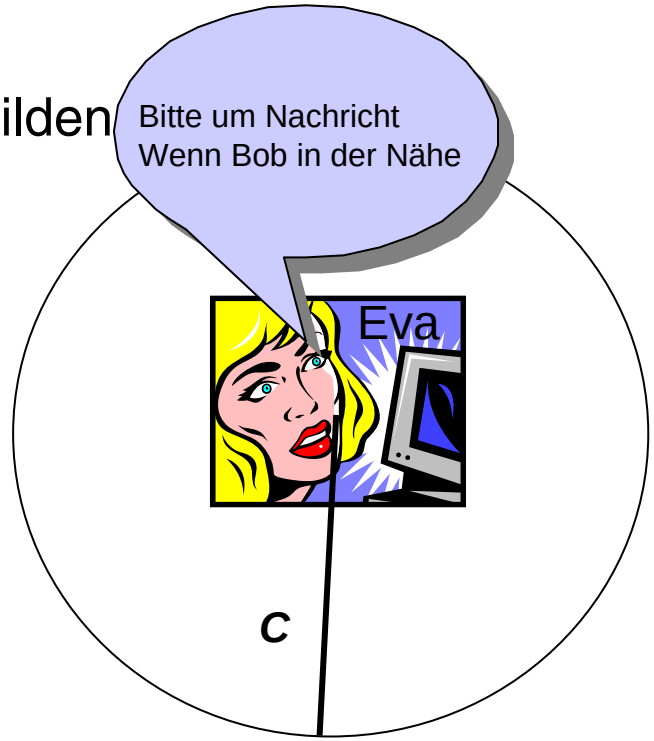
Datenschutzmechanismen für Ortsinformationen aus der Sicht zukünftiger Anwendungen

Georg Treu und Axel Küpper
[georg.treu|axel.kuepper]@ifi.lmu.de
Lehrstuhl für Mobile und Verteilte Systeme
Ludwig-Maximilians-Universität München

1 Motivation
Beispiel: proaktive Community-Dienste

- **Alarmiere Mitglied einer Community wenn...**
  - … ein anderes Mitglied in die Nähe kommt,
  - … es sich entfernt,
  - … Mitglieder ein Cluster bilden



- **Nähe spezifiziert durch kritische Distanz C**
- **Anforderungen**
  - Permanentes Verfolgen der beteiligten Mitglieder
  - Abgleich der Ortsinformationen

2 Agenda

- **Zukünftige LBS**
  - Merkmale der ersten und der „Next Generation“
  - Die Orts-Versorgungskette
  - Akteure der ersten und der „Next Generation“
- **Datenschutz**
  - Herausforderungen
  - Werkzeuge: Privacy Policies, Verschleierung, Anonymisierung, „Lügen“
- **Eigener Ansatz**
  - Anonymisierung proaktiver ortsbezogener Community-Dienste

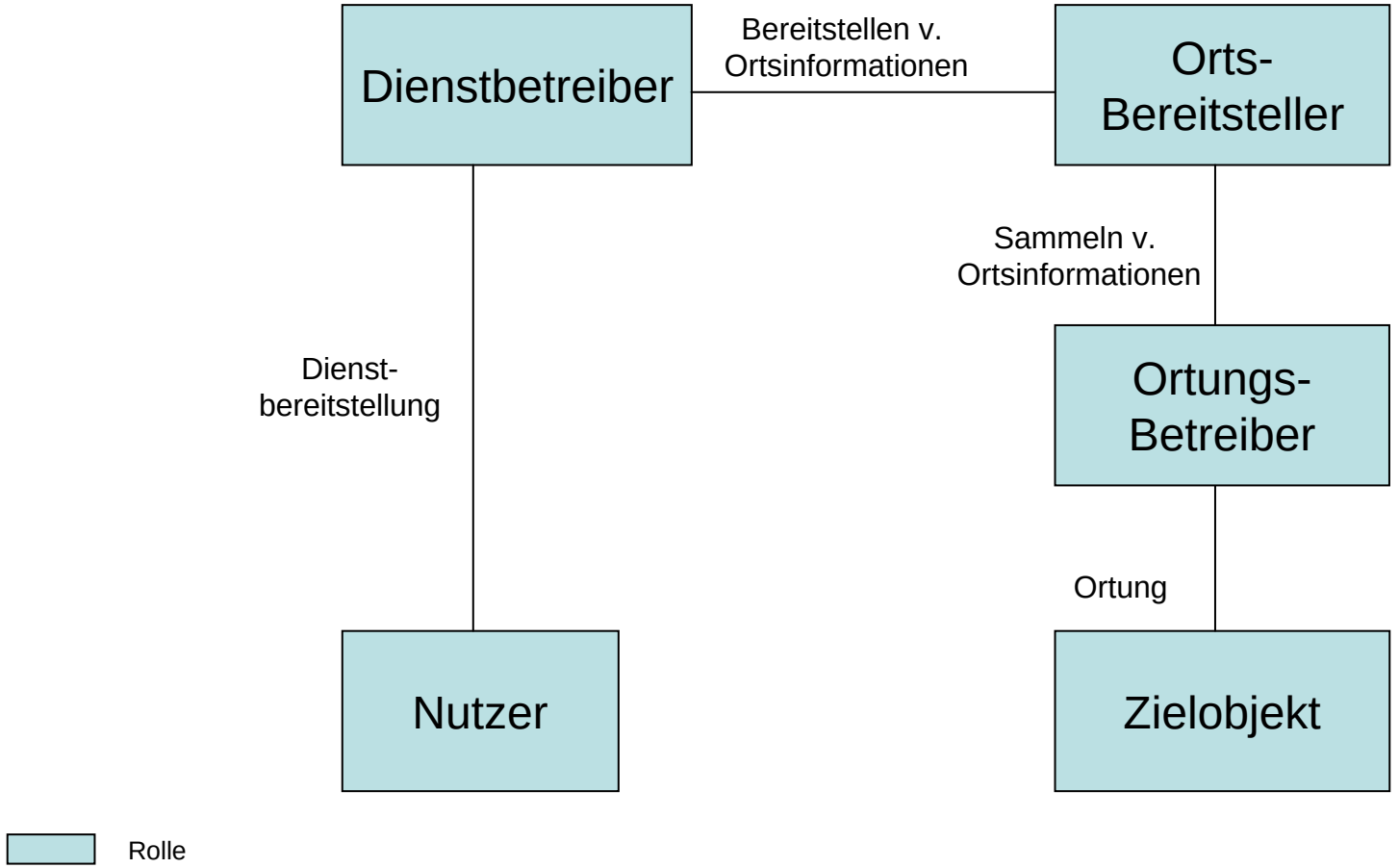
3 LBS
Merkmale der 1. Generation

- **Ortungsverfahren**
  - Cell-Id
  - Netzbasiert
  - Geringe Genauigkeit (abhängig von der Zellgröße)
- **Zielobjekt der Ortung**
  - Überwiegend Nutzer-Selbstortung
  - Ortung anderer Personen oder Objekte meist nicht realisiert
- **Nutzer/Dienst-Interaktion**
  - Reaktiv und synchron
  - Einmalige Ortung beim Aufruf des Dienstes

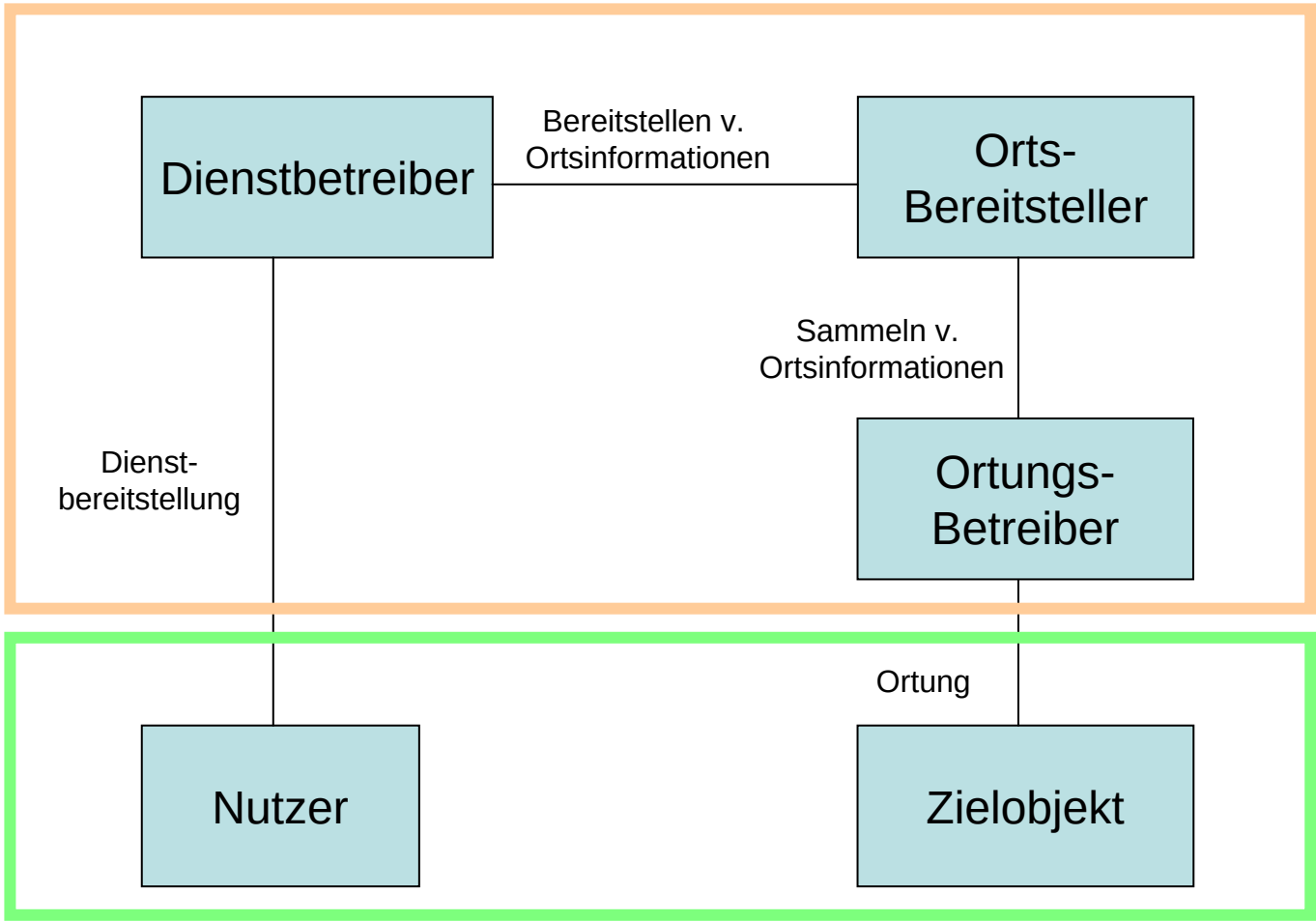
3 Zukünftige LBS
These: Merkmale der „Next Generation"

- **Ortungsverfahren**
  - Outdoor: GPS bzw. A-GPS
  - Indoor: WLAN-Fingerprinting oder Indoor-GPS
  - Überwiegend endgerätebasiert
- **Zielobjekt der Ortung**
  - "Location Sharing" zwischen verschiedenen Personen
  - Zentral oder Peer-to-Peer
- **Nutzer/Dienst-Interaktion**
  - Proaktiv und asynchron (d.h. Durchführung bestimmter Transaktionen beim Betreten oder Verlassen bestimmter Orte)
  - Permanente Verfolgung der Zielpersonen notwendig (Tracking)

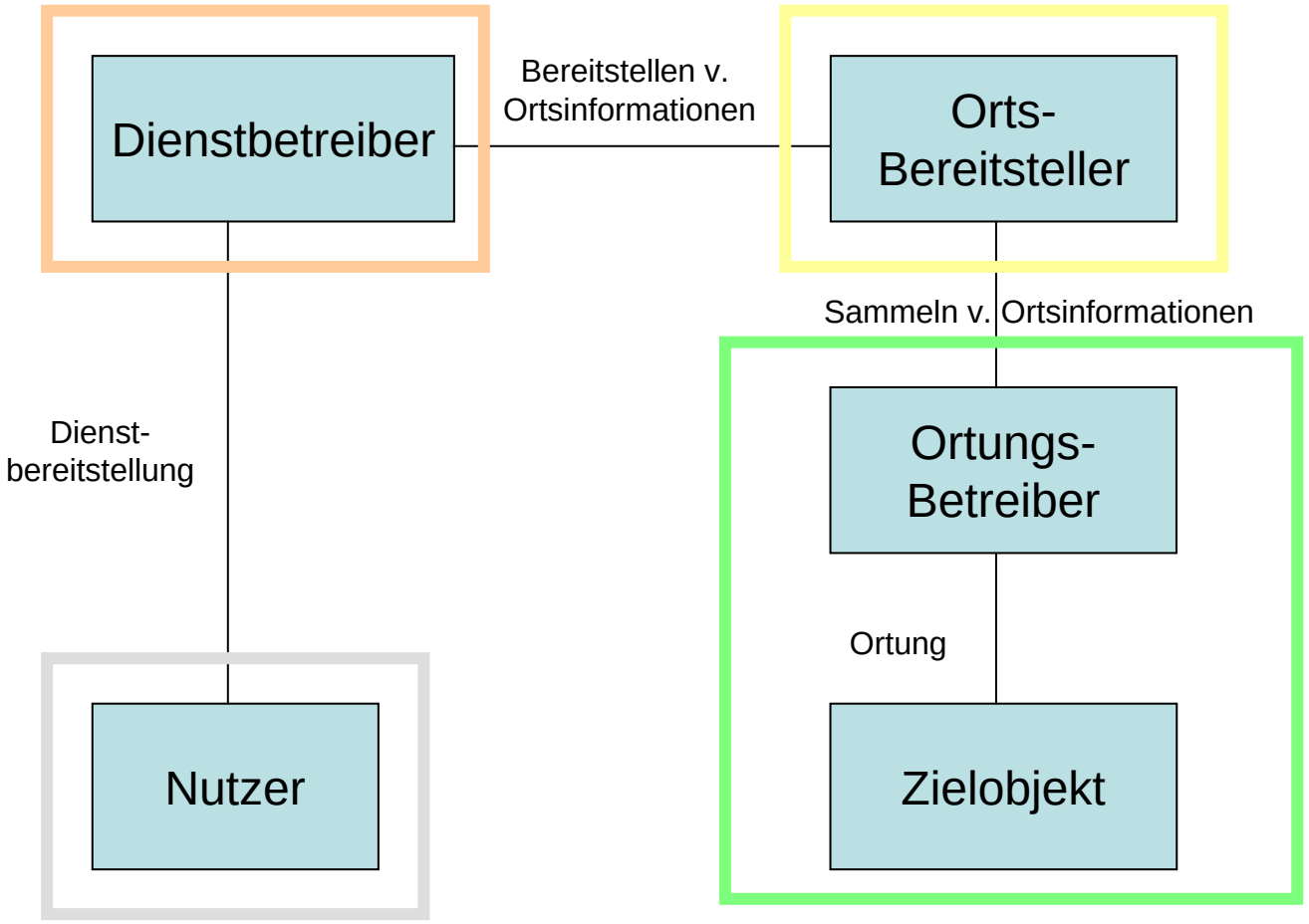
3 Zukünftige LBS
Die „Orts-Versorgungskette“



3 LBS
Akteure der 1. Generation



3 Zukünftige LBS
Akteure der „Next Generation“



Rolle

Dienstbetreiber unabhängig z.B. von Mobilfunkbetreiber

Endgerät-basierte Ortung z.B. mit GPS

Spezialisierter Anbieter?

Nutzer nicht notwendigerweise Zielobjekt

4 Datenschutz
Herausforderungen

- **Sicherheitsmechanismen (Privatheit, Authentifizierung, Integrität) vorhanden**
- **Problem: Datenschutz**
  - Datenschutz Hauptkriterium für Nutzerakzeptanz
  - Verschärfung der Problematik für zukünftige LBS:
    - Steigende Anzahl v. Akteuren
    - Fremdortung, d.h. Zielobjekt nicht notwendigerweise Nutzer
    - Nutzerverfolgung (bei proaktiven Diensten)
- **Mögliche Werkzeuge**
  - Privacy Policies
  - Verschleierung
  - „Lügen“
  - Anonymisierung

4 Datenschutz
Privacy Policies

- **Vereinbarung, Ortsinformationen nur für einen vorgegebenen Zweck zu gebrauchen**
- **Vorraussetzung: Mindestmaß an Vertrauen zwischen Ortsverwerter und Nutzer**

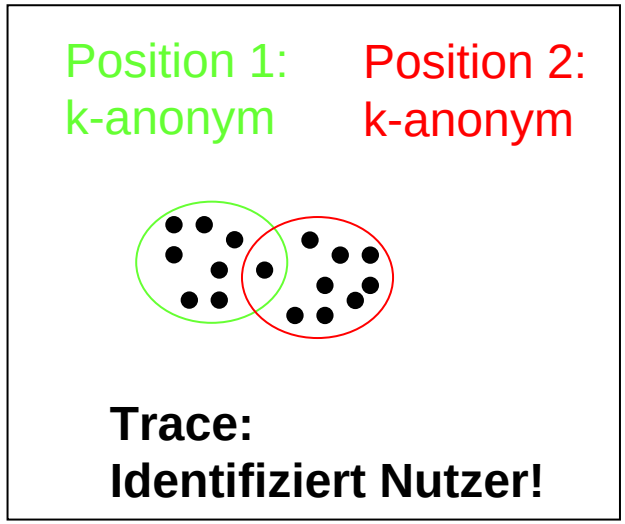
- **Relativ gut geeignet für LBS der 1. Generation**
  - Mobilfunkbetreiber und Nutzer einzige Akteure
  - Vertrauen vorhanden
- **Problematisch für LBS der „Next Generation“**
  - Vielzahl an Akteuren
  - Dynamische Anbieterauswahl

4 Datenschutz
Verschleierung

- **Vergröberung von Ortsinformation**
- **Keine Anonymität**
- **Ziel: korrekte Dienstnutzung trotz unscharfer Information (vgl. Duckham/Kulik ’05)**
- **Vorteile:**
  - Vergröberung bietet gewissen Schutz
  - Kein Vertrauen zu Ortsbereitsteller notwendig (vgl. k-Anonymität)
- **Nachteil:**
  - Nur teilweiser Schutz:
    - Positive Aussagen über Nutzer abgeschwächt, **negative nicht.**

4 Datenschutz
Anonymisierung I

- **Ziel: Geheimhaltung der Identität des Nutzers / Pseudonyme**
- **1. Cloaking of location data/k-anonymity (Gruteser/Grunwald ’03)**
  - Ortsbereitsteller gibt nur k-anonyme Ortsinformationen heraus
  - Probleme:
    - Grobe Qualitätsverschlechterung
    - Keine Anonymisierung vor Ortsbereitsteller möglich
    - k-Anonymität bezieht sich auf einzelnen „Position Fix“
      =>Kein Schutz von Traces einer Person
      =>Nicht anwendbar auf proaktive Dienste



4 Datenschutz
Anonymisierung II

- **2. Mix/App. Zones (Beresford/Stajano ’03)**
  - Pseudonymwechsel in Mix Zones
  - Dienstnutzung nur in Application Zones
    - Ausschluss nutzertypischer Zonen

    => Schutz vor statistischen Angriffen
  - Probleme
    - Application Zones zu restriktiv
    - Zukünftige LBS sind inhärent Zustandsbehaftet durch
      - Verfolgung, Profilhaltung
      - Gruppenzugehörigkeit
    - Konsistente Nutzeridentifikatoren notwendig !

    => Pseudonymwechsel kritisch

4 Datenschutz
Lügen

- **Option für gemeinschaftsbezogene Dienste**
- **Nicht-Orten lassen reicht nicht**
- **Soziales Problem:**
  - Bis jetzt:

    „Warum war Dein Handy ausgeschaltet?“
  - In zukünftigen LBS:

    „Warum läßt Du Dich nicht von mir orten?“

    Schutz durch Lügen
- **Sollte in Privacy Modellen unbedingt berücksichtigt werden**

5 Eigener Ansatz
Anonymisierung proaktiver Community-Dienste I

- **Idee: nur relative Distanzen zwischen Nutzern wichtig**
  - Datenschutz vor Dienstbetreiber bzw. Ortsbereitsteller
    - Endgerätebasierte Ortung (z.B. GPS)
    - Distanz-erhaltende Koordinatentransformationen
    - Gruppe hat gemeinsamen Schlüssel
    - Pseudonyme
    - Dienstbetreiber bzw. Ortsbereitsteller erhält transformierte Koordinaten
      => Relative Distanzen zwischen Nutzern noch herleitbar
    - Pseudonyme schwerer angreifbar

    =>Keine Pseudonymwechsel notwendig

    =>Keine Beschränkung auf Application Zones

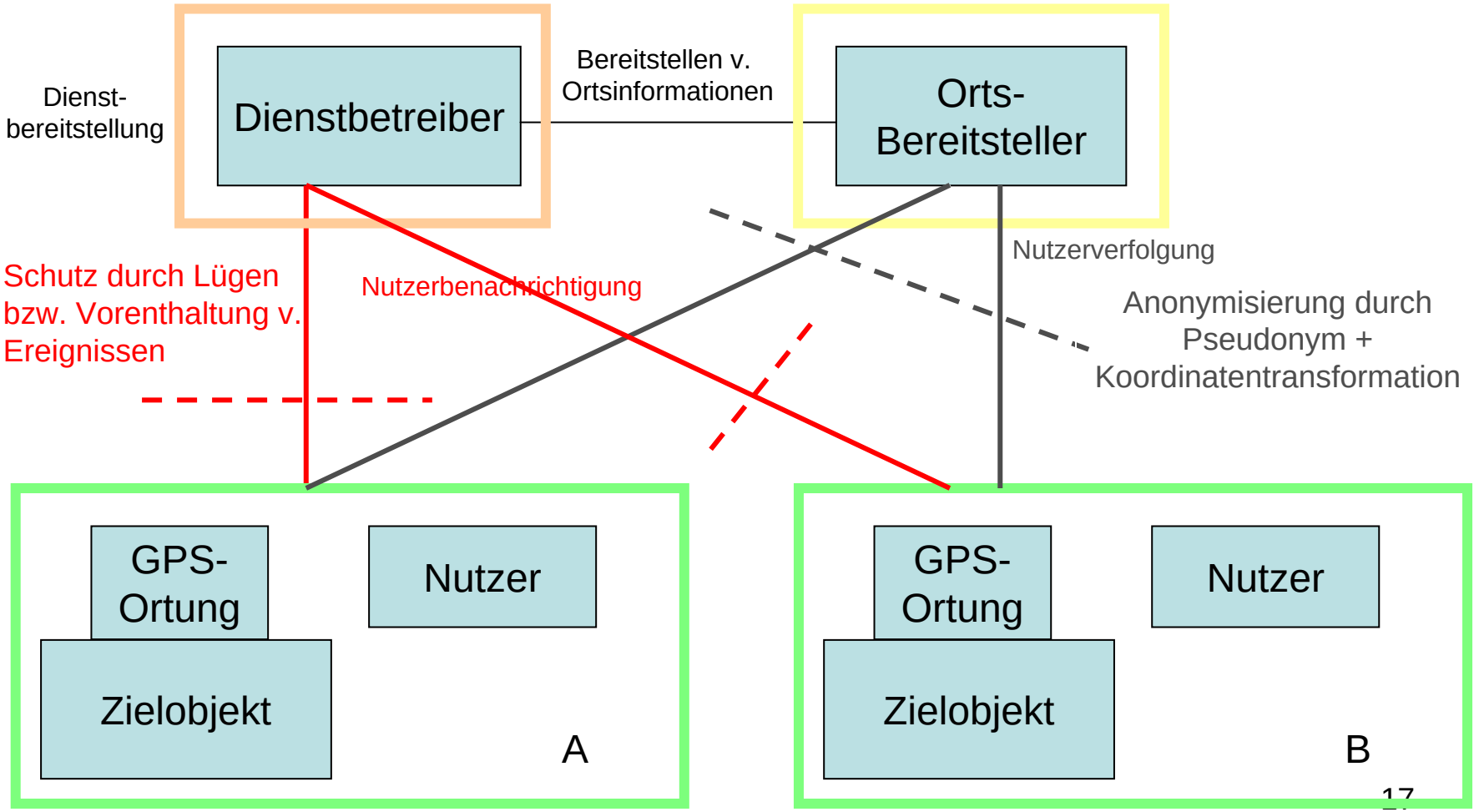
    =>Qualität der Ortsinformationen unverändert
  - Datenschutz der Nutzer voreinander:
    - Unterdrückung von Ereignissen durch Dienst
    - Entspricht Mischung aus Lügen und Privacy Policies

5 Eigener Ansatz
Anonymisierung proaktiver Community-Dienste II

- **Distanz-erhaltende Koordinatentransformation T**
- **Künstlicher Richtungsvektor**
- **Berechnung auf dem Endgerät:**
  - **T(k, t, x, y) -> (x´, y´)**
  - **Schlüssel k: ausgehandelt zwischen Gruppenmitgliedern**
    - **Rückgriff auf bestehende sichere Gruppenkommunikationsprotokolle**
  - **Zeit t: (exakte) Synchronization durch GPS**
- Problem 1: Statistischer Angriff durch Muster v. Straßenkarten
  => Lösung: künstlicher Richtungsvektor dynamisch

- Problem 2: Angriff auf künstl. Richtungsvektor durch mehrere stehende Gruppenmitglieder
  => Lösung: Verfolgung muss in gewissen Grenzen bleiben
  => künstlicher Vektor langfristig lokal

5 Eigener Ansatz
Anonymisierung proaktiver Community-Dienste III



6 Schlussbemerkungen
Zusammenfassung & Ausblick

- **Zusammenfassung**
  - Für proaktive und gemeinschaftsbezogene Dienste keine brauchbaren Anonymisierungsmechanismen vorhanden
  - Eigener Ansatz: könnte Problem für Teilmenge der Dienste lösen
- **Zukünftige Arbeiten**
  - Verstärkte Analyse des vorgestellten Ansatzes
- **Hinweis**

Axel Küpper

LOCATION-BASED SERVICES
Fundamentals and Operation

John Wiley & Sons
392 Seiten
August 2005
ISBN: 0-470-09231-9