



Vorlesung

Datenschutz und Privatheit in vernetzten Informationssystemen

Kapitel 8: Lokationsbasierte Dienste

Erik Buchmann
buchmann@ipd.uka.de

Wir danken Jürgen Czerny für seine Beiträge!



Agenda für heute

[Einführung](#)

[Zentrale Ansätze](#)

[Dezentrale Ansätze](#)

[Datenselbstschutz](#)

[Abschluss](#)

- Einführung: Lokationsbasierte Dienste
 - Methoden der Positionsbestimmung
 - Anwendungen
 - Datenschutzprobleme und -ziele
- Verfahren zum Datenschutz
 - zentral
 - dezentral
 - Datenselbstschutz





Lokationsbasierte Dienste



Beispiel: NavXS

[Einführung](#)

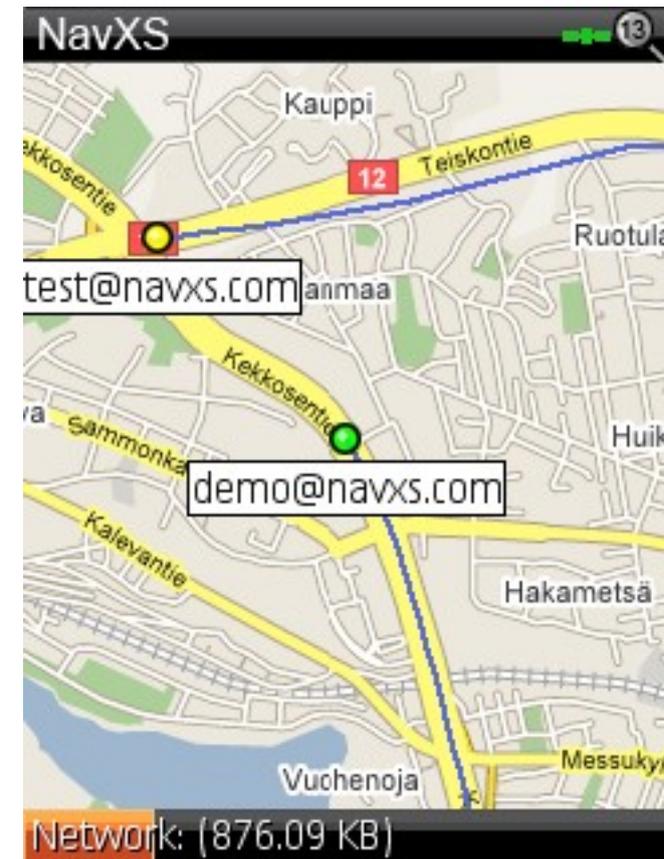
[Zentrale Ansätze](#)

[Dezentrale Ansätze](#)

[Datenselbstschutz](#)

[Abschluss](#)

- einfacher Austausch von Ortsinformationen
 - vergleichbar mit Instant Messaging, z.B. Skype, ICQ
- läuft auf Mobiltelefonen mit GPS





Beispiel: Panoramio

[Einführung](#)

[Zentrale Ansätze](#)

[Dezentrale Ansätze](#)

[Datenselbstschutz](#)

[Abschluss](#)

- Geotagging
 - Annotieren von Positionen mit Fotos und Texten

The screenshot shows the Panoramio website interface. At the top, there is a navigation bar with the Panoramio logo, links for 'Sign up', 'Upload', 'Places', and 'Tags', and a search bar. On the right side of the navigation bar, there are links for 'Forum', 'Blog', and 'Sign'. Below the navigation bar, there are two tabs: 'Popular (2042)' and 'All'. The main content area is a grid of photo thumbnails. On the right side, there is a satellite map of Karlsruhe, Germany, with several photo thumbnails overlaid on it, indicating their geographic locations. The map includes street names like 'Kaiserallee', 'Kriensstraße', and 'Sudwest', and district names like 'Weststadt' and 'Sudstadt'. A vertical scale bar and navigation controls are on the left side of the map.





Weitere Beispiele

[Einführung](#)

[Zentrale Ansätze](#)

[Dezentrale Ansätze](#)

[Datenselbstschutz](#)

[Abschluss](#)

- Routenplanung
 - *Wie komme ich von hier nach Heidelberg?*
- Points-of-Interest
 - *Wo ist das nächste griechische Restaurant?*
- Track-your-Child
 - *Wo ist der Nachwuchs gerade?*
- Flottenmanagement
 - *Wo befinden sich die Firmenwagen?*
- Abrechnung der Straßenmaut
 - *Fahrzeuge melden gefahrene Strecken an Zentrale.*





Möglichkeiten zur Positionsbestimmung

[Einführung](#)

[Zentrale Ansätze](#)

[Dezentrale Ansätze](#)

[Datenselbstschutz](#)

[Abschluss](#)

- Im Freien:
 - GPS
 - Triangulierung von Funkbaken
 - Datenbank von WLAN- oder Mobilfunkstationen (z.B. Google Latitude)
- Innerhalb von Gebäuden:
 - Infrarot-Baken (z.B. Active Badge)
 - Ultraschall (z.B. Active Bat)





GPS

Einführung

Zentrale Ansätze

Dezentrale Ansätze

Datenselbstschutz

Abschluss

- seit 1995 in Betrieb
- 31 (min.24) Satelliten 20km über dem Erdboden
- Ortung durch Empfang von mindestens 4 Satelliten
 - Genauigkeit: besser als 10m in 90% aller Messungen
- Verwendete Funkfrequenzen können Wasser oder Beton nicht durchdringen
 - kein Inneneinsatz
 - Probleme bei (starkem) Unwetter



Bild: www.gpsmagazine.com





Google Latitude

[Einführung](#)

[Zentrale Ansätze](#)

[Dezentrale Ansätze](#)

[Datenselbstschutz](#)

[Abschluss](#)

- Ortung über Datenbank von Mobilfunkzellen im Handy
 - Genauigkeit bestenfalls 200m, in dünnbesiedelten Gegenden (wenig Mobilfunkstationen) schlechter

Google latitude



Fred wants to hang out with his friends, and checks to see where they are.

See where your friends are right now

Enjoy Google Latitude on your phone, computer, or both.

Start using it on your phone

See your friends' locations and status messages and share yours with them.

Enter your number or visit google.com/latitude on your mobile web browser.

United States

Send a link to my phone

▶ [Will it work with my phone?](#)





Active Bat

[Einführung](#)

[Zentrale Ansätze](#)

[Dezentrale Ansätze](#)

[Datenselbstschutz](#)

[Abschluss](#)

- Person trägt Ultraschallsender
- System von Ultraschall-Sensoren im Gebäude
 - Sensoren messen Entfernung zum Ultraschallsender
- 720 Sensoren decken 1000qm auf 3 Gebäudeetagen ab
- Auflösung 3cm, 75 Objekte pro Sekunde
- mit mehreren Sendern pro Person kann auch Ausrichtung im Raum (Blickrichtung) bestimmt werden

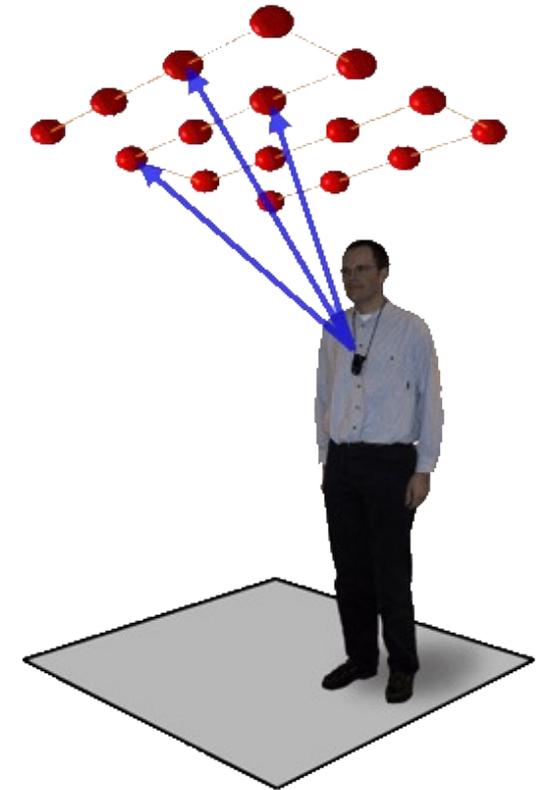


Bild: <http://www.cl.cam.ac.uk>





Datenschutzprobleme in LBS



Gespeicherte Daten

[Einführung](#)

[Zentrale Ansätze](#)

[Dezentrale Ansätze](#)

[Datenselbstschutz](#)

[Abschluss](#)

- **Einzelkoordinaten**
 - einzelne Anfragen nach POI (z.B. nächste Tankstelle)
- **Tracks**
 - Aufzeichnung des GPS-Datenstroms
 - Sequenzen von aufeinanderfolgenden Einzelanfragen, z.B. nach aktuellen Staumeldungen
- **Dienstbezogene Inhalte**
 - Anfragen, Annotationen beim Geotagging, etc.
- **Metadaten**
 - Nutzer, Zeit der Aufzeichnung
 - Dienstbezogene Metadaten, z.B. EXIF-Informationen in Fotos





Einzelkoordinaten

[Einführung](#)

[Zentrale Ansätze](#)

[Dezentrale Ansätze](#)

[Datenselbstschutz](#)

[Abschluss](#)

- Erlauben Rückschlüsse auf
 - aktuellen bzw. vergangenen Aufenthaltsort, z.B. das eigene Haus, Treffpunkt mit Freunden, Urlaubsziele
 - persönliche Vorlieben z.B. Restaurant, Kino, Sehenswürdigkeiten
 - Lebensumstände z.B. Arbeitgeber, Medizinische Einrichtungen
 - soziale Kontakte z.B. Analyse, ob sich unterschiedliche Personen zur gleichen Zeit an gleichen Koordinaten aufhalten





Tracks

[Einführung](#)

[Zentrale Ansätze](#)

[Dezentrale Ansätze](#)

[Datenselbstschutz](#)

[Abschluss](#)

- Erlauben (zusätzlich zu den Einzelkoordinaten) Rückschlüsse auf
 - Reiseverlauf
 - Geschwindigkeit
wichtig z.B. bei Verkehrsregeln
 - Reiseziel
z.B. durch extrapolierten der Route
 - Gewohnheiten
z.B. immer wiederkehrende Routen wie den Arbeitsweg





Dienstbezogene Inhalte

[Einführung](#)

[Zentrale Ansätze](#)

[Dezentrale Ansätze](#)

[Datenselbstschutz](#)

[Abschluss](#)

- Beispiel Panoramio:
Wer und was wurde fotografiert?
 - Rückschlüsse auf
 - Lebensumstände
 - soziale Kontakte
 - Interessen, Hobbies
 - Fähigkeiten (gute vs. schlechte Bilder)
 - etc.





Metadaten

[Einführung](#)

[Zentrale Ansätze](#)

[Dezentrale Ansätze](#)

[Datenselbstschutz](#)

[Abschluss](#)

- generisch, z.B. Zeit der Anfrage, Nutzer
 - generieren von Bewegungsprofilen möglich
- anwendungsspezifisch
 - Beispiel: Fotos in Panoramio speichern EXIF-Daten
 - Aufnahmezeit (kann sich von der Zeit der Dienstnutzung unterscheiden)
 - Kamera-Modell (teure Kamera?)
 - Aufnahmeparameter (unfähiger Fotograf?)
- Metadaten können als Quasi-Identifizierer dienen, d.h. Fingerabdruck, der Anwenderverhalten pseudonym nachverfolgbar macht





Datenschutz in LBS

[Einführung](#)

[Zentrale Ansätze](#)

[Dezentrale Ansätze](#)

[Datenselbstschutz](#)

[Abschluss](#)

- Inhalte und Metadaten meist nicht zu vermeiden
- Tracks durch Anfragefolgen ebenfalls oft unvermeidlich
- Je weniger genau die Positionsangaben, desto schlechter die Dienstqualität
 - grobe Ortsposition
 - Dienste geben ungenaue Ergebnisse zurück
 - Privatheit des Anwenders sichergestellt
 - genaue Ortsposition
 - hohe Dienstgüte
 - Standort des Anwenders wird Dritten kenntlich gemacht
- -> **Kompromiss erforderlich**





k-Anonymität auf Positionsdaten

[Einführung](#)

[Zentrale Ansätze](#)

[Dezentrale Ansätze](#)

[Datenselbstschutz](#)

[Abschluss](#)

- Wiederholung: k-Anonymität
 - *Eine Person ist k-Anonym, wenn sie von k-1 anderen nicht unterschieden werden kann.*
- Auf Koordinaten
 - ändere die Koordinaten von k Nutzern so, dass
 - sie ununterscheidbar werden
 - die Dienstqualität nur minimal sinkt
 - keine Zuordnung zu exakten Koordinaten möglich ist
- Methoden (Auswahl)
 - Koordinaten runden oder durch Region ersetzen
 - Zufallswerte addieren
 - Positionen durch Landmarken ersetzen





Angreifermodell

[Einführung](#)

[Zentrale Ansätze](#)

[Dezentrale Ansätze](#)

[Datenselbstschutz](#)

[Abschluss](#)

- Für uns relevant: Angreifer möchte an die Positionsdaten des Nutzers gelangen
 - fremden Dienst übernehmen oder eigenen Dienst anbieten, der Positionsdaten sammelt
 - unbemerktes Mithören der Kommunikation, z.B. als man-in-the-middle
 - Angriff auf eventuell vorhandenen Anonymisierungsdienst
 - selbst als Anonymisierungsdienst ausgeben, z.B. in Peer-basierten Verfahren
 - sich ins Anonymity Set einschleusen, z.B. als einer der k Mitglieder bei k -Anonymity





Kriterien für Datenschutzansätze

[Einführung](#)

[Zentrale Ansätze](#)

[Dezentrale Ansätze](#)

[Datenselbstschutz](#)

[Abschluss](#)

- technisch
 - Angriffsmöglichkeiten
 - Skalierbarkeit
 - Kommunikationsaufwand
 - Rechenaufwand
 - für Anonymisierung erforderliche Mindest-Nutzerdichte
 - Anwendbarkeit auf Anfragefolgen
- nicht-technisch
 - benötigtes Hintergrundwissen, Komplexität des Verfahrens
 - mentaler Aufwand, Aufmerksamkeit





Im Folgenden

[Einführung](#)

[Zentrale Ansätze](#)

[Dezentrale Ansätze](#)

[Datenselbstschutz](#)

[Abschluss](#)

- Zentralisierte Verfahren
 - CliqueCloak
 - Mix-Zones
- Dezentrale Verfahren
 - Routing Through the Mist
 - Peer-to-Peer Anonymisierung
- Verfahren zur Selbstanonymisierung
 - Anonymisierung durch Dummies





Zentrale Datenschutz- ansätze für LBS



CliqueCloak

Einführung

Zentrale Ansätze

Dezentrale Ansätze

Datenselbstschutz

Abschluss

- Zentralisiertes Verfahren, das zwischen Nutzer und Dienstanbieter geschaltet wird (Trusted Third Party)
- Algorithmus zum effizienten anonymisieren
- Eingaben:
 - *Positionen* (Anfragen) vieler Teilnehmer
 - *Minimaler Grad an Anonymität*, d.h., mindest- k für k -Anonymity
 - *Minimale räumlich-zeitliche Auflösung*, die an einen Dienst weitergegeben wird
- Ausgabe:
 - Spatio-temporal Cloaking Box (SCB) mit k Nutzern

B. Gedik, L. Liu: *Location Privacy in Mobile Systems: A Personalized Anonymization Model*. ICSCS'05





Anforderungen an CliqueCloak

Einführung

Zentrale An-
sätze

Dezentrale
Ansätze

Datenselbst-
schutz

Abschluss

- Spatial Containment
 - SCB muss die Position des Nutzers beinhalten
- Spatio-temporal Resolution
 - SCB darf nicht größer sein als vom Nutzer vorgegeben → Dienstgüte
- Content Preservation
 - der Inhalt einer Anfrage oder Eingabe darf nicht verändert werden





Ansatz

Einführung

Zentrale Ansätze

Dezentrale Ansätze

Datenselbstschutz

Abschluss

- Menge von Nachrichten $m = \langle u_{id}, r_{no}, \{t,x,y\}, k, \{d_t, d_x, d_y\}, C \rangle$
 - C: Inhalt der Nachricht
 - u_{id}, r_{no} : Nutzer-ID, Nachrichten-ID
 - $\{t,x,y\}$: Zeit, Koordinaten
 - $\{d_t, d_x, d_y\}$: Toleranzen für die Constraint Box
 - Rückgabe soll nicht mehr als +/- $d/2$ vom tatsächlichen Wert abweichen
 - k: minimale Zahl von Personen in Constraint Box
- Ziel: *Finde in der Menge der Nachrichten die Minimale Constraint Box für jeden Nutzer*





Algorithmus

Einführung

Zentrale An-
sätze

Dezentrale
Ansätze

Datenselbst-
schutz

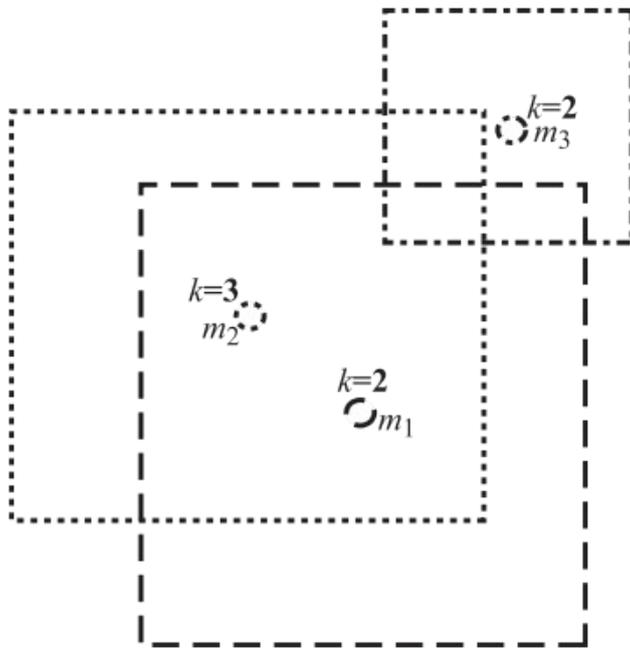
Abschluss

- füge jede Nachricht als Knoten in einen *Constraint-Graphen* ein
 - Kante von Knoten A zu Knoten B, wenn A innerhalb der Toleranzgrenzen $\{d_t, d_x, d_y\}$ von B liegt oder umgekehrt
- für jede Nachricht
 - suche im Constraint-Graphen eine Clique mit Kardinalität k
 - entferne die Clique aus dem Graphen
 - ersetze $\{t, x, y\}$ durch das Minimum Bounding Rectangle der Clique
- wenn d_t abgelaufen bevor Clique gefunden, informiere Nutzer und lösche Knoten aus Constraint Graph

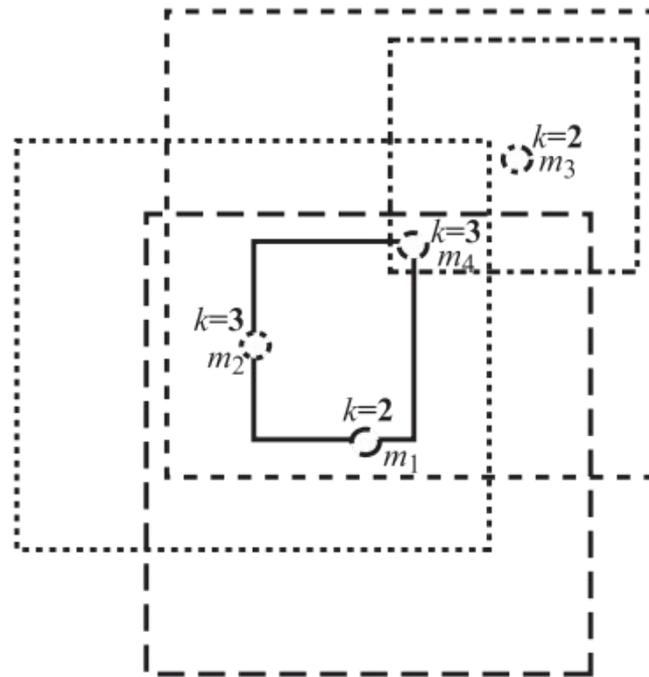




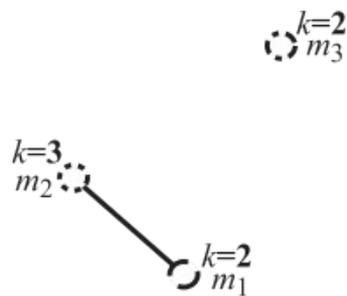
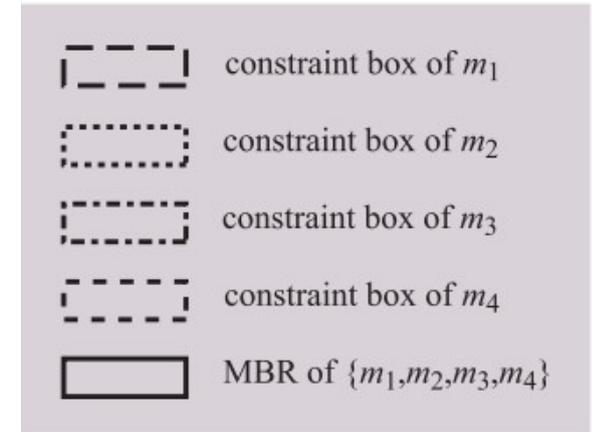
Beispiel



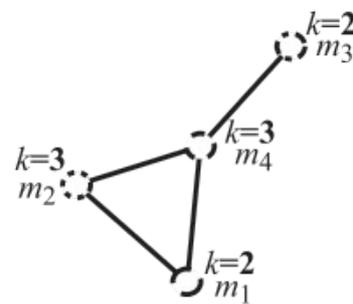
(a) spatial layout I



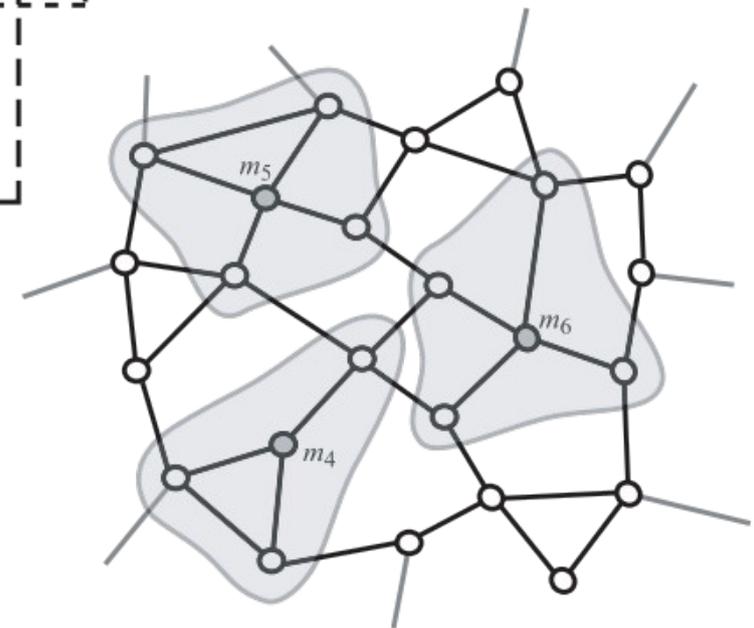
(b) spatial layout II



(c) constraint graph I



(d) constraint graph II



(e) constraint graph





Kritik

Einführung

Zentrale An-
sätze

Dezentrale
Ansätze

Datenselbst-
schutz

Abschluss

- Feingranulare Einstellung der Privatheit
- Single Point of Failure
- Cliquen-Suche ist sehr teuer
 - Verfahren skaliert schlecht
- bekannte Schwächen der k-Anonymität
 - z.B. wenn alle k Nutzer an exakt der gleichen Position
- Parametrisierung erfordert genaue Kenntnis der eigenen Privatheitsbedürfnisse → schwierig
- bei geringer Nutzerdichte Kompromisse bei k oder $\{d_t, d_x, d_y\}$ erforderlich
- Funktioniert nicht bei Anfragesequenzen





Mix Zones

Einführung

Zentrale Ansätze

Dezentrale Ansätze

Datenselbstschutz

Abschluss

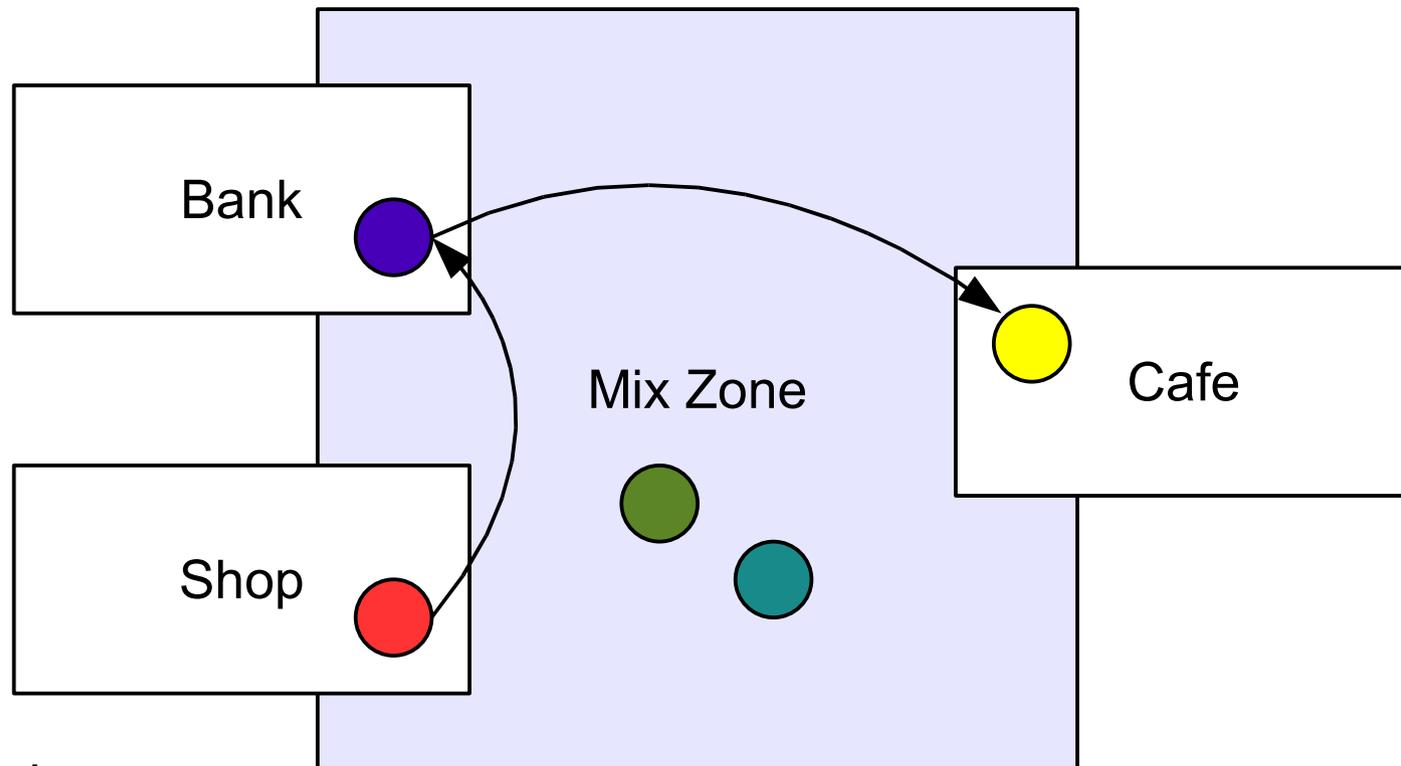
- Szenario: Anfragesequenzen, pseudonym nutzbare LBS
 - Beobachtung: Anonymisierung nützt nichts, wenn der Nutzer z.B. bis zu seinem Haus oder seiner Arbeitsstelle nachverfolgt werden kann
- Idee:
 - Positionsdaten werden nicht kontinuierlich, sondern mit zeitlichem Abstand (Update Period)
 - zwischen den Updates wechseln Nutzer ihr Pseudonym in sogenannten *Mix Zones*
 - viele pseudonyme Personen gehen hinein, andere pseudonyme Personen gehen heraus
 - Nutzer interagieren mit Diensten in *Application Zones*





Beispiel

- Application Zones: Shop, Bank, Cafe



Einführung

Zentrale An-
sätze

Dezentrale
Ansätze

Datenselbst-
schutz

Abschluss

A. Beresford, F. Stajano
*Location Privacy in
Pervasive Computing,*
Pervasive 2003





Effektivität des Konzepts

Einführung

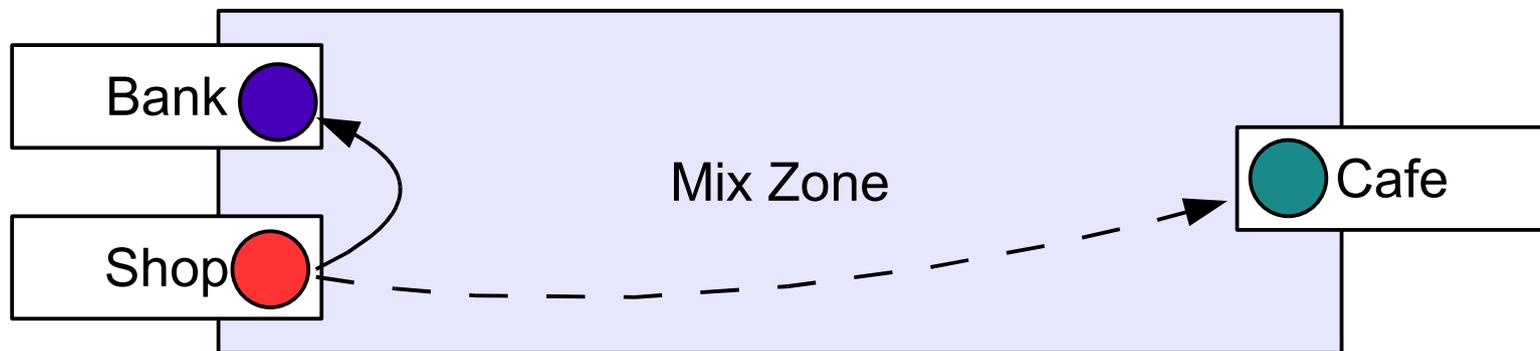
Zentrale Ansätze

Dezentrale Ansätze

Datenselbstschutz

Abschluss

- Abhängig von der Update Period
 - wenn Updates von Positionen in zu rascher Folge, können Nutzer Mix Zone nicht durchqueren, bleiben trotz anderem Pseudonym verfolgbar
- Abhängig von der Raumaufteilung
 - bei ungünstiger Ausgestaltung Wechsel der Application Area zwischen Updates unmöglich





Kritik

Einführung

Zentrale An-
sätze

Dezentrale
Ansätze

Datenselbst-
schutz

Abschluss

- funktioniert auch mit Anfragefolgen
- Skalierbar, wenig Rechenleistung und Kommunikation
- einfaches, verständliches Verfahren

- Single Point of Failure
- Starke Abhängigkeit von externen Faktoren
 - Raumaufteilung
 - Anzahl und Bewegung der Nutzer
 - Update Period
- statistische Angriffe möglich
 - wenn es unwahrscheinlich ist dass jemand bestimmte Orte nacheinander aufsucht
 - wenn Gehgeschwindigkeit der Personen bekannt





Dezentrale Datenschutz- ansätze für LBS



Routing Through the Mist

Einführung

Zentrale Ansätze

Dezentrale Ansätze

Datenselbstschutz

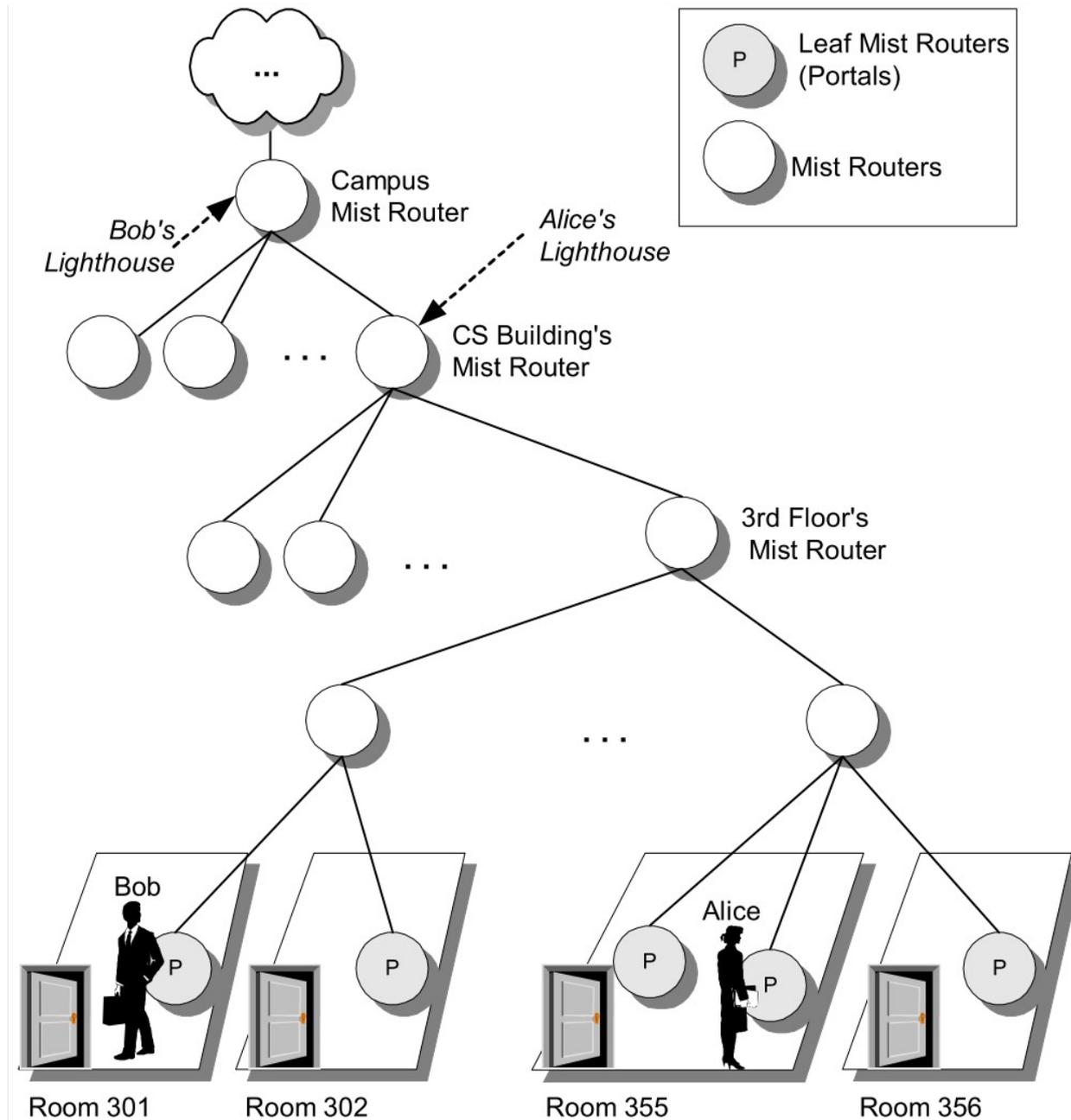
Abschluss

- “Durch den Nebel routen”: Ansatz zielt darauf ab, dass z.B. Mobilfunkstationen nicht wissen sollen, mit welchem Nutzer sie kommunizieren, aber wissen müssen wo er ist
- Hierarchie (Baum) von Routern
 - Blätter: einzelne konkrete Orte
 - Knoten: fassen Orte zusammen, z.B. Stadtteile, Städte, Länder
- Eingabe: Wahl eines Routers als “Leuchtturm”, der mit den eigentlichen Diensten kommuniziert
 - Leuchtturm tief im Baum: genauere Position
 - Leuchtturm weiter oben: gröbere Position
- Trennung von Position und Identität





Beispiel



Einführung

Zentrale Ansätze

Dezentrale Ansätze

Datenselbstschutz

Abschluss

Quelle: Routing Through The Mist
Al-Muhtad et al.



Trennung zwischen Identität und Position

Einführung

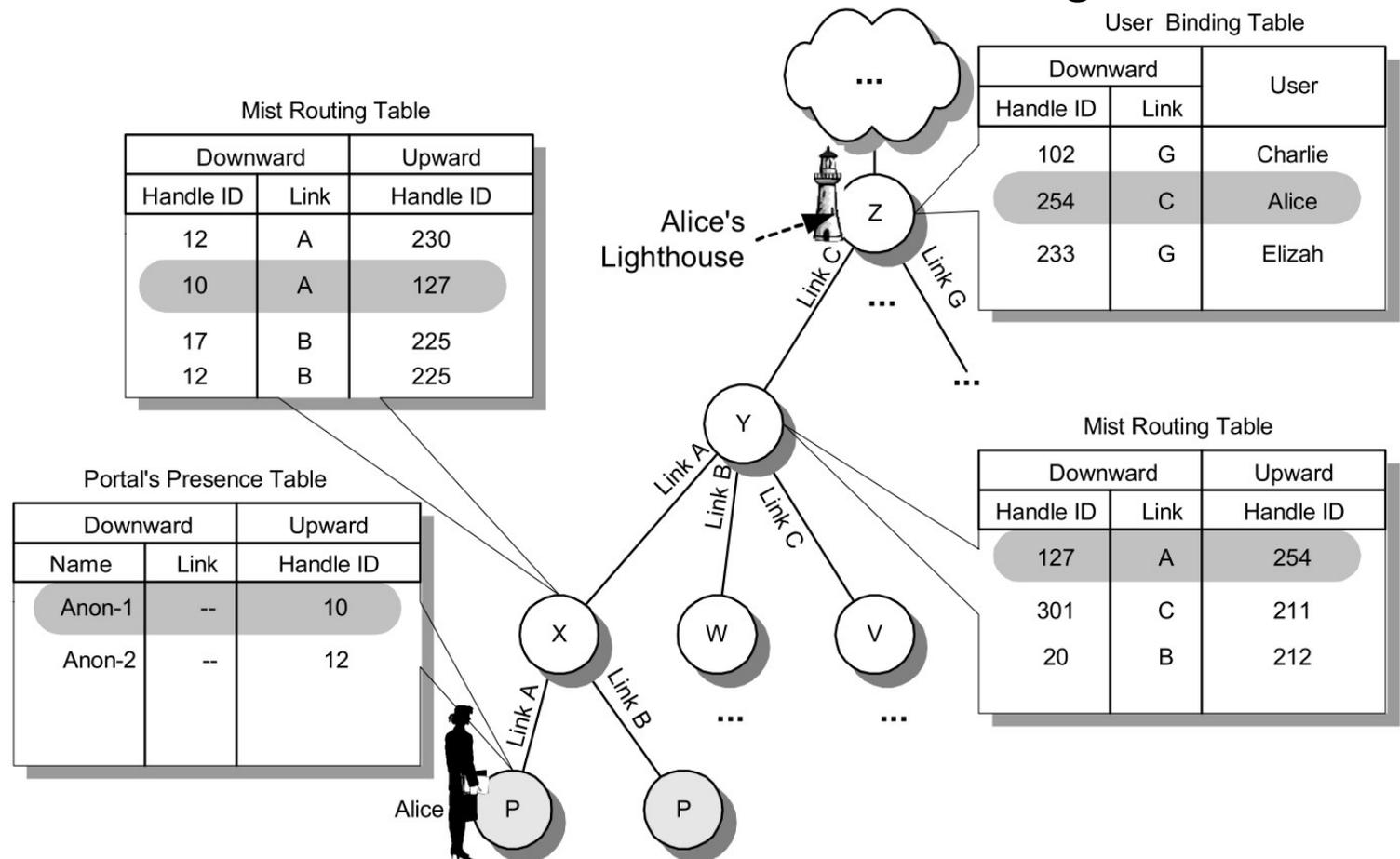
Zentrale Ansätze

Dezentrale Ansätze

Datenselbstschutz

Abschluss

- anonyme Kommunikation, Handle-IDs und Link-IDs
 - Portale kennen Nutzerposition, aber nicht Nutzer
 - Leuchttürme kennen Nutzer, aber nur eigene Position



Quelle: Routing Through The Mist
Al-Muhtad et al.



Mobile Nutzer

Einführung

Zentrale Ansätze

Dezentrale Ansätze

Datenselbstschutz

Abschluss

- Portale
 - können leicht automatisch gewechselt werden
 - z.B. wenn Nutzer Raum verlässt, für den der Router zuständig war
- Leuchttürme
 - müssen manuell gewählt werden, wenn Nutzer Zuständigkeitsbereich des Leuchtturms verlässt
 - Wahl des Leuchtturms entscheidet über Anonymisierungsgrad





Kritik

Einführung

Zentrale Ansätze

Dezentrale Ansätze

Datenselbstschutz

Abschluss

- gut skalierbar, kaum zusätzlicher Rechenaufwand
- einfaches, verständliches Verfahren
- Portale und Leuchttürme müssen vertrauenswürdig sein
 - dürfen Wissen nicht zusammenführen
 - Router egal: verschlüsselte Kommunikation
- Leuchtturmdichte ist entscheidend, Nutzerdichte ist egal
 - zuwenig Leuchttürme: unnötig grobe Positionsmeldungen
- erhöhter Kommunikationsoverhead
- Anfragefolgen generieren aussagekräftige Tracks, wenn Leuchttürme öfter gewechselt werden müssen





Peer-to-Peer Anonymisierung

Einführung

Zentrale Ansätze

Dezentrale Ansätze

Datenselbstschutz

Abschluss

- Szenario: mobile Anwender, die über Ad-Hoc-Netze kommunizieren und Geodaten an Dienste schicken
- Gruppen von Nutzern anonymisieren ihre Positionsdaten gegenseitig
 - Anonymisierungsmenge besteht aus den Nutzern, die grade in Funkreichweite sind
 - Dienst erhält bereits anonymisierte Daten, keine vertrauenswürdige 3. Partei erforderlich
- Eingabe:
 - k für Größe der Anonymisierungsmenge
 - A_{\min} als kleinstmögliche Anonymisierungsregion

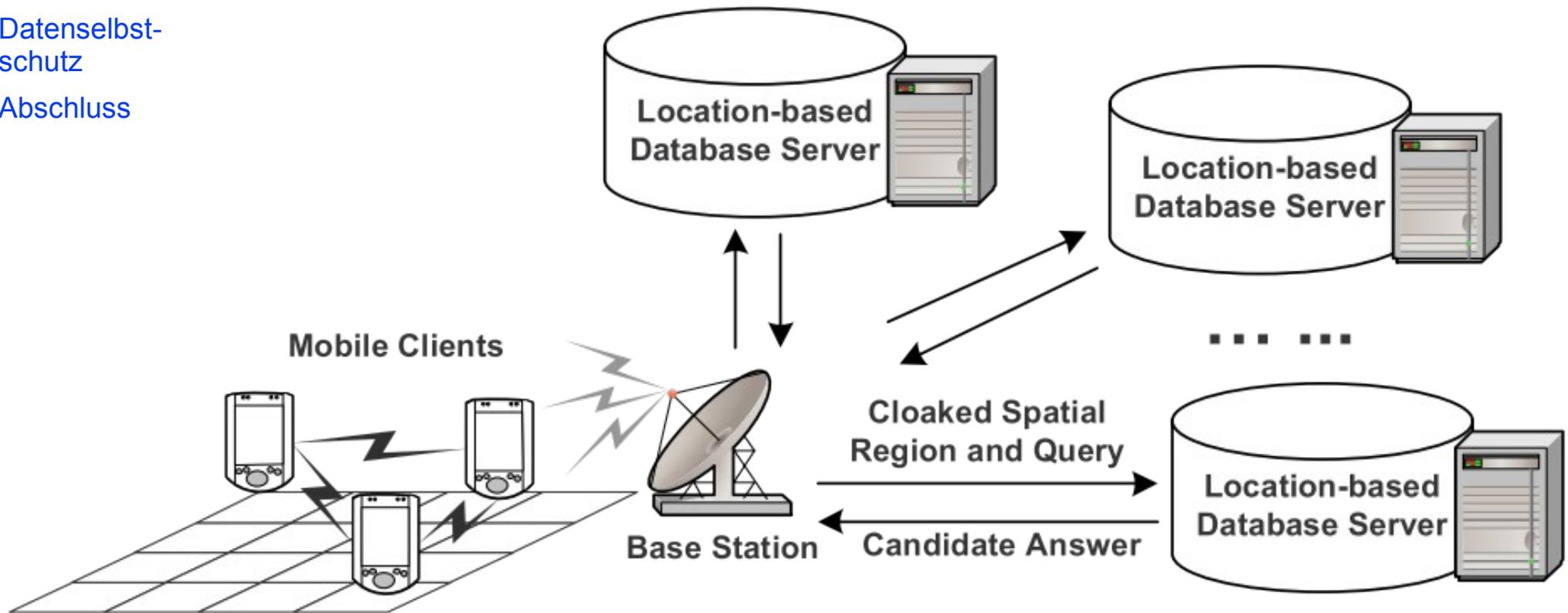
C. Chow, M. Mokbel, X. Liu: *A peer-to-peer spatial cloaking algorithm for anonymous location-based service*. GIS 2006





Systemarchitektur

- Einführung
- Zentrale Ansätze
- Dezentrale Ansätze
- Datenselbstschutz
- Abschluss





Beispiel

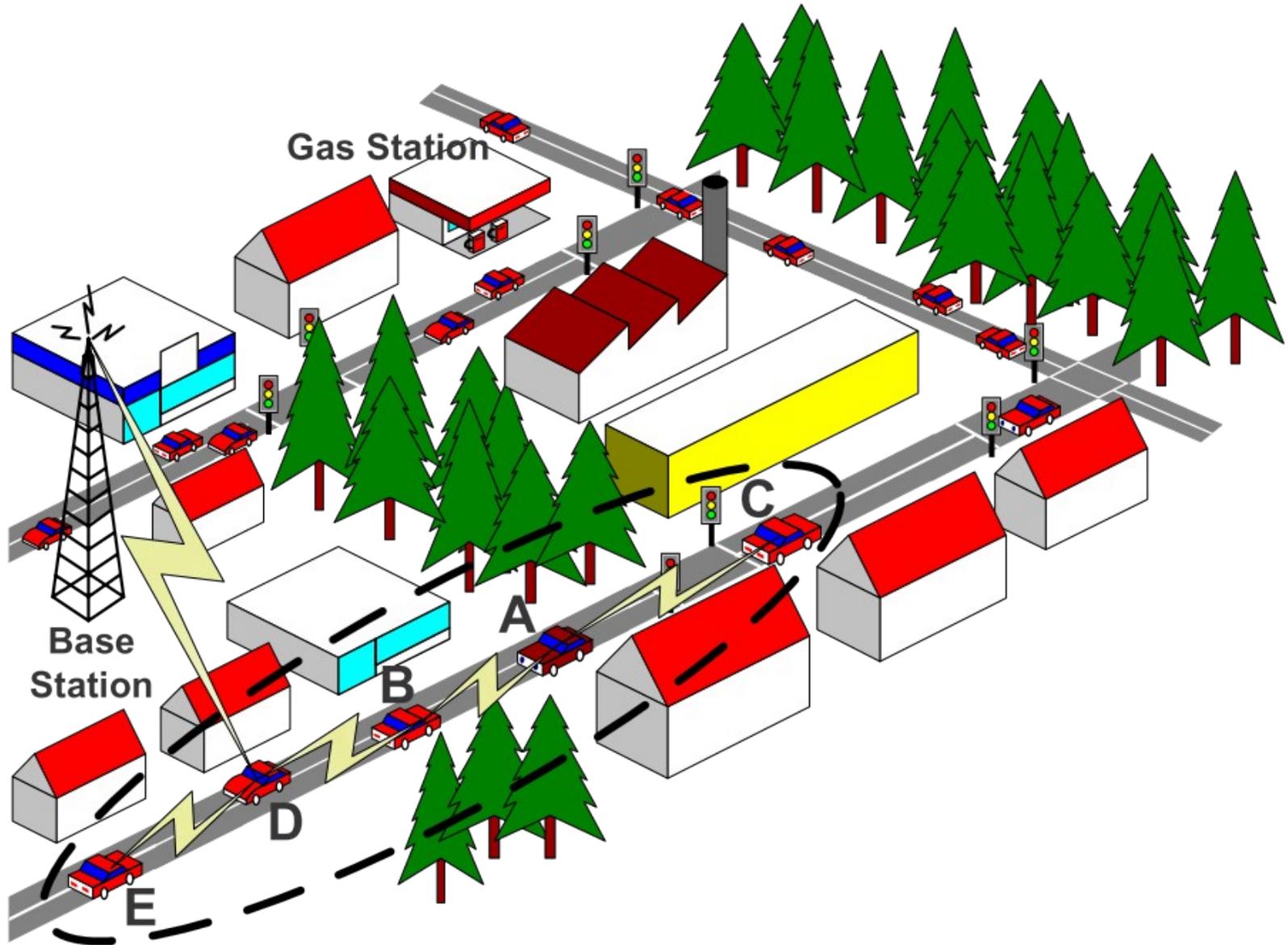
Einführung

Zentrale Ansätze

Dezentrale Ansätze

Datenselbstschutz

Abschluss





Verfahren (1/2)

Einführung

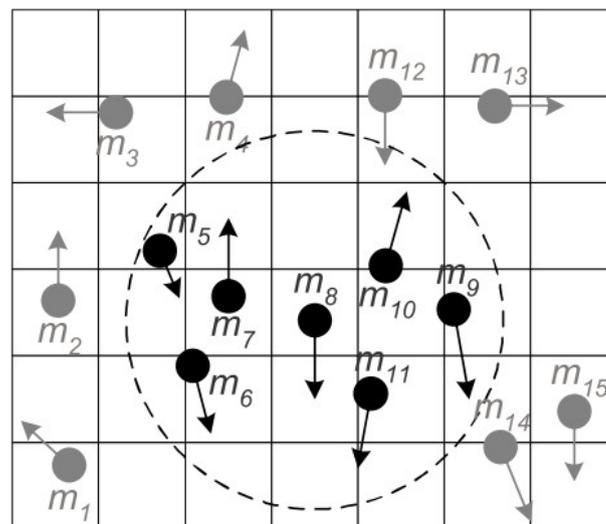
Zentrale Ansätze

Dezentrale Ansätze

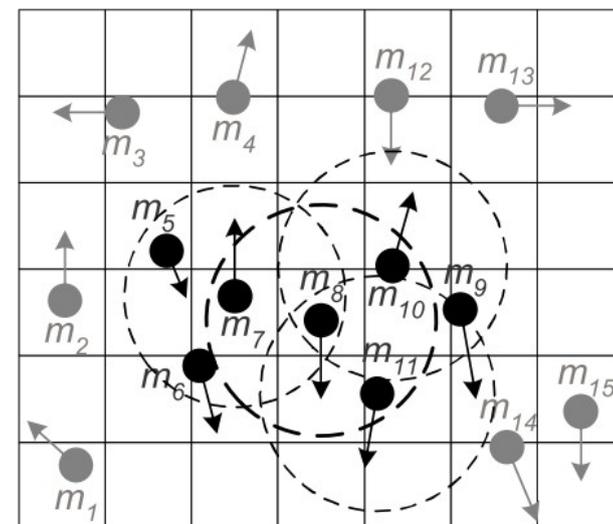
Datenselbstschutz

Abschluss

- Suche Teilnehmer in direkter Funkreichweite (Abb. a)
- Berechne Bewegungsvektoren, um Teilnehmer zu finden die in die gleiche Richtung unterwegs sind
 - Overhead durch Neuberechnung sparen
- Wenn weniger als $k-1$ Teilnehmer gefunden werden, suche multi-hop (Abb. b)



(a) Single-hop peer searching



(b) Multi-hop peer searching





Verfahren (2/2)

Einführung

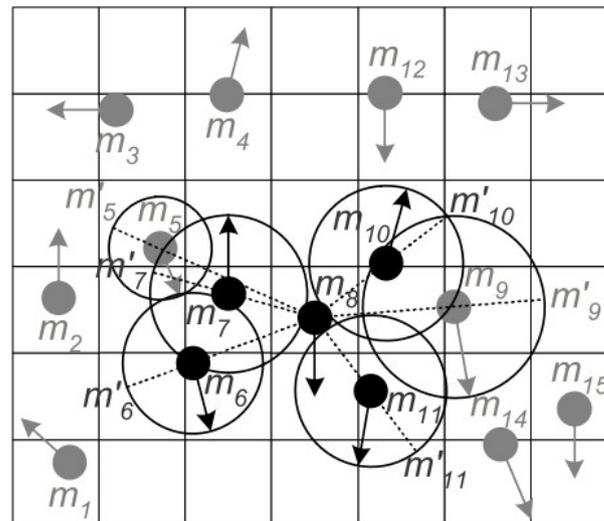
Zentrale Ansätze

Dezentrale Ansätze

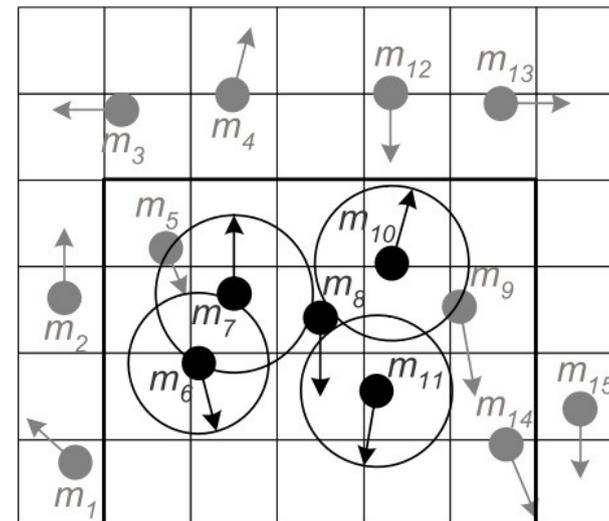
Datenselbstschutz

Abschluss

- Wenn $k-1$ Teilnehmer gefunden, bilde Anonymisierungsregion (Rechteck in Abb. d)
 - wähle Region so, dass kein Teilnehmer den Bereich während der Anfrage verlässt, selbst wenn er sich mit Maximalgeschwindigkeit (Kreise in Abb. c) direkt vom Anfrager entfernt (gestrichelte Linien in Abb. c)



(c) Location adjustment



(d) Cloaked spatial region





Kritik

Einführung

Zentrale Ansätze

Dezentrale Ansätze

Datenselbstschutz

Abschluss

- dezentrales Verfahren, kein Single Point of Failure
- skaliert gut, da durch jeden Peer neue Ressourcen hinzukommen
- intuitiver Ansatz

- hoher Kommunikationsaufwand
- Peer Group muss vertrauenswürdig sein (andererseits muss sich Angreifer beim Opfer befinden, kennt dessen Position also sowieso)
- Nutzerdichte ist problematisch, k Teilnehmer in direkter Funkreichweite erforderlich
- Wenn sich die Nutzer oft auseinanderbewegen, können einzelne Teilnehmer durch Anfragesequenzen identifiziert werden



A large, stylized graphic consisting of two concentric, thick rings. The outer ring is light green and the inner ring is grey. The rings are composed of several rectangular segments that meet at the corners, creating a slightly irregular, octagonal shape. The center of the graphic is a white square.

Verfahren zur Selbstanonymisierung in LBS



Anonymisierung durch Dummies

Einführung

Zentrale Ansätze

Dezentrale Ansätze

Datenselbstschutz

Abschluss

- Szenario: Sequenzen von Geo-Anfragen an einen Dienst
- Idee: Selbstanonymisierung durch das Generieren von $k-1$ 'gefälschten' Nutzern
 - Dienst erhält k unterschiedliche Koordinaten
 - eine echt, $k-1$ künstlich generiert
 - Dienst antwortet mit k Ergebnissen
 - nur Anwender weiß, welche Koordinate 'echt' ist, und kann das korrekte Anfrageergebnis
- Problem: realistische Dummies

H. Kido et al., *An Anonymous Communication Technique using Dummies for Location-based Services*, ICPS'05





Realistische Dummies

Einführung

Zentrale Ansätze

Dezentrale Ansätze

Datenselbstschutz

Abschluss

- Dummies nicht von echten Daten unterscheidbar
 - Autos fahren nicht, wo keine Straßen sind
 - realistische Bewegungsprofile
- *Moving in a Neighborhood*
 - nächste Position eines Dummies in Nachbarschaft vorheriger Position
- *Moving in a Limited Neighborhood*
 - nächste Position eines Dummies in Nachbarschaft vorheriger Position
 - zusätzlich: Dummies, die in einem zu dicht besetzten oder ungeeigneten Gebiet generiert werden, werden verworfen und durch neue ersetzt





Kritik

Einführung

Zentrale Ansätze

Dezentrale Ansätze

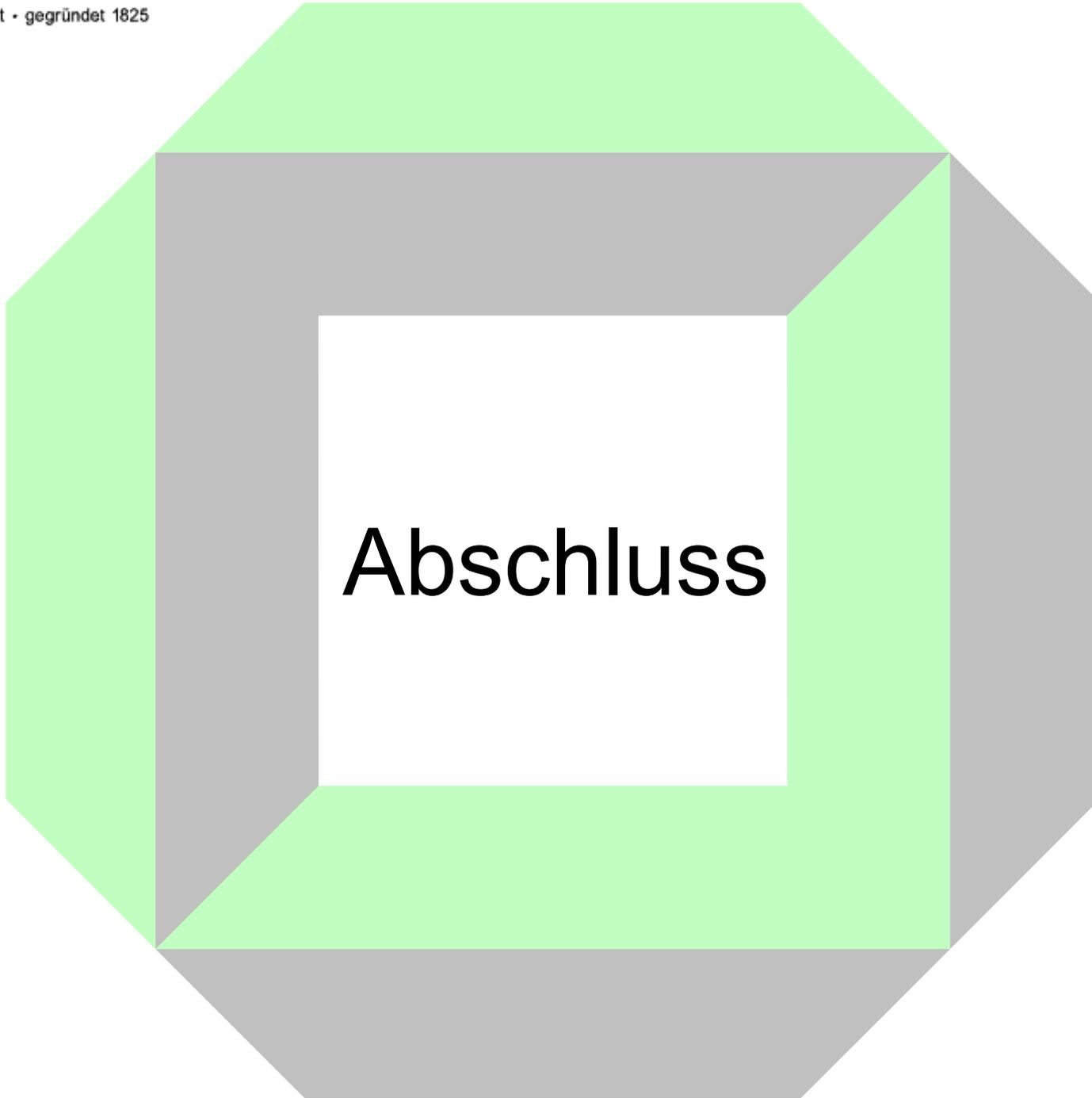
Datenselbstschutz

Abschluss

- verteiltes Verfahren, da von jedem Nutzer selbst durchzuführen
- funktioniert auch mit Anfragefolgen
- skaliert linear, da nur $k-1$ zusätzliche Anfragen je Nutzer gestellt werden

- hoher Rechen- und Kommunikationsoverhead auf dem Mobilgerät
- sehr schwierig, realistische Dummies zu erzeugen die sich nicht statistisch herausfiltern lassen
→ nicht intuitiv *sicher* anwendbar







Zusammenfassung

[Einführung](#)

[Zentrale Ansätze](#)

[Dezentrale Ansätze](#)

[Datenselbstschutz](#)

[Abschluss](#)

- Lokationsbasierte Dienste sind eine der attraktivsten zukünftigen Anwendungen
 - Aber: Datenschutzprobleme unvermeidlich
 - Kompromiss zwischen Privatheit und Dienstgüte
- Besonders problematisch: Tracks und Anfragefolgen, die das Erstellen von Tracks erlauben
 - Nutzer lassen sich 'herausmitteln', wenn jede Anfrage ein anderes Anonymity Set generiert
- Vorgestellte Verfahren
 - zentrale Ansätze
 - dezentrale Ansätze
 - Methode zum Datenselbstschutz





Literatur

- [1] Jürgen Czerny, *Datenschutz in lokationsbasierten Diensten*, Seminararbeit am IPD, 2007

http://dbis.ipd.uni-karlsruhe.de/img/content/SS07Czerny_DatenschutzLBS.pdf

