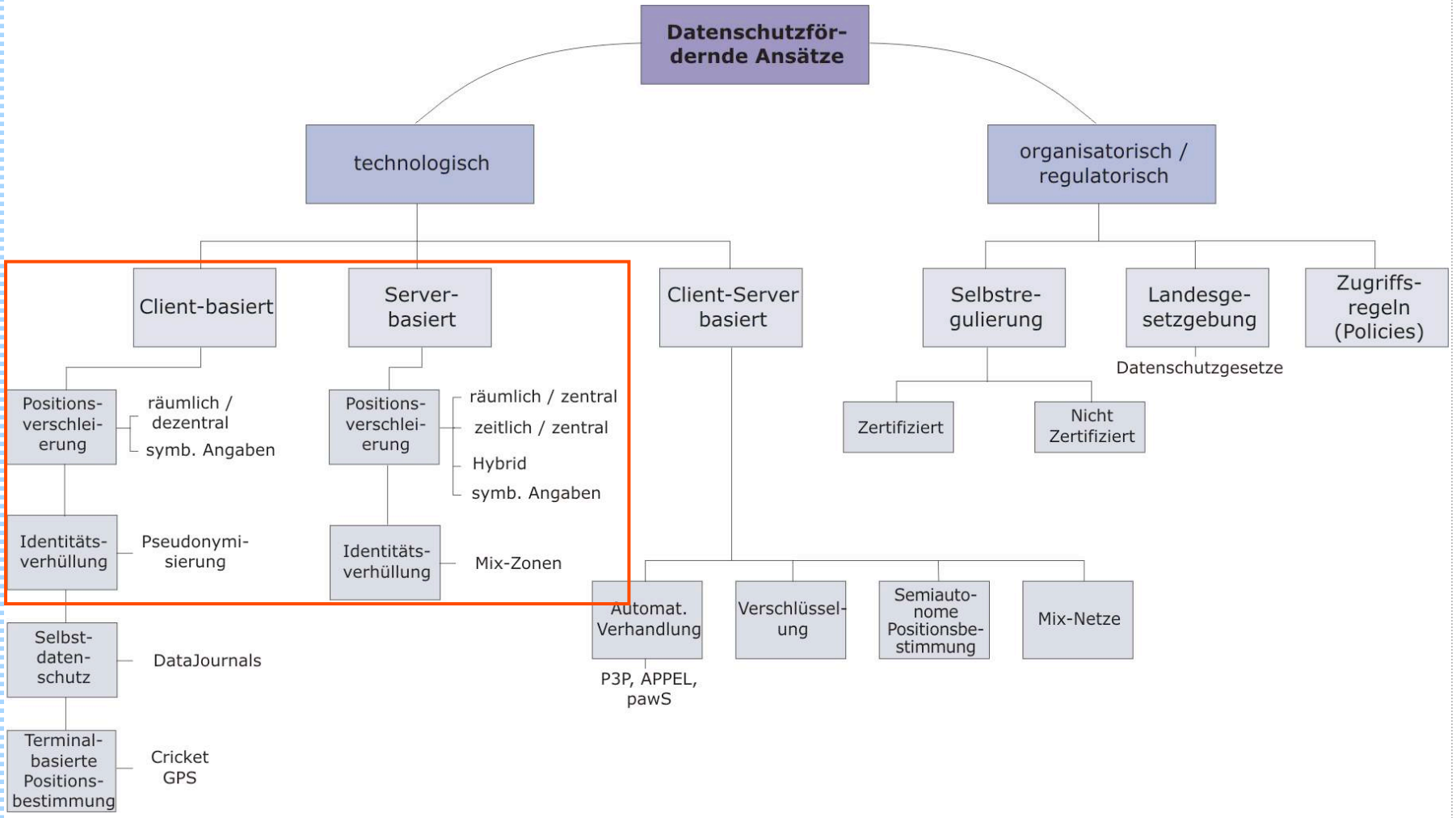
Einsatz datenschutzfreundlicher Ortungsverfahren



Gliederung

1. Überblick
2. Methoden und Verfahren unterhalb der Anwendungsschicht
3. Gestaltungsmöglichkeiten auf der Anwendungsschicht
   1. **Methoden zur Pseudonymisierung**
   2. Methoden zur Positionsverschleierung

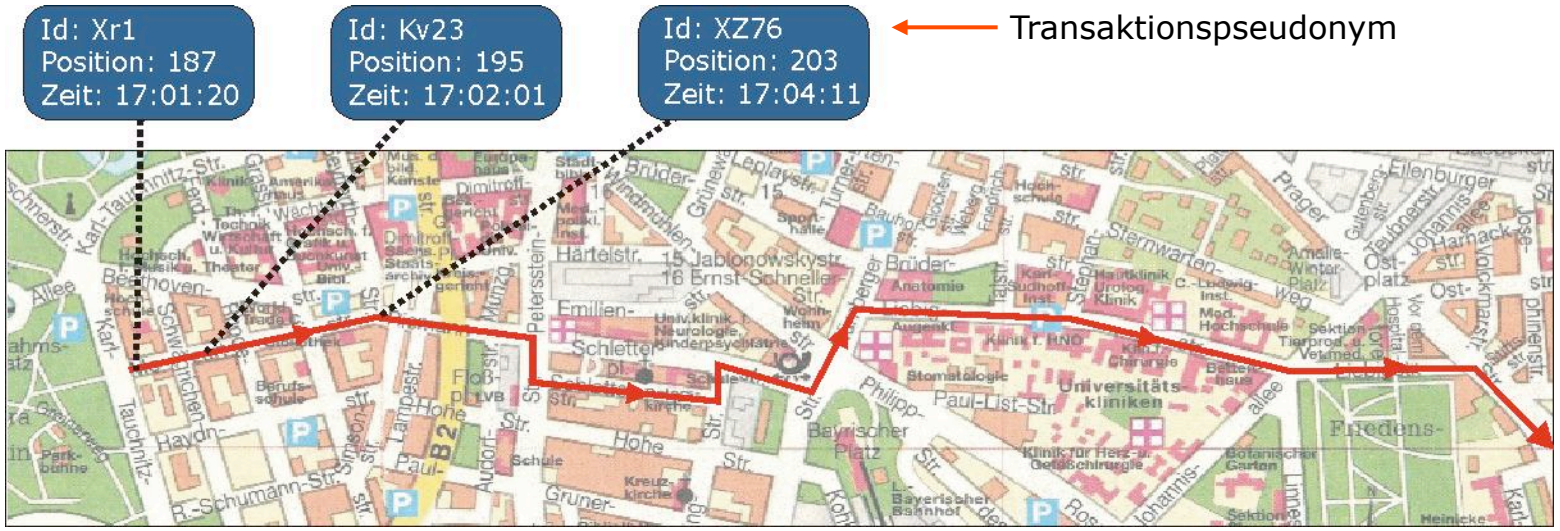
Bausteine zur Förderung des Datenschutz



Anonymisierung (1)

- Pseudonymisierung des identifizierenden Merkmals innerhalb einer Anfrage

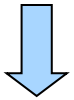
- Pseudonymvarianten:
  - (Merkmal wird nicht versendet)
  - Transaktionspseudonyme
  - Rollen-Beziehungspseudonyme
  - Beziehungspseudonyme und Weitere



Anonymisierung (2)

- Annahmen:
  - Positionsangaben sind hoch präzise (< 1 Meter)
  - sehr hohe Dienstnutzungsfrequenz
  - LBS-Dienstanbieter verzeichnet alle pseudonymisierten Dienst-anfragen in einer Datenbank

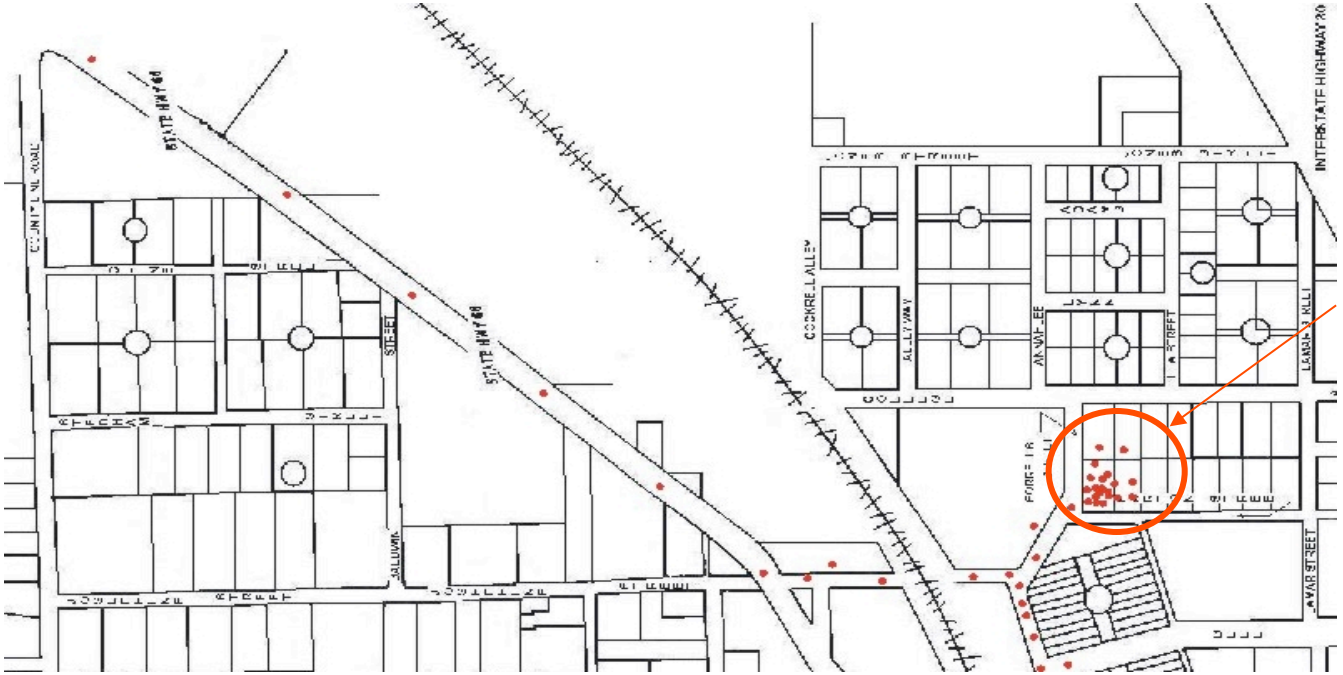
- Angriffsmöglichkeiten bei Verwendung von Transaktionspseudo-nymen:
  - Verknüpfung der einzelnen pseudonymisierten Dienstanfragen über Bewegungsverhalten möglich → pseudonymisiertes Bewegungsprofil
  - Bestimmung von häufig besuchten Aufenthaltsorten (Wohnung, Arbeitsplatz, Lieblings-Cafe etc.) → sog. „Home-Angriff"



  - nachschlagen der Identität in einem Register (Telefonbuch)

Anonymisierung (3)

- Home-Angriff:



- Anhaltsgrößen für Home-Bereiche:
  - hohe Verweildauern an einem Ort
  - Verlust des Positionsbestimmungssignals (GPS) kann als ein Betreten von Gebäuden gedeutet werden, ist allerdings mehrdeutig (hohe Bebauung, Batterieausfall)

Anonymisierung (4)

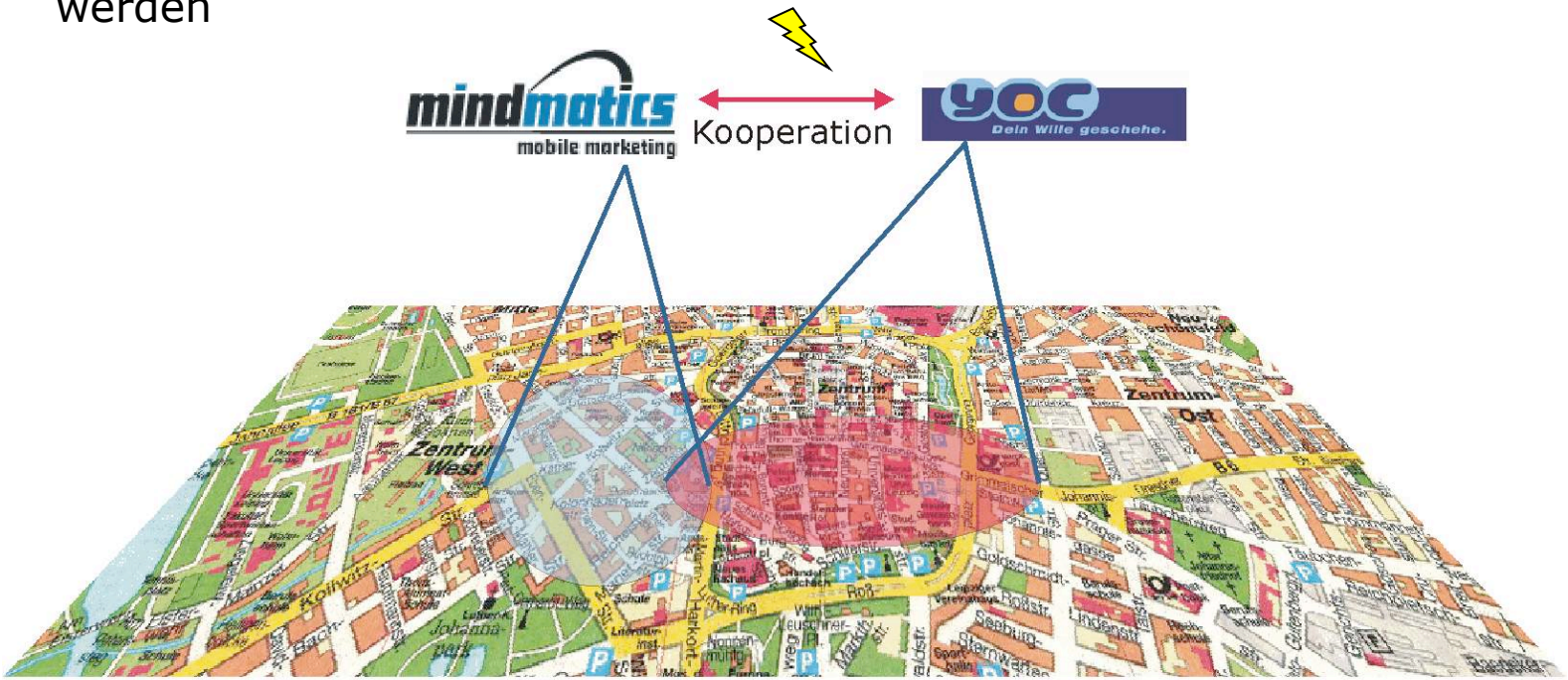
- Vorteile:
  - einfache Implementierung
  - keine spezielle Hardware notwendig
- Voraussetzungen:
  - geringe Dienstabrufhäufigkeit oder
  - niedrige Positionsauflösung
- Anwendungsgebiete:
  - Abfrage von nächstgelegenen Hotels
  - Suche nach Geldausgabeautomaten

Mix-Zonen (1)

- Annahme und Zielsetzung:
  - Unterschiedliche LBS-Dienstanbieter legen ihre gewonnenen pseudonymisierten Nutzerprofile zusammen

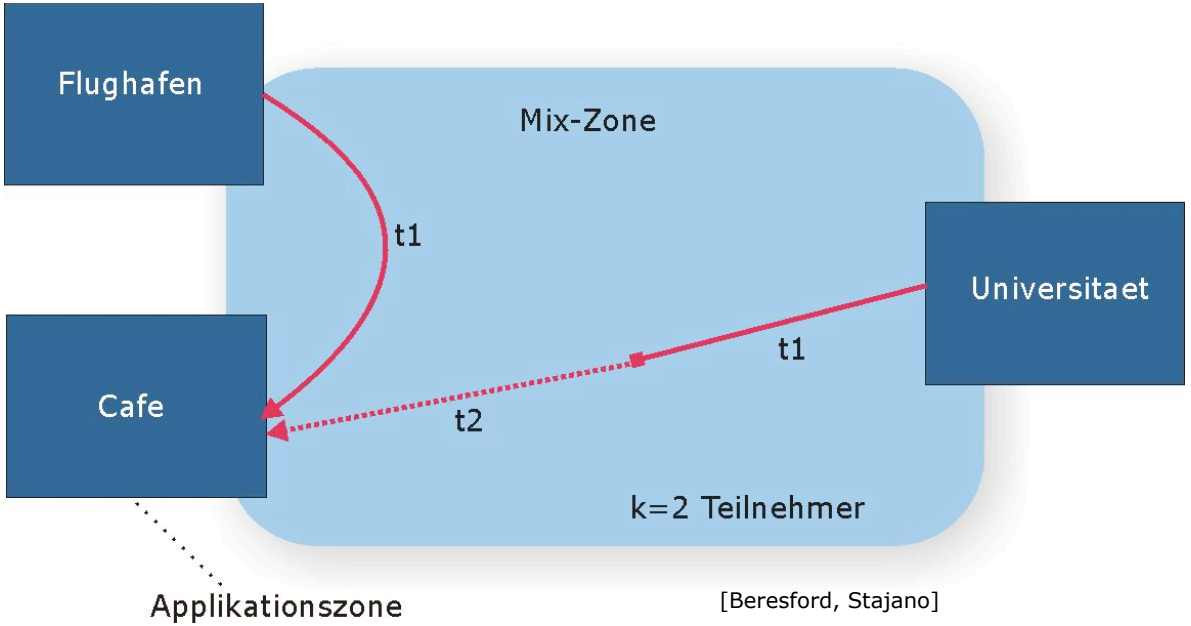
Zielsetzung

  - Verkettbarkeit der einzelnen pseudonymisierten Profile soll verhindert werden



Mix-Zonen (2)

- Funktionsweise:



[Beresford, Stajano]

- Definitionen:
  - **Applikationszone:** geografischer Bereich in dem Personen LBS-Dienste in Anspruch nehmen
  - **Mix-Zone:** Bereich in dem ein Teilnehmer keinen LBS-Dienst abonniert haben darf

Gliederung

1. Überblick
2. Methoden und Verfahren unterhalb der Anwendungsschicht
3. Gestaltungsmöglichkeiten auf der Anwendungsschicht
   1. Methoden zur Pseudonymisierung
   2. **Methoden zur Positionsverschleierung**

Räumliche Positionsverzerrung, Überblick (1)

- Ziel:
  - Schaffung einer Anonymitätsgruppe durch Anpassung der Positionsgenauigkeit

- Funktion:
  - Grundgedanke:

$$P_x^R = P_x + U$$

    - Abschneiden der letzten Stellen der Positionsinformation

$$\begin{Bmatrix} 51.04861\ \text{N} \\ 13.74138\ \text{O} \end{Bmatrix} \rightarrow \begin{Bmatrix} 51.048\ \text{N} \\ 13.741\ \text{O} \end{Bmatrix}$$

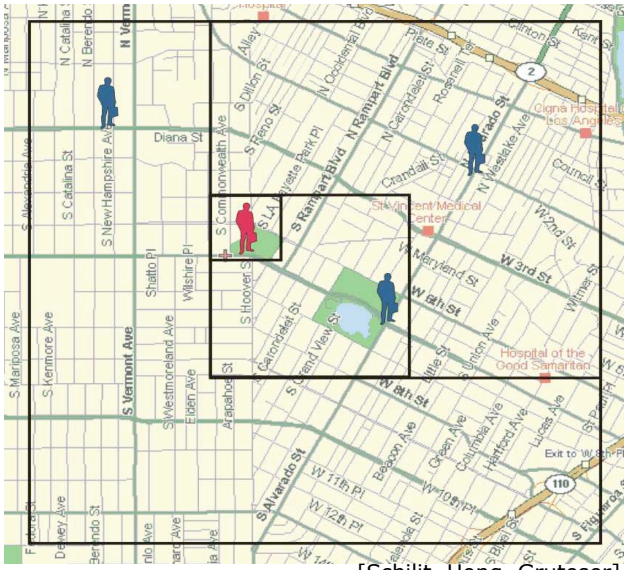
    - Hinzufügen eines Fehlers

Räumliche Positionsverzerrung, dezentral (2)

- dezentrale Variante:
  - Dimensionierung von *U* wird ausschließlich auf dem Endgerät festgelegt
  - Möglichkeiten der Dimensionierung:
    - Benutzer legt selbst eine maximale Ortungsgenauigkeit fest
      → mathematische Verschlechterung
    - Unschärfe wird durch das Ortungsverfahren bestimmt
- Vorteile:
  - Verfälschung der Ortung geschieht nur auf dem Endgerät
- Nachteile:
  - Bildung einer Anonymitätsgruppe nicht gewährleistet
  - eventuell unnötiger Verlust an Positionsgenauigkeit

Räumliche Positionsverzerrung, zentral (3)

- zentrale Variante:
  - Dimensionierung erfolgt bei einer TTP
  - Algorithmus bestimmt unter Berücksichtigung weiterer Dienstnutzer die minimale Verfälschung der Ortung
  - Anonymitätsgrad wird über k_{min} festgelegt



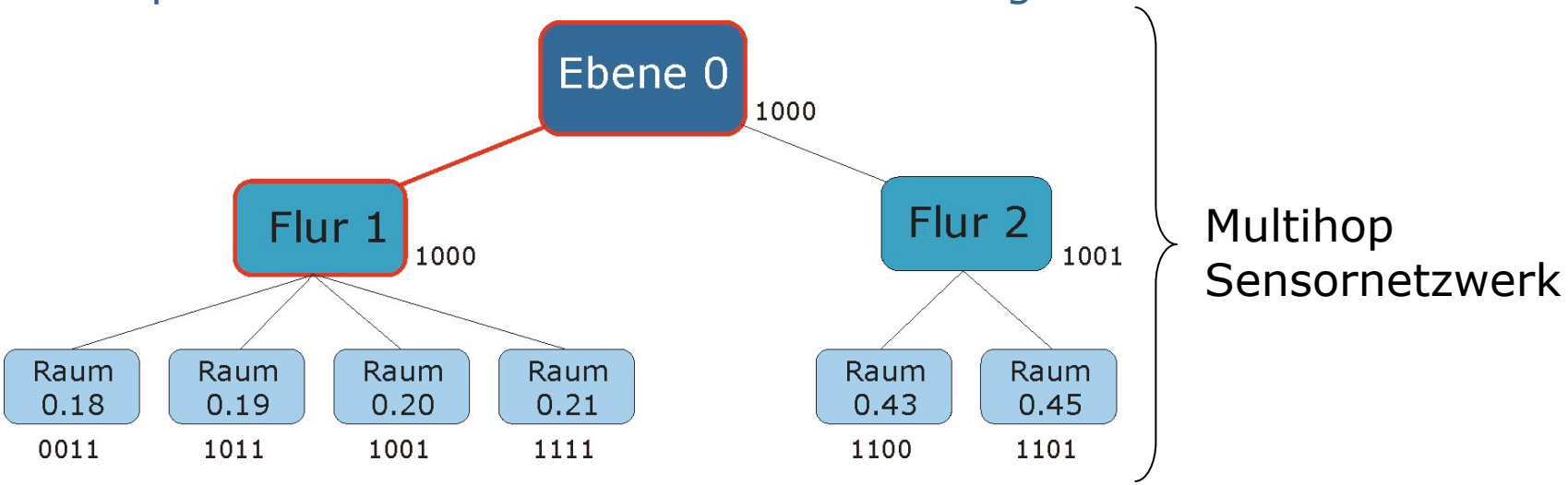
[Schilit, Hong, Gruteser]

- Vorteile:
  - die TTP stellt sicher, dass man sich in einer k-Anonymitätsgruppe befindet
  - es wird keine Ortungsgenauigkeit „verschwendet"

- Nachteil:
  - die Positionsinformationen müssen einem Dritten (TTP) anvertraut werden

Räumliche Positionsverzerrung, zentral (4)

- Beispiel anhand hierarchischer Positionsangaben:



  - Aufbau einer Positionsangabe:
    - » Raum 0.18: 0011 || 1000 || 1000
  - angepasste Positionsangabe:
    - » Flur 1: xxxx || 1000 || 1000

- Anwendung: vor allem in Gebäuden

Verzerrung der Zeitangaben (1)

- Ziel:
  - Schaffung einer Anonymitätsgruppe durch Anpassung des Zeitintervalls
- Funktion:
  - Grundgedanke:

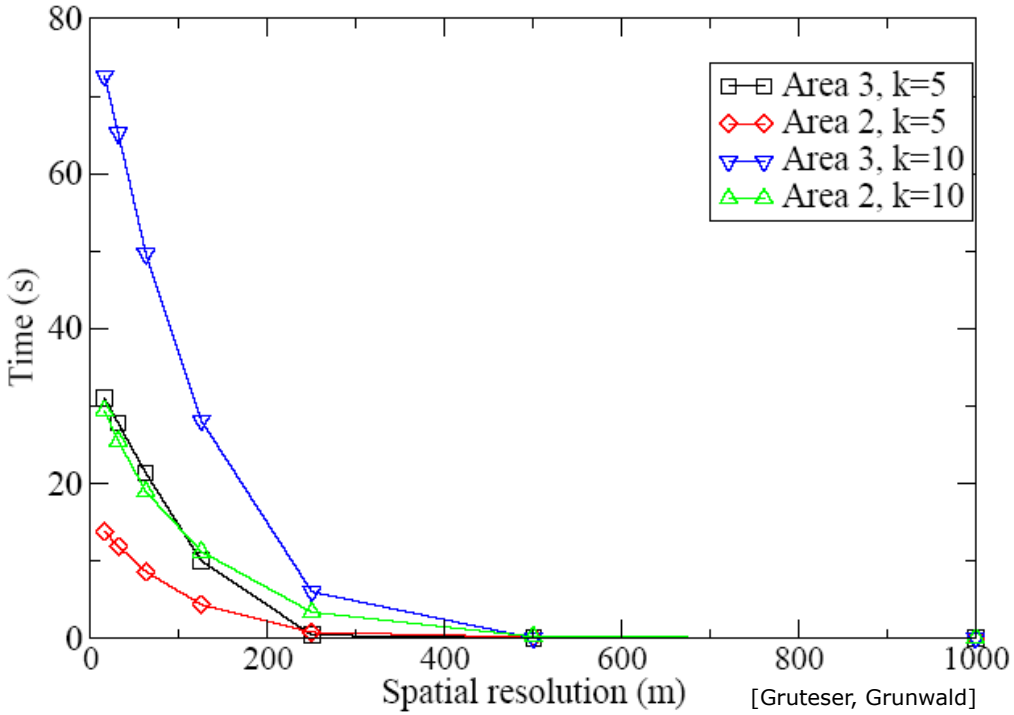
$$P = [x_1,x_2],[y_1,y_2],[t_1,t_2]$$

  - Zeitintervall $[t_1,t_2]$ wird so gewählt, dass k weitere Dienstnutzer sich im Bereich $[x_1,x_2],[y_1,y_2]$ befunden haben
- Anwendungsgebiete:
  - Autobahnen, Bundesstraßen
  - Einkaufspassagen, belebte Innenstädte

Kombination beider Verfahren

- Kombination von räumlicher Positionsverzerrung mit der Verzerrung von Zeitangaben

- Beispiel:

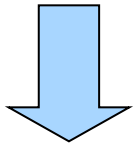


[Gruteser, Grunwald]

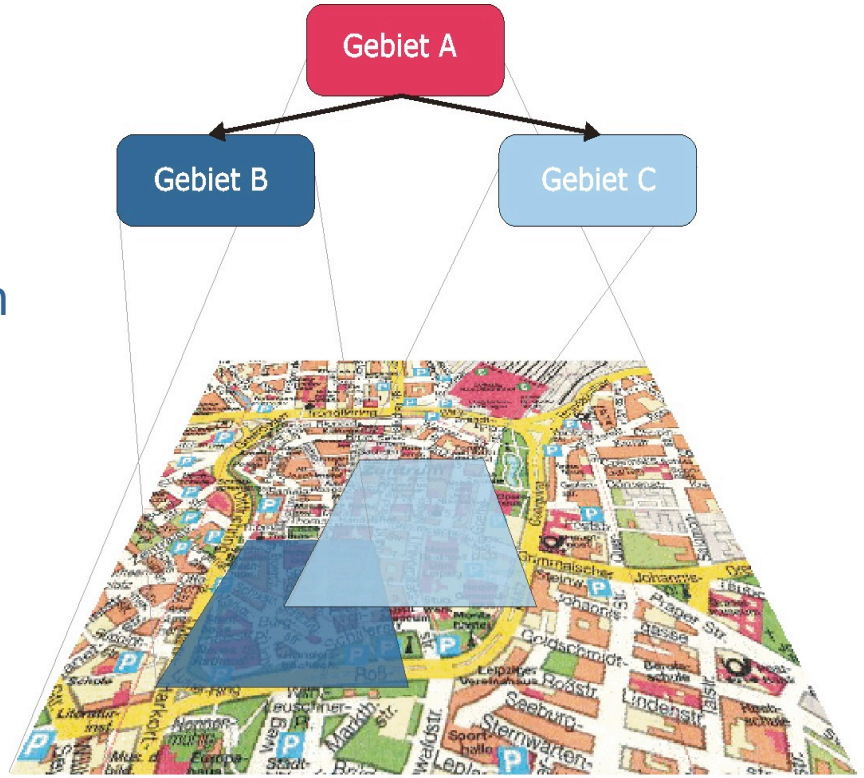
- Area 2: Autobahn mit einem Verkehr von durchschnittlich 70.000 Autos / 24 Std. (beidseitiger Verkehr)
- Area 3: städtische Hauptstraße mit ca. 6.000 Autos / 24 Std. (beidseitig)

Symbolische Positionsangaben – hierarchisch (1)

- Umwandlung von absoluten in symbolische Koordinaten
- jede symbolische Positionsangabe besitzt genau eine physisch Repräsentation



gegenseitige Umrechnung möglich



- Beispiel:
  - absolut: 51,04861N 13,74186O
  - symbolisch: /DE/Sachsen/Dresden/Semperoper

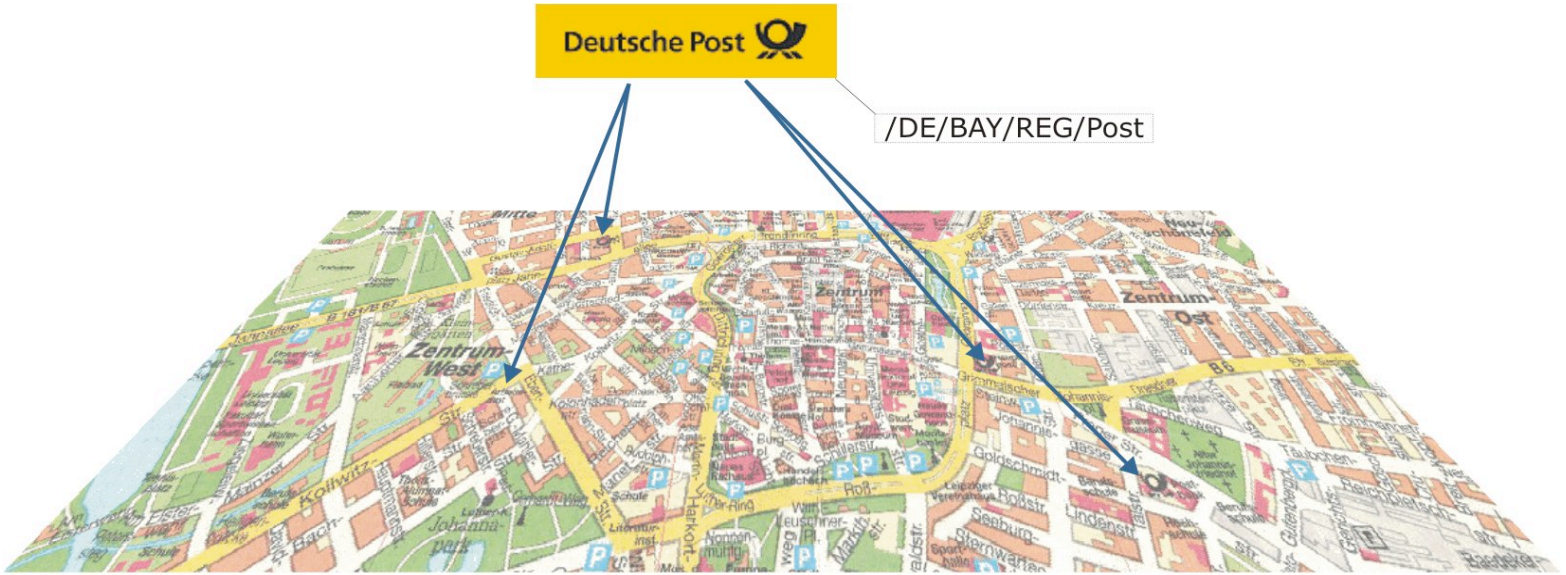
Symbolische Positionsangaben – hierarchisch (2)

- Vorteil:
  - kontextbezogen ist Positionsgenauigkeit höher als bei einfacher Positionsverschleierung
- Nachteile:
  - Erstellungsaufwand für die Umrechnungsregeln
  - symbolische Angaben können wieder in physische Koordinaten umgerechnet werden
  - Endgeräte benötigen unter Umständen Umrechnungsregeln

Symbolische Positionsangaben – virtuell (3)

- statt physisch vorhandene Orte als symbolische Koordinaten zu verwenden, werden virtuelle Einheiten gebildet

- Beispiele:
  - alle Postämter innerhalb einer Stadt → /DE/BAY/REG/Post
  - McDonalds in der Oberpfalz → /DE/OPF/McDonalds
  - Universitäten in Bayern → /DE/BAY/Universität



Symbolische Positionsangaben (4)

- Vorteile:
  - durch die Bildung von virtuellen Gruppen wird eine Einwegfunktion geschaffen

    $f : Position_{absolut} \rightarrow Position_{symbolisch}$

  - Kommunikation unter eigener Identität in vielen Fällen möglich
- Nachteile:
  - Ersterfassungsaufwand für die Umrechnungsregeln
  - u. U. Verbreitung der Regeln auf die Endgeräte
- Anwendungen:
  - ortsabhängige Werbung und Angebote

ich liebe es™

SCHLECKER COM

Hürden der datenschutzfreundlichen Gestaltung

1. Einsatz verschiedener Kommunikationsnetze
   → Outdoor: Mobilfunknetze, Metropolitan Area Networks
   → Indoor: WLAN, Bluetooth

2. Ausschluss netzseitiger Positionsbestimmungsverfahren

5. anwendungsspezifische Unterschiede
   → Push und Pull-Anwendung
   → unterschiedliche Pseudonymisierungsgrade

7. gesetzliche Unterschiede
   → Gesetzgebung variiert sehr stark in vielen Ländern voneinander

9. Interessen der Beteiligten