ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

inf | Informatik
Computer Science

Implikationen des ubiquitous Sensing am Beispiel von Location Privacy

Melanie Imhof

Distributed Systems Seminar

Überblick

- Motivation
- Anforderungen
- Lösungsansätze
  - Mix-Zonen
  - Path Confusion
- Schlussfolgerungen

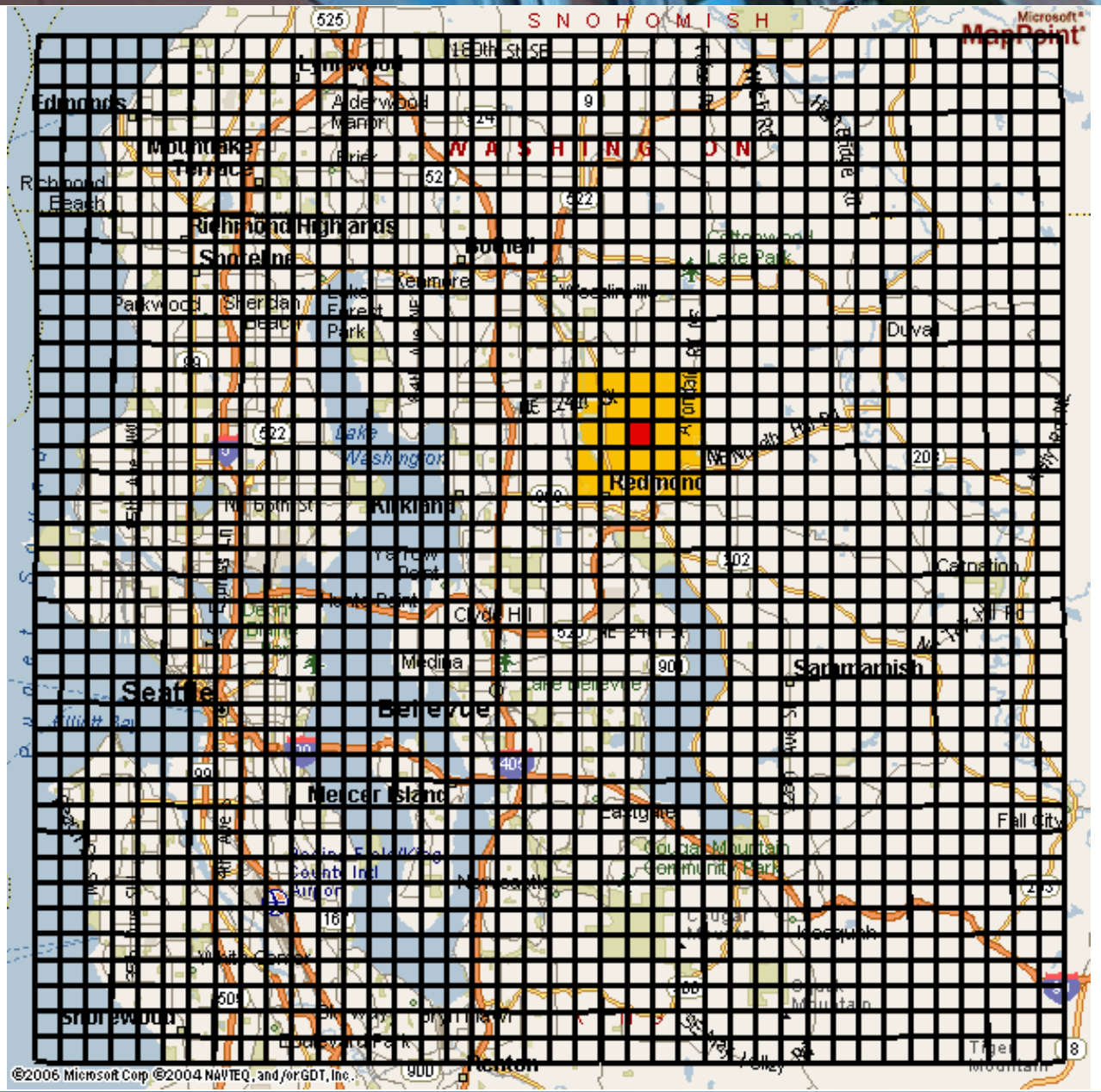
Motivation

- Ort ist Bestandteil der Funktionalität von Sensor-Applikationen
  - Benutzer will Privatsphäre schützen
- Schutz der Information über den aktuellen Aufenthaltsort (Location-Privacy)

Motivation- Predestination

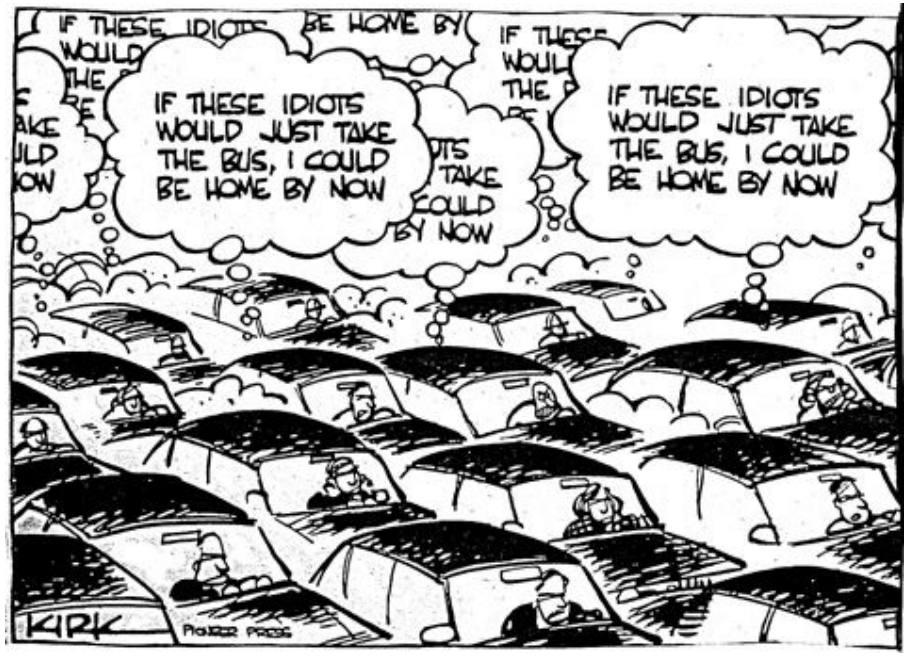
- Ziel einer Person möglichst genau voraussagen
- 169 Personen mit einem GPS-Sender
- Gitter über die Karte gelegt
  - 1600 Zellen mit Seitenlänge 1km
  - Basis-Wahrscheinlichkeit zugeordnet
- Open-World-Assumption
- Durchschnittliche Genauigkeit von 3 km


SNOHOMISH
Microsoft MapPoint
Lynnwood
180th St SE
Edmonds
Alderwood Manor
Mountlake Terrace
Brier
WASHINGTON
Richmond Beach
Richmond Highlands
Shoreline
Bothell
Cottonwood Lake Park
Kenmore
Woodinville
Parkwood
Sheridan Beach
Lake Forest Park
Duvall
84th Ave NE
NE 124th St
Avondale Rd NE
Lake Washington
NE Novelty Hill Rd
Redmond
15th Ave NW
NE 65th St
Kirkland
Kelly Rd NE
Yarrow Point
Carnation
Hunts Point
Clyde Hill
NE 24th St
Denny Blaine Park
Medina
Lake Bellevue
Sammamish
Seattle
Bellevue
Elliott Bay
Puget Sound
Mercer Island
Eastgate
Fall City
Boeing Field/King County Intl Airport
Cougar Mountain Community Park
Newcastle
Cougar Mountain
Issaquah
White Center
Squak Mountain
Shorewood
Skyway
Bryn Mawr
KING
Boulevard Park
Renton
Tiger Mountain
©2006 Microsoft Corp ©2004 NAVTEQ, and/or GDT, Inc.


SNOHOMISH
WASHINGTON
Microsoft MapPoint
Edmonds
Mountlake Terrace
Richmond Beach
Richmond Highlands
Shoreline
Bothell
Kenmore
Lake Forest Park
Lake Washington
Kirkland
Redmond
Duvall
Carnation
Clyde Hill
Medina
Seattle
Bellevue
Mercer Island
Issaquah
Fall City
Renton
Tiger Mountain
©2006 Microsoft Corp ©2004 NAVTEQ, and/or GDT, Inc.

Anforderungen

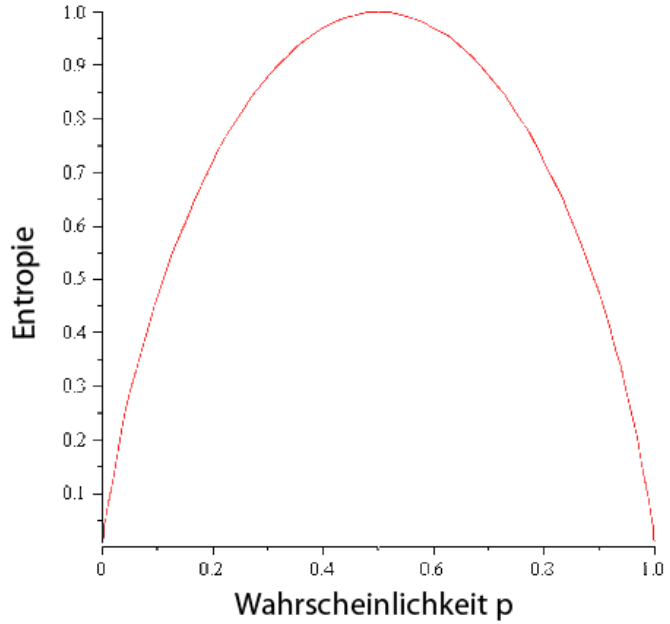
- 2 Beispiel Applikationen
  - Stau-Meldungen
  - Ortsbasierte Dienste



Niveau der Privatsphäre

$$H = -\sum_{i=1}^{i=N} p_i \log(p_i)$$

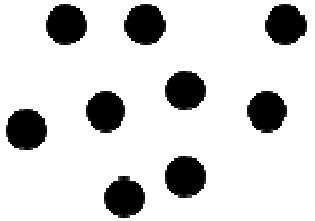
- Entropie maximal
  - Gleichverteilung maximiert Entropie
  - Unsicherheit beim Gegner maximal



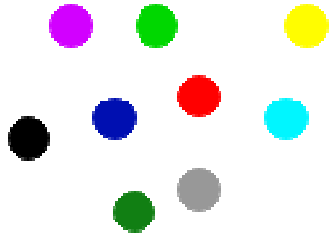
$\frac{1}{2}$	$\frac{1}{2}$

Anonymität und Pseudonymität

- Anonymität
  - Individuum nicht
    von den Anderen unterscheidbar
    - Nur eingeschränkt einsetzbar z.B Staumeldungen



- Pseudonymität
  - fixe Identität
    richtige Identität unbekannt
    - Langzeit Pseudonyme garantieren keine Sichheit



Anforderungen

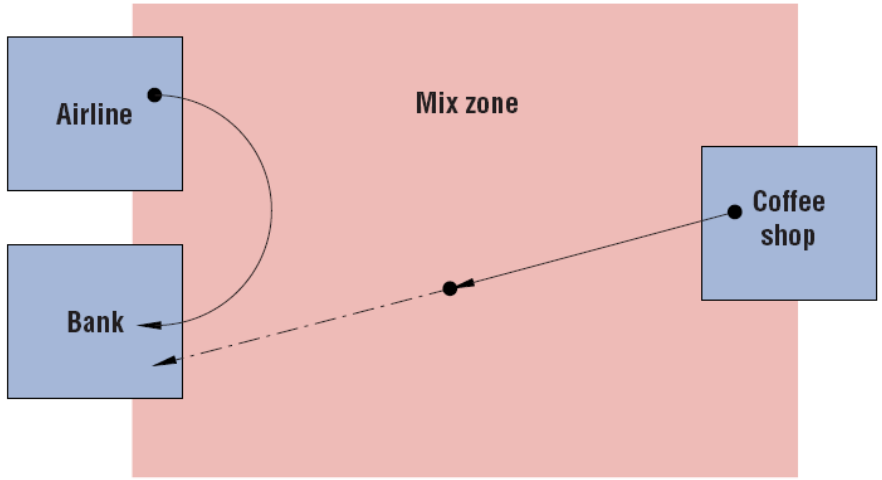
- Datenintegrität
  - Applikationsabhängig
- Wo ist die Information?
  - Vertrauenswürdiger Server
  - Direkt beim Benutzer
- Benutzerinteraktion
  - Manuell
  - Automatisch

Lösungsansätze

- Mix-Zonen (Universität von Cambridge)
- Path Confusion (Universität von New Jersey)

Mix-Zonen

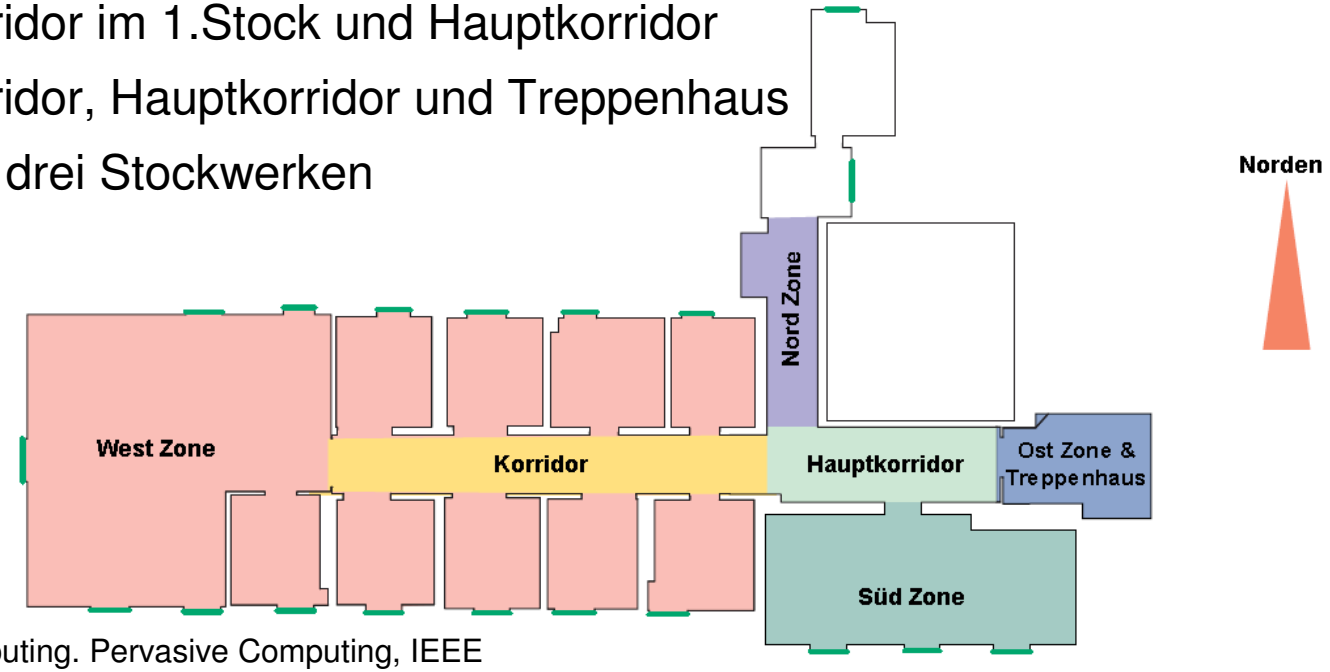
- temporäre Pseudonyme
  - wechseln in Mix-Zone
  - Update-Periodes
- Kommunikation über Proxy



Location privacy in pervasive computing. Pervasive Computing, IEEE

Mix-Zonen - Experiment

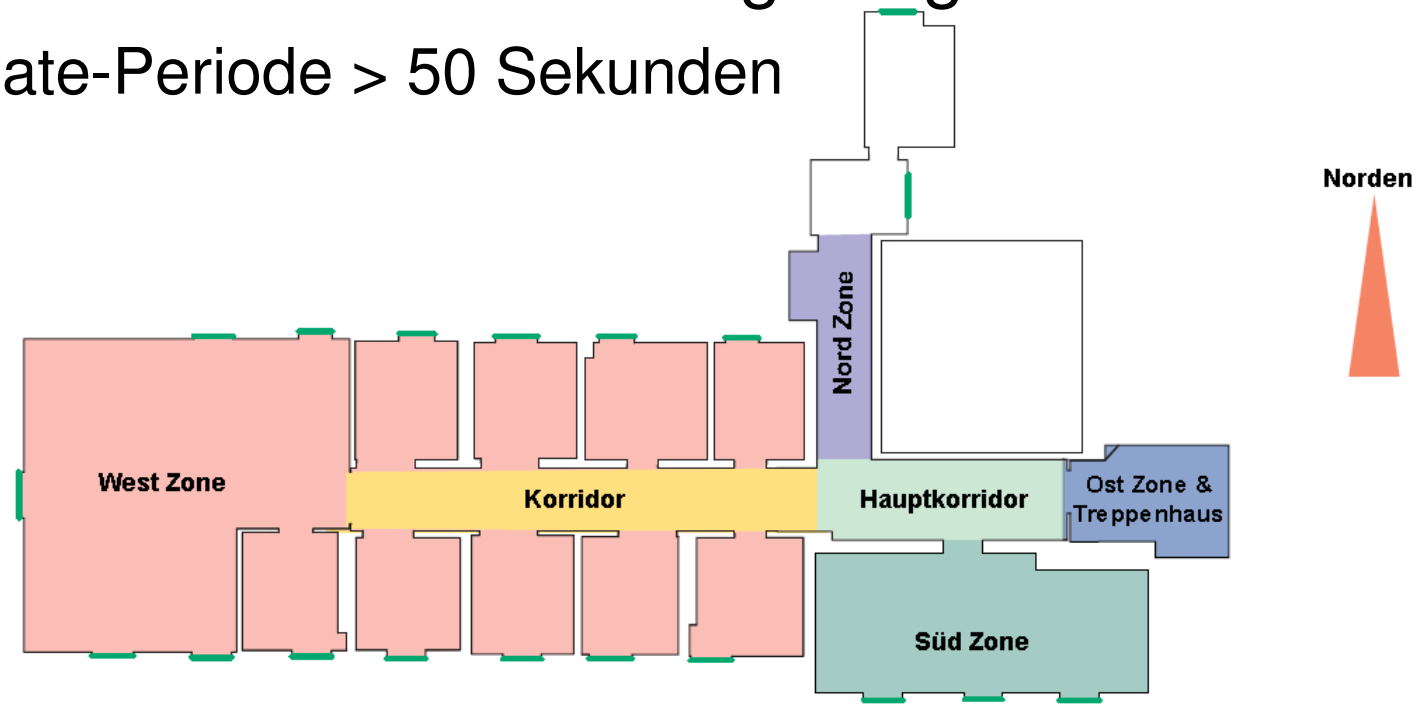
- Active Bat System im AT&T Lab
- 3 Mix-Zonen
  - z1: Korridor im 1.Stock
  - z2: Korridor im 1.Stock und Hauptkorridor
  - z3: Korridor, Hauptkorridor und Treppenhaus in allen drei Stockwerken



Location privacy in pervasive computing. Pervasive Computing, IEEE

Mix-Zonen - Resultate

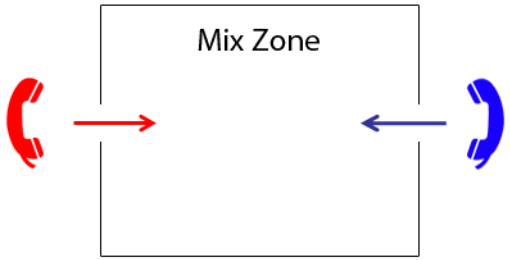
- Nur 50 Sekunden benötigt, um von der einen Seite von z3 zur Anderen zugelangen
  - Update-Periode > 50 Sekunden

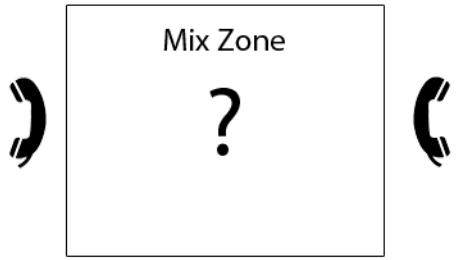


Location privacy in pervasive computing. Pervasive Computing, IEEE

Mix-Zonen - Resultate

- Vernachlässigung der Richtung
  - Ort und Richtung beim Betreten der Mix-Zone lassen auf Austrittspunkt schliessen



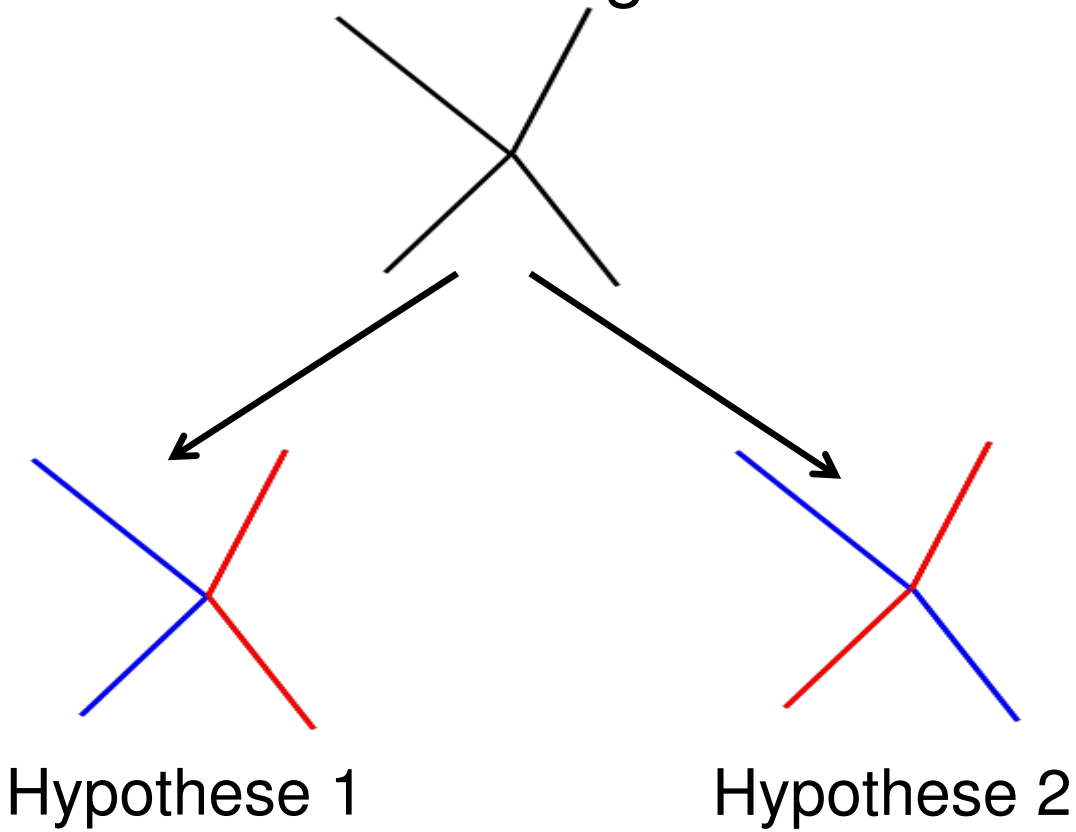


Mix-Zonen - Zukunft

- Anonymitätsgrad zu tief
  - keine Positionsaktualisierung
  - kritische Dienste löschen
  - Einführung von „dummy user“
- Ungewissheit über die Skalierbarkeit des Systems

Path Confusion - Algorithmus

- Unsicherheit bei Kreuzung zweier Pfade

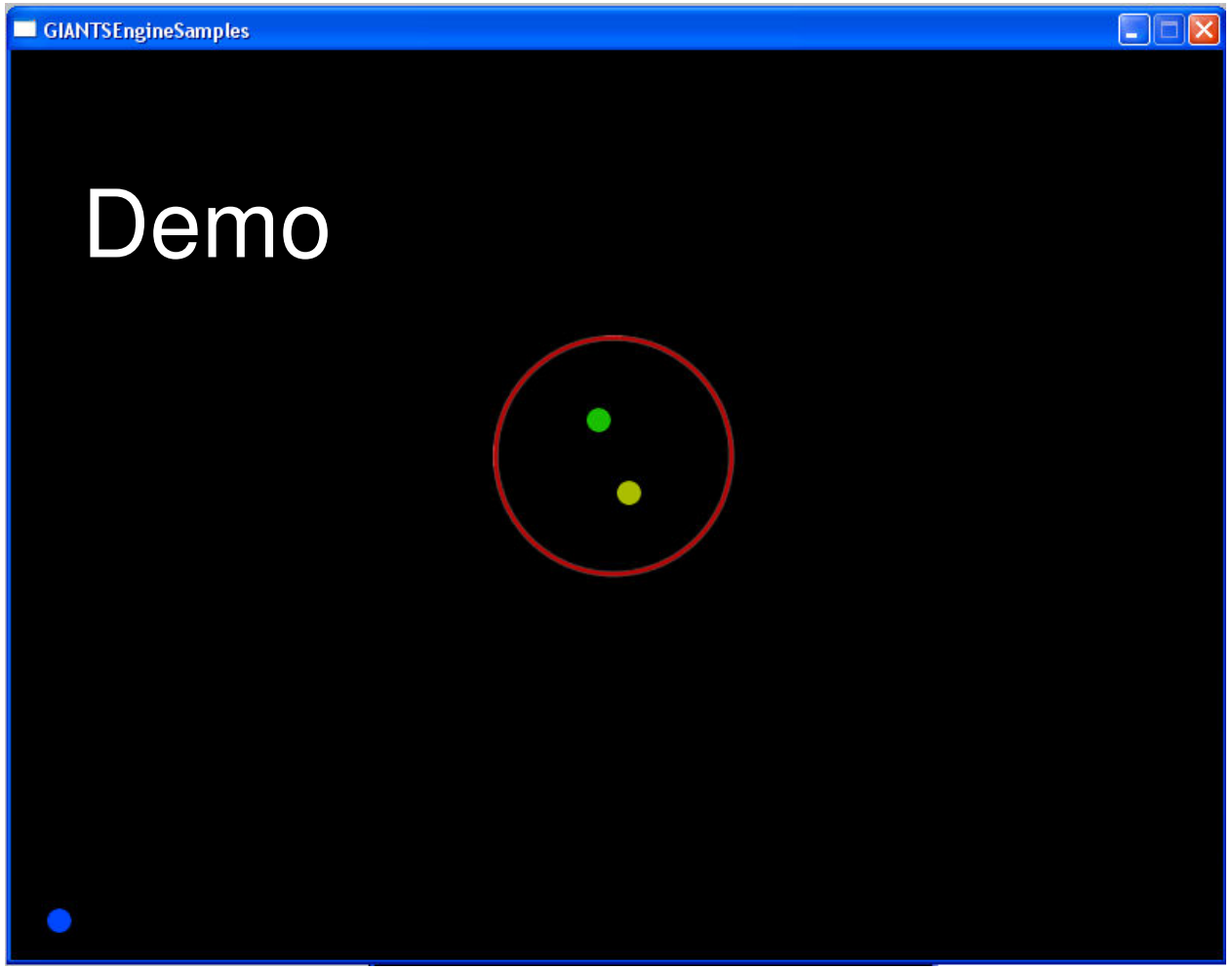


Path Confusion - Algorithmus

- Pfade verfälschen damit sie sich kreuzen
- Verfälschen wenn zwei Benutzer in Radius R
  - R ist Parameter der frei gewählt werden kann
- Benutzer werden auf Mittelpunkt gesetzt

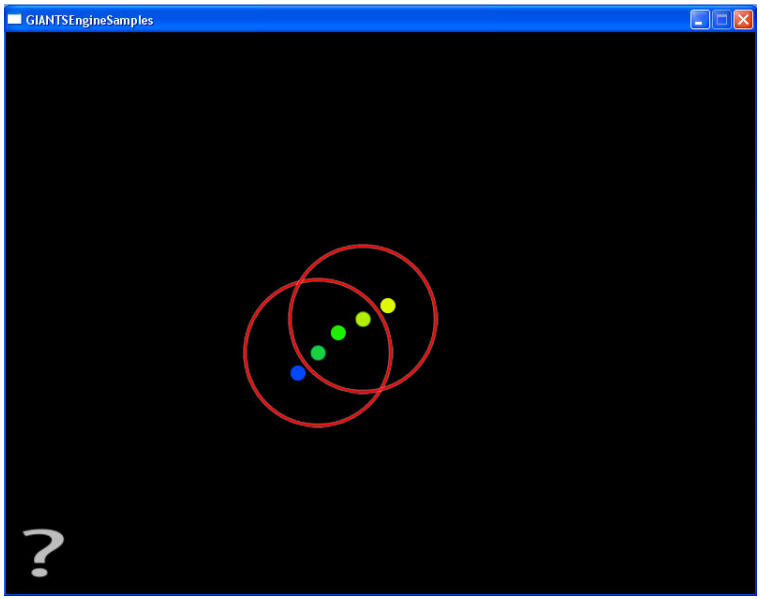
$$(\tilde{x}_n(k) - x_n(k))^2 + \left(\tilde{y}_n(k) - y_n(k)\right)^2 \leq R^2$$

Path Confusion - Algorithmus



Path Confusion - Algorithmus

- Optimierungsproblem
  - Kreiszuordnung nicht eindeutig
  - Optimale Kombination wählen



Path Confusion - Algorithmus

- Unsicherheit des Gegners maximieren

$$\max_{\forall \tilde{x}_n(k), \forall \tilde{y}_n(k)} \frac{1}{N} \sum_{i=1}^{I} p_i(k) d_i(k)$$

  - I Anzahl Hypothesen
  - x_n , y_n Originale Punkte
  - $\tilde{x}_n , \tilde{y}_n$ Verfälschte Punkte
  - p_i Wahrscheinlichkeit der Hypothese i
  - d_i Summe der Fehler der Hypothese i

Path Confusion - Probleme

- Zu komplex mit vielen Benutzern
  - Finden der Kreise
  - Optimierungsproblem
- Optimierte Version des Algorithmus muss noch gefunden werden

Schlussfolgerungen

- Verschiedene Anwendungen stellen unterschiedliche Anforderungen
- Ansatz für Pseudonyme: Mix-Zonen
  - Genügend Mix-Zonen?
  - Was wenn alleine in Mix-Zone?
  - Wie gross muss Update-Periode sein?
- Ansatz für Anonymität: Path Confusion
  - Komplexität